

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Instytut Nauk Prawnych
Wydział Prawa i Administracji

mgr Paweł Hajduk

Nauki prawne

**KOMPETENCJE ORGANÓW ADMINISTRACJI PUBLICZNEJ W OBSZARZE
PRZETWARZANIA DANYCH OSOBOWYCH WOBEC WYZWAŃ
TRANSFORMACJI CYFROWEJ**

Rozprawa doktorska

Rozprawa doktorska napisana pod
kierunkiem prof. dr hab. Grażyny Szpor,
Katedra Prawa Informatycznego WPiA
UKSW

Warszawa, wrzesień 2024 r.

Streszczenie rozprawy doktorskiej

Przedmiotem rozprawy doktorskiej jest analiza kompetencji wybranych organów administracji publicznej w obszarze przetwarzania danych osobowych z perspektywy zjawiska krzyżowania się tych kompetencji. Celem rozprawy doktorskiej jest weryfikacja tezy badawczej, że w obszarze przetwarzania danych osobowych ustanowione zostały organy administracji publicznej o krzyżujących się kompetencjach, co prowadzi do niepewności prawnej. Brak jest przy tym instrumentów prawnych, które mogą skutecznie zredukować negatywne skutki zjawiska krzyżowania się kompetencji w tym obszarze.

Aby zrealizować ten cel rozprawy, należało dokonać potwierdzenia albo falsyfikacji pomocniczych hipotez badawczych. Stąd też w pierwszym rozdziale rozprawy zbadano podstawowe pojęcia prawa administracyjnego, to jest pojęcia organu administracji publicznej, prawnych form działania tych organów, ich kompetencji i pojęć powiązanych – właściwości, zakresu działania, zadania i celu. Następnie w rozdziale drugim analizie poddano krzyżowanie się zakresów przedmiotowych aktów prawnych w obszarze przetwarzania danych osobowych z uwzględnieniem RODO jako podstawowego aktu prawnego w tym obszarze, w tym jego szerokiego i nieostrego zakresu przedmiotowego i podmiotowego, oraz aktów prawnych prawa unijnego i krajowego regulujących przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu, cyberbezpieczeństwo, prawo konkurencji, sztuczną inteligencję i europejskie przestrzenie danych oraz Aktu o Rynkach Cyfrowych i Aktu o Usługach Cyfrowych. Uzasadniono wybór tych aktów prawnych jako obszaru referencyjnego.

Następnie, wobec wykazania, że dochodzi do krzyżowania się zakresów przedmiotowych i podmiotowych aktów prawnych w obszarze referencyjnym celowe było, aby w rozdziale trzecim scharakteryzować kompetencje organów stosujących akty prawne w tym obszarze, poczynawszy od cech wspólnych tych organów, przez typologię ich kompetencji po charakterystykę wybranych organów i ich kompetencji na poziomie unijnym (Europejska Rada Ochrony Danych, Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Komisja Europejska jako organ unijnego prawa konkurencji, Grupa Wysokiego Szczebla, Europejska Rada ds. Usług Cyfrowych, Europejska Rada ds. Innowacji w zakresie Danych, Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji) i krajowym (Prezes Urzędu Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej, organy właściwe do spraw cyberbezpieczeństwa, Prezes Urzędu Ochrony Konkurencji i Konsumenta jako organ krajowego prawa konkurencji, organy właściwe w Akcie o Usługach Cyfrowych, organy

właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych, organy właściwe w Akcie w Sprawie Danych, organy właściwe w Akcie w Sprawie Sztucznej Inteligencji).

Pozytywna weryfikacja hipotezy o krzyżowaniu się kompetencji organów administracji publicznej w obszarze referencyjnym uczyniła zasadnym podjęcie próby sformułowania definicji zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych i jego typologii. Następnie zbadano instrumenty prawne do zredukowania negatywnych skutków tego zjawiska w wymiarze prawa materialnego, ustrojowego i procesowego, wykazując ich ograniczoną skuteczność. Dalej dokonano analizy tych negatywnych skutków, w tym obniżenia skuteczności prawa i zwiększenia niepewności prawnej. Rozdział czwarty zamknięto prawnoporównawczym ujęciem analizowanego zjawiska z perspektywy jurysdykcji Królestwa Niderlandów i Wielkiej Brytanii ograniczonym do rozwiązań przyjętych w tych jurysdykcjach w celu zredukowania negatywnych skutków analizowanego zjawiska.

Piąty i ostatni rozdział zatytułowano „Przyczyny zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych i postulaty *de lege ferenda*”. Jako pierwszą przyczynę tego zjawiska zidentyfikowano nieadekwatność odpowiedzi prawodawcy na przemiany spowodowane transformacją cyfrową skutkującą rozłączeniem regulacyjnym (*regulatory disconnect*). Drugą zaś jest wybór techniki legislacyjnej przez prawodawcę, aby obszar ten uregulować za pomocą zasad, terminów nieostrych metody opartej na ryzyku w celu zapewnienia neutralności technologicznej. Kolejną przyczynę stanowi niejasność taksonomiczna w odniesieniu do zasadności i sposobu wyodrębnienia kompleksowej gałęzi prawa, „prawa ochrony danych osobowych”. Jako czwartą przyczynę scharakteryzowano proces europeizacji prawa administracyjnego prowadzący do powstania złożonej struktury podmiotów administrujących bez wyraźnych hierarchicznych relacji między nimi. Ostatnią przyczyną są zaś rozbieżne cele wyznaczone poszczególnym organom administracji publicznej w obszarze przetwarzania danych osobowych. W drugiej części ostatniego rozdziału sformułowano cztery postulaty *de lege ferenda*. Jako pierwszy zgłoszono wyodrębnienie prawa danych jako odrębnej kompleksowej gałęzi prawa. Drugim postulatem jest centralizacja struktury stosowania RODO wobec największych podmiotów nadzorowanych i ustanowienie organów ochrony danych jako organów właściwych dla stosowania aktów prawnych w obszarze przetwarzania danych osobowych. Kolejny postulat to wprowadzenie efektywnych instrumentów współpracy między podmiotami administrującymi stosującymi akty prawne w obszarze przetwarzania danych osobowych. Ostatnim postulatem

de lege ferenda jest wprowadzenie instrumentu prawnego o charakterze klauzuli *safe harbour* dla podmiotów nadzorowanych.

Streszczenie rozprawy doktorskiej w języku angielskim

Dissertation summary in English

The subject of the doctoral dissertation is the analysis of the competences of selected public administration bodies in the area of personal data processing from the perspective of the phenomenon of intersecting competences. The aim of the dissertation is to verify the thesis that in the area of personal data processing public administration bodies with intersecting competences have been established, which leads to legal uncertainty. At the same time, there are no legal instruments that can effectively address the negative effects of the phenomenon of cross competences in this area.

In order to verify the above thesis, a number of auxiliary research hypotheses had to be verified. Hence, the first chapter of the dissertation analyses the basic concepts of administrative law, i.e. the concept of a public administration body, the legal form of action of these bodies, their competences and related concepts — jurisdiction, scope of action, task and purpose. Subsequently, the second chapter examines the intersection of the subject scopes of legal acts in the area of personal data processing, taking into account the RODO as the basic legal act in this area, including its broad and vague subject and object scope, as well as EU and national legal acts regulating anti-money laundering and terrorist financing, cyber security, competition law, artificial intelligence and European data spaces, and the Digital Markets Act and the Digital Services Act. The choice of these pieces of legislation as a reference area was justified.

Subsequently, as a result of the demonstration that there is an overlap between the material and personal scopes of legal acts in the reference area, it was advisable, in the third chapter, to characterise the competences of the bodies applying legal acts in this area, starting from the common features of these bodies, through a typology of their competences to the characteristics of selected bodies and their competences at EU level (European Data Protection Board, the Authority for Anti-Money Laundering and Countering the Financing of Terrorism, the European Union Agency for Cybersecurity, the Commission as an EU competition law authority, the High Level Group, European Board for Digital Services, European Council for Data Innovation, European Council for Artificial Intelligence) and at national level (President of the Personal Data Protection Authority, General Inspector of Financial Information, authorities competent for cyber security, President of the Office of Competition and Consumer Protection as an authority of national competition law, authorities competent for the Digital Services Act, authorities competent for data brokerage services and authorities competent for

registration of data altruism organisations, authorities competent for the Data Act, authorities competent for the Artificial Intelligence Act).

The positive verification of the hypothesis of cross-competence of public administration bodies in the reference area made it reasonable to try to formulate a definition of the phenomenon of cross-competence of public administration bodies in the area of personal data processing and its typology. Then, the legal instruments for addressing the negative effects of this phenomenon in the dimension of substantive, systemic and procedural law were examined, demonstrating their limited effectiveness towards addressing the negative effects of this phenomenon. Further, an analysis of these negative effects was made, including a reduction in the effectiveness of the law and an increase in legal uncertainty. The fourth chapter closes with a comparative legal view of the analysed phenomenon from the perspective of the jurisdictions of the Netherlands and the United Kingdom limited to the solutions adopted in these jurisdictions to address the analysed phenomenon.

The fifth chapter was entitled 'Causes of the phenomenon of cross competences of public administration bodies in the area of personal data processing and postulates *de lege ferenda*'. The inadequacy of the legislator's response to the transformations caused by the digital transformation resulting in regulatory disconnect was identified as the first cause of this phenomenon. The second is the legislator's choice of legislative technique to regulate this area by means of principles, vague terms of a risk-based method to ensure technological neutrality. Another reason is the taxonomic ambiguity regarding the rationale and manner in which a comprehensive branch of law — 'data protection law' — is distinguished. A fourth reason is characterised as the process of Europeanisation of administrative law leading to a complex structure of administrative entities without clear hierarchical relationships between them. The last reason, on the other hand, is the divergent goals set for individual public administration bodies in the area of personal data processing. In the second part of the last chapter four *de lege ferenda* postulates were formulated. The first one is the separation of data law as a distinct comprehensive branch of law. The second postulate is the centralisation of the structure of the application of the GDPR to the largest supervised entities and the establishment of data protection authorities as the competent authorities for the application of legal acts in the area of personal data processing. Another postulate is the introduction of effective instruments of cooperation between administrative entities applying legal acts in the area of personal data processing. The final postulate *de lege ferenda* is the introduction of a legal instrument in a “safe harbour” clause for supervised entities.

Słowa kluczowe

kompetencje; organy; administracji; publicznej; dane; osobowe

Key words

competences; public authorities; personal; data

Klasyfikacja tematyczna

Prawo administracyjne

Tytuł rozprawy doktorskiej w języku angielskim

Competences of Public Authorities in the Area of Processing of Personal Data in the Context of the Challenges of Digital Transformation

SPIS TREŚCI

WYKAZ SKRÓTÓW.....	11
WPROWADZENIE.....	22
Problem badawczy.....	22
Hipotezy badawcze	27
Struktura rozprawy.....	33
Metody badawcze	35
1. ROZDZIAŁ 1 – KOMPETENCJE ORGANÓW ADMINISTRACJI PUBLICZNEJ	
– PODSTAWOWE POJĘCIA.....	37
1.1. Wstęp	37
1.2. Pojęcia organu administracji publicznej i podmiotów administrujących.....	37
1.3. Pojęcie prawnych form działania administracji publicznej	41
1.4. Pojęcie kompetencji organów administracji publicznej	46
1.5. Pojęcia powiązane z pojęciem kompetencji organów administracji publicznej	50
1.5.1. Właściwość.....	50
1.5.2. Zakres działania.....	51
1.5.3. Zadanie	52
1.5.4. Cel	53
1.6. Termin „kompetencje cyfrowe” jako przykład wpływu transformacji cyfrowej na siatkę pojęciową prawa administracyjnego	54
1.7. Podsumowanie	60
2. ROZDZIAŁ 2 – KRZYŻOWANIE SIĘ ZAKRESU PRZEDMIOTOWEGO WYBRANYCH	
AKTÓW PRAWNYCH W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH.....	61
2.1. Wstęp	61
2.2. Ogólne Rozporządzenie o Ochronie Danych jako podstawowy akt prawny w obszarze przetwarzania danych osobowych	63
2.2.1. Ogólne Rozporządzenie o Ochronie Danych.	63
2.2.2. Ustawa o Ochronie Danych Osobowych.....	79
2.3. Szeroki i nieostry zakres przedmiotowy RODO	80
2.4. Szeroki i nieostry zakres podmiotowy RODO	88
2.5. Akty prawne prawa unijnego i krajowego regulujące przetwarzanie danych osobowych jako obszar referencyjny	91
2.6. Krzyżowanie się zakresu przedmiotowego Ogólnego Rozporządzenia o Ochronie Danych z aktami prawnymi prawa unijnego i krajowego regulującymi przetwarzanie danych osobowych	99
2.6.1. Akty prawne regulujące przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu.....	99
2.6.2. Akty prawne regulujące cyberbezpieczeństwo	108
2.6.3. Akty prawne prawa konkurencji, Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych	118
2.6.4. Akty prawne regulujące sztuczną inteligencję	137
2.6.5. Akty prawne regulujące europejskie przestrzenie danych	147
2.7. Podsumowanie	158

3. ROZDZIAŁ 3 – KOMPETENCJE WYBRANYCH ORGANÓW ADMINISTRACJI PUBLICZNEJ STOSUJĄCYCH AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH	160
3.1. Wstęp	160
3.2. Cechy wspólne organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych	161
3.3. Typologia kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych.....	164
3.4. Charakterystyka wybranych organów administracji publicznej na poziomie unijnym 167	
3.4.1. Europejska Rada Ochrony Danych	167
3.4.2. Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu	174
3.4.3. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa.....	177
3.4.4. Europejska Rada ds. Innowacji w zakresie Danych.....	181
3.4.5. Europejska Rada ds. Sztucznej Inteligencji i Europejski Urząd ds. Sztucznej Inteligencji 182	
3.4.6. Komisja Europejska jako organ unijnego prawa konkurencji i Grupa Wysokiego Szczebla 184	
3.4.7. Europejska Rada ds. Usług Cyfrowych.....	194
3.5. Charakterystyka wybranych organów na poziomie krajowym	195
3.5.1. Prezes Urzędu Ochrony Danych Osobowych	195
3.5.2. Generalny Inspektor Informacji Finansowej.....	210
3.5.3. Krajowe organy właściwe do spraw cyberbezpieczeństwa i CSRIT-y	216
3.5.4. Prezes Urzędu Ochrony Konkurencji i Konsumentów jako organ prawa konkurencji ..	221
3.5.5. Krajowe organy właściwe w Akcie o usługach cyfrowych	224
3.5.6. Organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych (Akt w sprawie Zarządzania Danymi).....	226
3.5.7. Organy właściwe w Akcie w sprawie Danych	229
3.5.8. Organy właściwe w Akcie w sprawie Sztucznej Inteligencji.....	231
3.6. Podsumowanie	235
4. ROZDZIAŁ 4 – KRZYŻOWANIE SIĘ KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ STOSUJĄCYCH AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH	237
4.1. Wstęp	237
4.2. Definicja krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych	238
4.3. Typologia krzyżowania się kompetencji organów	246
4.3.1. Kryterium typu kompetencji (właściwe i niewłaściwe)	246
4.3.2. Kryterium intencji prawodawcy (zamierzone i niezamierzone)	250
4.3.3. Kryterium perspektywy, w jakiej krzyżowanie się ujawnia (horyzontalne i wertykalne) 253	
4.4. Instrumenty prawne do zredukowania negatywnych skutków	255
4.4.1. Wymiar prawa materialnego	256
4.4.2. Wymiar prawa ustrojowego	260
4.4.3. Wymiar prawa procesowego	261
4.5. Skutki krzyżowania się kompetencji organów.....	274
4.5.1. Skutki dla administracji publicznej, podmiotów nadzorowanych i podmiotów danych 274	
4.5.2. Skutki dla gospodarki.....	286

4.6. Krzyżowanie się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych w ujęciu prawnoporównawczym	290
4.6.1. Królestwo Niderlandów	292
4.6.2. Wielka Brytania.....	295
4.7. Podsumowanie	299
5. ROZDZIAŁ 5 – PRZYCZYNY KRZYŻOWANIA SIĘ KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH I POSTULATY DE LEGE FERENDA.....	301
5.1. Wstęp	301
5.2. Przyczyna nr 1: Rozłączenie regulacyjne spowodowane transformacją cyfrową.....	302
5.3. Przyczyna nr 2: Wybór techniki prawodawczej spowodowany potrzebą zapewnienia neutralności technologicznej regulacji	309
5.4. Przyczyna nr 3: Proces europeizacji prawa administracyjnego	318
5.5. Przyczyna nr 4: Prawo ochrony danych osobowych jako prawo wszystkiego?	330
5.6. Przyczyna nr 5: Wyważenie różnych celów przez podmioty administrujące.....	337
5.7. Postulaty <i>de lege ferenda</i>	344
5.7.1. Postulat nr 1: Wyodrębnienie prawa danych jako odrębnej kompleksowej gałęzi prawa	345
5.7.2. Postulat nr 2: Centralizacja struktury stosowania RODO wobec największych podmiotów nadzorowanych i ustanowienie organów ochrony danych jako organów właściwych dla stosowania aktów prawnych w obszarze przetwarzania danych osobowych	348
5.7.3. Postulat nr 3: Wprowadzenie instrumentów współpracy między organami administracji publicznej stosującymi akty prawne w obszarze przetwarzania danych osobowych.....	352
5.7.4. Postulat nr 4: Wprowadzenie rozwiązań typu klauzula <i>safe harbour</i>	356
5.8. Podsumowanie	359
ZAKOŃCZENIE	361
SPIS ILUSTRACJI.....	368
WYKAZ ŹRÓDEŁ.....	369
AKTY PRAWNE.....	369
ORZECZNICTWO	379
DECYZJE ADMINISTRACYJNE, OPINIE I DOKUMENTY URZĘDOWE	382
LITERATURA	393
STRONY INTERNETOWE.....	440

WYKAZ SKRÓTÓW

AKTY PRAWNE¹

PRAWO MIĘDZYNARODOWE	
EKPC	Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.).
Konwencja 108	Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 z późn. zm.).
Protokół Dodatkowy	Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, sporządzony w Strasburgu dnia 8 listopada 2001 r. (Dz. U. z 2006 r. Nr 3, poz. 15).
PRAWO UNII EUROPEJSKIEJ	

¹ Specyfika tej rozprawy powoduje, że w niektórych podrozdziałach analizowany jest wyłącznie jeden akt prawny, a jednocześnie w całej rozprawie w ten sposób scharakteryzowano szereg aktów. Może powodować to trudności w lekturze rozprawy nawet pomimo stosowania systemu skrótów. Stąd też w rozprawie na początku niektórych podrozdziałów – tam, gdzie, zdaniem autora, ułatwia to lekturę pracy – niektóre skróty zdefiniowane w tej części zostały ponownie rozwinięte. Ponadto, z tych samych względów, niektóre skróty aktów zdefiniowane zostały przez pełne wyrazy, np. Rozporządzenie Dane Nicosobowe (zamiast literowego skrótu „Rozporządzenie FFD”) w nadziei, że uczyni to lekturę płynniejszą.

„AI Act” lub „Akt w sprawie Sztucznej Inteligencji”	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) PE/24/2024/REV/1 Dz. Urz. UE L, 2024/1689, 12.7.2024.
„Akt o Cyberbezpieczeństwie” lub „CSA”	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Tekst mający znaczenie dla EOG) PE/86/2018/REV/1 Dz. Urz. UE L 151, 7.6.2019, p. 15–69.
„Akt o Rynkach Cyfrowych” lub „DMA”	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Tekst mający znaczenie dla EOG) PE/17/2022/REV/1 Dz. Urz. UE L 265, 12.10.2022, p. 1–66.

„Akt o Usługach Cyfrowych” lub „DSA”	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Tekst mający znaczenie dla EOG) PE/30/2022/REV/1 Dz. Urz. UE L 277, 27.10.2022, p. 1–102.
„Akt w sprawie Danych” lub „Data Act”	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) PE/49/2023/REV/1 Dz. Urz. UE L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj
„Akt w sprawie Zarządzania Danymi” lub „DGA”	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Tekst mający znaczenie dla EOG) PE/85/2021/REV/1 Dz. Urz. UE L 152, 3.6.2022, p. 1–44.
TFUE	Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE. C 115 z 2008r., s. 47).
TUE	Traktat o Unii Europejskiej (wersja skonsolidowana: Dz. Urz. UE C 202 z 2016 r., s. 13).
KPP	KPP – Karta praw podstawowych (wersja skonsolidowana: Dz. Urz. UE C 202 z 2016

	r., s. 389).
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 199 z 2016 r., s. 1 z późn. zm.).
EUDPR	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Tekst mający znaczenie dla EOG.) PE/31/2018/REV/1 Dz. Urz. UE L 295, 21.11.2018, p. 39–98.
Dyrektywa AML IV	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. Urz. UE L 141 z 2015 r.,

	s. 73 z późn. zm.).
Dyrektywa AML V	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Tekst mający znaczenie dla EOG) PE/72/2017/REV/1 Dz. Urz. UE L 156, 19.6.2018, p. 43–74.
Dyrektywa AML VI	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1673 z dnia 23 października 2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnych (Dz. Urz. UE L 284 z 2018 r., s. 22).
Dyrektywa ePrivacy	Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE L 201 z 2002 r., s. 37 z późn. zm.).
Dyrektywa LED	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego

	przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW Dz. Urz. UE L 119, 4.5.2016, p. 89–131.
Dyrektywa ODO	Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 1995 r., s. 31 z późn. zm.).
Dyrektywa o Usługach Płatniczych	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L z 2015 r. nr 337, s. 35 z późn. zm.).
Dyrektywa NIS	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Dz. Urz. UE L 194, 19.7.2016, p. 1–30.
Dyrektywa NIS 2	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

	(dyrektywa NIS 2) (Tekst mający znaczenie dla EOG) PE/32/2022/REV/2 Dz. Urz. UE L 333, 27.12.2022, p. 80–152.
„Merger Control Regulation” lub „MCR”	Rozporządzenie Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu (Tekst mający znaczenie dla EOG) Dz. Urz. UE L 1, 4.1.2003, p. 1–25.
Rozporządzenie 1/2003	Rozporządzenie Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu (Dz. Urz. UE L 1, z 2003 r. Nr 1, str. 1 z późn. zm.).
Rozporządzenie Dane Niesobowe	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych niesobowych w Unii Europejskiej (Dz. Urz. UE L 303 z 2018 r., s. 59).
Rozporządzenie ePrivacy	Wniosek dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej) COM/2017/010 final - 2017/03 (COD).
PRAWO KRAJOWE	
Konstytucja RP	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz. U. nr 78, poz. 483 ze

	zm.).
KP	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2019 r. poz. 730 ze zm.).
KPA	Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2019 r. poz. 730 ze zm.).
PPSA	Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2019 r. poz. 60 ze zm.).
Prawo Telekomunikacyjne	Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34).
UODO	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 730 ze zm.).
UODO1997	Uchylona ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2018 r. poz. 723).
UKK	Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2023 r. poz. 1689 z późn. zm.).
UKSC	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.).
Ustawa o AML	Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2023 r. poz. 1124 z późn. zm.).
Ustawa o Działach	Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (t.j. Dz. U. z 2022 r. poz. 2512 z późn. zm.).
Ustawa LED	Ustawa z dnia 14 grudnia 2018 r. o ochronie

	danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r. poz. 1206).
Ustawa Wdrożeniowa	Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. poz. 730).
Zasady techniki prawodawczej	Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (t.j. Dz. U. z 2016 r. poz. 283).

CZASOPISMA NAUKOWE

BSP	Białostockie Studia Prawnicze
CLSR	Computer Law & Security Review
EPS	Europejski Przegląd Sądowy
EDPL	European Data Protection Law Review
Eur. J. Risk Regul.	European Journal of Risk Regulation
Int. Data Priv. Law	International Data Privacy Law
Int. Rev. Law Comput. Technol.	International Review of Law, Computers & Technology
J. Eur. Public Policy	Journal of European Public Policy
Law Innov. Technol.	Law, Innovation and Technology
MoP	Monitor Prawniczy

PiP	Państwo i Prawo
PPP	Przegląd Prawa Publicznego
RECoL	Review of European and Comparative Law
RPEiS	Ruch Prawniczy, Ekonomiczny i Socjologiczny
iKAR	internetowy Kwartalnik Antymonopolowy i Regulacyjny
ZNSA	Zeszyty Naukowe Sądownictwa Administracyjnego
ZNUJ	Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej

INNE SKRÓTY

AI	sztuczna inteligencja
AML	przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu
AMLA	Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu
CSIRT	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (<i>Computer Security Incident Response Team</i>)
EOG	Europejski Obszar Gospodarczy
EROD	Europejska Rada Ochrony Danych
EIOD	Europejski Inspektor Ochrony Danych
ETPC	Europejski Trybunał Praw Człowieka
EUR-LEX	Internetowy portal prawa UE zarządzany przez Urząd Publikacji UE dostępny pod adresem URL: https://eur-lex.europa.eu/content/welcome/about.html
TK	Trybunał Konstytucyjny
TSUE	Trybunał Sprawiedliwości Unii Europejskiej

OECD	Organizacja Współpracy Gospodarczej i Rozwoju
ONZ	Organizacja Narodów Zjednoczonych
NSA	Naczelny Sąd Administracyjny
PUODO	Prezes Urzędu Ochrony Danych Osobowych
GIIF	Główny Inspektor Informacji Finansowej
GIODO	Generalny Inspektor Ochrony Danych Osobowych
Grupa Robocza	Grupa Robocza Artykułu 29 do spraw Ochrony Danych
„KE” lub „Komisja”	Komisja Europejska
KNF	Komisja Nadzoru Finansowego
„organ nadzorczy ustanowiony na podstawie RODO” lub „organ ochrony danych”	niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO
t.j.	tekst jednolity
Sejm	Sejm Rzeczypospolitej Polskiej
SIP	System Informacji Prawnej
SN	Sąd Najwyższy
Prezes UOKiK	Prezes Urzędu Ochrony Konkurencji i Konsumentów
PUODO	Prezes Urzędu Ochrony Danych Osobowych
SIP LEX	System Informacji Prawnej LEX
RE	Rada Europy
UE	Unia Europejska
VLOPs	bardzo duże platformy internetowe
VLOSEs	bardzo duże wyszukiwarki internetowe
WSA	wojewódzki sąd administracyjny
Wielka Brytania	Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej
MC	Ministerstwo Cyfryzacji
OTK	Orzecznictwo Trybunału Konstytucyjnego

WPROWADZENIE

PROBLEM BADAWCZY

Historia ludzkości może zostać przedstawiona jako historia rozwoju techniki², ponieważ potrzeba innowacji wpisuje się w naturę człowieka.³ Zmiany w technice prowadziły do zmian ekonomicznych, społecznych i politycznych (nazwanych w tej rozprawie zmianami socjo-technicznymi⁴), które były przedmiotem zainteresowania prawodawców przez wieki. Motywacje prawodawców, aby regulować te zmiany, były różne, począwszy od postrzegania innowacyjnej techniki jako zagrożenia dla stabilności porządku społeczno-politycznego (np. ograniczenia w użyciu prasy drukarskiej przez Imperium Osmańskie⁵), przez potrzebę ochrony użytkowników przed fizycznymi niebezpieczeństwami nowej techniki (np. konieczność montowania pasów bezpieczeństwa w samochodach)⁶ aż po zapewnienie konkurencyjności rynków i ochronę praw człowieka⁷ (np. wobec praktyk gigantów cyfrowych w dwóch pierwszych dekadach XXI wieku)⁸.

Ostatnią rewolucyjną zmianą, jakiej doświadczyła ludzkość, jest trwająca wciąż od początku lat 90. ubiegłego wieku transformacja cyfrowa⁹ rozumiana jako proces zmian technicznych, ekonomicznych i społecznych o charakterze globalnym, spowodowanych

² Por. T. Hughes, *History of Technology* [in:] *International Encyclopedia of the Social & Behavioral Sciences*, edited by N. J. Smelser, P. B. Baltes, Amsterdam: 2001, <https://doi.org/10.1016/B0-08-043076-7/02648-6> (dostęp: 20.09.2024 r.).

³ Niniejsza rozprawa doktorska została w zasadniczej części napisana w ciągu trzech miesięcy, od stycznia do marca 2024 r. i jest efektem badań prowadzonych od 2020 r. Stan prawny rozprawy został zaktualizowany na wrzesień 2024 r., w którym to miesiącu autor złożył rozprawę i ukończył Szkołę Doktorską Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie zgodnie z Indywidualnym Planem Badawczym. To, kiedy rozprawa została napisana ma wpływ na sposób przeprowadzenia wywodu, podniesione argumenty i przykłady. Autor tej rozprawy ma świadomość ewolucji zagadnień analizowanych w tej rozprawie, związanych z nowymi i przewidywanymi aktami prawodawczymi na poziomie unijnym i krajowym, jak również orzecznictwem sądów unijnych i krajowych oraz stanowiskami organów dotyczących tych zagadnień. Autor rozprawy śledzi te zmiany. Przypuszczać należy, że między złożeniem rozprawy a jej obroną niektóre analizy i argumenty przestaną być w pełni aktualne lub ujawnione zostaną przykłady, które lepiej uzasadnią bronione w rozprawie hipotezy badawcze.

⁴ Użycie tego terminu inspirowane jest przez L. Bennett Moses, *Regulating in the Face of Sociotechnical Change* [in:] *The Oxford Handbook of Law, Regulation and Technology*, edited by R. Brownsword, E. Scotford, K. Yeung, Oxford 2017, <https://doi.org/10.1093/oxfordhb/9780199680832.013.49> (dostęp: 31.12.2023 r.).

⁵ J. Rubin, *Restrictions on the Printing Press* [in:] *Rulers, Religion, and Riches: Why the West Got Rich and the Middle East Did Not*, Cambridge 2017, s. 112-113.

⁶ R. J. Arnould, H. Grabowski, *Auto Safety Regulation: An Analysis of Market Failure*, „The Bell Journal of Economics” 1981, Vol. 12, No. 1, s. 27.

⁷ Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie, COM/2021/118 final.

⁸ W tym kontekście balansowanie rozbieżnych celów wyznaczonych poszczególnym organom administracji publicznej w obszarze przetwarzania danych osobowych jest przedmiotem analizy w podrozdziale 5.5. niniejszej rozprawy.

⁹ Proces ten rozumiany jest niejednoznacznie. Por. *Transformacja cyfrowa*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021.

przejściem od zapisu i przetwarzania danych w postaci analogowej do postaci cyfrowej oraz upowszechnieniem systemu informatycznego World Wide Web (WWW)¹⁰. Kluczową z perspektywy tej rozprawy konsekwencją jest radykalny wzrost liczby automatycznie przetwarzanych danych, w tym danych osobowych¹¹. Przykładowo, w 2016 r. ustalono, że 90% danych na świecie zostało wytworzonych w ciągu dwóch poprzedzających lat¹². Dane osobowe nie stanowią przy tym tylko informacji będących przedmiotem ochrony praw podstawowych, które są wolne od ekonomicznego uwikłania, ale także tworzą nową klasę aktywów niematerialnych, do których dostęp decyduje o efektywności i zyskowności podmiotów operujących w gospodarce cyfrowej¹³.

Ponieważ transformacja cyfrowa wpłynęła na wszystkie aspekty rzeczywistości, generując nowe szanse i ryzyka, doczekała się – tak jak inne zmiany socjotechniczne w przeszłości – odpowiedzi prawodawcy. W rozprawie poddany został analizie wycinek odpowiedzi prawodawcy unijnego i krajowego. Przedmiotem rozprawy są analiza kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych, przedstawienie zjawiska krzyżowania się tych kompetencji, jego przyczyn i rozwiązań dla skutków związanych z występowaniem tego zjawiska. Celem rozprawy jest weryfikacja głównej hipotezy badawczej, twierdzącej, że w obszarze przetwarzania danych osobowych ustanowione zostały organy administracji publicznej, których kompetencje krzyżują się. To prowadzi do niepewności prawnej, a brak jest instrumentów prawnych, które mogłyby ten problem skutecznie rozwiązać.

Dla zrozumienia kontekstu istotne jest, że zmiana socjotechniczna spowodowana transformacją cyfrową nie jest pierwszą zmianą spowodowaną rozwojem techniki, na której szanse i zagrożenia odpowiada prawodawca. Ponieważ transformacja cyfrowa jest trwającym procesem, odpowiedź ta nie może być ostateczna. Uwikłana jest ona w różne podejścia etyczne¹⁴ jednostek mających wpływ na stanowienie, stosowanie i wykładnię prawa oraz ich

¹⁰ A. Bounfour, 2.3 Digital Transformation [in:] Digital Futures, Digital Transformation: From Lean Production to Acceluction, Cham 2016, s. 20-23.

¹¹ Pojęcie danych osobowych zbadano w podrozdziale 2.3. rozprawy.

¹² European Parliamentary Research Service, M. Szczepański, *Is Data the New Oil? Competition Issues in the Digital Economy*, European Parliamentary Research Service 2020, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf) (dostęp: 7.09.2024 r.), s. 4.

¹³ Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, s. 9, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 15.09.2024 r.).

¹⁴ Por. *Oxford Handbook of Digital Ethics*, ed. by C. Véliz, Oxford 2023, <https://doi.org/10.1093/oxfordhb/9780198857815.001.0001> (dostęp: 19.12.2023 r.).

stosunek do innowacyjności¹⁵. To, jaki kształt przyjmą dojrzałe akty prawne w obszarze przetwarzania danych osobowych w UE, nie jest uzależnione tylko od samego przebiegu zmian socjotechnicznych, ale uwarunkowane jest również specyfiką ustroju UE i państw członkowskich oraz prawa administracyjnego w tych państwach i procesu europeizacji prawa administracyjnego¹⁶.

Odpowiedź prawodawcy unijnego (a w konsekwencji także krajowego) na transformację cyfrową (od początku lat 90. XX wieku do wybuchu pandemii COVID-19) była wielowektorowa, w tym nakierowana na ochronę własności intelektualnej¹⁷, ochronę konsumentów¹⁸ i handel elektroniczny¹⁹. W istotnej mierze (w tym w drugiej dekadzie XXI wieku) ciężar tej odpowiedzi skupiony był na ochronie danych osobowych, czego najważniejszym przykładem jest RODO. Ochrona danych osobowych wymagała przyjęcia nowych aktów prawnych, których podstaw aksjologicznych należy szukać w systemie ochrony praw człowieka. Prawo do ochrony danych osobowych i do prywatności stanowią bowiem prawa podstawowe chronione w KPP²⁰. Jednocześnie dane, w tym dane osobowe, identyfikowane są jako kluczowe aktywo gospodarki cyfrowej²¹.

Do krzyżowania się zakresów przedmiotowych aktów prawnych stanowiących odpowiedź na transformację cyfrową dochodzi w specyficznej relacji między tymi aktami prawnymi. RODO jest aktem prawa unijnego stosowanym bezpośrednio, podczas gdy akty prawne, z którymi zakres przedmiotowy RODO się krzyżuje, są również rozporządzeniami prawa unijnego, dyrektywami albo ustawami w krajowych porządkach prawnych (implementującymi dyrektywy lub nie). Jako obszar referencyjny²² dla prowadzonych badań

¹⁵ Por. T. A. Hemphill, *The Innovation Governance Dilemma: Alternatives to the Precautionary Principle*, „Technology in Society” 2020, Vol. 63, <https://doi.org/10.1016/j.techsoc.2020.101381> (dostęp: 20.09.2024 r.).

¹⁶ Przyczyny zjawiska krzyżowania się kompetencji organów administracji publicznej w tym obszarze omówione zostały w rozdziale 5. niniejszej rozprawy.

¹⁷ Np. Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, Dz. U. L 167 z 22.6.2001, s. 10-19; Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (Wersja skodyfikowana) (Tekst mający znaczenie dla EOG), Dz. Urz. UE L 111 z 5.5.2009, s. 16-22.

¹⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Tekst mający znaczenie dla EOG.) PE/26/2019/REV/1.

¹⁹ Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz. Urz. UE L 178, 17.7.2000, p. 1–16.

²⁰ Odpowiednio w art. 7 i 8 KPP.

²¹ European Parliamentary Research Service, M. Szczepański, *Is data the new oil? Competition issues in the digital economy*, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf) (dostęp: 7.09.2024 r.), s. 4.

²² Uzasadnienie wyboru obszaru referencyjnego przedstawiono w podrozdziale 2.5. rozprawy.

w odniesieniu do krzyżowania się zakresu przedmiotowego RODO z innymi aktami prawnymi wybrane zostały unijne i krajowe akty regulujące przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu, cyberbezpieczeństwo, prawo konkurencji, Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych, sztuczną inteligencję oraz europejskie przestrzenie danych (Akt w Sprawie Zarządzania Danymi i Akt w Sprawie Danych)²³.

Jednak jaka relacja zachodzi pomiędzy zjawiskiem krzyżowania się zakresu przedmiotowego aktów prawnych w obszarze przetwarzania danych osobowych, a krzyżowaniem się kompetencji organów stosujących te akty? Problem jest głębszy niż tylko ustalenie, że krzyżowanie się zakresu przedmiotowego aktów z natury rzeczy musi prowadzić do niejasnych relacji między kompetencjami organów, które je stosują. Tak sformułowany problem nie byłby nowością w prawie administracyjnym. Jego istota w odniesieniu do przetwarzania danych osobowych dotyczy sposobu konstruowania przepisów w tym obszarze. Wybór prawodawcy jest podyktowany specyfiką przedmiotu regulacji, czyli przetwarzaniem danych osobowych w kontekście transformacji cyfrowej. Przepisy konstruowane są bowiem w taki sposób, aby zachować neutralność technologiczną i podlegać horyzontalnemu stosowaniu (w odniesieniu do wszystkich sektorów gospodarki)²⁴. Stąd też przedstawienie zjawiska krzyżowania się kompetencji tych organów nie jest możliwe bez uprzedniej analizy krzyżowania się zakresu przedmiotowego aktów prawnych normujących przetwarzanie danych osobowych.

W obszarze referencyjnym zidentyfikowane zostały następujące organy administracji publicznej na poziomie unijnym, których kompetencje się krzyżują: Europejska Rada Ochrony Danych, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Komisja Europejska jako organ unijnego prawa konkurencji, Grupa Wysokiego Szczebla, Europejska Rada ds. Usług Cyfrowych, Europejska Rada ds. Innowacji w zakresie Danych, Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji. Z kolei na poziomie krajowym zidentyfikowano następujące organy: Prezes Urzędu Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej, organy właściwe do spraw cyberbezpieczeństwa, Prezes Urzędu Ochrony Konkurencji i Konsumenta jako organ krajowego prawa konkurencji, organy właściwe w Akcie o Usługach Cyfrowych, organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych, organy właściwe

²³ Krzyżowanie się zakresu przedmiotowego RODO z aktami prawnymi w tym obszarze referencyjnym zbadano w podrozdziale 2.6. rozprawy.

²⁴ Wybór prawodawcy, aby obszar przetwarzania danych osobowych uregulować za pomocą zasad konkretyzowanych na etapie stosowania prawa, poddany został analizie w podrozdziale 5.3. rozprawy.

w Akcie w sprawie Danych i organy właściwe w Akcie w sprawie Sztucznej Inteligencji²⁵. Kierując się potrzebą ograniczenia objętości rozprawy i mając na względzie zmieniający się kształt projektów aktów prawnych, podjęto decyzję, aby z zakresu rozprawy wyłączyć analizę konkretnych rozwiązań w zakresie krajowych (polskich) organów administracji publicznej, które zostały albo zostaną ustanowione na skutek operacjonalizacji w krajowym porządku prawnym następujących aktów prawnych: Aktu o Usługach Cyfrowych, Aktu w sprawie Danych, Aktu w sprawie Zarządzania Danymi i Aktu w sprawie Sztucznej Inteligencji. W odniesieniu do tych aktów dokonano analizy ich przepisów w zakresie, w jakim nakładają na prawodawcę krajowego obowiązek ustanowienia określonych organów.

Zjawiska krzyżowania się zakresu przedmiotowego aktów prawnych i kompetencji organów w tym obszarze nie są nowym problemem. Zwracano na to uwagę już w dokumentach EIOD w 2014 r.²⁶, a zatem jeszcze w czasie obowiązywania Dyrektywy ODO. Zmianie uległa jednak skala tych zjawisk w dwóch wymiarach. Po pierwsze, sam proces transformacji cyfrowej, zwłaszcza na skutek zmian spowodowanych pandemią COVID-19²⁷, nabrał przyspieszenia. Z każdym rokiem pogłębia się cyfryzacja wszystkich aspektów rzeczywistości nie tylko polskiej i europejskiej, lecz także globalnej. Po drugie, w konsekwencji tych wszechogarniających zmian prawodawca unijny podjął w ostatnich latach szereg inicjatyw prawodawczych, które realizowane są w ramach Europejskiej Strategii Cyfrowej²⁸ i Europejskiej Strategii w zakresie Danych²⁹. Celem tych strategii są suwerenność cyfrowa UE w zglobalizowanej gospodarce przy zachowaniu zrównoważonego wzrostu³⁰ i stworzenie jednolitego rynku danych na podstawie europejskich przestrzeni danych, który zapewni innowacyjność oraz konkurencyjność przy poszanowaniu praw podstawowych³¹. Obie te strategie odnoszą się do przetwarzania danych osobowych. W celu ich realizacji przyjęto na

²⁵ Kompetencje organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych zbadane zostały w rozdziale 3. rozprawy.

²⁶ Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 15.09.2024 r.).

²⁷ Por. także W. Wiewiórowski, Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią, „Europejski Przegląd Sądowy” 2020, nr 6, s. 20-33.

²⁸ Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie, COM/2021/118 final.

²⁹ Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska strategia w zakresie danych, COM(2020) 66 final.

³⁰ Komunikat prasowy Cyfrowa dekada Europy: Komisja wyznacza kierunek w celu utworzenia do 2030 r. Europy opartej na technologiach cyfrowych, 9.03.2021 r., https://ec.europa.eu/commission/presscorner/detail/pl/IP_21_983 (dostęp: 15.09.2024 r.).

³¹ Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska strategia w zakresie danych, COM(2020) 66 final.

poziomie unijnym następujące akty prawne (w szczególności): Akt o Rynkach Cyfrowych, Akt o Usługach Cyfrowych, Akt w sprawie Sztucznej Inteligencji³², Akt w sprawie Zarządzania Danyymi i Akt w sprawie Danych. Relacja zakresu przedmiotowego tych aktów wobec RODO jest badana w tej rozprawie³³.

Czym jednak jest samo zjawisko krzyżowania się tych kompetencji? W literaturze polskiej i europejskiej brakuje jego kompleksowego ujęcia teoretycznego. Aby tę lukę wypełnić, w rozprawie podjęto próbę zdefiniowania tego zjawiska³⁴ i zaproponowano jego typologię³⁵. Analiza krzyżowania się kompetencji wpisana jest w klasyczne problemy prawa administracyjnego, w tym pojmowania kompetencji organów administracji publicznej³⁶. Jest to o tyle problematyczne, że samo pojęcie kompetencji (węzłowe przecież dla nauki prawa administracyjnego) wciąż jest niejednoznaczne. Co więcej, niejednoznaczność ta uległa dalszemu pogłębieniu wskutek wprowadzenia w ostatnich latach do języka prawniczego i prawnego terminu „kompetencje cyfrowe”³⁷. W konsekwencji, zjawisko to jest wyzwaniem dla stanowienia, stosowania i wykładni prawa administracyjnego, a także dla ochrony praw podstawowych i rozwoju gospodarki unijnej oraz krajowej³⁸. Analiza jego skutków prowadzi do pytania o zmiany, jakie mogłyby zostać wprowadzone, aby zredukować ich negatywny wpływ³⁹. W perspektywie przyczyn analizowanego zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych w rozprawie sformułowano cztery postulaty *de lege ferenda*.

HIPOTEZY BADAWCZE

Przeprowadzone badania doprowadziły do sformułowania głównej hipotezy badawczej:

W obszarze przetwarzania danych osobowych ustanowione zostały organy administracji publicznej, których kompetencje krzyżują się, co prowadzi do niepewności prawnej, a brak

³² Zgodnie z *European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, 2020. Ten dokument, chociaż jest odrębny od Europejskiej Strategii Cyfrowej, pozostaje z nim spójny.

³³ W podrozdziałach 2.6.3.-2.6.5. rozprawy.

³⁴ Analiza dokonana w podrozdziale 4.2. rozprawy.

³⁵ Sformułowano w podrozdziale 4.3. rozprawy.

³⁶ Pojęcie kompetencji scharakteryzowano w podrozdziale 1.4. rozprawy.

³⁷ Ewolucja pojęcia kompetencji jako przykład wpływu prawodawstwa stanowiącego odpowiedź na transformację cyfrową na podstawowe pojęcia prawa administracyjnego przedstawiona została w podrozdziale 1.6. rozprawy.

³⁸ Skutki tego zjawiska scharakteryzowano w podrozdziale 6.2. rozprawy.

³⁹ Postulaty *de lege ferenda* sformułowano zostały w podrozdziale 5.7. rozprawy.

jest instrumentów prawnych, które mogłyby ten problem skutecznie rozwiązać.

Dokonanie weryfikacji głównej hipotezy badawczej wymagało sformułowania pomocniczych hipotez badawczych:

- I. Pojęcie kompetencji organów administracji publicznej jest niejednoznaczne. Na ustalenie znaczenia terminu „kompetencje” w języku prawnym wpływa wprowadzenie użycia terminu „kompetencje cyfrowe” na określenie całokształtu wiedzy, umiejętności i postaw umożliwiających pełnowartościowe funkcjonowanie w społeczeństwie cyfrowym. Na potrzeby tej rozprawy kompetencje organów administracji publicznej rozumiane będą jako całokształt uprawnień i obowiązków organu administracji publicznej. Organy wyposażone zostały w kompetencje, aby wykonywać przyznane im zadania w wyznaczonych przez prawo celach.
- II. Zakres przedmiotowy i podmiotowy RODO jest szeroki i nieostry, ponieważ celem prawodawcy unijnego było zapewnienie możliwie pełnej realizacji praw podstawowych do ochrony danych osobowych i prywatności. Z analizy orzecznictwa TSUE w odniesieniu do Dyrektywy ODO i RODO wynika, że TSUE dokonywał stopniowego poszerzenia tych zakresów przez wykładnię rozszerzającą podstawowych pojęć, które te zakresy wyznaczają, to jest „dane osobowe”, „przetwarzanie danych osobowych”, „administrator danych osobowych” i „współadministrator danych osobowych”.
- III. Zakres przedmiotowy RODO krzyżuje się z zakresem przedmiotowym unijnych i krajowych aktów prawnych w obszarze przetwarzania danych osobowych, które wybrane zostały jako obszar referencyjny dla przeprowadzonych badań, to jest aktów prawnych regulujących:
 - a. przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu;
 - b. cyberbezpieczeństwo;
 - c. prawo konkurencji, Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych;
 - d. sztuczną inteligencję;
 - e. europejskie przestrzenie danych.
- IV. W obszarze referencyjnym zidentyfikowane zostały następujące organy administracji publicznej, których kompetencje krzyżują się z sobą:

- a. na poziomie unijnym: Europejska Rada Ochrony Danych, Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Komisja Europejska jako organ unijnego prawa konkurencji, Grupa Wysokiego Szczebla, Europejska Rada ds. Usług Cyfrowych, Europejska Rada ds. Innowacji w zakresie Danych, i Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji;
 - b. na poziomie krajowym: Prezes Urzędu Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej, organy właściwe do spraw cyberbezpieczeństwa, Prezes Urzędu Ochrony Konkurencji i Konsumenta jako organ krajowego prawa konkurencji, organy właściwe w Akcie o Usługach Cyfrowych, organy właściwe do spraw usług pośrednictwa danych, i organy właściwe do spraw rejestracji organizacji altruizmu danych, organy właściwe w Akcie w sprawie Danych i organy właściwe w Akcie w sprawie Sztucznej Inteligencji.
- V. Zasadne jest wyróżnienie następujących typów kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych:
 - a. proceduralne w toku prowadzonych postępowań w celu wyjaśnienia sprawy lub wobec podmiotów nadzorowanych;
 - b. naprawcze;
 - c. współpracy;
 - d. doradcze, informacyjne oraz edukacyjne.
- VI. Zjawisko krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych należy zdefiniować jako sytuację, w której co najmniej dwóm organom administracji publicznej przyznane zostały kompetencje w tej samej sprawie albo w odniesieniu do tego samego zagadnienia w taki sposób, że może prowadzić to do rozstrzygnięcia tej samej sprawy lub tego samego zagadnienia odmiennie.
- VII. Zasadne jest wyróżnienie następujących typów krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych:
 - a. właściwe i niewłaściwe;

- b. zamierzone (kiedy było to intencją prawodawcy) i niezamierzone (kiedy nie było to intencją prawodawcy);
- c. w wymiarze horyzontalnym (w sytuacji, w której krzyżowanie się kompetencji ujawnia się z perspektywy organów administracji publicznej) i wertykalnym (w sytuacji, w której krzyżowanie się kompetencji ujawnia się z perspektywy podmiotów nadzorowanych i podmiotów danych).

VIII. Brak jest skutecznych instrumentów prawnych do rozwiązania negatywnych skutków, które wynikają z tego zjawiska. Chociaż prawodawca dostrzegł ryzyko jego występowania, to instrumenty, które zostały ustanowione, aby przeciwdziałać jego negatywnym konsekwencjom, okazały się niewystarczające. Za niewystarczające należy uznać te instrumenty zarówno w wymiarze prawa administracyjnego procesowego (np. rozstrzyganie sporów o właściwość i instrumenty współpracy na poziomie krajowym i unijnym), ustrojowego (przyznanie kompetencji w sprawach „dotyczących przetwarzania danych osobowych” organom ochrony danych na podstawie poszczególnych aktów, np. Data Act), jak i prawa administracyjnego materialnego (np. tzw. klauzule „bez uszczerbku”).

IX. Nieskuteczne są instrumenty prawne w prawie administracyjnym materialnym, w tym tzw. klauzule „bez uszczerbku”. Nazywane są „sztuczkami retorycznymi”, ponieważ niejasne jest ich znaczenie i rola w zestawieniu z wyborem techniki legislacyjnej, aby obszar ten uregulować za pomocą zasad (bardziej niż reguł), metody opartej na ryzyku z terminów nieostrych. Z kolei instrumenty prawne w prawie procesowym umożliwiają rozstrzyganie sporów o właściwość między organami administracji publicznej na gruncie skonkretyzowanych spraw rozstrzyganych w drodze decyzji administracyjnych, a zatem nie można używać ich prospektywnie i abstrakcyjnie, co nie pozwala usunąć niepewności prawnej dotyczącej, np. wydawania instrumentów prawnych typu *soft law*. Spory o właściwość między organami administracji publicznej w obszarze przetwarzania danych osobowych nie mogą być także rozstrzygnięte na podstawie Konstytucji RP, ponieważ w tym trybie mogą być rozstrzygane jedynie spory między centralnymi konstytucyjnymi organami, do których nie można zaliczyć analizowanych organów. Chociaż niektóre przepisy KPA, zwłaszcza art. 7b KPA, mogłyby – będąc odpowiednio wykładane – stanowić podstawę do współpracy podmiotów administrujących w obszarze przetwarzania w odniesieniu do wykonywania kompetencji o charakterze „władczym”,

to jednak niejednoznaczny sposób ich sformułowania i brak ugruntowanej interpretacji w orzecznictwie sądów administracyjnych odbiera im de lege lata przymiot skutecznych instrumentów prawnych do zredukowania negatywnych skutków analizowanego zjawiska.

X. Zjawisko to powoduje następujące skutki:

- a. prowadzi do pogłębienia niepewności prawnej zarówno po stronie samych organów administracji publicznej, podmiotów nadzorowanych i podmiotów danych w odniesieniu do podziału kompetencji między organami i prawidłowej wykładni aktów prawnych w obszarze przetwarzania danych osobowych, a w konsekwencji powoduje obniżenie skuteczności stosowania aktów prawnych w tym obszarze; ponadto, stanowi zagrożenie dla realizacji zakazu *ne bis in idem* w prawie administracyjnym w odniesieniu do rozstrzygania tej samej sprawy przez różne organy administracji publicznej oraz dla ochrony praw podstawowych;
- b. ponadto, niepewność prawna spowodowana tym zjawiskiem stanowi barierę dla rozwoju nowoczesnej gospodarki w Polsce i w Unii Europejskiej.

XI. Zjawisko krzyżowania się kompetencji organów administracji publicznej występuje także w innych jurysdykcjach. Do ograniczonej analizy prawoporównawczej wybrana została jurysdykcja Królestwa Niderlandów jako przykład dojrzałej jurysdykcji unijnej i jurysdykcja Wielkiej Brytanii jako przykład jurysdykcji prawa *common law*. Z analizy wynika, że w obu tych jurysdykcjach krzyżowanie się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych stanowi wyzwanie, dla którego nie ma efektywnego rozwiązania. Dowodzi to, że to zjawisko (obecne także w innych jurysdykcjach) jest konsekwencją rozłączenia regulacyjnego spowodowanego transformacją cyfrową, którego prawodawca nie mógł uniknąć. Nie sposób bowiem, aby prawodawca – czy to europejski, czy krajowy – był zdolny, aby nie tylko przewidzieć, ale również zredukować z wyprzedzeniem problemy społeczne, ekonomiczne i polityczne spowodowane transformacją cyfrową, której jedną z kluczowych cech jest przetwarzanie danych osobowych na masową skalę. Jednocześnie w obu tych jurysdykcjach przyjęto rozwiązania, których celem jest zredukowanie negatywnych skutków zjawiska krzyżowania się kompetencji przez powołanie podmiotów o funkcji koordynującej działania podejmowane przez poszczególne organy administracji publicznej.

XII. Zidentyfikowane zostały wymienione poniżej przyczyny zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych.

- a. Nieadekwatność odpowiedzi prawodawcy unijnego i krajowego na przemiany spowodowane transformacją cyfrową, co skutkuje rozłączeniem regulacyjnym (*regulatory disconnect*).
- b. Wybór przez prawodawcę techniki legislacyjnej w oparciu o założenie, że należy obszar ten uregulować za pomocą zasad, terminów nieostrych i metody opartej na ryzyku, przede wszystkim w celu zapewnienia neutralności technologicznej. Doprowadziło to do użycia wykładni operatywnej przez organy administracji publicznej przy pomocy metody celowościowej i funkcjonalnej.
- c. Niejasność taksonomiczna w odniesieniu do „prawa ochrony danych osobowych”. Brak jasności co do sposobu wyodrębnienia kompleksowej gałęzi prawa w tym obszarze stanowi problem dla stanowienia, stosowania i wykładni prawa, który będzie narastał wraz ze zwiększeniem liczby aktów prawnych, pogłębiając istniejący już chaos. Konsekwentne wyodrębnienie kompleksowej gałęzi jest niezbędne dla zmniejszenia negatywnych skutków zjawiska krzyżowania się kompetencji, ponieważ umożliwi zmniejszenie tego chaosu i zwiększenie spójności m.in. przez wyznaczenie granic ujednolicenia siatki pojęciowej. Pozwoliłoby to także wyznaczyć granice tej gałęzi, a następnie w ich ramach przyjąć jej zasady, które pomagałyby w jednolitej wykładni, i ustalić kompetentne podmioty administrujące.
- d. Proces europeizacji prawa administracyjnego prowadzący do powstania złożonej struktury podmiotów administrujących bez wyraźnych hierarchicznych relacji między nimi. Kluczowe akty prawne w obszarze przetwarzania danych osobowych przyjęte zostały na poziomie prawa unijnego, podczas gdy stosowane są (w większości) na poziomie prawa krajowego przez organy administracji publicznej powołane przez krajowego prawodawcę. Prawodawca unijny, pomimo kształtowania prawa materialnego w tym obszarze, ograniczony jest w kształtowaniu prawa proceduralnego z powodu zasady autonomii proceduralnej państw członkowskich. Ogranicza to prawodawcę unijnego w możliwości wprowadzenia efektywnych instrumentów administracyjnego prawa procesowego, które mogłyby ten problem rozwiązać. Ponadto, może to prowadzić do rozbieżności

w wykładni tych unijnych aktów prawnych między państwami członkowskimi z różnymi kulturami prawnymi oraz z różnym stosunkiem do prywatności i ochrony danych osobowych.

- e. Rozbieżne cele wyznaczone poszczególnym organom administracji publicznej w obszarze przetwarzania danych osobowych. W badanym obszarze referencyjnym każdemu z ustanowionych podmiotów administrujących można przypisać określony cel, który albo wskazany został w przepisach ustanawiających dany podmiot, albo może być wywiedziony z celów danego aktu prawnego. Wszystkie te cele współistnieją i realizowane są w ramach jednego systemu administracji publicznej. Ostatecznie wszystkie te cele są komplementarne względem siebie, ponieważ służą jednemu dobru wspólnemu, jednak w odizolowaniu istnieje ryzyko, że realizacja jednego z nich może odbywać się kosztem drugiego w ujęciu prakseologicznym.

XIII. W perspektywie tak scharakteryzowanych przyczyn zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych i w odniesieniu do przedstawionego problemu badawczego sformułowano cztery postulaty *de lege ferenda*: 1) wyodrębnienie prawa danych jako odrębnej kompleksowej gałęzi prawa; 2) centralizacja struktury stosowania RODO wobec największych podmiotów nadzorowanych i ustanowienie organów ochrony danych jako organów właściwych dla stosowania aktów prawnych w obszarze przetwarzania danych osobowych; 3) wprowadzenie efektywnych instrumentów współpracy między podmiotami administrującymi stosującymi akty prawne w obszarze przetwarzania danych osobowych; 4) wprowadzenie rozwiązania typu klauzula „*safe harbour*” dla podmiotów nadzorowanych. Realizacja tych postulatów nie doprowadzi do całkowitego wyeliminowania problemu, ponieważ nie umożliwia eliminacji jego przyczyn o charakterze strukturalnym. Ich realizacja pozwoliłaby jednak zmniejszyć negatywne skutki spowodowane zjawiskiem krzyżowania się kompetencji i umożliwiłaby dalszy rozwój tego obszaru regulacji w sposób dojrzały i efektywniejszy.

STRUKTURA ROZPRAWY

Aby zweryfikować główną hipotezę badawczą i hipotezy pomocnicze, w rozprawie doktorskiej w pierwszym rozdziale dokonano przedstawienia podstawowych pojęć prawa

administracyjnego, które są istotne dla tego zjawiska. To są pojęcia organu administracji publicznej, prawnych form działania organów administracji publicznej, kompetencji organów administracji publicznej i pojęcia powiązane (właściwość, zakres działania, zadanie i cel).

Następnie, przeprowadzono analizę krzyżowania się zakresu przedmiotowego aktów prawnych w obszarze przetwarzania danych osobowych, z uwzględnieniem RODO, w tym jego szerokiego zakresu przedmiotowego i podmiotowego, oraz aktów prawnych prawa unijnego i krajowego regulujących przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu, cyberbezpieczeństwo, prawo konkurencji, Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych, sztuczną inteligencję i europejskie przestrzenie danych. Uzasadniono także wybór właśnie tych aktów prawnych jako obszaru referencyjnego dla prowadzonych badań.

W rozdziale trzecim przedmiotem badania uczyniono kompetencje organów stosujących akty prawne w obszarze przetwarzania danych osobowych, począwszy od analizy cech wspólnych tych organów, przez typologię ich kompetencji po to, aby dokonać charakterystyki wybranych organów i ich kompetencji na poziomie unijnym (Europejska Rada Ochrony Danych, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Komisja Europejska jako organ unijnego prawa konkurencji, Europejska Rada ds. Innowacji w zakresie Danych, Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji) i krajowym (Prezes Urzędu Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej, organy właściwe do spraw cyberbezpieczeństwa, Prezes Urzędu Ochrony Konkurencji i Konsumenta jako organ krajowego prawa konkurencji, organy właściwe w Akcie o Usługach Cyfrowych, organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych, organy właściwe w Akcie w sprawie Danych, organy właściwe w Akcie w sprawie Sztucznej Inteligencji).

Z kolei w rozdziale czwartym analizie poddano samo krzyżowanie się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych. Wprowadzono definicję obserwowanego zjawiska i zaproponowano jego typologię, następnie zbadano instrumenty prawne do rozwiązania problemu w wymiarze prawa materialnego, ustrojowego i procesowego. Dalej zaś omówiono skutki krzyżowania się kompetencji, kończąc na jego ujęciu prawnoporównawczym z perspektywy Królestwa Niderlandów i Wielkiej Brytanii ograniczonym do analizy rozwiązań przyjętych w tych jurysdykcjach w celu zredukowania negatywnych skutków badanego fenomenu.

Ostatni, piąty rozdział charakteryzuje przyczyny krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych

osobowych: rozłączenie regulacyjne spowodowane transformacją cyfrową; wybór prawodawcy, aby obszar przetwarzania danych osobowych uregulować za pomocą zasad konkretyzowanych na etapie stosowania prawa; pojmowania prawa ochrony danych osobowych jako kompleksowej gałęzi prawa, będącej „prawem wszystkiego”; balansowanie prawa do ochrony danych osobowych z innymi prawami podstawowymi lub celami ogólnymi i proces europeizacji prawa administracyjnego. W rozdziale tym sformułowano także postulaty *de lege ferenda*.

METODY BADAWCZE

W rozprawie doktorskiej zastosowano przede wszystkim metodę dogmatyczną⁴⁰ z wykorzystaniem metody historycznoprawnej⁴¹ w ograniczonym zakresie. Przy wykorzystaniu metody dogmatycznej dokonano analizy aktów prawa unijnego i krajowego w obranym obszarze referencyjnym, z uwzględnieniem polskiej i anglojęzycznej literatury przedmiotu i orzecznictwa polskich sądów administracyjnych, Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości Unii Europejskiej. Metoda dogmatyczna została użyta do badania decyzji, opinii i dokumentów urzędowych wydanych przez organy administracji publicznej stosujące akty prawne w obszarze przetwarzania danych osobowych. Metoda dogmatyczna była kluczowa dla analizy podstawowych pojęć dla przedmiotu rozprawy, zakresu przedmiotowego aktów prawnych w obszarze przetwarzania danych osobowych, kompetencji organów administracji publicznej stosujących te akty i krzyżowania się ich kompetencji, a także dla przedstawienia przyczyn oraz skutków tego zjawiska. Metodę dogmatyczną wykorzystano w ujęciu funkcjonalnym, czyli z perspektywy celów i skutków zjawisk prawnych (w tym wypadku zjawiska krzyżowania się kompetencji organów administracji publicznej); zatem nie tylko tego, co jest normatywnie postulowane, ale też tego, co faktycznie realizowane⁴². Do zbadania skutków i sformułowania postulatów *de lege ferenda* pomocniczo wykorzystano, oprócz nauki prawa administracyjnego, także dorobek nauki administracji⁴³. W odniesieniu do badania pojęć kompetencji i kompetencji cyfrowych

⁴⁰ W ramach metody dogmatycznej badaniu podlegają nie tylko same akty prawne, lecz także literatura, orzecznictwo i decyzje oraz inne dokumenty organów administracji publicznej. Należy odróżnić metodę dogmatyczną od wykładni prawa. Por. D. V. Kędzierski, *Metodologia i paradygmat polskich szczegółowych nauk prawnych*, „Transformacje prawa prywatnego” 2018, nr 3, s. 13-16.

⁴¹ P. Wszolek, O metodach badawczych stosowanych w nauce prawa administracyjnego dla poznania prawa jako wypowiedzi normatywnej, PPP 2011, nr 7-8, s. 9-43.

⁴² D. V. Kędzierski, *Metodologia i paradygmat polskich szczegółowych nauk prawnych*, „Transformacje prawa prywatnego” 2018, nr 3, s. 34-35.

⁴³ Z. Leoński, *Nauka administracji*, Warszawa 2010, s. 15, 19-20.

zastosowano technikę badawczą⁴⁴ polegającą na analizie ilościowej występowania terminu „kompetencje” i „kompetencje cyfrowe” w SIP LEX i EUR-LEX. Celem była weryfikacja pomocniczej hipotezy badawczej: czy pojęcie kompetencji uległo zmianie na skutek legislacji unijnej i krajowej stanowiącej odpowiedź na transformację cyfrową.

W ograniczonym zakresie użyto także metody prawnoporównawczej. Jej zastosowanie było niezbędne, aby udzielić odpowiedzi na pomocnicze pytania badawcze dotyczące tego, czy problem krzyżowania się kompetencji organów administracji publicznej występuje także w innych jurysdykcjach unijnych (do porównania obrano jurysdykcję Królestwa Niderlandów jako przykład dojrzałej jurysdykcji unijnej w kulturze prawnej prawa stanowionego) i Wielkiej Brytanii jako jurysdykcji systemu *common law*. Ma to wartość poznawczą z dwóch powodów. Po pierwsze, problem krzyżowania się kompetencji organów administracji publicznej wynika z aktów prawnych ustanowionych na poziomie prawa unijnego i wpisany jest w zjawisko europeizacji prawa administracyjnego. Zatem jego analiza z perspektywy innej jurysdykcji unijnej pozwoliła ustalić, że problem ten nie dotyczy tylko Polski, ale jest obecny w innych państwach członkowskich UE. Po drugie, analiza jurysdykcji Wielkiej Brytanii wykazała, że problem badawczy występuje nie tylko w UE, lecz także w jurysdykcjach nieunijnych (choćby bliskich jurysdykcjom unijnym), co świadczy o tym, że jego przyczyny są głębsze niż sama aktywność prawodawcy unijnego i krajowego, ale wynikają z trudności adekwatnego zredukowania negatywnych skutków zmian społeczno-technicznych. Wykorzystanie metody prawnoporównawczej stanowi wyzwanie zwłaszcza w odniesieniu do aktów prawnych w obszarze przetwarzania danych osobowych jako części prawa administracyjnego, ponieważ przeprowadzenie prawidłowej analizy wymaga poznania całego porządku prawnego danej jurysdykcji z uwzględnieniem specyfiki konstytucyjnej i ustrojowej oraz kultury prawnej⁴⁵.

⁴⁴ P. Wszolek, O metodach badawczych stosowanych w nauce prawa administracyjnego dla poznania prawa jako wypowiedzi normatywnej, PPP 2011, nr 7-8, s. 9-43.

⁴⁵ E. J. Eberle, *The Methodology of Comparative Law*, „Roger Williams University Law Review” 2011, Vol. 16, No. 1, http://docs.rwu.edu/rwu_LR/vol16/iss1/2, s. 52 (dostęp: 20.09.2024 r.). P. Ishwara Bhat, *Comparative Method of Legal Research: Nature, Process, and Potentiality* [in:] idem, *Idea and Methods of Legal Research*, New Delhi: Oxford University Press 2020, <https://doi.org/10.1093/oso/9780199493098.003.0009>, s. 270, 300 (dostęp: 28.12.2023 r.).

1. ROZDZIAŁ 1 – KOMPETENCJE ORGANÓW ADMINISTRACJI PUBLICZNEJ – PODSTAWOWE POJĘCIA

1.1. WSTĘP

Celem pierwszego rozdziału jest scharakteryzowanie podstawowych pojęć prawa administracyjnego w zakresie niezbędnym do weryfikacji głównej hipotezy badawczej. W literaturze pojęcie kompetencji organu administracji publicznej jest niejednoznaczne. Stąd też analizie poddane jest pojęcie organu administracji publicznej i podmiotów administrujących, prawnych form działania administracji publicznej, kompetencji organów administracji publicznej i pojęć zakresowo powiązanych – właściwości, zakresu działania, zadania i celu. Na potrzeby tej rozprawy przyjęto, że kompetencje organów administracji publicznej to całokształt uprawnień i obowiązków organu administracji publicznej. W ostatniej części zbadano wprowadzenie do użycia w języku prawnym terminu „kompetencje cyfrowe” jako przykład zwiększenia niejednoznaczności siatki pojęciowej prawa administracyjnego na skutek prawodawstwa unijnego i krajowego stanowiącego odpowiedź na transformację cyfrową. Badania tego dokonano przy pomocy analizy ilościowej występowania tego terminu w SIP LEX.

1.2. POJĘCIA ORGANU ADMINISTRACJI PUBLICZNEJ I PODMIOTÓW ADMINISTRUJĄCYCH

Dla rozważenia problemu kompetencji organów administracji publicznej w obszarze ochrony danych osobowych istotne jest uprzednie zdefiniowanie terminu „organu administracji publicznej”. Jest to węzłowe pojęcie dla ustrojowego prawa administracyjnego z perspektywy struktury systemu administracji publicznej i relacji pomiędzy podmiotami w tym systemie⁴⁶. W literaturze słusznie podnosi się, że na skutek zmian ustrojowych w administracji publicznej, w szczególności w wyniku procesów decentralizacyjnych (w tym powołania samorządu terytorialnego i zawodowego oraz europeizacji prawa administracyjnego) powstała odmienna od dotychczas znanej i zidentyfikowanej, rozbudowana struktura systemu administracji, która nie jest dostatecznie klarowna i efektywna⁴⁷.

⁴⁶ J. Jagielski, M. Wierzbowski, *Prawo administracyjne*, Warszawa 2020, s. 173.

⁴⁷ J. Zimmermann, *Prawo administracyjne*, Warszawa 2020, s. 179.

Te zmiany prowadzą do konkluzji, że przed wyjaśnieniem znaczenia tego terminu należy w pierwszej kolejności ustalić, czym są podmioty w ramach struktury systemu administracji publicznej, w szczególności czy wszystkie podmioty, którym w ramach tej struktury przyznano uprawnienia i obowiązki, można określić jako organy. W systemie administracji publicznej istnieją podmioty, które nie stanowią organów administracji publicznej *per se*, ale realizują zadania publiczne i wyposażone zostały we władztwo ze sfery *imperium*, a zatem mają przymioty właściwe dla organów administracji publicznej. Dlatego też w doktrynie prawa administracyjnego wyróżniono dwie kategorie: „podmioty administracji” i „podmioty administrujące”⁴⁸. Obie łączy fakt, że wszystkie te podmioty wykonują administrację. „Podmioty administracji” ujmowane są w doktrynie jako podmioty dedykowane, stworzone do wykonywania administracji⁴⁹. Z kolei pojęcie „podmioty administrujące” jest szersze, ma charakter funkcjonalny. Każdy podmiot władzy publicznej wykonujący funkcje administracji publicznej jest podmiotem administrującym, ale nie każdy podmiot administrujący może być zaliczony do podmiotów władzy publicznej (administracji). To pojęcie jest przydatne dla badania nowoczesnej administracji publicznej, ponieważ jego otwarta formuła pozwala na objęcie wszelkich form organizacyjnych wykonywania administracji publicznej w interesie publicznym, niezależnie od tego, czy chodzi o podmiot publiczny, czy niepubliczny (prywatny) posiadający osobowość prawną lub bez tej osobowości, wykonujący funkcje władcze lub działający w formach niewładczych (takich jak fundusze, agencje, czy organizacje społeczne realizujące zadania zlecone)⁵⁰.

Doktryna nie wypracowała jednoznacznej definicji „organu administracji publicznej”. Formułowanie definicji kluczowych terminów prawa administracyjnego napotyka problemy wynikające z wyjątkowej złożoności prawa administracyjnego, a w konsekwencji trudności ujęcia w sposób kompleksowy istoty kluczowych terminów. W odniesieniu do pojęcia „organu administracji publicznej” J. Boć wskazuje na trzy problemy konstruowania definicji: łączenie cech funkcjonalnych z organizacyjnymi, dodawanie do treści definicji elementów zbędnych i wykorzystywanie pojęć, których należałoby używać oddzielnie⁵¹. Identyfikacja cech

⁴⁸ M. Stahl, *Rozdział I. Zagadnienia wstępne*, § 1. *Określenia jednostek organizacyjnych wykonujących zadania administracji publicznej, ich zróżnicowanie i uwarunkowania*, [w:] *Prawne formy działania administracji*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2013, s. 27.

⁴⁹ J. Jagielski, M. Wierzbowski, *Prawo administracyjne*, Warszawa 2020, s. 173.

⁵⁰ M. Szyrski, § 1. *Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń*, II. *Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych*, 1. *Uwagi wstępne* [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, t. 9, red. G. Szpor, B. Szmulik, Warszawa 2015, Legalis.

⁵¹ J. Boć, *Prawo administracyjne*, Wrocław 2005, s. 135-140.

dystynktywnych organu administracji publicznej nie jest prosta. Nie można jednak stwierdzić, że przymioty organu administracji publicznej posiadają wyłącznie podmioty, które w ten sposób zostały nazwane przez prawodawcę.

Termin „organ administracji publicznej” zdefiniowany został w prawie administracyjnym procesowym. Zgodnie z art. 5 § 2 ust. 3 KPA, przez „organy administracji publicznej rozumie się: ministrów, centralne organy administracji rządowej, wojewodów, działające w ich lub we własnym imieniu inne terenowe organy administracji rządowej (zespolonej i niezespolonej), organy jednostek samorządu terytorialnego oraz organy i podmioty wymienione w art. 1 pkt 2 KPA”. W odniesieniu do tej definicji w literaturze argumentuje się, że jest ona szeroka, co podyktowane jest potrzebami prawa procesowego, a w konsekwencji należy uznać jej konwencjonalny charakter, dlatego że termin ten w odniesieniu do prawa ustrojowego winien być pojmowany wężziej, nie obejmując podmiotów realizujących funkcje zlecone administracji publicznej⁵².

Możliwe jest przyjęcie dwojakiego, szerokiego albo wąskiego, pojęcia „organu administracji publicznej”. Jako punkt wyjścia przy definiowaniu organu administracji należy rozważyć szersze kryterium nazywane funkcjonalnym. Z tej perspektywy organem jest każdy podmiot, któremu powszechnie obowiązujące prawo przyznaje kompetencje z zakresu prawa administracyjnego, przy czym bez znaczenia pozostaje, czy podmiot ten stanowi część struktury administracji państwowej, samorządowej czy też znajduje się poza strukturą administracji publicznej⁵³. Za istotę jego wyodrębnienia i podstawę jego działania uznawane są własne kompetencje przypisane ustawowo organowi. Konsekwencją funkcjonalnej perspektywy jest wniosek, że zadania realizowane będą nie tylko przez organy administracji publicznej nazwane w ten sposób za pomocą aktów prawnych, lecz także przez te podmioty (administrujące), które na podstawie ustawy realizują te zadania lub wykonują zadania zlecone przy pomocy kompetencji. W tym właśnie rozumieniu termin „organ administracji publicznej” używany jest w tej rozprawie.

Natomiast oprócz tego szerokiego pojęcia „organu administracji publicznej” możliwe jest także pojęcie w znaczeniu węższym, nazywanym ścisłym. Zgodnie z nim, organem administracji jest „prawnie wyodrębniona część aparatu administracji, działająca w imieniu państwa lub samorządu, w ramach przyznanych kompetencji i upoważniona do stosowania

⁵² Por. *Komentarz do art. 5 KPA* [w:] B. Adamiak, B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2022, Legalis.

⁵³ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 77.

określonych środków prawnych⁵⁴”. J. Zimmermann⁵⁵ wskazuje na cechy wyróżniające organu administracji publicznej, których wyróżnienie w istocie zbliżone jest do cytowanej wyżej wąskiej definicji E. Ury: (i) osobowy substrat organu w postaci osoby lub grupy osób, które sprawują określoną funkcję; (ii) wyodrębnienie organizacyjne w ramach struktury państwa lub samorządu terytorialnego; (iii) prawne umocowanie do działania o randze ustawowej w imieniu i na rachunek państwa; (iv) wyposażenie we władztwo umożliwiające realizację tego działania.

W konsekwencji złożoności prawa administracyjnego, w doktrynie powstały rozmaite typologie organów administracji publicznej w ramach struktury administracji, w szczególności według następujących kryteriów: hierarchicznej struktury administracji, sposobu kreowania organów, charakteru osobowego i roli decyzyjnej organów⁵⁶. Po pierwsze, można wyróżnić organy zdecentralizowane i scentralizowane, co jest odpowiednikiem podziału na administrację rządową i samorządową, przy czym organy samorządowe dzielone są ze względu na rodzaj samorządu – terytorialnego, zawodowego i gospodarczego. Organy w ramach administracji rządowej charakteryzują się zależnością (w różnym stopniu) od Rady Ministrów, Prezesa Rady Ministrów lub poszczególnych ministrów. Opisując ten podział, wskazuje się, że istnieją specyficzne podmioty, które funkcjonują z większym zakresem niezależności (jak na przykład Urząd Dozoru Technicznego) lub w formach o różnym statusie prawnym⁵⁷. Odrębnym podziałem jest podział według kryterium właściwości miejscowej na organy naczelne wymienione w Konstytucji RP i organy centralne, które nie są w niej wymienione, ale również obejmują właściwością miejscową obszar całego państwa⁵⁸, oraz organy terenowe o węższej przestrzennie (np. ograniczonej do województwa) właściwości miejscowej⁵⁹. J. Zimmermann wyróżnia także organy naczelne jako organy znajdujące się najwyżej w hierarchii danego pionu organizacyjnego, oraz organy niższego szczebla, których charakterystyką jest, że nie znajdują się najwyżej w hierarchii danego pionu⁶⁰. Osobno wyróżnić można także organy ze względu na sposób i charakter podejmowania decyzji, to znaczy na organy jednoosobowe, gdzie piastunem organu jest jeden człowiek i kolegialne, gdzie piastunem organu jest pewne kolegium, grupa

⁵⁴ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 77.

⁵⁵ J. Zimmermann, *Prawo administracyjne*, Warszawa 2020, s. 162-163.

⁵⁶ M. Stahl, *Rozdział I. Zagadnienia wstępne*, § 3. *Organy administracji publicznej, organy administrujące, rodzaje organów* [w:] *Prawne formy działania administracji*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2013, s. 70-77; por. także J. Zimmermann, *Prawo administracyjne*, Warszawa 2020, s. 174-178.

⁵⁷ J. Jagielski, M. Wierzbowski, *Prawo administracyjne*, Warszawa 2020, s. 177.

⁵⁸ Por. w odniesieniu do organów centralnych: M. G. Jarentowski, *Legislacyjne aspekty ustroju centralnych organów administracji rządowej*, PPP 2011, nr 5, s. 3-12.

⁵⁹ Por. J. Szmit, 1.5. Zakres podmiotowy administracji rządowej [w:] idem, *Konstytucyjny wzorzec reżimu zatrudnienia członków korpusu służby cywilnej*, Warszawa 2024, SIP LEX.

⁶⁰ J. Zimmermann, *Prawo administracyjne*, Warszawa 2020, s. 174-175.

osób. Zaletą organów jednoosobowych jest większa sprawność podejmowania decyzji z perspektywy operacyjnej, natomiast organów kolegialnych – możliwość uwzględnienia odmiennych perspektyw wynikających z odmiennych doświadczeń osób wchodzących w skład kolegium organu⁶¹.

Ponadto, dla tej rozprawy istotne jest, że w literaturze wyróżnia się grupę tak zwanych niezależnych organów regulacyjnych. Do tej kategorii należy zaliczyć m.in. Prezesa Urzędu Ochrony Konkurencji i Konsumenta, Przewodniczącego Komisji Nadzoru Finansowego, Prezesa Urzędu Regulacji Energetyki. Organy te ustanowione zostały przez prawodawcę krajowego w konsekwencji operacjonalizacji prawa unijnego i wyposażone zostały w rozbudowane kompetencje do regulacji określonego sektora gospodarki i cechuje je pewien poziom niezależności rozumianej jako zdolność decydowania w sposób niepodporządkowany wobec bieżącej polityki rządowej, przy prowadzeniu współpracy z organami unijnymi i odpowiednikami krajowymi w państwach członkowskich w ramach sieci administracyjnych⁶². Chociaż z perspektywy doktryny prawa administracyjnego wydzielenie niezależnych organów regulacyjnych jest dyskusyjne z uwagi na brak wyraźnego kryterium odróżniającego, to z perspektywy funkcjonalnej wyróżnienie takiej grupy jest zasadne i ma wartość poznawczą.

1.3. POJĘCIE PRAWNYCH FORM DZIAŁANIA ADMINISTRACJI PUBLICZNEJ

Aby rozważać pojęcie kompetencji organów administracji publicznej, należy najpierw przeanalizować, w jaki sposób organy administracji publicznej mogą realizować te kompetencje, a zatem czym są prawne formy ich działania. W literaturze przyjmowane jest pojęcie prawnych form działania administracji jako prawnie określonego typu konkretnej czynności organu administracji⁶³. Z definicji tej wyprowadzić można dystynkcję między działaniem administracji na zewnątrz, wobec podmiotów administrowanych i wewnątrz, w ramach systemu administracji. Stąd też część przedstawicieli doktryny wyróżnia

⁶¹ M. Stahl, *Rozdział I. Zagadnienia wstępne, § 3. Organy administracji publicznej, organy administrujące, rodzaje organów*, [w:] *Prawne formy działania administracji*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2013, s. 75.

⁶² S. Dudzik, I. Kawka [w:] *Europeizacja prawa administracyjnego*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2014, s. 523-524. Por. także A. Żurawik, 2.2.3.4. *Organy regulacyjne* [w:] *System Prawa Administracyjnego Procesowego*, t. 4: *Postępowania autonomiczne i szczególne. Postępowania niejurysdykcyjne*, red. A. Matan, Warszawa 2021, SIP LEX.

⁶³ J. Starościek [w:] *System prawa administracyjnego* t. 3, red. T. Rabska, J. Łętowski, Warszawa 1978, s. 40.

„administracyjny” i „kierowniczy” tryby stosowania prawa administracyjnego⁶⁴. Od form działania administracji należy odróżnić metody działania, które mogą być opisywane jako odmienne formy stylu działania organów, wynikające z praktyki administracyjnej wykształconej przez te organy⁶⁵.

W zależności od tego, jakie zadania ma realizować organ, wyposażony jest on w formy działania różne pod względem charakteru wykonywania i skutków prawnych. Nie wszystkie te formy działania mają charakter stosowania prawa w rozumieniu skonkretyzowanych aktów wobec zindywidualizowanego podmiotu. Część autorów uważa jednak, że zakresem terminu „prawne formy” nie są objęte działania faktyczne, którym nie można przypisać doniosłości prawnej, a nadto również milczenie i bezczynność organu⁶⁶. Zdarza się, że akty prawne, przyznając określonemu organowi zadania, nie precyzują form działania, w jakich te zadania mają być zrealizowane. Wówczas to na organie spoczywa obowiązek, aby zdecydować – przy zastosowaniu ogólnych zasad prawa administracyjnego – o wyborze odpowiedniej formy działania do realizacji określonego zadania⁶⁷.

Wobec wielości prawnych form działania administracji w literaturze stworzono ich typologie i wyróżniono kryteria, według których dokonywano klasyfikacji tych form. Różnice w poszczególnych typologiach wynikają z różnic w rozumieniu roli administracji publicznej. Te typologie wzajemnie się uzupełniają i mają wartość poznawczą, oddając złożoność i bogactwo prawnych form działania administracji publicznej. Za J. Zimmermannem wyróżnia się co najmniej sześć odrębnych kryteriów podziału prawnych form działania administracji: kryterium władztwa (działania władcze i niewładcze), kryterium skutku prawnego (działania prawne i faktyczne), kryterium stosunku do obowiązującego prawa (działania polegające na stanowieniu prawa i stosowaniu prawa), kryterium charakteru działania prawnego (administracyjnoprawny lub cywilnoprawny charakter działania administracji), kryterium sfery skutku prawnego (sfera zewnętrzna, poza administracją i sfera wewnętrzna) i kryterium adresata skutku prawnego (działania o charakterze indywidualnym, skierowane do określonego podmiotu i działania o charakterze generalnym)⁶⁸. Osobne propozycje wyodrębnienia prawnych form działania administracji prezentowane były w doktrynie, między innymi przez

⁶⁴ J. Wróblewski, *Sądowe i pozasądowe stosowanie prawa – problemy teorii i ideologii*, „Studium Prawno-Ekonomiczne” 1981, t. 26, s. 7-21.

⁶⁵ J. Zimmermann, *Prawo administracyjne*, Warszawa 2020, s. 345.

⁶⁶ K.M. Ziemiński, *Podstawy problematyki* [w:] *Prawe formy działania administracji*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2013, s. 4-5.

⁶⁷ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 145.

⁶⁸ J. Zimmermann, *Prawo administracyjne*, Warszawa 2020, s. 345-351.

J. Borkowskiego (czynności prawne, które kształtują stosunki prawne i działania podejmowane wskutek tworzenia faktów, nie przez kreowanie stosunków prawnych)⁶⁹ i A. Błasia (akty normatywne, formy działań faktycznych [o charakterze materialno-technicznym, informacyjne, zmierzające do nawiązywania współpracy, wykonywane w celu stosowania prawa], umowy [cywilnoprawne i publicznoprawne])⁷⁰.

W literaturze przyjmuje się, w ślad za J. Starościakiem, sześć podstawowych prawnych form działania administracji: 1) stanowienie aktów normatywnych; 2) wydawanie aktów administracyjnych; 3) zawieranie umów; 4) zawieranie porozumień administracyjnych; 5) działalność społeczno-organizatorska; 6) czynności materialno-techniczne⁷¹. Akt normatywny definiowany jest jako „władcze rozstrzygnięcie organu władzy publicznej (organu administracji rządowej lub samorządu terytorialnego), zawierające normy postępowania skierowane do ogólnie określonego adresata w abstrakcyjnie określonej sytuacji⁷²”. Cechą charakterystyczną aktów normatywnych jest to, że są to akty o charakterze generalnym, zatem skierowane do adresata poprzez określenie jego cech, i o charakterze abstrakcyjnym. Akty te z zasady nie podlegają jednorazowemu wykonaniu, lecz mają zastosowanie ogólne, kreując określoną sytuację prawną podmiotów administrowanych w postaci uprawnienia lub obowiązku.

Z kolei akty administracyjne są uznawane za powszechną prawną formę działania administracji. Akty administracyjne, podobnie jak akty normatywne, mają charakter władczy oparty na konkretnej podstawie prawnej prawa powszechnie obowiązującego, w tym znaczeniu, że wywołują skutki prawne (tworzą uprawnienia lub obowiązki) poprzez samo ich wydanie. Natomiast cechą odróżniającą akty administracyjne jest ich podwójna konkretność, co oznacza, że rozstrzygają konkretną sprawę konkretnego adresata⁷³, a zatem – w odróżnieniu od aktów normatywnych – zasadniczo podlegają jednorazowemu wykonaniu. Doktryna dokonuje różnych podziałów aktów administracyjnych. Nie zagłębiając się w dyskusję w tym przedmiocie, należy wskazać na dwa najczęściej wskazywane kryteria wyróżniające prawne formy działania administracji. Po pierwsze, kryterium adresata aktu, czyli akty zewnętrzne (np. decyzje administracyjne), skierowane do adresata, który nie jest prawnie zależny, i akty wewnętrzne, skierowane do adresatów podległych służbowo. Po drugie, kryterium treści, czyli akty konstytutywne, które kreują określone skutki prawne w postaci zmiany praw

⁶⁹ J. Borkowski, *Decyzja administracyjna*, Łódź-Zielona Góra 1999, s. 17-18.

⁷⁰ A. Błaś, *Prawne formy działania administracji publicznej* [w:] *Prawo administracyjne*, red. J. Boć, Wrocław 2008, s. 328.

⁷¹ J. Starościak [w:] *System prawa administracyjnego*, t. 3, red. T. Rabska, J. Łętowski, Warszawa 1978, s. 45.

⁷² J. Jagielski, M. Wierzbowski, *Prawo administracyjne*, Warszawa 2020, s. 346.

⁷³ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 153.

i obowiązków administracyjnoprawnych z chwilą ich wydania, oraz akty deklaratoryjne, które stwierdzają zaistnienie określonego stanu prawnego, powstałego z mocy prawa⁷⁴. Aktem administracyjnym o najszerszym zastosowaniu jest decyzja administracyjna. Charakteryzowana jest jako kwalifikowany akt administracyjny o charakterze zewnętrznym, który rozstrzyga sprawę co do istoty w całości lub w części albo w inny sposób kończy ją w danej instancji⁷⁵, albo też jako orzeczenie organu administracji publicznej o wiążących konsekwencjach obowiązującej normy prawa administracyjnego dla indywidualnie określonego podmiotu i w konkretnej sprawie⁷⁶. Oprócz wymiaru materialnoprawnego istotny jest wymiar proceduralny decyzji administracyjnej. Decyzja musi spełniać wymogi formalne określone w art. 107 KPA, zgodnie z którym decyzja administracyjna zawiera: 1) oznaczenie organu administracji publicznej; 2) datę wydania; 3) oznaczenie strony lub stron; 4) powołanie podstawy prawnej; 5) rozstrzygnięcie; 6) uzasadnienie faktyczne i prawne; 7) odpowiednie pouczenia; 8) podpis z podaniem imienia i nazwiska oraz stanowiska służbowego pracownika organu upoważnionego do wydania decyzji.

Zawieranie porozumień administracyjnych to jedna z niewładczych form działania administracji. Definiowane jest jako dwustronna lub wielostronna czynność z zakresu prawa administracyjnego dokonywana przez podmioty, z których co najmniej jeden wykonuje zadania z zakresu administracji publicznej. Taka czynność dochodzi do skutku na podstawie oświadczeń woli tych podmiotów⁷⁷. Przedmiotem porozumień administracyjnych są sprawy z zakresu prawa administracyjnego, nie zaś prawa cywilnego, a w tym sensie porozumienia te służą realizacji określonych zadań publicznych na podstawie aktów prawnych prawa administracyjnego, które dopuszczają zawarcie danego porozumienia⁷⁸.

Chociaż zasadniczo administracja publiczna działa w tzw. sferze *imperium*, to jednak, aby realizować niektóre zadania publiczne, zwłaszcza dotyczące potrzeb gospodarczych społeczeństwa (np. gospodarowania odpadami), korzysta z prawnych form działania z obszaru prawa cywilnego, na przykład zawiera umowy cywilnoprawne. Są to działania w sferze *dominium*, realizowane na zasadzie równości stron zgodnie z zasadami prawa prywatnego⁷⁹. Źródłem tych działań z perspektywy administracji jest jednak istnienie podstaw prawnych w prawie administracyjnym, które umożliwiają podjęcie tych działań i ich realizację

⁷⁴ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 154-156.

⁷⁵ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 163.

⁷⁶ W. Dawidowicz, *Polskie prawo administracyjne*, Warszawa 1980, s. 47.

⁷⁷ J. Jagielski, M. Wierzbowski, *Prawo administracyjne*, Warszawa 2020, s. 365.

⁷⁸ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 175-178.

⁷⁹ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 179-180.

w odniesieniu do określonych zadań. Te działania realizowane są w szczególności w trybie ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych⁸⁰. Działalność społeczno-organizatorska i czynności materialno-techniczne stanowią postać czynności faktycznych realizowanych przez administrację. Czynności faktyczne, podobnie jak czynności prawne, mają swoje źródło w przepisach prawa i stosują się do nich zasady ogólne prawa administracyjnego⁸¹.

Cechą charakterystyczną działalności społeczno-organizatorskiej jest, że akty prawne w odniesieniu do tych form nie przewidują możliwości zastosowania przez organy przymusu administracyjnego celem ich realizacji. Nie oznacza to jednak, że są to działania nieefektywne. Przeciwnie, mogą one przynieść nawet bardziej pożądane skutki niż działania z wykorzystaniem przymusu administracyjnego. Niektóre zadania administracji publicznej, zwłaszcza w obszarach wymagających inicjatywy po stronie społeczeństwa, mogą być realizowane przez organy administracji publicznej wyłącznie przez niewładcze formy działania, ponieważ prawodawca nie wyposażył tych organów w inne formy działania w celu realizacji tych zadań⁸². Drugim typem działań faktycznych, wyodrębnionym w doktrynie, są czynności materialno-techniczne organów administracji. Definiowane są one jako „działania organów administracji, które będąc czynnościami faktycznymi, oparte są na wyraźnej podstawie prawnej i wywołują konkretne skutki prawne”⁸³. Istotne jest, że czynności te wywołują określone skutki prawne, które swoje źródło mają w przepisach prawa. Cechą odróżniającą czynności materialno-techniczne od czynności społeczno-organizatorskich jest, że mają one charakter działań władczych. Natomiast charakter ten powstaje nie przez kreowanie norm, lecz przez podejmowane działania, które, jak zostało wskazane, może rodzić określone skutki prawne.

W literaturze formułowany jest pogląd, że pojęcie prawnych form działania administracji w polskiej nauce prawa administracyjnego ukształtowane zostało w zasadniczym stopniu jeszcze w uwarunkowaniach poprzedniego ustroju politycznego. Tymczasem, w konsekwencji transformacji ustrojowej, a następnie członkowska Polski w UE, które wywołały dynamiczną zmianę prawa administracyjnego, ustanowione zostały liczne, nieznane dotąd formy działania administracji. Charakterystyczne jest wprowadzenie ich prawnych form w postaci możliwości wydawania *soft law* (prawa miękkiego) przez organy administracji publicznej, takich jak plany,

⁸⁰ Dz. U. z 2019 r. poz. 1843 ze zm.

⁸¹ K. Kłosowska, *Czynności faktyczne jako prawna forma działania administracji*, Rzeszów 2009.

⁸² E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 187-188.

⁸³ J. Jagielski, M. Wierzbowski, *Prawo administracyjne*, Warszawa 2020, s. 376.

strategie operacyjne czy programy⁸⁴. Zmiany legislacyjne, wywołane przede wszystkim europeizacją prawa administracyjnego, wpływają na ewolucję pojęcia nowych form prawnych działania administracji. Wymaga to przynajmniej rozważenia zaproponowania ich nowej typologii. W niniejszej rozprawie w obszarze referencyjnym zbadane zostały właśnie takie nowe, dotychczas nieznane prawne formy działania administracji, ustanowione obok „klasycznych”, np. wydawania decyzji administracyjnych.

1.4. POJĘCIE KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ

Pojęcie „kompetencji organów administracji publicznej” jest podstawowe dla nauki prawa administracyjnego. Stanowi punkt odniesienia dla zidentyfikowania i opisanego pozycji podmiotów administrujących względem siebie i względem podmiotów administrowanych. W doktrynie rozważania w przedmiocie tego pojęcia prowadzone są od kilkudziesięciu lat. Wciąż brak jest zgody, czym jest to pojęcie i jaka jest jego relacja do innych, zbliżonych pojęć nauki prawa administracyjnego, jak „właściwość” czy „zakres działania”. Również prawodawca unijny i krajowy posługuje się nim w sposób wieloznaczny i niekonsekwentny.

Termin „kompetencje” nie ma definicji legalnej⁸⁵. Jego rozumienie stanowi od kilkudziesięciu lat przedmiot ożywionej debaty⁸⁶. W doktrynie wskazuje się na trzy sposoby traktowania tego terminu. Pierwszy polega na unikaniu jednoznacznych wypowiedzi na jego temat. Drugi zasadza się na próbie stworzenia rozbudowanej jego definicji. Trzeci, typowy dla autorów wykorzystujących ten termin dla dalszych rozważań, opiera się na stworzeniu definicji szczegółowej na potrzeby prowadzonej analizy⁸⁷. Dodatkowo, w teorii prawa termin „kompetencje” rozumiany jest inaczej niż w nauce prawa administracyjnego⁸⁸. W naukach teoretycznoprawnych wyrażany jest pogląd (będący przedmiotem dyskusji), że kompetencję

⁸⁴ J. Zimmermann, *Prawo administracyjne*, Warszawa 2020, s. 352.

⁸⁵ J. Bułakowski, *O kompetencjach organów administracji morskiej z perspektywy teorii prawa administracyjnego*, „Kortowski Przegląd Prawniczy”, 3/2018, s. 47.

⁸⁶ Rozdział I Istota koordynacji, § 4. Kompetencja koordynacyjna, I. Pojęcie kompetencji i budowa normy kompetencyjnej [w:] R. Stankiewicz, *Koordynacja w prawie administracyjnym*, Warszawa 2019, Legalis.

⁸⁷ M. Szyrski, § 1. Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń, II. Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych, 3. Kompetencja, [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, t. 9, red. G. Szpor, B. Szmulik, Warszawa 2015, Legalis.

⁸⁸ Ł. Prus, B. Kowalczyk, *Część pierwsza Aktualności, Redefiniowanie pojęć prawa administracyjnego w warunkach umiędzynarodowienia relacji administracyjnych, Wstęp*, pkt. IV [w:] red. W. Jakimowicz, *Aktualność pojęć prawa administracyjnego*, Warszawa 2021, SIP LEX.

należy rozumieć jako czynność konwencjonalną o prawnej doniosłości, przy czym odróżnić należy normę kompetencyjną, która wyznacza sposób dokonania danej czynności⁸⁹.

M. Matczak wskazuje na dwa podstawowe konteksty, w jakich termin „kompetencje” używany jest w prawie administracyjnym. Jako pierwszy wskazuje kontekst relacji poziomej, w którym organ odnosi swoją pozycję i sytuację wobec innych organów na tym samym poziomie hierarchicznym. Jest to poziom relacji, na którym prowadzona jest dyskusja na temat sporów kompetencyjnych i sporów o właściwość. W tym kontekście terminy „kompetencja” i „właściwość” bywają używane zamiennie. Z kolei drugi kontekst to kontekst relacji pionowej, w której realizuje się władztwo administracyjne względem podmiotów administrowanych. W kontekście relacji pionowej termin „kompetencja” używany jest naprzemiennie z terminem „uprawnienie”. To rozróżnienie obu kontekstów znajduje również odzwierciedlenie w orzecznictwie sądowym⁹⁰.

Z kolei J. Zimmermann zwraca uwagę na trzy rozumienia kompetencji: kompetencję jako zdolność lub możliwość działania, kompetencję jako upoważnienie i kompetencję jako uprawnienie⁹¹. W pierwszym znaczeniu termin ten oznacza atrybut organu umożliwiający podejmowanie przez niego działań, który sformułowany został w normie prawnej. Drugie rozumienie odnosi się do możliwości działania w zakresie konkretnej sprawy w konkretnej sytuacji („upoważnienia do działania”). Natomiast trzecie odnosi się do podziału na uprawnienia i obowiązki; przez kompetencje należy rozumieć uprawnienia organu skorelowane z obowiązkami podmiotu, który podlega jego władztwu⁹².

Za J. Niczyporukiem należy wskazać, że przez termin „kompetencje” rozumie się „oparte na przepisach prawa administracyjnego upoważnienie i obowiązki działania organu administracji publicznej”⁹³, przy czym pomiędzy tymi elementami istnieje współzależność w tym rozumieniu, że uprawnienia przyznane są organom, aby realizowały one wyznaczone im zadania⁹⁴. Podobną w istocie rzeczy definicję proponuje M. Ćwiertnia⁹⁵. Ta propozycja

⁸⁹ J. Niczyporuk, *Kompetencja administracyjna*, „Annales UMCS” 1999, vol. XLVI, s. 136.

⁹⁰ M. Matczak, *Rozdział VI. Kompetencja*, § 33. *Pojęcie kompetencji w nauce prawa administracyjnego*, I. Dwa konteksty ujęcia kompetencji [w:] *Instytucje prawa administracyjnego*, red. R. Hauser, A. Wróbel, Z. Niewiadomski Warszawa 2015, Legalis.

⁹¹ M. Szyrski, § 1. *Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń*, II. *Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych*, 3. *Kompetencja*, [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*. t. 9, red. G. Szpor, B. Szmulik Warszawa 2015, Legalis.

⁹² J. Zimmermann, *Aksjomaty prawa administracyjnego*, Warszawa 2013, s. 163-168.

⁹³ J. Niczyporuk, *Regulacja kompetencji administracji leśnej*, BSP 2015, nr 18, s. 55-56.

⁹⁴ J. Niczyporuk, *Regulacja kompetencji administracji leśnej*, BSP 2015, nr 18, s. 55-56.

⁹⁵ M. Ćwiertnia, *Charakter prawny kompetencji administracyjnych organów egzekucyjnych*, PPP 2018, nr 5, s. 94.

odpowiada także definicjom kompetencji w literaturze wybranych państw członkowskich UE, np. zgodnie ze stanowiskiem rumuńskiego badacza D. Vieriu, kompetencja organu administracji stanowi zespół praw i obowiązków organu, dla których realizacji organ posiada uprawnienie do wydawania aktów administracyjnych (*„the competence represents the ensemble of rights and obligations of a public administration authority or of a public servant for the realization of which it also has the ability to adopt or issue judicial administrative acts”*)⁹⁶.

W literaturze wyróżniane są także pojęcia kompetencji ogólnej i szczególnej⁹⁷. Przez kompetencję ogólną pojmuje się zakreszenie generalnego wskazania spraw, obszaru, którym zajmuje się organ. Z kolei przez kompetencję szczególną należy rozumieć konkretne wskazanie spraw, które przyznane zostały do załatwienia przez dany organ. Granica pomiędzy tymi dwoma rodzajami kompetencji nie jest poprowadzona precyzyjnie⁹⁸.

Dla J. Borkowskiego kompetencja to „zdolność organu do powodowania prawnie wiążących następstw”⁹⁹. Z kolei, zgodnie ze stanowiskiem J. Bocia, o kompetencji można mówić jako konstrukcji łączącej prawo z formą prawną działania administracji – w ujęciu dynamicznym i statycznym. Ujęcie dynamiczne oznacza analizę kompetencji z perspektywy sformułowania określonej normy, przesłanek jej zastosowania i tego konsekwencji. W tym ujęciu kompetencja może być definiowana jako zdolność organu do „skonkretyzowanego aktualizowania, w drodze odpowiedniego postępowania, potencjalnego obowiązku działania sformułowanego przez prawo”¹⁰⁰. Natomiast wykorzystanie ujęcia statycznego pozwala wydzielić grupy kompetencji z porządku prawnego i przypisać je organowi, co pozwala odnieść wszystkie kompetencje do „ogólnego celu i całości zadań stawianych administracji w prawie”¹⁰¹.

⁹⁶ D. Vieriu, *Legal Requests of the Authority Administrative Act*, „Journal of Law and Administrative Sciences” 2015, s. 813.

⁹⁷ M. Szyrski, § 1. *Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń*, II. *Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych*, 3. *Kompetencja* [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*. t. 9, red. G. Szpor, B. Szmulik Warszawa 2015, Legalis.

⁹⁸ M. Matczak, *Rozdział VI. Kompetencja, § 33. Pojęcie kompetencji w nauce prawa administracyjnego, IV. Wybrane aspekty podziału kompetencji między organami administracji* [w:] *Instytucje prawa administracyjnego*, red. R. Hauser, A. Wróbel, Z. Niewiadomski Warszawa 2015, Legalis.

⁹⁹ E. Olejniczak-Szałowska [w:] *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, red. M. Stahl Warszawa 2013, s. 185.

¹⁰⁰ J. Boć (red.), *Prawo administracyjne*, Wrocław 2005, s. 145.

¹⁰¹ J. Boć (red.), *Prawo administracyjne*, Wrocław 2007, s. 144-145.

Jeszcze odmienną definicję kompetencji zaproponował W. Góralczyk. Wskazał, że kompetencja to „przyznana prawem zdolność do ciągłego lub powtarzalnego podejmowania przez organ państwa czynności prawnych oraz takich czynności faktycznych, które bezpośrednio wiążą się z czynnościami prawnymi”¹⁰². Definicja ta jest pojemna, mieści w sobie szeroki zakres działalności organów, przy czym skupiona jest wokół pojęcia czynności prawnych i pojęcia czynności faktycznych, których zdolność podejmowania przyznana została organom na podstawie prawa.

W kontekście sporów kompetencyjnych zgłaszany jest postulat kompetencyjności, na który składają się trzy warunki: wyłączność kompetencyjna, pojemność kompetencyjna i przejrzystość kompetencyjna¹⁰³. Postulat wyłączności kompetencyjnej oznacza, że do wykonywania zadania lub rozstrzygania określonej sprawy winien być powołany wyłącznie określony organ. W. Góralczyk opisał sytuację, w której ten sam obszar może być objęty działaniem różnych organów. Natomiast organy te powinny realizować wyłącznie przyznane im zadania, co zwiększa sprawność procesu administrowania¹⁰⁴. W świetle tego postulatu należy odczytać także postulat przejrzystości kompetencyjnej, zgodnie z którym uprawnienia i zadania organów powinny być określone możliwie jednoznacznie, z wyraźnym rozróżnieniem granic tych uprawnień i zadań względem pozostałych organów w systemie administracji¹⁰⁵. J. Dobkowski wskazuje, że w celu rozgraniczenia obszarów kompetencji organów w prawie administracyjnym wprowadzane są mechanizmy reguł kolizyjnych, które najczęściej przybierają formułę domniemania zadań na rzecz organu o właściwości ogólnej (czyli tak zwana kompetencja zbiorcza)¹⁰⁶. Z kolei pojemność kompetencyjna to odpowiedni stosunek zakresu zadań do zakresu uprawnień w kontekście umiejscowienia organu w strukturze administracji, tak w wymiarze ilościowym, jak i w wymiarze „dopasowania rodzajów kompetencji do cech charakterystycznych organu”¹⁰⁷. Te trzy pojęcia mają charakter postulatywny, co oznacza, że stanowią wezwanie do kształtowania przepisów zgodnie z nimi¹⁰⁸. W tym kontekście słusznie wskazuje A. Jakubowski, że należy negatywnie ocenić sytuację, w której prawodawca wyznacza organowi zadania, lecz nie przyznaje mu uprawnień

¹⁰² W. Góralczyk, *Zasada kompetencyjności w prawie administracyjnym*, Warszawa 1986, s. 32.

¹⁰³ Por. W. Góralczyk, *Zasada kompetencyjności w prawie administracyjnym*, Warszawa 1986.

¹⁰⁴ W. Góralczyk, *Zasada kompetencyjności w prawie administracyjnym*, Warszawa 1986, s. 19.

¹⁰⁵ W. Góralczyk, *Zasada kompetencyjności w prawie administracyjnym*, Warszawa 1986, s. 21.

¹⁰⁶ J. Dobkowski, *Kompetencja administracyjna (niektóre uwagi na kanwie pracy A. Matczaka „Kompetencja organu administracji publicznej”*, Kraków 2004) [w:] *Studia z zakresu nauk prawnoustrojowych*, t. 1, *Mimesclinea*, pod red. J. Sługockiego, Bydgoszcz 2008, s. 113.

¹⁰⁷ E. Ura, *Prawo administracyjne*, Warszawa 2006, s. 81.

¹⁰⁸ W. Góralczyk, *Zasada kompetencyjności w prawie administracyjnym*, Warszawa 1986, s. 21.

i obowiązków (kompetencji) niezbędnych do realizacji tych zadań w kontekście zasady optymalnej pojemności kompetencyjnej organu¹⁰⁹. W literaturze podkreśla się, że określona kompetencja wymaga uprzedniej normy kompetencyjnej, wobec tego, że działania administracji publicznej oparte są na zasadzie legalizmu. Norma taka opisywana jest jako nośnik dla samej kompetencji. Nie ma w niej zawartego obowiązku wobec podmiotu nadzorowanego – norma ta przyznaje natomiast określonemu organowi kompetencję do działania¹¹⁰. Z. Cieślak argumentuje, że kompetencja wyznacza granicę ingerencji podmiotów administrujących w stosunki społeczne tak w wymiarze podmiotowym, jak i przedmiotowym¹¹¹. Dokonany wyżej przegląd stanowisk doktryny w odniesieniu do pojęcia kompetencji prowadzi do wniosku, że jest ono niejednoznaczne. Na potrzeby niniejszej rozprawy zasadnym jest przyjęcie rozumienia „kompetencji organów administracji publicznej” jako całokształtu uprawnień i obowiązków tych organów¹¹².

1.5. POJĘCIA POWIĄZANE Z POJĘCIEM KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ

Jak zostało wskazane powyżej, w literaturze termin „kompetencje” rozumiany jest niejednoznacznie – raz jako uprawnienia, innym razem jako zadania, jeszcze w innym miejscu – jako zakres działalności, albo też jako właściwość organu. Te rozbieżności występują nie tylko w doktrynie, ale również w aktach prawnych¹¹³. Wymagają one syntetycznego zbadania.

1.5.1. WŁAŚCIWOŚĆ

Pojęcie kompetencji utożsamiane bywa z pojęciem właściwości. M. Matczak wskazuje, że drugie z nich odnosi się do zakresu spraw przyznanych określonemu organowi do załatwienia. Właściwość w tym ujęciu to warunki, od których uzależnione jest wykonywanie

¹⁰⁹ A. Jakubowski, *Zasada ciągłości administracji publicznej a właściwość rzeczowa organów (studium przypadku)*, PiP 2015, nr 12, s. 63.

¹¹⁰ M. Matczak, *Rozdział VI. Kompetencja, § 33. Pojęcie kompetencji w nauce prawa administracyjnego, III. Kompetencja a pojęcia pokrewne na gruncie nauki prawa administracyjnego* [w:] *Instytucje prawa administracyjnego*, red. R. Hauser, A. Wróbel, Z. Niewiadomski Warszawa 2015, Legalis.

¹¹¹ Z. Cieślak [w:] Z. Cieślak, I. Lipowicz, Z. Niewiadomski, *Prawo administracyjne. Część ogólna*, Warszawa 2002, s. 97.

¹¹² E. Olejniczak-Szałowska [w:] *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, red. M. Stahl, Warszawa 2013, s. 184.

¹¹³ D. Mazurkiewicz, *Pojęcie kompetencji w prawie administracyjnym*, PiP 1988, nr 3, s. 72.

kompetencji¹¹⁴. Właściwość to „określenie prawnej zdolności organu administracji do podejmowania czynności, zwłaszcza w ramach postępowania administracyjnego”¹¹⁵. Pojęcie właściwości wykorzystywane jest przede wszystkim w kontekście prawa administracyjnego procesowego. Wyróżnia się właściwość rzeczową, miejscową i funkcjonalną. Właściwość rzeczowa w literaturze definiowana jest jako jednocześnie upoważnienie i obowiązek nałożony na organ do rozstrzygnięcia określonej kategorii spraw administracyjnych¹¹⁶. Z kolei właściwość miejscowa to zdolność organu do rozstrzygnięcia spraw w zakresie jego właściwości rzeczowej na przypisanym jemu obszarze¹¹⁷. Wreszcie właściwość funkcjonalna, inaczej zwana także instancyjną, używana jest do zidentyfikowania rodzajów spraw, które załatwiane są przez organy wyższego rzędu¹¹⁸. Właściwość funkcjonalna bywa określana jako element właściwości rzeczowej¹¹⁹. Podkreślenia wymaga, że organy administracji prawnej mają obowiązek badania właściwości z urzędu, to znaczy zobowiązane są, aby weryfikować, czy posiadają możliwość i obowiązek do podejmowania określonych czynności¹²⁰. Należy zgodzić się z poglądem M. Szyrskiego, że pomiędzy pojęciami kompetencji i właściwości należy wprowadzić rozróżnienie¹²¹.

1.5.2. ZAKRES DZIAŁANIA

Osobno w kontekście kompetencji organów administracji publicznej wyróżniany jest zakres działania organu administracji. Twierdzi się, że pojęcie zakresu działania organu różni się od pojęcia kompetencji (pomimo że bywają używane zamiennie), ponieważ ten pierwszy stanowi wytyczną określającą sferę, w jakiej organ obowiązany jest działać, lecz nie tworzy

¹¹⁴ M. Matczak, *Rozdział VI. Kompetencja, § 33. Pojęcie kompetencji w nauce prawa administracyjnego, III. Kompetencja a pojęcia pokrewne na gruncie nauki prawa administracyjnego* [w:] *Instytucje prawa administracyjnego*, red. R. Hauser, A. Wróbel, Z. Niewiadomski Warszawa 2015, Legalis.

¹¹⁵ P. Przybysz, *3.4. Kompetencja* [w:] idem, *Instytucje prawa administracyjnego*, Warszawa 2020, SIP LEX.

¹¹⁶ A. Wróbel, *Komentarz do art. 20* [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, Warszawa 2021, SIP LEX.

¹¹⁷ K. Klonowski, *Komentarz do art. 21* [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. H. Knysiak-Sudyka, Warszawa 2019, SIP LEX.

¹¹⁸ C. Martysz, *Komentarz do art. 19*, [w:] G. Łaszczyca, A. Matan, C. Martysz, *Kodeks postępowania administracyjnego. Komentarz*, t. 1, *Komentarz do art. 1-103*, Warszawa 2010, SIP LEX.

¹¹⁹ P. Sołtysiak, *Komentarz do art. 19* [w:] *Kodeks postępowania administracyjnego. Komentarz do art. 1-60*, t. 1, red. M. Karpiuk, P. Krzykowski, A. Skóra Olsztyn 2020, SIP LEX.

¹²⁰ M. Bursztynowicz, M. Sługocka, *Komentarz do art. art. 19* [w:] M. Bursztynowicz, M. Sługocka, *Postępowanie administracyjne dla jednostek samorządu terytorialnego. Komentarz*, Warszawa 2020, SIP LEX.

¹²¹ M. Szyrski, *§ 1. Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń, II. Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych, 3. Inne pochodne tego pojęcia* [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, t. 9, red. G. Szpor, B. Szmulik, Warszawa 2015, Legalis.

natomiast uprawnienia do podjęcia działania jak w przypadku kompetencji¹²². Zasadnie wskazuje się, że organowi, ze względu na zasadę legalizmu, na podstawie norm powinny zostać przyznane określone uprawnienia i obowiązki oraz prawne formy działania, aby realizować określone zadania, natomiast samo dokonanie przydziału określonego zakresu działania nie jest wystarczające, aby kompetencje w tym zakresie były wykonywane¹²³.

1.5.3. ZADANIE

W literaturze wskazuje się, że kompetencja w relacji poziomej (względem innych organów) oznacza zadania przyznane poszczególnym organom do wykonania¹²⁴. M. Matczak wskazuje, że w kontekście relacji pionowej nie występuje utożsamianie kompetencji z zadaniami, natomiast ma to miejsce właśnie w relacji poziomej¹²⁵. Doktryna wyróżnia trzy cechy, które odróżniają kompetencje od zadań. Po pierwsze, kompetencje to uprawnienia, jak i obowiązki, a zadania mogą mieć wyłącznie charakter obowiązku. Po drugie, kompetencje, w odróżnieniu od zadań, mogą stanowić podstawę do nawiązania stosunku administracyjnoprawnego. Po trzecie, formułowany jest zasadny pogląd, że relacja kompetencji do zadań winna być rozumiana w ten sposób, że organy administracji publicznej wyposażone zostały w kompetencje (rozumiane jako całokształt uprawnień i obowiązków) w celu wykonywania zadań¹²⁶, zatem kompetencje powinny być adekwatnie dobrane do zadań¹²⁷. Zadania należy definiować za A. Monarchą-Matlak jako ustanowiony w prawie obowiązek osiągnięcia określonego celu w interesie publicznym przez określony podmiot¹²⁸. W konsekwencji, termin „zadanie” nie powinien być używany zamiennie z terminem „kompetencje”,¹²⁹ a jego znaczenie należy odróżnić również od znaczenia „obowiązku”¹³⁰.

¹²² M. Szyrski, § 1. *Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń*, II. *Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych*, 3. *Kompetencja* [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, t. 9, red. G. Szpor, B. Szmulik, Warszawa 2015, Legalis.

¹²³ B. Mik, *Glosa do uchwały SN z dnia 14 listopada 2007 r., BSA-4110-5/07*, Prok.i Pr. 2008, nr 6, s. 170.

¹²⁴ M. Matczak, *Kompetencje organu administracji publicznej*, Kraków 2004, s. 58.

¹²⁵ M. Matczak, *Kompetencje organu administracji publicznej*, Kraków 2004, s. 60.

¹²⁶ H. Wolska, *Realizacja zadań publicznych przez spółkę komunalną w systemie zamówień publicznych*, Warszawa 2018, s. 4.

¹²⁷ J. Zimmermann, *Zadanie* [w:] idem, *Alfabet prawa administracyjnego*, Warszawa 2022, SIP LEX.

¹²⁸ A. Monarcha-Matlak, 8. *Obowiązki prawne administracji a zadania publiczne* [w:] *Obowiązki administracji w komunikacji elektronicznej*, Warszawa 2008, SIP LEX.

¹²⁹ W. Jakimowicz, *Normatywne uwarunkowania realizowania kompetencji prawodawczych*, RPEiS 2015, nr 3, s. 169.

¹³⁰ W przedmiocie relacji pojęcia zadania i pojęcia obowiązku w prawie administracyjnym zob.: A. Monarcha-Matlak, 8. *Obowiązki prawne administracji a zadania publiczne* [w:] *Obowiązki administracji w komunikacji elektronicznej*, Warszawa 2008, SIP LEX.

Pomimo tego, prawodawca unijny i krajowy często niekonsekwentnie posługuje się terminem „zadania” na określenie obowiązków organu administracji publicznej (tak jest na przykład w odniesieniu do obowiązków organów ochrony danych, które w art. 57 RODO nazwane zostały „zadaniami”). Należy wskazać przy tym, że zasadnym jest nie tylko klarowne odróżnienie kompetencji od zadań organów administracji publicznej, ale także – z uwagi na wzrastającą rolę podmiotów prywatnych w wykonywaniu administracji publicznej – jednoznaczne ustalenie reguł współpracy między tymi podmiotami a organami¹³¹.

1.5.4. CEL

Pojęcie celu należy odróżnić od pojęcia zadania, chociaż oba te pojęcia pozostają powiązane¹³². Cel zdefiniowany jest w *Słowniku języka polskiego PWN* jako „miejsce, do którego się zmierza”¹³³. W tym rozumieniu cel podmiotu administrującego to taki efekt jego działań, którego osiągnięcie zostało mu wyznaczone i do którego powinien on dążyć, co zwykle związane jest z realizacją określonej wartości¹³⁴. Wyznaczenie celu nadaje zatem kierunek działalności podmiotu administrującego, co wpływa na sposób wykonywania przez niego kompetencji oraz organizację pracy urzędu obsługującego podmiot administrujący, co stanowi przedmiot badania nauki o administracji. Takie rozumienie celu znajduje potwierdzenie w stanowisku literatury, zgodnie z którym przez zadania należy rozumieć ciąg działań, realizowanych w konkretnym momencie w kierunku realizacji celów. Natomiast cele wyznaczają długoterminowy pożądany efekt tego ciągu działań¹³⁵, a postać normatywna norm celowościowych zawiera zwykle bezpośrednie odwołanie do pożądanego dobra lub wartości¹³⁶.

¹³¹ G. Szpor, *Wymogi związane z Dyrektywą INSPIRE. Zakres regulacji zagospodarowania przestrzennego*, „Kontrola Państwowa” 2016, nr 2 specjalny, s. 74.

¹³² Por. G. Szpor, 3. *Cele i zadania w polskim systemie prawa* [w:] *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza*, red. A. Matan, Warszawa 2022, SIP LEX.

¹³³ Cel, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/sjp/cel;2447324.html> (dostęp 01.09.2024 r.).

¹³⁴ Por. G. Szpor, 3. *Cele i zadania w polskim systemie prawa* [w:] *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza*, red. A. Matan, Warszawa 2022, SIP LEX.

¹³⁵ M. Szyrski, § 1. *Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń*, II. *Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych*, 2. *Zadanie i cel* [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, t. 9, red. G. Szpor, B. Szmulik, Warszawa 2015, Legalis.

¹³⁶ M. Maciejewski, *Normy celowościowe i normy zadaniowe w prawie administracyjnym. Dobra chronione jako ustawowe cele organów administracji* [w:] *Dobra chronione w prawie administracyjnym*, red. Z. Duniewska, Łódź 2014, s. 55.

1.6. TERMIN „KOMPETENCJE CYFROWE” JAKO PRZYKŁAD WPŁYWU TRANSFORMACJI CYFROWEJ NA SIATKĘ POJĘCIOWĄ PRAWA ADMINISTRACYJNEGO

Na skutek odpowiedzi prawodawcy unijnego i krajowego na transformację cyfrową wprowadzono do języka prawnego i prawniczego termin „kompetencje cyfrowe”, którego znaczenie należy odróżnić od znaczenia terminu „kompetencje organów administracji publicznej”¹³⁷. Analiza terminu „kompetencje” w języku ogólnym na podstawie definicji w *Słowniku języka polskiego PWN* i słowniku języka angielskiego *Cambridge Dictionary* pozwala wyróżnić co najmniej dwa znaczenia. Pierwszym jest „zakres uprawnień urzędu lub urzędnika do zajmowania się określonymi sprawami i podejmowania dotyczących ich decyzji”¹³⁸. Analogiczną definicję sformułowano w *Cambridge Dictionary*: „the power of a person, business, court, or government to deal with something or take legal decisions”¹³⁹, w tłumaczeniu: „władztwo osoby, przedsiębiorstwa, sądu albo rządu do poradzenia sobie z zagadnieniem lub do powzięcia prawnych decyzji”. Dotychczas w języku prawnym i prawniczym terminu „kompetencje” używano przede wszystkim w tym właśnie znaczeniu w odniesieniu do organów administracji publicznej. Niejednoznaczność pojęcia kompetencji organów administracji publicznej scharakteryzowano powyżej.

Zgodnie natomiast z drugim znaczeniem, za *Słownikiem języka polskiego PWN*, kompetencja to także „zakres czyjejś wiedzy, umiejętności i doświadczenia”. Natomiast, zgodnie z definicją w języku angielskim¹⁴⁰, kompetencja to „an important skill that is needed to do a job”, czyli: „istotna umiejętność potrzebna do wykonania konkretnej pracy”. To drugie znaczenie terminu „kompetencji”, tj. w konotacji z określoną wiedzą i umiejętnościami jednostki, używane jest we frazie „kompetencje cyfrowe”. Analiza terminu „kompetencji” w tym znaczeniu jest przedmiotem intensywnego badania przez inne dziedziny nauki, np. nauki

¹³⁷ Por. także analizę i wnioski w: G. Szpor, P. Hajduk, *Digital Competences and Digital Skills in the Legal Regulation of the Digital Transformation of the European Union*, „Review of European and Comparative Law” 2024, Vol. 56, No. 1, <https://doi.org/10.31743/recl.17139> (dostęp: 20.09.2024 r.).

¹³⁸ *Kompetencja*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/sjp/kompetencja;2564077> (dostęp 1.09.2024 r.).

¹³⁹ *Competence*, [hasło w:] *Cambridge Dictionary* [online], <https://dictionary.cambridge.org/dictionary/english/competence> (dostęp 1.09.2024 r.).

¹⁴⁰ Użycie słowa „kompetencje” (*competence*) w liczbie mnogiej w języku angielskim jest kontrowersyjne (por. <https://www.britannica.com/dictionary/eb/qa/what-is-the-plural-form-of-competence>), ale występuje ono w liczbie mnogiej w oficjalnych dokumentach urzędowych, np. Komisji Europejskiej (por. R. Vuorikari, S. Kluzer, Y. Punie, *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes*, Luksemburg: Urząd Publikacji Unii Europejskiej 2022, <https://publications.jrc.ec.europa.eu/repository/handle/JRC128415> (dostęp: 20.09.2024 r.).

ekonomiczne¹⁴¹. Zestawienie polskiej i angielskiej definicji terminu „kompetencja” w języku powszechnym w drugim znaczeniu pokazuje, że w języku polskim do kompetencji zalicza się zarówno wiedzę, jak i umiejętności (oraz doświadczenie), podczas gdy w języku angielskim tylko umiejętności¹⁴². Ta niejednoznaczność rozumienia tego terminu ujawnia się także w języku prawnym, co wynika z przeprowadzonej analizy strukturalnej występowania tego terminu w obowiązujących aktach prawnych w SIP LEX (odczytu dokonano na dzień 26 stycznia 2024 r.). Wskazana niejednoznaczność terminu „kompetencje cyfrowe” prowadzi do pytania o jego definicję. Posługiwanie się możliwie jednoznacznymi terminami jest pomocne zarówno w prowadzeniu badań naukowych, jak i stanowieniu, stosowaniu oraz wykładni prawa, ponieważ ujednolicenie ich zmniejsza ryzyko sporów o charakterze pozornym, które wynikają z odmiennego rozumienia tych samych terminów¹⁴³.

Zanim jednak zostanie podjęta próba sformułowania definicji, należy rozważyć, czy użycie tego terminu jest uzasadnione, czy też bardziej odpowiednie byłyby inne terminy. Dyskusja w tej kwestii jest już prowadzona w literaturze¹⁴⁴. Zasadne wątpliwości budzi przede wszystkim relacja znaczenia terminu „kompetencje cyfrowe” do innych terminów pokrewnych, w szczególności do terminu „umiejętności cyfrowe”, który albo jest używany obok „kompetencji cyfrowych” w wyrażeniu „umiejętności i kompetencje cyfrowe”¹⁴⁵, albo stanowi rodzaj kompetencji¹⁴⁶, albo też używany jest jako ich synonim¹⁴⁷.

¹⁴¹ A. Piwowarczyk, *Kompetencje komunikacji międzykulturowej: Rozwój kompetencji przyszłych ekonomistów i menedżerów*, Warszawa 2020, s. 11-27, w tym przegląd wybranych definicji kompetencji w tabeli na s. 11-12.

¹⁴² Por. także G. Szpor [w:], *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, red. J. Gołaczyński, Warszawa 2022, s. 82.

¹⁴³ Por. P. Lisowski, Część pierwsza: O aktualności. Między asercją a wątpliwością – kilka refleksji o aktualności pojęć w prawie administracyjnym w kontekście ich normatywizacji. 10. Zakończenie [w:] *Aktualność pojęć prawa administracyjnego*, red. W. Jakimowicz, Warszawa 2021, SIP LEX.

¹⁴⁴ G. Szpor [w:] *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, red. J. Gołaczyński, Warszawa 2022, s. 82.

¹⁴⁵ Np. art. 2 lit. f) Załącznika III *Synergia z Programami Unijnymi* i art. 2 lit. c) Załącznika III *Synergia z Programami Unijnymi* rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1781 z dnia 13.09.2023 w sprawie ustanowienia ram dotyczących środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników oraz zmiany rozporządzenia (UE) 2021/694 (akt w sprawie czipów) Dz. Urz. UE L z 2023 r. nr 229, s. 1.

¹⁴⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1288/2013 z dnia 11 grudnia 2013 r. ustanawiające „Erasmus+”: unijny program na rzecz kształcenia, szkolenia, młodzieży i sportu oraz uchylające decyzje nr 1719/2006/WE, 1720/2006/WE i 1298/2008/WE (Dz. Urz. UE L z 2013 r. nr 347, s. 50 z późn. zm.). Tutaj w odniesieniu do kompetencji kluczowych.

¹⁴⁷ Np. motyw 16 do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/241 z 12.02.2021, Dz. Urz. UE L z 2021 r. nr 57, s. 17 z późn. zm.

Terminu „kompetencje cyfrowe” użyto w 106¹⁴⁸ obowiązujących aktach prawnych, przy czym struktura jego występowania jest następująca: Dziennik Ustaw i Monitor Polski – 24 wyniki, Dzienniki UE – 16 wyników, Dzienniki resortowe – 16 wyników oraz Dzienniki wojewódzkie – 50 wyników. Przykładowo, terminu „kompetencje cyfrowe” użyto w tytule ustawy z dnia 7 lipca 2023 r. o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli¹⁴⁹, której przedmiotem jest określenie zasad i trybu przyznawania wsparcia uczniom i nauczycielom w związku z rozwojem kompetencji cyfrowych (art. 1). Na poziomie unijnym termin „kompetencje cyfrowe” zastosowano, na przykład, w motywie 26 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)¹⁵⁰ w odniesieniu do edukacyjnych zadań ENISA: „ENISA powinna również przyczyniać się do zaspokajania potrzeb w zakresie szkoleń i materiałów szkoleniowych, w tym potrzeb organów publicznych, oraz, w stosownych przypadkach, zaspokajać w znacznym stopniu potrzeby szkoleniowe instruktorów, w oparciu o ramy kompetencji cyfrowych dla obywateli, mając na celu pomaganie państwom członkowskim oraz instytucjom, organom i jednostkom organizacyjnym Unii w rozwoju ich własnych zdolności szkoleniowych”.

Dla porównania, termin „umiejętności cyfrowe” pojawia się w 79 obowiązujących aktach prawnych, z następującą strukturą występowania: Dziennik Ustaw i Monitorze Polskim – 7 wyników, Dzienniki UE – 64 wyniki, Dzienniki resortowe – 4 wyniki oraz Wojewódzkie Dzienniki Urzędowe – 4 wyniki. Oznacza to, że chociaż termin „kompetencje cyfrowe” jest ogólnie bardziej upowszechniony niż termin „umiejętności cyfrowe”, to krajowy polski prawodawca preferuje użycie terminu „kompetencje cyfrowe” (42 przypadki) niż terminu „umiejętności cyfrowe” (7 przypadków) w Dzienniku Ustaw i Monitorze Polskim. Przykładowo, termin „umiejętności cyfrowe” został zastosowany dwa razy w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2021/695 z dnia 28 kwietnia 2021 r. ustanawiającym program ramowy w zakresie badań naukowych i innowacji Horyzont Europa oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie oraz uchylającym

¹⁴⁸ W odniesieniu do wyszukiwarki w SIP LEX podkreślić należy, że wynik 106 rekordów odnosi się do liczby aktów prawnych (dokumentów), w których wyszukiwany termin został użyty, a nie do liczby użyc tego terminu w tych aktach (dokumentach). Ustalono to po dokonaniu dodatkowego badania sposobu działania wyszukiwarki.

¹⁴⁹ Dz. U. poz. 1369.

¹⁵⁰ Dz. Urz. UE L z 2019 r. nr 151, s. 15.

rozporządzenia (UE) nr 1290/2013 i (UE) nr 1291/2013¹⁵¹ w odniesieniu do zapewnienia synergii programu „Synergia” z programem „Cyfrowa Europa” (pkt 7 Załącznika IV „Synergia z Innymi Programami Unijnymi”) m.in. przez: „podejmowane w Programie inicjatywy na rzecz programów nauczania ukierunkowanych na rozwój umiejętności i kompetencji (*skills and competencies*), w tym inicjatywy realizowane w odpowiednich WWiI utworzonych przez EIT, były uzupełniane budowaniem zdolności w zakresie zaawansowanych umiejętności cyfrowych (*digital skills*) wspieranym w ramach programu „Cyfrowa Europa”. Jak wynika z tego cytatu, w rozporządzeniu tym użyto terminu „kompetencje” w jednej frazie z terminem „umiejętności”, ale nie użyto terminu „kompetencje cyfrowe”. Oznacza to, że dla prawodawcy termin „kompetencje” ma inny zakres znaczeniowy niż termin „umiejętności”, a „umiejętności” nie stanowią w konsekwencji elementu „kompetencji”. W innym akcie, rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2021/241 z 12.02.2021 r.¹⁵² ustanowiono Instrument na rzecz Odbudowy i Zwiększania Odporności (art. 1 rozporządzenia). Termin „umiejętności cyfrowe” został użyty w tym akcie 7 razy, m.in. w motywie 16. w odniesieniu do „reform i inwestycji w następne pokolenie, dzieci i młodzież [które] mają zasadnicze znaczenie dla promowania edukacji i umiejętności, w tym umiejętności cyfrowych (*digital skills*), podnoszenia umiejętności, przekwalifikowywania się i zmiany kwalifikacji ludności aktywnej zawodowo, programów integracji osób bezrobotnych (...)” oraz w przypisie 5. do Załącznika VII *Metodyka znakowania cyfrowego w ramach Instrumentu* w odniesieniu do wyjaśnienia terminu „umiejętności cyfrowe” w tabeli: „Dotyczy umiejętności cyfrowych na wszystkich poziomach i obejmuje: wysoce specjalistyczne programy edukacyjne mające na celu szkolenie specjalistów w dziedzinie technologii cyfrowych (tj. programy ukierunkowane na technologię); szkolenie nauczycieli (...)”.

Dla stanowienia, stosowania i wykładni prawa oraz prowadzenia badań naukowych zasadne byłoby ujednolicenie znaczenia terminu „kompetencje cyfrowe”¹⁵³. Z przyczyn funkcjonalnych istotne jest, aby zakres znaczeniowy tego terminu był na tyle szeroki, aby obejmował wszystkie elementy niezbędne do pełnowartościowego funkcjonowania w społeczeństwie cyfrowym. Dla pełnowartościowego funkcjonowania potrzebne jest zarówno posiadanie odpowiedniej wiedzy informatycznej (np. o podstawach funkcjonowania komputerów) i umiejętności cyfrowych (np. umiejętność krytycznego poszukiwania treści

¹⁵¹ Dz. Urz. UE L z 2021 r. nr 170, s. 1

¹⁵² Dz. Urz. UE L z 2021 r. nr 57, s. 17 z późn. zm.

¹⁵³ Por. także G. Szpor, *Rozdział 25. Model podnoszenia kompetencji cyfrowych*, [w:] *Internet Hacking*, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski Warszawa 2023, SIP Legalis.

w zasobach Internetu), oraz wypracowanie właściwych postaw, które doprowadzą do ich połączenia¹⁵⁴ (np. aby zapewnić ochronę przed atakami phishingowymi).

Rozumienie kompetencji jako całokształtu wiedzy, umiejętności i postaw jest obecne w prawodawstwie unijnym, np. w art. 2 pkt. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1288/2013 z dnia 11 grudnia 2013 r. ustanawiające „Erasmus+”: unijny program na rzecz kształcenia, szkolenia, młodzieży i sportu¹⁵⁵: „kompetencje kluczowe oznaczają podstawowy zbiór wiedzy, umiejętności i postaw, których każda osoba potrzebuje do spełnienia i rozwoju osobistego, aktywności obywatelskiej, włączenia społecznego i zatrudnienia (...)”. Taką definicję zakresową kompetencji cyfrowych sformułowano w odniesieniu do krajowego rządowego Programu Rozwoju Kompetencji Cyfrowych. Zgodnie z nią, kompetencje cyfrowe to „harmonijna kompozycja wiedzy, umiejętności i postaw umożliwiających życie, uczenie się i pracę w społeczeństwie cyfrowym, tj. społeczeństwie wykorzystującym w życiu codziennym i pracy technologie cyfrowe”¹⁵⁶. W tym dokumencie wyróżniono trzy rodzaje kompetencji: informatyczne (m.in. obsługę komputera, bezpieczne korzystanie z Internetu, użycie metod wywodzących się z informatyki w programowaniu i tworzeniu informatycznych rozwiązań problemów), informacyjno-komunikacyjne (m.in. wyszukiwanie informacji, ich rozumienie oraz ich selekcionowanie i krytyczna ocena) oraz funkcjonalne (m.in. wykorzystanie powyższych kompetencji w różnych sferach życia w sposób bezpieczny)¹⁵⁷. Tak sformułowaną definicję należy ocenić jako kompleksową, ponieważ obejmuje te aspekty wiedzy, umiejętności i postaw pozwalających na skuteczne i bezpieczne funkcjonowanie w społeczeństwie cyfrowym, jednocześnie umieszczając kompetencje cyfrowe w szerszym horyzoncie innych kompetencji, które są wobec nich komplementarne. W konsekwencji, tę definicję kompetencji cyfrowych należy uznać za najbardziej adekwatną we wskazanej wyżej perspektywie funkcjonalnej¹⁵⁸.

¹⁵⁴ G. Szpor [w:] Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego, red. J. Gołaczyński, Warszawa 2022, s. 84.

¹⁵⁵ Akt utracił moc z dniem 1 stycznia 2021 r. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1288/2013 z dnia 11 grudnia 2013 r. ustanawiające „Erasmus+”: unijny program na rzecz kształcenia, szkolenia, młodzieży i sportu oraz uchylające decyzje nr 1719/2006/WE, 1720/2006/WE i 1298/2008/WE (Dz. Urz. UE L z 2013 r. nr 347, s. 50 z późn. zm.).

¹⁵⁶ Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych” (M. P. z 2023 r. poz. 318), Załącznik, s. 6.

¹⁵⁷ Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych” (M. P. z 2023 r. poz. 318), Załącznik, s. 6.

¹⁵⁸ Por. także G. Szpor [w:] Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego, red. J. Gołaczyński, Warszawa 2022, s. 82-83.

Jak wykazano wyżej, pojęcie kompetencji organów administracji publicznej jest niejednoznaczne. W ostatnich latach do języka prawnego wprowadzono termin „kompetencje cyfrowe”, co powoduje podwójną trudność. Po pierwsze, termin ten sam w sobie jest rozumiany niejednolicie, w szczególności jest używany jako wyrażenie równoznaczne do „umiejętności cyfrowych” albo też umiejętności są zaliczane jako jeden z elementów tych kompetencji. Aby zachować całościowe ujęcie problemu, termin „kompetencje cyfrowe” powinien być rozumiany jako obejmujący zarówno wiedzę, jak i umiejętności oraz postawy w sposób sformułowany w krajowym Programie Rozwoju Kompetencji Cyfrowych przywołanym wyżej¹⁵⁹. W tym też znaczeniu użycie tego terminu jest bardziej adekwatne niż użycie terminu „umiejętności cyfrowe”, który ze swojego zakresu wyklucza element wiedzy, co w konsekwencji mogłoby prowadzić do zmniejszenia zainteresowania rozwojem i finansowaniem tego elementu¹⁶⁰, kluczowego dla postępu technicznego.

Po drugie, wprowadzenie terminu „kompetencje cyfrowe” do języka prawnego wpłynęło na pogłębienie niespójności siatki terminologicznej prawa administracyjnego przez zwiększenie niejednoznaczności samego terminu „kompetencje”. Termin ten był dotychczas używany w odniesieniu do organów administracji publicznej, jednak wobec tych zmian terminu tego używa się także na określenie wiedzy, umiejętności i postaw cyfrowych. Zatem zamiast zwiększenia uporządkowania użycia tego terminu i jego znaczenia w języku prawnym, doszło do zjawiska przeciwnego – pogłębienia nieporządku. W tym kontekście dyskusyjne jest, czy zasadne było wprowadzenie terminu „kompetencje cyfrowe” do języka prawnego, czy też bardziej odpowiednim było konsekwentne używanie terminu „kompetencje” wyłącznie w odniesieniu do całokształtu uprawnień i obowiązków organu administracji publicznej. Dyskusyjne byłoby jednak wówczas jaki termin jest odpowiedni na określenie wiedzy, umiejętności i postaw cyfrowych. Chociaż to drugie rozwiązanie (czyli używanie terminu „kompetencje” wyłącznie w odniesieniu do organu) byłoby bardziej adekwatne z perspektywy nauki prawa administracyjnego, to na obecnym etapie trudno zidentyfikować lepszy termin na określenie wiedzy, umiejętności i postaw niezbędnych do funkcjonowania w społeczeństwie cyfrowym niż „kompetencje cyfrowe”. Zastosowanie tego terminu zostało już bowiem szeroko przyjęte w prawie krajowym i unijnym, a nadto odpowiada ono jednemu ze znaczeń w języku

¹⁵⁹ Por. analizę i wnioski w artykule: G. Szpor, P. Hajduk, *Digital Competences and Digital Skills in the Legal Regulation of the Digital Transformation of the European Union*, „Review of European and Comparative Law” 2024, Vol. 56, No. 1, s. 207–223, <https://doi.org/10.31743/recl.17139> (dostęp: 20.09.2024 r.).

¹⁶⁰ Por. G. Szpor, P. Hajduk, *Digital Competences and Digital Skills in the Legal Regulation of the Digital Transformation of the European Union*, „Review of European and Comparative Law” 2024, Vol. 56, No. 1, s. 221–222, <https://doi.org/10.31743/recl.17139> (dostęp: 20.09.2024 r.).

powszechnym. Postulowanie odwrócenia tego procesu jest na tym etapie nierealistyczne, zatem zasadne pozostaje postulowanie ujednolicenia znaczenia terminu „kompetencje cyfrowe” w zaproponowany wyżej sposób, przy jednoczesnym zachowaniu w świadomości, że termin „kompetencje” jest wieloznaczny nie tylko w wielopoziomowej regulacji cyfrowej, ale także w nauce prawa administracyjnego.

1.7. PODSUMOWANIE

Analiza dokonana w pierwszym rozdziale prowadzi do ustalenia, że pojęcie kompetencji organów administracji publicznej jest niejednoznaczne. Na ustalenie znaczenia terminu „kompetencje” w języku prawnym wpływa wprowadzenie użycia terminu „kompetencje cyfrowe” na określenie całokształtu wiedzy, umiejętności i postaw. Należy zgodzić się z poglądem I. Lipowicz, że do zaburzenia siatki pojęciowej w prawie administracyjnym dochodzi nie tylko z powodu aktywności prawodawcy, ale także ze względu na niespójne tłumaczenie prawa europejskiego, brak ujednolicenia pojęć w naukach prawnych i powiązanych obszarach¹⁶¹. Na potrzeby tej rozprawy kompetencje organów administracji publicznej rozumiane będą jako całokształt uprawnień i obowiązków organu administracji publicznej. Organy wyposażone zostały w kompetencje, aby wykonywać przyznane im zadania w wyznaczonych przez prawo celach. Organy nie wykonują tych kompetencji w odosobnieniu, lecz stanowią element całości – struktury administracji publicznej podlegającej przemianom związanym z europeizacją prawa administracyjnego. Stąd też w niniejszej rozprawie ich kompetencje w obszarze przetwarzania danych osobowych zostaną zestawione po uprzednim zidentyfikowaniu obszaru referencyjnego i analizy krzyżowania się zakresu przedmiotowego RODO i innych aktów prawnych w obszarze przetwarzania danych osobowych.

¹⁶¹ I. Lipowicz, *Dylematy zmiany siatki pojęciowej w nauce prawa administracyjnego* [w:] *Koncepcja systemu prawa administracyjnego*, red. J. Zimmermann, Warszawa 2007, s. 41.

2. ROZDZIAŁ 2 – KRZYŻOWANIE SIĘ ZAKRESU PRZEDMIOTOWEGO WYBRANYCH AKTÓW PRAWNYCH W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

2.1. WSTĘP

Przedmiotem drugiego rozdziału jest analiza krzyżowania się zakresu przedmiotowego wybranych unijnych i krajowych aktów prawnych w obszarze przetwarzania danych osobowych. Aby umieścić tę analizę w kontekście przetwarzania danych osobowych, konieczna jest najpierw analiza zakresu przedmiotowego i podmiotowego RODO jako podstawowego aktu prawnego regulującego ten obszar oraz uzasadnienie wyboru określonych aktów prawnych jako obszaru referencyjnego dla prowadzonych badań.

Jedną z przyczyn zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych jest rozłączenie regulacyjne spowodowane transformacją cyfrową i wybór prawodawcy, aby obszar ten uregulować z wykorzystaniem zasad konkretyzowanych dopiero na etapie stosowania prawa¹⁶². Stąd też, scharakteryzowanie krzyżowania się zakresu przedmiotowego tych aktów prawnych jest niezbędne przed przystąpieniem do badania kompetencji organów administracji publicznej ustanowionych przez te akty.

Zakres przedmiotowy i podmiotowy RODO jest szeroki oraz nieostry, ponieważ prawodawca chciał zapewnić możliwie pełną realizację prawa podstawowego do ochrony danych osobowych i prawa podstawowego do prywatności. Z analizy orzecznictwa TSUE wynika, że TSUE dokonywał stopniowego poszerzenia obu tych zakresów przez wykładnię rozszerzającą podstawowych pojęć wyznaczających te zakresy: „dane osobowe”, „przetwarzanie danych osobowych”, „administrator danych osobowych” i „współadministrator danych osobowych”. W tym rozdziale postawiona została hipoteza, że zakres przedmiotowy RODO krzyżuje się z zakresem przedmiotowym unijnych i krajowych aktów prawnych w obszarze przetwarzania danych osobowych, które wybrane zostały jako obszar referencyjny dla badań, to jest:

- a. aktów prawnych regulujących przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu;
- b. aktów prawnych regulujących cyberbezpieczeństwo;

¹⁶² Szerzej por. rozdział 5 tej rozprawy.

- c. prawa konkurencji, Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych;
- d. aktów prawnych regulujących sztuczną inteligencję;
- e. aktów prawnych regulujących europejskie przestrzenie danych.

Liczba unijnych i krajowych aktów prawnych, które kompleksowo, sektorowo lub incydentalnie normują przetwarzanie danych osobowych przekracza co najmniej sto pozycji. Stąd też, dla weryfikacji hipotezy badawczej, konieczne jest dokonanie selekcji tych aktów. Wybór został dokonany przy uwzględnieniu następujących czynników:

- 1) kompletności tych aktów rozumianej w ten sposób, że regulują one określoną dziedzinę spraw w sposób całościowy, ustanawiając własne organy administracji publicznej do ich stosowania;
- 2) cele tych aktów prawnych, będąc komplementarnymi z RODO, nie są z nimi w pełni zbieżne, np. w celu przeciwdziałania praniu brudnych pieniędzy i finansowaniu terroryzmu zasadne byłoby przetwarzanie możliwie szerokiego zakresu danych osobowych;
- 3) nowości tych aktów przy uwzględnieniu, że analiza nowych aktów ma wyższą wartość poznawczą.

Przy wyborze nie uwzględniono aktów prawnych regulujących przetwarzanie danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, ponieważ w Polsce organem administracji publicznej ustanowionym na podstawie tych aktów jest PUODO, a zatem ten sam organ, który został ustanowiony na podstawie RODO. Dokonanie takiej analizy byłoby zatem mniej istotne dla weryfikacji głównej hipotezy badawczej. Obszar referencyjny nie obejmuje również m.in. aktów prawnych regulujących przetwarzanie danych osobowych w sektorze łączności elektronicznej. Jest tak dlatego, że kluczowy dla tego sektora projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej) przewiduje wprost, że niezależnymi organami nadzorczymi będą organy ochrony danych osobowych. Wprowadzenie tego rozwiązania rozwiąże problem krzyżowania się kompetencji organów administracji publicznej w odniesieniu do tego sektora. Stąd też włączenie tych aktów prawnych do obszaru referencyjnego nie jest zasadne. Dodatkowo, z uwagi na zintensyfikowaną aktywność prawodawcy unijnego i krajowego oraz publikację wielu nowych wytycznych, opinii i decyzji organów krajowych i unijnych oraz wyroków w ostatnich latach w tym obszarze dokonano jedynie selektywnej analizy. W szczególności analizą nie objęto

projektów aktów prawnych prawa krajowego, które nie zostały opublikowane w Dzienniku Ustaw lub innym właściwym publikatorze do dnia 30 czerwca 2024 r.

Aby zrealizować cel postawiony w tym rozdziale, przedstawiono najpierw RODO jako podstawowy akt prawny w obszarze przetwarzania danych osobowych, a następnie przeanalizowano zakres przedmiotowy i podmiotowy RODO z uwzględnieniem pojęć „przetwarzanie danych osobowych”, „administrator danych osobowych” i „współadministrator danych osobowych”. W dalszej kolejności, uzasadniony został wybór określonych unijnych i krajowych aktów prawnych regulujących przetwarzanie danych osobowych jako obszar referencyjny dla prowadzonych badań. W ostatnim zaś podrozdziale dokonano analizy krzyżowania się zakresu przedmiotowego RODO z aktami prawnymi prawa unijnego i krajowego regulującymi przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu, cyberbezpieczeństwo, prawo konkurencji, Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych, sztuczną inteligencję oraz europejskie przestrzenie danych.

2.2. OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH JAKO PODSTAWOWY AKT PRAWNY W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

2.2.1. OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH.

RODO, które weszło w życie 25 maja 2018 r., jest podstawowym (głównym) aktem prawnym w obszarze przetwarzania danych osobowych. Wynika to zarówno z użycia w nazwie aktu terminu „ogólne” („ogólne rozporządzenie”), jak i z brzmienia art. 1 ust. 1 określającego jego przedmiot w sposób szeroki: „ustanowienie przepisów o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych”. Oznacza, że zarówno swobodny przepływ danych osobowych (por. art. 1 ust. 3 RODO), jak i ochrona osób fizycznych w związku z przetwarzaniem tych danych stanowią osobne, ale współistniejące cele regulacji, które powinny zostać pogodzone w taki sposób, aby „przetwarzanie danych osobowych [zorganizowane było tak], aby służyło ludzkości” (motyw 4 RODO). Należy podkreślić, że przedmiotem RODO nie jest – wbrew powielanemu w dyskusjach skrótowi – ochrona danych osobowych, lecz ochrona osób fizycznych w związku z przetwarzaniem danych osobowych. Ta subtelna, ale istotna różnica stanowi wskazówkę, że wykładnia RODO powinna być dokonywana z perspektywy ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, a nie z perspektywy ochrony danych jako takich. Takie ujęcie nakierowuje również na kontekst prawno-człowieczy RODO, ponieważ ochrona osób fizycznych w związku z przetwarzaniem danych osobowych

jest prawem podstawowym zgodnie z – przywołanym już w pierwszym motywie RODO – art. 8 ust. 1 KPP, które jednak nie jest prawem bezwzględny (motyw 4 RODO)¹⁶³, podobnie jak prawo do prywatności (art. 7 KPP). W europejskim systemie praw człowieka ochrona praw podstawowych w Karcie Praw Podstawowych wzmacnia się wzajemnie z ochroną praw człowieka w EKPC (por. art. 53 KPP)¹⁶⁴, a praktyka orzecznictwa TSUE i ETPC pokazuje, że sądy te orzekają w sposób (zasadniczo) zapewniający spójność między oboma aktami, co jest charakterystyczne również w odniesieniu do prawa do prywatności¹⁶⁵ (art. 8 ust. 1 i 2 EKPC; prawo do ochrony danych osobowych nie zostało, w odróżnieniu od KPP, wyodrębnione w EKPC jako samodzielne prawo¹⁶⁶).

To, że aksjologicznych podstaw RODO należy szukać w tradycji praw człowieka (por. art. 1 ust. 2 RODO) widoczne jest w ambitnych celach, jakie przed nim postawiono (zgodnie z motywem 2 RODO: „przyczynienie się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi”), które wykraczają poza gospodarczy charakter wspólnotowej integracji gospodarek (choć i to jest jednym z celów). Sformułowanie przez prawodawcę unijnego tych celów wykraczających poza integrację gospodarczą możliwe było z powodu przemian ustrojowych UE na skutek wejścia w życie w 2009 r. Traktatu z Lizbony¹⁶⁷. Na jego podstawie wprowadzono art. 16 TFUE w obecnym brzmieniu¹⁶⁸, a KPP uzyskała moc prawną prawa pierwotnego UE. Dla porównania, podstawę prawną dla Dyrektywy ODO stanowił art. 95 (dawny artykuł 101a) Traktatu Ustanawiającego Europejską Wspólnotę Gospodarczą, którego celem było tylko „ustanowienie i funkcjonowanie rynku wewnętrznego”. Tytułem uzupełnienia

¹⁶³ Por. także J. P. M. Bonnici, *Exploring the non-absolute nature of the right to data protection*, „International Review of Law, Computers & Technology” 2014, No. 28, <https://doi.org/10.1080/13600869.2013.801590> (dostęp: 20.09.2024 r.), s. 131-143.

¹⁶⁴ Por. także J. Kokott, Ch. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, Int. Data Priv. Law, Vol. 3, Iss. 4, <https://doi.org/10.1093/idpl/ipt017> (dostęp: 20.09.2024 r.), s. 222-223.

¹⁶⁵ Por. A. Rosas, *The Court of Justice of the European Union: A Human Rights Institution?* „Journal of Human Rights Practice” 2022, Vol. 14, Iss. 1, <https://doi.org/10.1093/jhuman/huac020> (dostęp: 20.09.2024 r.), s. 208–211; J. Podkowik, R. Rybski, M. Zubik, *Judicial dialogue on data retention laws: A breakthrough for European constitutional courts?* „International Journal of Constitutional Law” 2021, Vol. 19, Iss. 5, <https://doi.org/10.1093/icon/moab132> (dostęp: 20.09.2024 r.), s. 1599, w którym autorzy analizują orzecznictwo ETPC, TSUE i sądów konstytucyjnych w sprawach dotyczących retencji danych.

¹⁶⁶ Por. M. A. Nowicki [w:] *Komentarz do Konwencji o ochronie praw człowieka i podstawowych wolności* [w:] *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, Warszawa 2021, art. 8, SIP LEX.

¹⁶⁷ Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r. (Dz. U. z 2009 r. nr 203, poz. 1569).

¹⁶⁸ Por. J. Sobczak [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, T. 1 (art. 1-89), red. D. Miąsik, N. Półtorak, A. Wróbel, Warszawa 2012, art. 16, SIP LEX.

perspektywy prawno-człowieczej wymaga wskazania, że system europejskiej ochrony danych osobowych jest złożony. Oprócz prawa unijnego, państwa członkowskie (także Polska) są sygnatariuszami aktu prawa międzynarodowego regulującego przetwarzanie danych osobowych – Konwencji 108 Rady Europy (sporządzonej w 1981 r.), a proces ratyfikacji zmodyfikowanej wersji Konwencji 108 jest w toku¹⁶⁹. Chociaż ani Konwencja 108, ani jej zmodernizowana wersja nie są przedmiotem analizy w tej rozprawie, to akty te pozostają komplementarne względem RODO i wzmacniają system europejskiej (i wykraczającej poza kontynent europejski) ochrony danych osobowych¹⁷⁰.

Charakterystyka RODO dokonana w tym podrozdziale nie jest w założeniu ani kompleksowa, ani wyczerpująca. W literaturze polskiej i anglojęzycznej dostępnych jest wiele pozycji, w których takiej charakterystyki dokonano zarówno w odniesieniu do całego aktu¹⁷¹, jak i poszczególnych problemów¹⁷², a źródło poznania RODO stanowią opinie i wytyczne wydane przez EROD¹⁷³ i Grupę Roboczą¹⁷⁴, która działa na podstawie art. 29 Dyrektywy

¹⁶⁹ Rada Europy, Convention 108+ <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=223> (dostęp: 20.09.2024 r.).

¹⁷⁰ Por. J. Ukrow, Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108, *European Data Protection Law Review* 2018, Vol. 4, Iss. 2, s. 239; C. de Terwangne, Privacy and data protection in Europe: Council of Europe's Convention 108+ and the European Union's GDPR [in:] *Research Handbook on Privacy and Data Protection Law*, ed. by G. Gonzalez, R. van Brakel, P. de Hert, Cheltenham 2022, s. 10-35.

¹⁷¹ Przykładowo: P. Fajgielski, Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022; RODO. *Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018; *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. by Ch. Kuner, et al. Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 8.01.2024 r.); *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwinski, SIP Legalis 2021; *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła Warszawa 2018; M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016; Council of Europe, *Handbook on European Data Protection Law: 2018 edition*, 2018.

¹⁷² Przykładowo: czasopisma naukowe dedykowane kwestiom związanym z ochroną danych osobowych, jak „*European Data Protection Law Review*” i „*International Data Privacy Law*”; O. Lynskey, *The foundations of EU data protection law*, Oxford 2015; M. Kulkarni, A. Mondal, K. K. Singh, *GDPR: A Bibliometric Analysis*, [in:] *Proceedings of the International Conference on Cognitive and Intelligent Computing. Cognitive Science and Technology*, ed. by A. Kumar, G. Ghinea, S. Merugu et al., Singapore 2022, https://doi.org/10.1007/978-981-19-2350-0_1 (dostęp: 20.09.2024 r.); T. Naef, *Data Protection Without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, Cham 2023; G. Dorfleitner, L. Hornuf, J. Kreppmeier, *Promise not fulfilled: FinTech, data privacy, and the GDPR*, „*Electronic Markets*” 2023, Vol. 33, No. 1, s. 33; J. Ausloos, *The Right to Erasure in EU Data Protection Law*, Oxford 2020; I. Graef, M. Husovec, and N. Purtova, *Data portability and data control: lessons for an emerging concept in EU law*, „*German Law Journal*” 2018, Vol. 19, No. 6, s. 1359-1398.

¹⁷³ RODO: wytyczne, zalecenia, najlepsze praktyki, https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_pl (dostęp: 15.09.2024 r.).

¹⁷⁴ Komisja, *Opinions and recommendations*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (dostęp: 15.09.2024 r.).

ODO. Podstawowym celem jest identyfikacja i zbadanie zagadnień, które są istotne dla weryfikacji głównej hipotezy badawczej, w tym zakresu przedmiotowego i podmiotowego RODO wydzielonych do osobnych podrozdziałów poniżej. Aby zachować kompletność i spójność wyводу w tej rozprawie (badającej wiele aktów prawnych) oraz umożliwić referowanie do pojęć i rozwiązań zastosowanych w RODO dokonano syntetycznego omówienia RODO (zasadniczo rozdziałów I-V) oraz UODO, przy czym analizy pozycji ustrojowej i kompetencji organów ustanowionych na poziomie tych aktów na poziomie unijnym i krajowym dokonano w rozdziale 3. rozprawy.

RODO jest aktem prawa unijnego – rozporządzeniem, co oznacza, że ma zasięg ogólny, wiąże w całości i jest stosowane bezpośrednio w państwach członkowskich (art. 288 TFUE)¹⁷⁵. Prawodawca unijny nałożył na państwa członkowskie obowiązek ustanowienia aktów prawnych, które umożliwią stosowanie RODO w krajowych porządkach prawnych (np. ustanowienie krajowych organów nadzorczych zgodnie z zasadą autonomii instytucjonalnej, rozdział VI – Niezależne organy nadzorcze), oraz pozostawił prawodawcom krajowym pewną swobodę w odniesieniu do niektórych kwestii, np. art. 87 RODO (Przetwarzanie krajowego numeru identyfikacyjnego), art. 88 RODO (Przetwarzanie w kontekście zatrudnienia), art. 89 RODO (Przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych), art. 9 ust. 4 (Dalsze warunki w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia).

RODO nie stanowiło pierwszego aktu prawnego w UE, który regulował ochronę osób fizycznych w związku z przetwarzaniem danych osobowych i swobodny przepływ takich danych. Do wejścia w życie RODO obowiązywała uchylona przez RODO Dyrektywa ODO przyjęta w 1995 r., która implementowana była następnie przez państwa członkowskie. Chociaż RODO wprowadza szereg nowych rozwiązań, np. *privacy by design* i *privacy by default* (art. 25 RODO), prawo do usunięcia danych (art. 17 RODO), to zasadniczo czerpie z dorobku Dyrektywy ODO¹⁷⁶, np. w zakresie siatki pojęciowej („administrator” i „przetwarzający” – art. 2 lit d)-e) Dyrektywy ODO i art. 4 pkt 7)-8) RODO) oraz kryteriów legalności przetwarzania danych (art. 7 Dyrektywy ODO i art. 6 RODO). Intencją prawodawcy

¹⁷⁵ W przedmiocie znaczenia bezpośredniego obowiązywania, bezpośredniego stosowania i bezpośredniego skutku rozporządzenia patrz: T. Jaroszyński, *4. Bezpośrednie obowiązywanie, bezpośrednie stosowanie i bezpośredni skutek* [w:] *Rozporządzenie Unii Europejskiej jako składnik systemu prawa obowiązującego w Polsce*, Warszawa 2011, SIP LEX.

¹⁷⁶ Por. W. R. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa*, „Krajowa Rada Sądownictwa” 2013, nr 1, s. 14-26.

unijnego przy przyjmowaniu RODO nie była zmiana „ram co do celów i zasad”, ale przede wszystkim przeciwdziałanie „rozdrobnieniu sposobów realizacji ochrony danych osobowych” w UE¹⁷⁷. Stąd też decyzja, aby RODO przyjęte zostało jako rozporządzenie, a nie jako dyrektywa (która wiąże państwa członkowskie, zgodnie z art. 288 TFUE, w odniesieniu do rezultatu, który ma być osiągnięty, jednak pozostawia swobodę wyboru formy i środków).

Przed dokonaniem syntetycznej charakterystyki, konieczne jest poczynienie uwagi związanej ze sposobem, w jaki w RODO sformułowane są przepisy. RODO bazuje na podejściu opartym na ryzyku¹⁷⁸ (*risk-based approach*) i neutralności technicznej. Oba te rozwiązania mają zapewnić elastyczność w realizacji RODO, aby umożliwić ją we wszystkich państwach członkowskich we każdym sektorze gospodarki, które różnią się zasadniczo i sposobem przetwarzania danych, i ryzykiem z nim związanym (np. różnice między przetwarzaniem danych osobowych przez przedsiębiorstwo produkujące części samochodowe i klinikę ginekologiczną). W konsekwencji, obowiązywanie RODO nie powinno być uzależnione od techniki użytej do przetwarzania danych (neutralność techniczna; motyw 15 RODO)¹⁷⁹, ani też RODO nie powinno kazuistycznie rozstrzygać jakie konkretnie rozwiązania prawne, organizacyjne i techniczne są zgodne z RODO. Ta (względna) łatwość (elastyczność¹⁸⁰) w przystosowywaniu RODO do różnych okoliczności faktycznych osiągnięta została przez wybór unormowania przetwarzania danych osobowych w RODO za pomocą zasad (art. 5 RODO) i terminów nieostrych (przykładowo art. 32 ust. 1 RODO: „administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne”), przy jednoczesnym nałożeniu na administratora obowiązku rozliczalności, czyli zdolności do wykazania przestrzegania obowiązków wynikających z RODO z uwzględnieniem „ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia” (art. 24 ust. 1 RODO)¹⁸¹.

¹⁷⁷ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), COM/2012/011 final - 2012/0011 (COD), pkt 1 uzasadnienia.

¹⁷⁸ Por. C. Quelle, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach, Eur. J. Risk Regul. 2018, Vol. 9, Iss.3, <https://doi.org/10.1017/err.2018.47> (dostęp: 20.09.2024 r.); R. Gellert, The risk-based approach to data protection, Oxford 2020.

¹⁷⁹ Por. J. Wong, T. Henderson, *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, Int. Data Priv. Law 2019, t. 9, nr 3, <https://doi.org/10.1093/idpl/ipz008> (dostęp: 6.11.2024 r.), s. 173–191.

¹⁸⁰ *Elastyczny*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/sjp/elastyczny%3B2556392> (dostęp 1.09.2024 r.).

¹⁸¹ Konieczność zapewnienia neutralności technologicznej i podejście oparte na ryzyku jako przyczyny zjawiska krzyżowania się kompetencji zbadano w podrozdziale 5.3.

RODO podzielone jest na 99 artykułów, które umieszczono w jedenastu rozdziałach: *Przepisy ogólne* (rozdział I; art. 1-4); *Zasady* (rozdział II; art. 5-11); *Prawa osoby, której dane dotyczą* (rozdział III; art. 12-22); *Administrator i podmiot przetwarzający* (rozdział IV; art. 24-43); *Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych* (rozdział V; art. 44-50); *Niezależne organy nadzorcze* (rozdział VI; art. 51-59); *Współpraca i spójność* (rozdział VII; art. 60-76); *Środki ochrony prawnej, odpowiedzialność i sankcje* (rozdział VIII; art. 77-84); *Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem danych* (rozdział IX; art. 85-91); *Akty delegowane i akty wykonawcze* (rozdział X; art. 92-93) oraz *Przepisy końcowe* (rozdział XI; art. 94-99). RODO scharakteryzowane zostanie przy przyjęciu systematyki ustanowionych przez nie same zasad, które następnie konkretyzowane są przez obowiązki administratorów i podmiotów przetwarzających oraz praw podmiotów danych¹⁸². Najpierw jednak analizie poddany będzie zakres terytorialny obowiązywania RODO. Zakres przedmiotowy i podmiotowy RODO scharakteryzowany zostanie w oddzielnych podrozdziałach poniżej, ponieważ ustalenie tych zakresów jest kluczowe dla weryfikacji hipotezy o krzyżowaniu się zakresu RODO z innymi aktami prawnymi w obszarze przetwarzania danych osobowych.

Zakres terytorialny RODO normuje art. 3 RODO, określając trzy przypadki, w których RODO znajduje zastosowanie. Po pierwsze, zgodnie z art. 3. ust. 1 RODO, RODO stosuje się do przetwarzania danych osobowych w związku z działalnością jednostki organizacyjnej¹⁸³ administratora lub podmiotu przetwarzającego w UE, niezależnie od miejsca tego przetwarzania. Oznacza to, przykładowo, że RODO ma zastosowanie nie tylko do przetwarzania danych osób przebywających w UE, ale stosuje się nawet jeżeli dochodzi do przetwarzania danych osób z państw trzecich (np. mieszkańców Stanów Zjednoczonych Ameryki czy Egiptu; por. także motyw 14 RODO), o ile dochodzi do niego w związku z działalnością jednostki organizacyjnej w UE¹⁸⁴. Drugi przypadek jest najbardziej skomplikowany i jednocześnie zasadniczo rozszerza zakres obowiązywania RODO poza

¹⁸² Wybrane zagadnienia z RODO zbadano także w innych podrozdziałach tego rozdziału i w innych rozdziałach rozprawy w odniesieniu do krzyżowania się czy to zakresu przedmiotowego aktów prawnych z RODO (np. pseudonimizacja i anonimizacja scharakteryzowane w podrozdziale 2.6.5.), czy też w odniesieniu do kompetencji organów (np. znaczenie terminów „transgraniczne przetwarzania” i „organ nadzorczy, którego sprawa dotyczy” przy dokonywaniu analizy kompetencji organów ochrony danych w 3.5.1. podrozdziale).

¹⁸³ W odniesieniu do pojęcia jednostki organizacyjnej por. wyrok TSUE z 1.10.2015, C-230/14, Weltimmo p. 28-31.

¹⁸⁴ EROD, *Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3)*, Wersja 2.0 12 listopada 2019 r., s. 5-14; przykład nr 4 na s. 10.

terytorium UE¹⁸⁵. RODO znajduje bowiem zastosowanie (art. 3 ust. 2 RODO) także do przetwarzania danych podmiotów danych przebywających w UE przez administratora lub procesora bez jednostki organizacyjnej w UE, jeżeli przetwarzanie „wiąże się” z oferowaniem tym podmiotom towarów lub usług w UE (niezależnie od ich odpłatności) lub monitorowaniem ich zachowania, o ile ma miejsce w UE. Decydujące znaczenie ma w odniesieniu do tego przypadku nie to, gdzie jednostkę organizacyjną ma administrator lub procesor, lecz to, że dochodzi do przetwarzania danych osób przebywających w UE w dwóch wskazanych wyżej wypadkach, czyli np. także wtedy, kiedy kanadyjskie przedsiębiorstwo (niemające organizacyjnego łącznika z UE) oferuje aplikację z mapami turystycznymi dla europejskich miast, przetwarzając dane jej użytkowników celem spersonalizowanej reklamy¹⁸⁶. Z kolei art. 3 ust. 3 RODO dotyczy sytuacji, kiedy przetwarzania dokonuje administrator niemający jednostki organizacyjnej w UE, ale mający tę jednostkę w miejscu, w którym zastosowanie znajduje prawo państwa członkowskiego na podstawie prawa międzynarodowego publicznego. Jak wskazano, zakres terytorialny obowiązywania RODO ustanowiono w sposób szeroki, co w literaturze nazywane jest „eksterytorialnym” charakterem RODO, ponieważ znajduje zastosowanie nie tylko do podmiotów z jednostką organizacyjną w UE, ale także do podmiotów, które nie mają tego organizacyjnego łącznika, ale w szczególnych przypadkach przetwarzają dane podmiotów danych przebywających na terytorium UE, co podyktowane jest potrzebą zapewnienia skutecznej ochrony podstawowych praw do ochrony danych osobowych i prywatności¹⁸⁷. Jednakże konsekwencją takiego uregulowania zakresu terytorialnego jest ryzyko faktycznej niemożliwości stosowania RODO wobec administratorów i podmiotów przetwarzających bez jednostki organizacyjnej w UE¹⁸⁸.

Zasady dotyczące przetwarzania danych osobowych zostały ustanowione w art. 5 ust. 1-2 RODO, który stanowi modyfikację art. 6 ust. 1-2 Dyrektywy ODO, a także art. 6 Konwencji 108. W RODO wyróżniono następujące zasady przetwarzania danych osobowych: zgodności z prawem, rzetelności i przejrzystości; ograniczenia celu przetwarzania; minimalizacji danych;

¹⁸⁵ Por. B. Van Alsenoy, *Reconciling the (Extra)Territorial Reach of the GDPR with Public International Law* [in:] *Data Protection and Privacy Under Pressure. Transatlantic Tensions, EU Surveillance and Big Data*, ed. by G. Vermeulen, E. Lievens, Antwerpen: Maklu, 2018, s. 85-90.

¹⁸⁶ EROD, Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3), Wersja 2.0 12 listopada 2019 r., przykład nr 9 na s. 17.

¹⁸⁷ Por. P. de Hert, M. Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, *Int. Data Priv. Law* 2016, Vol. 6, No. 3, <https://doi.org/10.1093/idpl/ipw008> (dostęp: 20.09.2024 r.), s. 231, 238.

¹⁸⁸ P. de Hert, M. Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, *Int. Data Priv. Law* 2016, Vol. 6, No. 3, <https://doi.org/10.1093/idpl/ipw008> (dostęp: 20.09.2024 r.), s. 231, 239.

prawidłowości danych; ograniczenia przechowywania danych; integralności i poufności ich przetwarzania; oraz rozliczalności. Listę tych zasad należy uznać za rozbudowaną. Zasady te stanowią punkt odniesienia przy wykładni pozostałych norm w RODO, która powinna być dokonywana w taki sposób, aby zapewnić możliwie pełną realizację zasad. Ponadto, administratorzy są wprost zobowiązani – zgodnie z ostatnią zasadą rozliczalności – do przestrzegania tych zasad i wykazania tego przestrzegania (art. 5 ust. 2 RODO), a zatem zasady te stanowią samodzielną podstawę odpowiedzialności, co nie zawsze ma miejsce w odniesieniu do norm o charakterze zasad. Wprowadzenie do RODO norm-zasad (co stanowi kontynuację tradycji Konwencji 108 i Dyrektywy ODO) należy uznać za uzasadnione, ponieważ tak sformułowane normy spełniają co najmniej trzy kryteria zaliczenia ich do norm-zasad, które wyróżnione zostały przez J. Wróblewskiego: 1) zostały one wyodrębnione i wprost nazwane zasadami, co oznacza ich wyższość nad pozostałymi normami w RODO, 2) bazując na art. 8 KPP, stanowią uzasadnienie dla pozostałych norm w RODO; 3) stanowią element integrujący pozostałe normy w RODO¹⁸⁹. Wyodrębnienie zasad w RODO ma funkcję porządkującą, co jednocześnie wskazuje na aspirację prawodawcy unijnego, aby akty prawne nakierowane na ochronę danych osobowych stanowiły odrębną kompleksową gałąź prawa z własnymi zasadami¹⁹⁰. Zasady ustanowione w RODO zostaną poniżej syntetycznie scharakteryzowane.

Zasada zgodności przetwarzania z prawem (inaczej zwana zasadą legalności; art. 5 ust. 1 lit. a RODO) skonkretyzowana jest przez art. 6 RODO określający podstawy (warunki legalności) przetwarzania danych osobowych (ust. 1-3) i normujący ich przetwarzanie w celu innym niż pierwotny (ust. 4), co stanowi z kolei konkretyzację zasady ograniczenia celu¹⁹¹ (art. 5 ust. 1 lit. b: „zbieranie [danych osobowych] w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami”). W art. 6 ust.1 RODO ustanowiono sześć odrębnych podstaw do uznania legalności przetwarzania: zgoda podmiotu danych (lit. a); niezbędność przetwarzania do wykonania

¹⁸⁹ Por. J. Wróblewski, *Prawo obowiązujące a „ogólne zasady prawa”*, „Zeszyty Naukowe UŁ Nauki humanistyczno-społeczne, seria I” 1965, z. 42., s. 17 – 38, s. 21; cyt. za: S. Wronkowska, M. Zieliński, Z. Ziemiński, „Zasady prawa” w perspektywie teorii prawa oraz szczegółowych nauk prawnych, RPEiS 1974, t. 36, z. 2, s. 1-14, s. 3.

¹⁹⁰ Por. Z. Kmiecik, *Ogólne zasady prawa i postępowania administracyjnego*, Warszawa 2000, s. 35-36. Wybór prawodawcy unijnego, aby przetwarzanie danych osobowych uregulować za pomocą norm-zasad i terminów nieostrych oraz podejścia opartego na ryzyku jest przedmiotem analizy w podrozdziale 5.3.

¹⁹¹ Por. Grupa Robocza, *Opinion 03/2013 on Purpose Limitation*, WP 203, 2.04.2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; por. także: I. Hahn, *Purpose Limitation in the Time of Data Power: Is There a Way Forward?*, EDPL 2021, Vol. 7, Iss. 1, <https://doi.org/10.21552/edpl/2021/1/7> (dostęp: 09.09.2024 r.).

umowy z podmiotem danych lub do podjęcia działań na jego żądanie przed zawarciem umowy¹⁹² (lit. b); wykonanie obowiązku prawnego przez administratora (lit. c); ochrona żywotnych interesów podmiotu danych lub innej osoby (lit. d); niezbędność przetwarzania do wykonania zadania w interesie publicznym lub przy sprawowaniu władzy publicznej (lit. e); tak zwany „uzasadniony interes”. Podstawy przetwarzania wskazane w lit. c) i e) wyżej winny być ustanowione w prawie Unii lub w prawie państwa członkowskiego zgodnie z precyzyjnymi wymogami przewidzianymi w art. 6 ust. 3 RODO, co w praktyce nakłada na administratora obowiązek rozważenia czy przepisy prawa, na podstawie których dokonuje przetwarzania spełniają te wymogi. Osobno omówione zostaną dwie podstawy przetwarzania – zgoda i „uzasadniony interes”.

Zgoda podmiotu danych w potocznym mniemaniu uznawana bywa za preferowaną podstawę przetwarzania. To, że uzyskanie zgody podmiotu danych jest istotnym elementem europejskiego modelu ochrony danych osobowych (o czym świadczy choćby jej samodzielne wskazanie jako podstawy przetwarzania w art. 8 ust. 2 KPP), nie oznacza jeszcze, że przetwarzanie danych osobowych na tej podstawie jest „bezpieczniejsze” niż w przypadku innych podstaw¹⁹³. RODO nie wprowadza żadnej hierarchii między podstawami przetwarzania. Co więcej, w wielu sytuacjach przetwarzanie na podstawie zgody może okazać się z perspektywy administratora mniej korzystne, ponieważ zgodę można w każdym czasie wycofać (art. 7 ust. 3 RODO), co nie powinno mieć miejsca, na przykład, kiedy przetwarzanie danych osobowych jest w rzeczywistości potrzebne administratorowi do wykonania obowiązku prawnego. Termin „zgoda” zdefiniowano w art. 4 ust. 11 RODO, zgodnie z którym jest to „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych”, co w szczególności oznacza, że udzielenie zgody wymaga świadomego, aktywnego działania i nie można jej domniemywać. Warunki wyrażenia zgody unormowano w art. 7 ust. 1-4 RODO, nakładając na administratora obowiązek wykazania faktu wyrażenia zgody przez podmiot danych (ust. 1), transparentny sposób zapytania o zgodę (ust. 2), możliwość wycofania zgody w każdym czasie tak łatwo, jako zgody udzielono (ust. 3) i okoliczności wpływające na ocenę dobrowolności udzielenia

¹⁹² EROD, Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pl.pdf (dostęp: 15.09.2024 r.).

¹⁹³ Grupa Robocza, *Opinion 15/2011 on the definition of consent*, WP187, 13.06.2011, s. 7-8.

zgody (ust. 4)¹⁹⁴. W sposób szczególny prawodawca unijny uregulował warunki wyrażenia zgody przez dziecko (art. 8 ust. 1-3 RODO), wprowadzając ukończenie szesnastu lat jako granicę do samodzielnego udzielenia zgody (państwa członkowskie mogą obniżyć tę granicę do lat trzynastu zgodnie z ust. 1 *in fine*), ale dotyczy to tylko świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, których pojęcie jest przedmiotem dyskusji w literaturze¹⁹⁵.

Drugą z podstaw przetwarzania scharakteryzowaną w niniejszej pracy jest art. 6 ust. 1 lit. f RODO (tzw. „uzasadniony interes”), zgodnie z którym przetwarzanie jest zgodne z prawem, jeżeli „jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności” podmiotu danych. Już z brzmienia tego przepisu wynika, że spełnienie tej przesłanki wymaga dokonania wyważenia uzasadnionych interesów administratora (lub strony trzeciej) w stosunku do interesów lub praw i wolności podmiotu danych (co nazwane jest „testem balansującym”). Przetwarzanie może być uznane za zgodne z prawem tylko w przypadku, jeżeli ten pierwszy przewyższy ten drugi, a jednocześnie przetwarzanie jest niezbędne (w uproszczeniu, nie ma innego sposobu), aby go zrealizować¹⁹⁶. Pojęcie uzasadnionego interesu administratora było przedmiotem opinii Grupy Roboczej pod rządami Dyrektywy ODO, zgodnie z którą taki interes musi spełniać łącznie trzy przesłanki: być zgodny z prawem, rzeczywisty (zatem nie hipotetyczny) i sformułowany na tyle jasno, że możliwe jest przeprowadzenie testu balansującego, czego przykładem jest tradycyjny marketing bezpośredni, dochodzenie lub obrona przed roszczeniami, prowadzenie badań naukowych i zapobieganie oszustwom¹⁹⁷. Z kolei w odniesieniu do interesów lub praw i wolności podmiotu danych wskazuje się, że należy interpretować je szeroko,¹⁹⁸ a przy dokonywaniu testu balansującego należy wziąć pod uwagę szereg czynników, w tym: charakter i sposób przetwarzania danych, status podmiotów danych (np. czy są to dzieci lub osoby

¹⁹⁴ Więcej informacji w przedmiocie pojęcia zgody i warunków jej udzielania w: EROD, *Wytoczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679*, wersja 1.1, 04.05.2020.

¹⁹⁵ Por. E. Lievens, V. Verdoodt, Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation, CLSR 2018, Vol. 34, No. 2, s. 272.

¹⁹⁶ I. Kamara, P. de Hert, *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, „Brussels Privacy Hub” 2018, Vol. 4, No. 12, s. 13, <https://ssrn.com/abstract=3228369>. (dostęp: 20.09.2024 r.).

¹⁹⁷ Grupa Robocza, Opinion 06/2014 on the „Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, WP217, 9.04.2014, s. 25.

¹⁹⁸ Grupa Robocza, Opinion 06/2014 on the „Notion of legitimate, interests of the data controller under Article 7 of Directive 95/46/EC”, WP217, 9.04.2014, s. 29-30.

z niepełnosprawnością intelektualną) i stopień asymetryczności w relacji między podmiotami danych a administratorem¹⁹⁹. Podmioty danych na podstawie art. 21 ust. 1 RODO mają prawo do wniesienia sprzeciwu wobec przetwarzania danych na podstawie art. 6 ust. 1 lit. f RODO, którego zgłoszenie oznacza co do zasady konieczność zaprzestania przetwarzania, chyba, że administrator wykaże prawnie uzasadnione podstawy do przetwarzania o kwalifikowanym charakterze.

W RODO (art. 9) ustanowiono szczególne warunki do przetwarzania szczególnych kategorii danych osobowych (nazywanych także „danymi wrażliwymi”), do których zalicza się dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne (zdefiniowane w art. 4 pkt. 13 RODO), dane biometryczne (w celu jednoznacznej identyfikacji podmiotu danych; zdefiniowane w art. 4 pkt 14 RODO), dane dotyczące zdrowia (zdefiniowane w art. 4 pkt 15 RODO) oraz seksualności i orientacji seksualnej. Dane osobowe dotyczące wyroków skazujących i naruszeń prawa nie są zaliczane w RODO do szczególnych kategorii, lecz uregulowane są osobno w art. 10 RODO (w odróżnieniu do Konwencji 108, w której ta kategoria jest zaliczona do danych wrażliwych; por. art. 6 Konwencji 108). Przetwarzanie danych wrażliwych, których katalog ma charakter zamknięty, jest z zasady zakazane zgodnie z art. 9 ust. 1 RODO. Kolejny ustęp przewiduje jednak dziesięć wyjątkowych warunków, których spełnienie wyłącza zakaz przetwarzania tych danych, w tym wyraźnej zgody podmiotu danych (art. 9 ust. 2 lit. a RODO), upublicznienia tych danych przez podmiot danych w sposób oczywisty (art. 9 ust. 2 lit. e RODO) lub jeżeli przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń (art. 9 ust. 2 lit. f RODO) lub do celów profilaktyki zdrowotnej lub medycyny pracy, diagnozy medycznej i leczenia (art. 9 ust. 2 lit. h RODO). Spełnienie tych warunków obwarowane jest dodatkowymi obowiązkami, np. wprowadzeniem odpowiednich środków ochrony praw podstawowych i interesów podmiotów danych²⁰⁰. Fakt przetwarzania danych wrażliwych ma konsekwencje dla pozostałych obowiązków administratora, np. ich przetwarzanie na dużą skalę wymaga

¹⁹⁹ DPD, D.P.D., Balboni, D.C., Imperiali, R., Macenaite, M. and Case, C., 2022. *Legitimate interest*, ed. by Ch. F. Mondschein, C. Monda [in:] *Elgar Encyclopedia of Law and Data Science*, ed. by G. Comandé, Cheltenham 2022, s. 209-215.

²⁰⁰ Por. L. Georgieva, Ch. Kuner, *Article 9. Processing of special categories of personal data* [in:], *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 17.01.2024 r.), s. 381–382.

przeprowadzenia i udokumentowania uprzedniej oceny skutków przetwarzania dla ochrony danych (art. 32 ust. 3 lit. b RODO)²⁰¹.

Zasady rzetelności (*fairness*²⁰²) i przejrzystości przetwarzania danych (art. 5 ust. 1 lit. a RODO) wymienione zostały przez prawodawcę unijnego obok siebie. Relacja między nimi jest w literaturze przedmiotem dyskusji, ponieważ jedna z zasad bywa wyjaśniana przez elementy drugiej²⁰³. Nie pogłębiając wywodu w odniesieniu do tej dyskusji, wskazać należy, że obie te zasady wzajemnie się wzmacniają. Zgodnie ze stanowiskiem Grupy Roboczej, zapewnienie przejrzystości przetwarzania pomaga w zapewnieniu rzetelności przetwarzania²⁰⁴. Zasada przejrzystości realizowana jest przez wypełnienia przez administratora obowiązków z art. 12-14 RODO, w tym obowiązków informacyjnych wobec podmiotów danych (por. motyw 39 RODO), które stanowią jednocześnie prawa podmiotów danych. Istotą tych obowiązków jest kompleksowe, ale zrozumiałe (art. 12 ust. 1 RODO; motyw 58 i 60 RODO) przedstawienie podmiotom danych informacji o przetwarzaniu ich danych osobowych, w tym celach tego przetwarzania, kategoriach przetwarzanych danych, odbiorcach danych (art. 13 i 14 RODO). Celem tego obowiązku, oprócz realizacji zasady przejrzystości, jest wzmocnienie realizacji zasady rozliczalności. Transparentność powoduje bowiem, że administratorzy są zobowiązani proaktywnie wykazywać zgodność przetwarzania z RODO wobec podmiotów danych. Nadto, obowiązki te umożliwiają możliwość realizacji pozostałych praw przez podmioty danych, ponieważ dają im informacje na temat faktu i sposobu przetwarzania ich danych osobowych.

Zgodnie z zasadą minimalizacji, dane osobowe powinny być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane”. Podobnie jak w przypadku zasady rzetelności, także zasada minimalizacji nie jest rozumiana jednolicie²⁰⁵.

²⁰¹ Por. L. Georgieva, Ch. Kuner, *Article 9. Processing of special categories of personal data* [in:], *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 17.01.2024 r.), s. 382.

²⁰² Pobocznie wskazać należy, że dyskusyjne wydaje się czy słowo „rzetelność” jest odpowiednim wyborem. W wersji angielskiej zastosowano słowo *fairness*, a wersja francuska używa słowa *loyale*. Być może bardziej adekwatnym wyborem w języku polskim byłoby słowo „uczciwość”.

²⁰³ G. Malgieri, *The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation*, *Proceedings of FAT* '20*, January 27–30, 2020, ACM, New York, NY, USA, <https://ssrn.com/abstract=3517264>. (dostęp: 17.01.2024 r.).

²⁰⁴ Grupa Robocza, *Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018*, WP260 Rev.01 <https://ec.europa.eu/newsroom/article29/items/622227/en> (dostęp: 15.09.2024 r.), s. 5. W tym dokumencie także więcej informacji na temat realizacji zasady przejrzystości. Por. także M. Kuba, *Zasada przejrzystości przetwarzania danych osobowych jako instrument ochrony autonomii informacyjnej pracownika*, MoP 2020, nr 12, doi:10.32027/MOPR.20.12.2.

²⁰⁵ A. J. Biega, P. Potash, Z. Daumé et al., *Operationalizing the Legal Principle of Data Minimization for Personalization*, [in:] *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20)*, New York 2020, <https://doi.org/10.1145/3397271.3401034> (dostęp: 20.09.2024 r.), s. 399.

Składają się na nią trzy elementy, które pozostają powiązane ze sobą i wymagają jednoczesnego uwzględnienia. Pierwszym jest adekwatność (odpowiedniość) przetwarzanych danych w odniesieniu do celu przetwarzania, co może paradoksalnie oznaczać konieczność przetwarzania większej liczby danych, jeżeli tylko w ten sposób pozwala to zrealizować, np. zasadę przejrzystości. Drugim jest stosowność (w wersji angielskiej *relevant*), co oznacza, że przetwarzane powinny być tylko te dane, które są istotne dla osiągnięcia celu. Powiązane jest to z ostatnim elementem – ograniczeniem przetwarzanych danych do minimum niezbędnego do osiągnięcia celu²⁰⁶. Z zasadą minimalizacji ściśle powiązana jest zasada ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO), której treścią jest obowiązek przechowywania danych w formie umożliwiającej identyfikację podmiotu danych wyłącznie przez okres niezbędny do celów przetwarzania. Z zasady tej wynika obowiązek ustalenia okresów retencji (przechowywania) danych osobowych i wprowadzenia środków organizacyjnych oraz technicznych umożliwiających monitorowanie upływu tych okresów oraz ich usuwania po ich upływie. W praktyce jest to trudne do wykonania, ponieważ te same dane osobowe przetwarzane są często w różnych celach jednocześnie (np. wykonanie umowy z podmiotem danych, dochodzenie i obrona przed roszczeniami, wykonanie obowiązków wynikających z prawa podatkowego), a zatem okresy przechowywania dla tych samych danych mogą być różne dla różnych celów przetwarzania. Ta zasada doznaje wyjątków w odniesieniu do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO (art. 5 ust. 1 lit. e *in fine* RODO).

Z perspektywy zapewnienia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa kluczowa jest zasada integralności i poufności, która nakłada obowiązek przetwarzania danych tak, aby zapewnić ich odpowiednie bezpieczeństwo przy wykorzystaniu takich właśnie środków. Zasada ta uzupełniona jest przez ogólny obowiązek administratora do wdrażania odpowiednich środków technicznych i organizacyjnych, aby zapewnić przetwarzanie danych zgodne z prawem (art. 24 RODO). Koresponduje z nią także obowiązek wdrażania *privacy by design* (uwzględniania ochrony danych w fazie projektowania, przy określaniu sposobów przetwarzania) i *privacy by default* (domyślna ochrona danych). Komplementarne do tej zasady są również obowiązki ustanowione w sekcji 2 (*Bezpieczeństwo danych osobowych*) rozdziału IV (*Administrator i podmiot przetwarzający*). Art. 32 ust. 1

²⁰⁶ A. J. Biega, P. Potash, Z. Daumé et al., Operationalizing the Legal Principle of Data Minimization for Personalization, [in:] Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20), New York 2020, <https://doi.org/10.1145/3397271.3401034> (dostęp: 20.09.2024 r.), s. 400.

RODO nakłada zarówno na administratora, jak i podmiot przetwarzający obowiązek zapewnienia bezpieczeństwa przetwarzania przy uwzględnieniu szeregu okoliczności, w tym wskazanego wyżej ryzyka, jak i stanu wiedzy technicznej w odniesieniu do środków technicznych i organizacyjnych oraz kosztów ich wdrażania. Jak zostało już wskazane, przyjęte w RODO podejście na zasadzie ryzyka i neutralność technologiczna powoduje, że RODO nie rozstrzyga kazuistycznie jakie środki techniczne i organizacyjne powinny zostać przez administratora i podmioty przetwarzające wdrożone, pozostawiając im decyzję o wyborze tych środków i dostarczając kryteriów, które winny być przy tej ocenie uwzględnione. Decyzja ta powinna być podejmowana przy uwzględnieniu zasady rozliczalności.

Zasada rozliczalności wyłączona do osobnego ustępu 2 w art. 5 RODO statuuje obowiązek przestrzegania przez administratora wszystkich powyższych zasad i nakłada na niego obowiązek wykazania tego przestrzegania, a przez to uważana jest w literaturze za węzłową zasadę w RODO²⁰⁷. RODO wprowadziło reguły komplementarne wobec tej zasady. Jedną z nich (która, oprócz rozliczalności, służy także zapewnieniu integralności i poufności) jest obowiązek przeprowadzenia przez administratora w określonych przypadkach (art. 35 ust. 3 RODO) oceny skutków przetwarzania dla ochrony danych przed jego rozpoczęciem (art. 35 ust. 1 RODO)²⁰⁸. Minimalne elementy, jakie powinna zawierać ta ocena wskazano w art. 35 ust. 7 RODO, obejmując m.in. ocenę proporcjonalności i niezbędności przetwarzania względem jego celów oraz ocenę ryzyka naruszenia praw lub wolności podmiotów danych oraz środki w celu zaradzenia temu ryzyku. Za kolejną należy uznać także obowiązek zgłaszania przez administratora naruszenia ochrony danych (por. art. 4 pkt 12 RODO) organowi nadzorczemu (art. 33 RODO) i zawiadomienia podmiotu danych o tym naruszeniu, jeżeli może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 34 ust. 1 RODO)²⁰⁹. Dodatkowo, RODO w Sekcji 5 (*Kodeksy postępowania i certyfikacja*) wprowadza

²⁰⁷ P. de Hert, G. Lazcoz, When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance, EDPL 2022, Vol. 8, No. 31-40 s. 5.

²⁰⁸ Por. Grupa Robocza, *Guidelines on Data Protection Impact Assessment (DPIA)*, WP248 Rev.01 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711 (dostęp: 1.09.2024 r.).

²⁰⁹ Por. Grupa Robocza, *Guidelines on Personal data breach notification under Regulation 2016/679*, Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018, WP250 Rev.01, <https://ec.europa.eu/newsroom/article29/items/612052/en> (dostęp: 1.09.2024 r.).

dwa instrumenty – sektorowe kodeksy postępowania²¹⁰ (art. 40-41 RODO) i certyfikację²¹¹ (art. 42 RODO). Chociaż korzystanie z nich nie oznacza istnienia domniemania zgodności przetwarzania z RODO, to pozwala pomóc w wykazaniu, że obowiązki wykonywane są prawidłowo (por. np. art. 24 ust. 3 RODO i art. 25 ust. 3 RODO).

Krótkiej charakterystyki wymagają także prawa podmiotów danych (rozdział III RODO), które nie zostały poddane analizie wyżej, zwłaszcza w odniesieniu do zasady przejrzystości. Prawa podmiotów danych w RODO pełnią dwojaką funkcję. Po pierwsze, wzmacniają wypełnianie obowiązków przez wprowadzenie instrumentów, dających podmiotom danych możliwość wystosowania żądań do administratorów (np. prawo do sprostowania danych i prawo do usunięcia danych), których niespełnienie może być sankcjonowane. Po drugie mają umożliwić skuteczną realizację podstawowego prawa do ochrony danych osobowych przez podmioty danych. Podmioty danych mają prawo m.in. do dostępu do danych²¹² (art. 15 RODO) i sprostowania danych (art. 16 RODO), prawo do usunięcia danych zwane „prawem do bycia zapomnianym” w przypadkach wskazanych w art. 17 ust. 1 RODO (art. 17 RODO), do ograniczenia przetwarzania w przypadkach wskazanych w art. 18 ust. 1 RODO i prawo do przenoszenia danych²¹³ (art. 20 RODO). Komplementarnym do powyższych praw jest art. 22 RODO dotyczący zautomatyzowanego podejmowania decyzji wobec podmiotów danych²¹⁴, tym profilowania²¹⁵, który ustanawia prawo podmiotów danych, aby nie podlegać takiej decyzji, opierającej się wyłącznie na

²¹⁰ Por. EROD, *Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem* 2016/679, Wersja 2.0 4.06.2019 r. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pl.pdf (dostęp: 1.09.2024 r.); por. także: E. Lachaud, E., *Adhering to GDPR codes of conduct: A possible option for SMEs to GDPR certification*, „Journal of Data Protection & Privacy” 2019, Vol. 3, No. 1, s.48-68.

²¹¹ Por. EROD, *Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia*, Wersja 3.0 4.06.2019 r., https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_p1.pdf (dostęp: 1.09.2024 r.); por. także: E. Koulierakis, *Certification as Guidance for Data Protection by Design*, Int. Rev. Law Comput. Technol. 2024, Vol. 38, No. 2, <https://doi.org/10.1080/13600869.2023.2269498>, (dostęp: 7.09.2024 r.).

²¹² Por. M. Kupiec, Uprawnienie do uzyskania od administratora informacji o odbiorcach lub o kategoriach odbiorców a cele prawa dostępu do danych. Glosa do wyroku TS z dnia 12 stycznia 2023 r., C-154/21 (RW przeciwko Österreichische Post AG), EPS 2023, nr 6, s. 46-51.

²¹³ Por. Grupa Robocza, *Guidelines on the right to data portability, Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017*, WP 242 rev.01, <https://ec.europa.eu/newsroom/article29/items/611233/en> (dostęp: 1.09.2024 r.). Por. także W. R. Wiewiórowski, *Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych*, EPS 2017, nr 5, s. 23-30.

²¹⁴ Wskazać należy, że w ostatnim orzecznictwie TSUE przyjęto szeroką wykładnię pojęcia „automatycznego podejmowania decyzji”, co wzmacnia argument o stosowaniu rozszerzającej wykładni pojęć w RODO; por. wyrok TSUE z 7.12.2023, C-634/24, SCHUFA.

²¹⁵ Profilowanie i automatyczne podejmowanie decyzji są pojęciami powiązanymi, ale o odmiennym znaczeniu, por. A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wrocław 2019, s. 179-181.

automatycznym przetwarzaniu. Prawa podmiotów danych nie mają charakteru absolutnego w tym znaczeniu, że prawodawca wyłącza albo ogranicza ich zastosowanie w określonych przypadkach, np. w odniesieniu do automatycznego podejmowania decyzji w art. 22 ust. 2 RODO (w trzech przypadkach: jeżeli jest do niezbędne do wykonania umowy, jeżeli jest dozwolone prawem albo jeżeli wyrażono zgodę), a także w odniesieniu do „prawa do bycia zapomnianym”,²¹⁶ jeżeli przetwarzanie jest niezbędne do m.in. korzystania z prawa do wolności wypowiedzi i informacji (art. 17 ust. 3 lit. a RODO) oraz celów archiwalnych w interesie publicznym (art. 17 ust. 3 lit. d RODO). Wzmocnieniem realizacji praw podmiotów danych jest ustanowienie w RODO możliwości dochodzenia przez podmioty roszczeń cywilnoprawnych (art. 79 RODO), w tym prawa do dochodzenia odszkodowania za szkodę majątkową lub niemajątkową poniesioną w wyniku naruszenia RODO (art. 82 ust. 1 RODO)²¹⁷.

Dla ograniczenia praw podmiotów danych (art. 12-22 i art. 34 RODO) i obowiązków administratora lub podmiotu przetwarzającego (w tym wynikających z art. 5 RODO) istotny jest art. 23 RODO, który wprowadza możliwość ograniczenia zakresu tych praw i obowiązków w prawie UE lub w prawie państwa członkowskiego (wymogi aktu prawnego w art. 23 ust. 2 RODO), o ile nie narusza to „istoty podstawowych praw i wolności” oraz „w demokratycznym społeczeństwie” jest to niezbędny i proporcjonalny (co koresponduje z przesłankami ograniczenia w korzystaniu z praw i wolności w art. 52 KPP) środek służącym dziesięciu celom ujętym w zamkniętym katalogu w art. 23 ust. 1 RODO, w tym m.in. bezpieczeństwu narodowemu; obronie; bezpieczeństwu publicznemu; zapobieganiu przestępczości; zapobieganiu naruszeniom zasad etyki w zawodach regulowanych; egzekucji roszczeń cywilnoprawnych. Pomimo że prawodawca unijny wprowadza rozbudowane zabezpieczenia ograniczające możliwość naruszania tego wyjątku, to katalog tych celów należy uznać za szeroki i nieostry w niektórych przypadkach, zwłaszcza w odniesieniu do art. 23

²¹⁶ To prawo ustanowione wprost w RODO było wcześniej przedmiotem wyroku TSUE w sprawie Google Spain C-131/12, 13.04.2014. Jego ustanowienie i wykonywanie oraz jego ograniczenia są przedmiotem dyskusji w literaturze, ponieważ stanowi „radikalną realizację prawa do prywatności”, które może prowadzić do „przepisania historii”; patrz: A. De Baets, *A historian's view on the right to be forgotten*, Int. Rev. Law Comput. Technol. 2016, Vol. 30, No. 1-2, <http://dx.doi.org/10.1080/13600869.2015.1125155> (dostęp: 20.09.2024 r.), s. 57-66. Por. także R. C. Post, *Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere*, „Duke Law Journal” 2018, Vol. 67, No. 5, s. 981.

²¹⁷ W odniesieniu do zagadnienia dochodzenia odszkodowania na podstawie art. 82 ust. 1 RODO: J. Knetsch, *The compensation of non-pecuniary loss in GDPR infringement cases*, „European Journal of Privacy Law & Technologies” 2020 (Special Issue), s. 63-70. S. Mulders, *The relationship between the principle of effectiveness under Art. 47 CFR and the concept of damages under Art. 82 GDPR*, Int. Data Priv. Law 2023, Vol. 13, Iss. 3, s. 169-181. G. Potjewijd, S. Yakovleva, F. Carvalho de et al., *Mass damage claims for GDPR infringements: multi-jurisdictional perspective*, „Mass Claims: An International Journal with European Focus” 2021, nr 1, s. 5-26.

ust. 1 lit. e RODO, gdzie wskazane zostały „inne ważne cele leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego”.

2.2.2. USTAWA O OCHRONIE DANYCH OSOBOWYCH

UODO, czyli Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, stanowi operacjonalizację RODO do krajowego, polskiego systemu prawnego, co wywieść można z brzmienia art. 1 ust. 1 UODO, zgodnie z którym UODO stosuje się do „ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym RODO”. Oznacza to, że zakres obowiązywania UODO jest określony przez zakres obowiązywania RODO. UODO uchyliło poprzednio obowiązującą UODO⁹⁷. Tak jak wskazano wyżej, chociaż RODO jest rozporządzeniem unijnym stosowanym bezpośrednio, to nałożyło na prawodawcę unijnego obowiązek wprowadzenia rozwiązań, które zapewnią skuteczność jego stosowania, i pozostawiło prawodawcy krajowemu ograniczoną swobodę w uregulowaniu niektórych kwestii (przykłady wskazane wyżej). Tak jak w odniesieniu do organów nadzorczych ustanowionych na podstawie RODO, analiza pozycji ustrojowej, kompetencji PUODO jak i odrębnego charakteru postępowania przed PUODO dokonana zostanie w rozdziale 3 rozprawy.

Zakres przedmiotowy UODO sprecyzowano w art. 1 ust. 2, zgodnie z którym UODO określa: podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu (rozdział 2); warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji oraz tej certyfikacji (rozdział 3); tryb zatwierdzenia kodeksu postępowania (rozdział 5); organ właściwy w sprawie ochrony danych osobowych, czyli PUODO (rozdział 6); postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych (rozdział 7); tryb europejskiej współpracy administracyjnej (rozdział 8); kontrolę przestrzegania przepisów o ochronie danych osobowych (rozdział 9); odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem (rozdział 10); oraz odpowiedzialność karną i administracyjne kary pieniężne (rozdział 11).

W art. od 2 do 6a UODO zawarto wyłączenia w stosowaniu RODO, w tym w całości w odniesieniu do działalności służb specjalnych (art. 6 pkt 2 UODO; dotyczy to działalności Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego) oraz do realizacji niektórych obowiązków administratorów, zwłaszcza obowiązku informacyjnego wobec podmiotów danych z art. 13 i 14 RODO m.in., w zakresie działalności związanej

z materiałami prasowymi, działalności literackiej, artystycznej oraz wypowiedzi akademickich, w sytuacji zmiany celu przetwarzania i pośredniego pozyskiwania danych osobowych w trakcie wykonywania zadań publicznych oraz w związku z przetwarzaniem danych osobowych w ramach wykonywania kompetencji przez Prezydenta RP.

Rozdział 2 UODO (art. 8-11a) uszczegóławia obowiązki administratorów i podmiotów przetwarzających dotyczące wyznaczenia inspektora ochrony danych wynikające z art. 37 RODO przez wskazanie jakie podmioty i organy publiczne są zobowiązane do wyznaczenia tego inspektora (tj. jednostki sektora finansów publicznych, instytuty badawcze i Narodowy Bank Polski) oraz unormowanie trybu i formy zawiadamianie PUODO o dokonaniu tego wyznaczenia. W rozdział 3 (art. 12-14) i 4 (art. 15-26) unormowano warunki i tryb certyfikacji z art. 42 RODO oraz akredytacji podmiotu certyfikującego w zakresie, w jakim kwestie te nie zostały uregulowane w RODO, to jest w odniesieniu do kwestii proceduralnych, jak np. treść dokumentu potwierdzającego certyfikację (art. 21 UODO). Rozdział 5 (art. 27-33) UODO spełnia podobną funkcję jak rozdziały 3 i 4 UODO, to znaczy uzupełnia RODO o niezbędne elementy proceduralne, regulując opracowywanie i zatwierdzanie kodeksów postępowania, o których mowa w art. 40-41 RODO, oraz warunki i tryb akredytacji podmiotów monitorujących ich przestrzeganie. Z perspektywy ochrony praw przez podmioty danych istotny jest rozdział 10, który rozstrzyga, że do dochodzenia roszczeń cywilnoprawnych z tytułu naruszenia RODO, w tym odpowiedzialności odszkodowawczej (art. 79 i 82 RODO), zastosowanie znajdują przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny w kwestiach prawa materialnego (art. 92 UODO), a w kwestiach proceduralnych – ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (art. 100 UODO) w zakresie nieuregulowanym w UODO.

2.3. SZEROKI I NIEOSTRY ZAKRES PRZEDMIOTOWY RODO

Przez „zakres przedmiotowy” należy rozumieć, zgodnie z § 3 ust. 2 Zasad techniki prawodawczej, „stosunki, które [dany akt prawny] reguluje”²¹⁸. Zakres przedmiotowy RODO sformułowany został w sposób szeroki (podobnie jak zakres przedmiotowy Dyrektywy ODO²¹⁹ i UODO²²⁰). Jest to uzasadniony zabieg, którego celem jest możliwe szeroka ochrona

²¹⁸ G. Wierczyński, Komentarz do rozporządzenia w sprawie „Zasad techniki prawodawczej” [w:] Redagowanie i ogłaszanie aktów normatywnych. Komentarz, Warszawa 2016, Załącznik 1 § 3, pkt 6.

²¹⁹ Por. art. 2 lit. a Dyrektywy ODO.

²²⁰ Por. art. 2 i 6 UODO97.

podstawowych praw i wolności osób fizycznych, w tym praw do ochrony danych osobowych (art. 1 ust. 2 RODO). Konsekwencją tego jest jednak nieostry²²¹ zakres przedmiotowy RODO, co oznacza, że z przyczyn semantycznych niepewnym jest jakie to dokładnie stosunki objęte są zakresem przedmiotowym RODO, a w konsekwencji zaistnienie jakich stosunków powoduje konieczność wypełnienia obowiązków ustanowionych w RODO. W tym podrozdziale zbadano definicję „przetwarzania danych osobowych” jako pojęcia kluczowego dla ustalenia zakresu przedmiotowego RODO z uwzględnieniem różnicy między „danymi osobowymi” i „danymi nie-osobowymi” oraz scharakteryzowano ujęcie danych osobowych w wymiarze ekonomicznym jako aktywa niematerialnego kluczowego dla transformacji cyfrowej.

Materialny zakres zastosowania określony został w art. 2 ust. 1, zgodnie z którym RODO „ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych”. W ustępie 2 wprowadzono cztery wyłączenia: 1) w ramach działalności nieobjętej zakresem prawa UE (np. sprawy bezpieczeństwa narodowego²²²); 2) w ramach wykonywania działań zewnętrznych UE i wspólnej polityki zagranicznej oraz bezpieczeństwa; 3) przez osobę fizyczną w ramach czynności o „czysto osobistym lub domowym charakterze”²²³; 4) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar²²⁴. Ustęp 3 rozstrzyga, że przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne UE uregulowane jest odrębnie; obecnie jest to uregulowane w EUDPR. Granica tych wyłączeń, zwłaszcza trzeciego i czwartego, jest dyskusyjna²²⁵. Z tak zidentyfikowanego materialnego zakresu wynika w uproszczeniu, że RODO – z uwzględnieniem dyskusyjnych

²²¹ W przedmiocie terminów nieostrych i zbiorów rozmytych w logice por. J. Hertrich-Woleński, *Nieostrość I Definicje Regulujące* [w:] *Odmiany współczesnej nauki o polityce*, red. P. Borowiec, R. Kłosowicz, P. Ścigaj, 1:315–28. Kraków 2014; U. Wybraniec-Skardowska, *O konceptualizacji wiedzy nieostrej*, „Filozofia Nauki” 1996, t. 4, nr. 3, s. 45–62.

²²² Por. P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, art. 2, pkt 11, SIP LEX.

²²³ To wyłączenie znane jest w literaturze anglojęzycznej jako tak zwane *household exemption*. Granice tego wyłączenia są niejasne i rozumiane są zawężająco, por. B. van de Sloot, *Home Is Where the Heart Is: The Household Exemption in the 21st Century*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law” 2023, Vol.14, No. 1, s. 34–53.

²²⁴ Jest to unormowane przez Dyrektywę LED i Ustawę LED. O dyskusyjnej relacji zakresu RODO do zakresu Dyrektywy LED w podrozdziale 2.5. powyżej. Por. także M. Brewczyńska, *A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation* [in:] *Research handbook on EU data protection law*, Cheltenham 2022, s. 91–114.

²²⁵ Patrz dwa powyższe przypisy.

wyłączeń – ma zastosowanie do każdego przetwarzania danych osobowych żyjących (por. motyw 27 RODO) osób fizycznych w ramach czynności innych niż „o czysto osobistym lub domowym charakterze”, chyba, że przetwarzane dane miałyby nie stanowić zbioru danych (zdefiniowany w art. 4 pkt 6 RODO), co jednak w rzeczywistości transformacji cyfrowej należy uznać za sytuację bardzo rzadką dotyczącą jedynie pojedynczych danych osobowych przetwarzanych manualnie i wypadkowo²²⁶, a na potrzeby niniejszej pracy pomijalną.

Kluczowym dla ustalenia materialnego zakresu RODO jest ustalenie znaczenia „przetwarzania danych osobowych”, która to fraza zbudowana jest z dwóch terminów: „przetwarzania” i „danych osobowych”. Oba te terminy zdefiniowane zostały w RODO. Przetwarzanie to, zgodnie z art. 4 pkt 1 RODO, każda „operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany”, co uzupełniono przykładami takimi jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie i pobieranie. Definicję tę należy ocenić jako szeroką i w taki sposób wyklądać, co odpowiada – jak wskazano wyżej – celowi zapewnienia ochrony praw podstawowych. Podane przykłady należy uzupełnić o orzecznictwo TSUE na gruncie Dyrektywy ODO aktualne także pod rządami RODO, np. umieszczanie danych na stronie internetowej²²⁷, ujawnianie danych przez wyszukiwarkę internetową w formie wyników wyszukiwania²²⁸ i transfer danych do państwa trzeciego^{229,230}.

Znacznie większy problem stanowi analiza pojęcia danych osobowych. Wyczerpująca analiza pojęcia danych osobowych jest tak obszerna, że wymagałaby przygotowania odrębnej rozprawy doktorskiej. W tym podrozdziale celem jest wykazanie, że jest to pojęcie niejednoznaczne, a zakres znaczeniowy terminu „danych osobowych” jest nieostry, co powoduje, że nieostry jest także zakres przedmiotowy RODO, który wyznaczany jest właśnie przez zakres znaczeniowy danych osobowych. Nieostrą i szeroką definicję sformułowano w art. 4 pkt 1 RODO. Zgodnie z nią, są to „wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”, przy czym „możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować”. Taką osobę

²²⁶ D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018, art. 2, pkt 13, SIP LEX.

²²⁷ Wyrok TSUE, C-101/01, Lindqvist, 6.11.2003, p. 25.

²²⁸ Wyrok TSUE, C-131/12, Google Spain, 13.05.2014, p. 26-31.

²²⁹ Wyrok TSUE, C-362/14, Schrems I, 6.10.2015, p. 45.

²³⁰ Przywołanie trzech powyższych przykładów orzecznictwa za: *Article 4(2). Processing*, [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. by Ch. Kuner et al., Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 17.01.2024 r.), s. 120.

nazywa się „osobą, której dane dotyczą” lub „podmiotem danych”. Definicja ta uzupełniona jest o bardziej lub mniej oczywiste przykłady: „imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”²³¹. Należy podkreślić, że RODO osobno definiuje dane dotyczące zdrowia²³², dane biometryczne²³³ i dane genetyczne²³⁴, które zaliczają się do szczególnych kategorii danych (art. 9 ust. 1 RODO), co oznacza, że ich ochrona jest wzmocniona przez wprowadzenie dodatkowych obowiązków związanych z ich przetwarzaniem.

Definicja „danych osobowych”²³⁵ jest czteroelementowa²³⁶: „wszelkie informacje”, „o” (*relating to*), „osobie fizycznej”, „zidentyfikowanej lub możliwej do zidentyfikowania”. Prawodawca unijny użył wyrażenia „wszelkie informacje”, aby podkreślić, że chodzi o informacje dotyczące każdego aspektu osoby fizycznej²³⁷. Należy zgodzić się z poglądem P. Fajgielskiego, że użycie terminu „informacja” stanowi uproszczenie, a pojęcia danych i informacji – wbrew propozycji prawodawcy – nie można używać zamiennie, ponieważ jego znaczenie jest odmienne w różnych dyscyplinach naukowych²³⁸, np. w informatyce przyjmuje się, że komunikat zawiera informację o ile redukuje niepewność²³⁹, w przeciwnym wypadku dane (symbole z alfabetu „utrwalone na nośniku celem reprezentowania czegoś”²⁴⁰) nie mają charakteru informacji. W kontekście przetwarzania danych przez „informację” rozumieć

²³¹ Mogą to być także informacje nieprawdziwe czy subiektywne, np. oceny pracownika lub ucznia. Por. M. Czerniawski, *Pisemne odpowiedzi egzaminowanego oraz komentarze egzaminatora jako dane osobowe. Glosa do wyroku TS z dnia 20 grudnia 2017 r.*, C-434/16, SIP LEX/el. 2018.

²³² Art. 4 pkt 15 RODO. Pojęcie danych dotyczących zdrowia (nazywanych także danymi medycznymi) jest również niejednoznaczne.

²³³ Art. 4 pkt 14 RODO. Por. K. Gałęzowska, *Dane biometryczne a dane behawioralne*, MoP 2022, nr 21, s. 2079.

²³⁴ Art. 4 pkt 13 RODO.

²³⁵ Zasadniczo analogiczna do definicji z art. 2 lit. a Dyrektywy ODO.

²³⁶ Grupa Robocza, *Opinion No. 4/2007 on the concept of personal data*, WP 136, 20.06.2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, s. 25 (dostęp: 1.09.2024 r.).

²³⁷ E. Kuczkowska, *Glosa aprobowująca do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13 kwietnia 2021 r.*, sygn. akt II SA/Wa 1898/20, RAiP 2021, nr 3, s. 269-279, s. 272, przypisy 6 i 7 i przywołana tam literatura.

²³⁸ P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2022, art. 4, pkt 4, SIP LEX.

²³⁹ *Informacja*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 204.

²⁴⁰ *Dane*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 97.

należy jednak wszelkie formy komunikatów wyrażone lub zapisane w dowolny sposób²⁴¹. Jest to zatem szerokie rozumienie tego terminu. W odniesieniu do drugiego elementu, czyli „o” („*relating to*” czyli raczej „dotyczący” osoby fizycznej), Grupa Robocza wyróżniła trzy typy związku między informacją a osobą fizyczną, które powodują, że ten element jest spełniony: 1) treść informacji – kiedy informacja w swojej treści odnosi się wprost do tożsamości osoby fizycznej; 2) cel informacji – kiedy informacja przez cel jej przetwarzania może służyć do oceny lub wpływu na zachowanie osoby fizycznej; 3) skutek informacji –kiedy informacja nie odnosi się wprost do tożsamości osoby fizycznej, ani nie jest nakierowana na powyższy cel, ale jest prawdopodobne, że jej przetwarzanie może mieć wpływ na prawa lub wolności osoby fizycznej²⁴². To stanowisko Grupy Roboczej znajduje potwierdzenie w orzecznictwie TSUE²⁴³. Tak jak w przypadku „informacji”, element „o” (osobie fizycznej) interpretować należy zatem w sposób szeroki.

Trzeci element, tj. „osoba fizyczna”, oznacza, że danymi osobowymi w rozumieniu RODO nie są dane dotyczące podmiotów innych niż osoby fizyczne, np. osób prawnych, ale są nimi już dane osób fizycznych prowadzących jednoosobową działalność gospodarczą²⁴⁴. Nie są nimi także dane dotyczące osób zmarłych (por. motyw 27 RODO). Najbardziej dyskutowanym elementem definicji „danych osobowych” jest przesłanka „zidentyfikowania lub możliwości zidentyfikowania” osoby fizycznej. Samo „zidentyfikowanie osoby fizycznej” nie powoduje znacznych trudności. Oznacza natychmiastowe ustalenie tożsamości konkretnej osoby fizycznej na podstawie tych informacji, bez potrzeby dalszych działań²⁴⁵. Wyzwanie powoduje natomiast interpretacja „możliwości zidentyfikowania”. Jeszcze na gruncie

²⁴¹ P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2022, art. 4, pkt 4, SIP LEX.

²⁴² Grupa Robocza, *Opinion No. 4/2007 on the concept of personal data*, WP 136, 20.06.2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, s. 25 (dostęp: 2.09.2024 r.).

²⁴³ Wyrok TSUE, C-434/16, Nowak, 20.12.2017, p. 35. Wyrok przywołany za L. A. Bygrave, L. Tosoni, *Article 4(1). Personal data* [in:], *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 19.01.2024 r.), s. 110.

²⁴⁴ Council of Europe, European Court of Human Rights, European Data Protection Supervisor and European Union Agency for Fundamental Rights, *Handbook on European data protection law – 2018 edition*, Publications Office of the European Union, 2018, s. 95-96. Patrz w odniesieniu do firmy osoby prawnej, w której umieszczono imię i nazwisko osoby fizycznej: TSUE, C-92/09 i C-93/09, Volker, 9.11.2010, p. 53.

²⁴⁵ P. Litwiński [w:] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), red. P. Litwiński [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński art. 4, pkt 13 (nb 13), SIP Legalis.

Dyrektywy ODO było to przedmiotem dyskusji w literaturze niemieckiej²⁴⁶ w kwestii „obiektywnego” albo „subiektywnego” (czyli uzależnionego od dostępu podmiotu identyfikującego do środków to umożliwiających) charakteru możliwości identyfikacji, w odniesieniu do której TSUE w wyroku *Breyer* przychylił się do zobiektywizowanej, ale złagodzonej wersji. Jej kwintesencją jest, że o spełnieniu tego elementu nie decyduje istnienie abstrakcyjnie rozumianego dostępu do wszelkich możliwych środków, lecz do tych, którymi podmiot identyfikujący mógłby się posłużyć²⁴⁷. W odniesieniu do aktualności tego poglądu w stanie prawnym po wejściu w życie RODO podnoszono, że brzmienie nowego (zmienionego względem motywu 26 Dyrektywy ODO) motywu 26 RODO wskazuje raczej na wybór subiektywnego rozumienia „możliwości identyfikacji”²⁴⁸ przez prawodawcę unijnego, chociaż pozostaje to przedmiotem dyskusji, zwłaszcza w kontekście rozbieżności w orzecznictwie²⁴⁹. Pomocny w wykładni winien być właśnie motyw 26 RODO, zgodnie z którym „należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej”. Pomimo tego, w literaturze wskazuje się wciąż, że nie jest możliwe jednoznaczne ustalenie *a priori*, jaka kategoria informacji stanowi dane osobowe²⁵⁰. Ponadto, sformułowano tezę o relatywizacji pojęcia danych osobowych rozumianej jako traktowanie tej samej informacji jako stanowiącej dane osobowe zależnie od tego, jaki podmiot dokonuje jej przetwarzania, wskazując na rozbieżności w orzecznictwie w odniesieniu do „subiektywnego” lub „obiektywnego” rozumienia identyfikacji i postulując wydanie przez EROD kompleksowej opinii w przedmiocie zakresu znaczeniowego terminu „danych osobowych”²⁵¹.

²⁴⁶ Por. Opinia Rzecznika Generalnego w sprawie C-582/14, Breyer, 12.05.2016, ECLI:EU:C:2016:339, p. 23-24.

²⁴⁷ Wyrok TSUE z 19.10.2016 r., C-582/14, BREYER, pkt. 44 i 49; D. Lubasz, A. Szkurlat, *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, MoP 2021, nr 23, s. 78.

²⁴⁸ P. Litwiński, Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych. Glosa do wyroku TS z dnia 19 października 2016 r., C-582/14, EPS 2017, 5, 49-54, s. 54.

²⁴⁹ D. Lubasz, A. Szkurlat, *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, MoP 2021, nr 23, s. 80.

²⁵⁰ Rozdział I. Dane osobowe, pseudonimizacja i anonimizacja. 1. Pojęcie danych osobowych [w:] *Ochrona danych osobowych w sektorze publicznym*, red. P. Litwiński, Waszawa 2022, SIP Legalis.

²⁵¹ D. Lubasz, A. Szkurlat, *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, MoP 2021, nr 23, s. 77 i następne; oraz przywołane tam orzecznictwo. Por. także A. El Khoury, *Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat*, Eur. J. Risk Regul. 2017, Vol. 8, No. 1, <https://doi.org/10.1017/err.2016.26> (dostęp: 20.09.2024 r.), s. 191-197, gdzie posłużono się użytecznym porównaniem do eksperymentu kota Schrödingera w fizyce kwantowej. F.J.Z. Borgesius, *Singling out people without knowing their names—Behavioural targeting, pseudonymous data, and the new Data Protection Regulation*, „Computer Law & Security Review” 2016, 32(2), s. 256-271.

Istotnie, w orzecznictwie sądów unijnych i krajowych pojęcie danych osobowych jest rozumiane szeroko i polega relatywizacji w powyższym rozumieniu. Sądy rozstrzygały, że dane osobowe mogą stanowić, np. numery ksiąg wieczystych²⁵², numery tablic rejestracyjnych pojazdów mechanicznych (choć istnieją sprzeczne linie orzecznicze w polskich sądach administracyjnych)²⁵³, odpowiedzi osoby egzaminowanej i komentarze egzaminatora²⁵⁴, czy numer umowy kredytowej (z perspektywy banku będącego kredytodawcą)²⁵⁵. O słuszności porównania dokonywania kwalifikacji danej informacji jako „danych osobowych” do eksperymentu kota Schrödingera w fizyce kwantowej²⁵⁶ świadczą dwa wyroki wydane przez sądy unijne w 2023 r. Zgodnie z wyrokiem TSUE z 9.11.2023 r. w sprawie *Gesamtverband Autoteile-Handel*, numer VIN (numer identyfikacji pojazdu) stanowi dane osobowe, o ile „osoba mająca do niego dostęp mogłaby dysponować środkami umożliwiającymi wykorzystanie go w celu zidentyfikowania właściciela pojazdu, do którego odnosi się, lub osoby, która może użytkować ten pojazd na podstawie tytułu prawnego innego niż prawo własności”²⁵⁷. Natomiast zgodnie z wyrokiem Sądu (*the General Court*) z 26.04.2023 w sprawie SRB rozstrzygnięto, że o tym czy przekazane informacje (podlegające uprzedniej pseudonimizacji) stanowią „dane osobowe” decyduje możliwość odbiorcy do przypisania tej informacji do osób fizycznych²⁵⁸.

Ostatnie z przywołanych orzeczeń sądów unijnych prowadzi do uwagi, że zakresem materialnym RODO nie są objęte dane anonimowe (por. motyw 26 RODO), chociaż objęte są nim już dane pseudonimizowane, który to proces definiowany jest w RODO jako

²⁵² Na przykład: wyrok NSA z 26.09.2018 r., I OSK 11/17, SIP LEX nr 2573629; wyrok WSA w Warszawie z 5.05.2021 r., II SA/Wa 2222/20, SIP LEX nr 3209095;

²⁵³ Za A. Partyk, T. Partyk, *Numer rejestracyjny pojazdu jako dane osobowe*, SIP LEX/el. 2020, por: Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 13.04.2017 r., VII SA/Wa 1069/16; Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 25.04.2014 r., II SA/Wa 30/14. Także (przywołanie za M. Gawroński, *Prezentacja w czasie Konferencji Urzędu Ochrony Danych Osobowych „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów”*, 31.03.2023, <https://uodo.gov.pl/pl/file/4249>); wyrok Sądu Administracyjnego w Kolonii, Niemcy, 16.02.2017 r., 13 K 6093/15, wyrok Wyższego Sądu Administracyjnego w Münster, Niemcy, 19.10.2017 r. 16 A 770/17.

²⁵⁴ Wyrok TSUE z 20.12.2017 r., C-434/16, Peter Nowak v. Data Protection Commissioner, ZOTSiS 2017, nr 12, poz. I-994.

²⁵⁵ Wyrok WSA w Warszawie z 22.04.2021 r., II SA/Wa 1865/20, SIP LEX nr 3178526. D. Karwala, A. Zdanczyc-Leśniak, *Numer umowy kredytowej jako dane osobowe. Glosa do wyroku WSA z dnia 22 kwietnia 2021 r., II SA/Wa 1865/20*, M.Pr.Bank. 2022, nr 2, s. 61-71.

²⁵⁶ A. El Khoury, *Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat*, Eur. J. Risk Regul. 2017, Vol. 8, No. 1, <https://doi.org/10.1017/err.2016.26> (dostęp: 20.09.2024 r.). Por. także A. El Khoury, *Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data through Quantum Mechanics*, „Erasmus Law Review” 2018, Vol. 11, No 3, s. 165-177.

²⁵⁷ Wyrok TS z 9.11.2023 r., C-319/22, *Gesamtverband Autoteile-Handel E.V. przeciwko Scania CV AB*, SIP LEX nr 3622953, pkt 48.

²⁵⁸ Wyrok S(Pi) z 26.04.2023 r., T-557/20, *Jednolita Rada Ds. Restrukturyzacji i Uporządkowanej Likwidacji przeciwko Europejskiemu Inspektorowi Danych*, SIP LEX nr 3523116, pkt 96-97.

„przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej” (art. 4 pkt 5 RODO). W tym rozumieniu, pseudonimizacja stanowi jedną z technik, której zastosowanie zwiększa bezpieczeństwo przetwarzania danych, ale nie powoduje wyłączenia obowiązywania RODO. Dane zanonimizowane są natomiast danymi nieosobowymi (por. art. 3 pkt 1 Rozporządzenia Dane Nieosobowe w zw. z art. 2 pkt 1 Data Act), których przetwarzanie nie podlega RODO. W literaturze słusznie argumentuje się jednak, że skuteczna anonimizacja informacji stanowiących dane osobowe jest technicznie trudna²⁵⁹, a nadto w kontekście rozwoju nowych technik, np. w dziedzinie informatyki kwantowej, poprzednio prawidłowo wybrane i zastosowane metody anonimizacji mogą okazać się nieskuteczne, prowadząc do identyfikacji osób fizycznych, co uczyni te informacje na powrót danymi osobowymi²⁶⁰. Oznacza to, że wyznaczenie granicy między danymi osobowymi a danymi nieosobowymi (granicy zakresu przedmiotowego RODO) jest trudne²⁶¹. Zgodnie z art. 2 ust. 2 Rozporządzenia Dane Nieosobowe, do zbiorów danych zawierających dane osobowe i nieosobowe do części zbioru złożonej z danych nieosobowych zastosowanie ma tylko Rozporządzenie Dane Nieosobowe, ale już w przypadku zbiorów z danymi nieosobowymi i osobowymi nierozzerwalnie ze sobą związanymi, do całego zbioru zastosowanie znaleźć powinno RODO. Tak szerokie i nieostre pojmowanie danych osobowych ma konsekwencje dla dogmatycznych prób systematyzacji aktów prawnych w obszarze przetwarzania danych osobowych i wyróżnienia osobnej kompleksowej gałęzi prawa, na przykład „prawa ochrony danych osobowych” (szerzej w tej kwestii w podrozdziale 5.5.).

²⁵⁹ Por. Z. He, *From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law*, „Digital Society” 2023, Vol. 2, <https://doi.org/10.1007/s44206-023-00043-5> (dostęp: 20.09.2024 r.). E. M Weitzenboeck, P. Lison, M. Cyndecka et al., *The GDPR and unstructured data: is anonymization possible?*, Int. Data Priv. Law 2022, t. 12, nr 3, <https://doi.org/10.1093/idpl/ipac008> (dostęp: 20.09.2024 r.), s. 184–206. Por. także: Grupa Robocza, *Opinion 05/2014 on Anonymisation Techniques*, WP216, 10.04.2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (dostęp: 20.09.2024 r.).

²⁶⁰ M. Finck, F. Pallas, *They who must not be identified—distinguishing personal from non-personal data under the GDPR*, Int. Data Priv. Law 2020, Vol.10, Iss. 1, <https://doi.org/10.1093/idpl/ipz026> (dostęp: 20.09.2024 r.), s. 16.

²⁶¹ M. Finck, F. Pallas, *They who must not be identified—distinguishing personal from non-personal data under the GDPR*, Int. Data Priv. Law 2020, Vol.10, Iss. 1, <https://doi.org/10.1093/idpl/ipz026> (dostęp: 20.09.2024 r.), s. 36: „If it could never be taken for granted that personal data has been successfully transformed into non-personal data, then any information that was ever in the scope of the GDPR would need to be presumed to forever remain within that scope”. („Jeżeli nigdy nie będzie można przyjąć za pewnik, że dane osobowe zostały skutecznie zamienione w dane nieosobowe, wówczas należałoby założyć, że wszelkie informacje, które kiedykolwiek wchodziły w zakres RODO, na zawsze pozostaną w tym zakresie.”).

Scharakteryzowane wyżej pojęcie danych osobowych jest refleksem perspektywy prawno-człowieczej, która stanowi podstawę dla ochrony tych danych w RODO. Jednak dane osobowe, będąc przedmiotem tej ochrony, stanowią także aktywo niematerialne istotne dla gospodarki transformacji cyfrowej²⁶² i reprezentują tym samym znaczną wartość ekonomiczną²⁶³. Ta perspektywa – chociaż wykracza poza rozumienie danych osobowych w RODO²⁶⁴ – pozostaje istotna dla innych kompleksowych gałęzi prawa, np. prawa konkurencji²⁶⁵ w odniesieniu do oceny nadużycia pozycji dominującej²⁶⁶ i kontroli koncentracji²⁶⁷. Ten „podwójny charakter” danych osobowych – jako przedmiotu ochrony prawno-człowieczej i jednocześnie aktywa niematerialnego – powoduje krzyżowanie się zakresu przedmiotowego RODO i prawa konkurencji, które poddano analizie w podrozdziale 2.6.3. poniżej. Konkludując wątek zakresu przedmiotowego RODO, w literaturze sformułowano propozycję, aby w kontekście danych osobowych stanowiących „przedmiot własności” traktować je jako „aktywo systemowe” w tym sensie, że ich wartość ekonomiczna nie wynika z tego, że są zindywidualizowaną informacją, ale z tego, że stanowią element zbioru, który z kolei używany jest w określonym układzie ekonomicznym, na przykład przez sieci społecznościowe²⁶⁸.

2.4. SZEROKI I NIEOSTRY ZAKRES PODMIOTOWY RODO

Zakres podmiotowy aktu prawnego to „krąg podmiotów, do których [akt prawny] się odnosi” (§ 3 ust. 2 *in fine* Zasad Techniki Prawodawczej). Zakres podmiotowy RODO wyznaczony jest przez pojęcia „osoby, której dane dotyczą”, „administratora”,

²⁶² Por. S. K. Chakraborty, A. K. Koshy, A. Raghunath, *Data As Property: Towards a Property Based Model?*, „Global Privacy Law Review” 2023, Vol. 4, Iss. 4, <https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/4.4/GPLR2023025> (dostęp: 20.09.2024 r.), s. 181-193.

²⁶³ J. Grzeszak, K. Łukasik, I. Święcicki, *Ile warte są nasze dane?*, Warszawa: Polski Instytut Ekonomiczny 2021, https://pie.net.pl/wp-content/uploads/2022/01/PIE-Raport_Wartosc_danych.pdf (dostęp: 20.09.2024 r.). Zgodnie z tym dokumentem, wartość danych polskich użytkowników dla Google wyniosła ponad 4 mld PLN.

²⁶⁴ Por. B. Custers, G. Malgieri, *Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data*, CLSR 2022, Vol. 45.

²⁶⁵ Por. przykładowo Ch. Ducuing, *Data as infrastructure? A study of data sharing legal regimes*, „Competition and Regulation in Network Industries” 2020, Vol. 21, No 2, s. 124-142.

²⁶⁶ K. Singh; S. Mishra, *Mapping the Inter-Relation of Abuse of Dominant Position and Merger Control RegimeIs Big Data: The Curious Case of WhatsApp Privacy Policy*, „Journal of National Law University Delhi” 2020, Vol. 7, Iss. 1-2, s. 62-65.

²⁶⁷ K. Singh; S. Mishra, *Mapping the Inter-Relation of Abuse of Dominant Position and Merger Control RegimeIs Big Data: The Curious Case of WhatsApp Privacy Policy*, „Journal of National Law University Delhi” 2020, Vol. 7, Iss. 1-2, s. 66-69.

²⁶⁸ N. Purtova, *The Illusion of Personal Data as No One's Property*, *Law Innov. Technol.* 2015, Vol. 7, No. 1, <https://doi.org/10.1080/17579961.2015.1052646> (dostęp: 20.09.2024 r.), s. 109.

„współadministratora” i „podmiotu przetwarzającego”. Pojęcie „osoby, której dane dotyczą” (podmiotu danych) zostało zbadane przy dokonywaniu charakterystyki zakresu przedmiotowego RODO. Zakres podmiotowy RODO w pozostałym zakresie scharakteryzowany jest syntetycznie poniżej.

Zgodnie z art. 4 pkt 7 RODO, administrator to „osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych”. Z kolei współadministratorami jest co najmniej dwóch administratorów, jeżeli – zgodnie z art. 26 ust. 1 RODO – „wspólnie ustalają cele i sposoby przetwarzania”, co nakłada na nich obowiązek wspólnego uzgodnienia zakresu odpowiedzialności za wypełnianie obowiązków ustanowionych w RODO. Podmiotem przetwarzającym jest natomiast (por. art. 4 pkt 8 RODO), „osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora”, co najczęściej wymaga zawarcia umowy powierzenia przetwarzania danych (art. 28 ust. 3 RODO).

Z zestawienia tych definicji wynika, że kluczowym dla ustalenia zakresu znaczeniowego tych terminów jest element „ustalania celów i sposobów przetwarzania”²⁶⁹. Podobnie jak zakres przedmiotowy RODO, tak również zakres podmiotowy RODO interpretowany jest w sposób rozszerzający, aby zapewnić możliwie pełną ochronę praw i wolności podmiotów danych²⁷⁰. Jak wskazała O. Lyskey, z orzecznictwa TSUE w sprawach dotyczących zakresu podmiotowego RODO wynika, że próg uznania danego podmiotu za administratora jest niski, a relacja między pojęciem „administratora” a pojęciem „współadministratora” pozostaje niejasna, to jest dyskusyjne jest, jak wyznaczyć granicę zakresów obu tych pojęć, której przekroczenie powoduje, że ustalenie celów i sposobów przetwarzania jest już uznane za „wspólne”²⁷¹. Przykładowo²⁷², TSUE w sprawie *Wirtschaftsakademie* za administratora (współadministratora) uznał administratora fanpage’a, czyli strony na portalu społecznościowym Facebook w zakresie gromadzenia danych osobowych odwiedzających ten

²⁶⁹ Por. M. Czerniawski, Rozdział II. Instytucja współadministrowania a pojęcie „ustalania” celów i sposobów przetwarzania danych osobowych – zarys problemu [w:] Rok RODO, red. W. Wiewiórowski, H. Wolska, Warszawa 2019, SIP Legalis.

²⁷⁰ Por. EROD, *Wytyczne 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO*, Wersja 2.0, 07.07.2021, pkt 14, s. 10, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en, (dostęp: 8.09.2024 r.); por. także przywołane tam orzecznictwo: wyrok TSUE, C-210/16, *Wirtschaftsakademie*, 05.06.2018, pkt 28; wyrok TSUE, C-40/17, *Fashion ID*, 29.07.2019, pkt 66.

²⁷¹ O. Lyskey, *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.), s. 307-313.

²⁷² Oba przykładowe orzeczenia wydano na gruncie Dyrektywy ODO, w której nie użyto terminu „współadministrator”.

fanpage przez ten portal danych w celu statystyki odwiedzających użytkowników²⁷³. W podobnym kierunku TSUE zawyrokował w sprawie *Fashion ID*, rozstrzygając, że status administratora (współadministratora) uzyskuje podmiot, która „umieszcza na swojej stronie internetowej wtyczkę osoby trzeciej (która to osoba trzecia udostępniła ową wtyczkę), co skutkuje gromadzeniem i przekazywaniem danych osobowych użytkownika”, przy czym status współadministratora ograniczony jest tylko do tego przetwarzania, którego „współokreśla on sposoby i cele”²⁷⁴. Oznacza to, że uzyskanie statusu współadministratora (a w konsekwencji zostanie objętym obowiązkami przewidzianymi w RODO) możliwe jest także w sytuacjach, w których dany podmiot (współ)decyduje w jedynie niewielkim zakresie całego ciągu czynności przetwarzania, nie mając przy tym wpływu na dalsze czynności przetwarzania²⁷⁵.

Podsumowując, szeroki i nieostry zakres przedmiotowy i podmiotowy RODO wynikający z brzmienia samego RODO, poprzedzającej ją Dyrektywy ODO oraz orzecznictwa sądów unijnych i krajowych powoduje, że nie można jednoznacznie z góry ustalić, do jakich stosunków i do jakich podmiotów RODO ma zastosowanie. Tego ustalenia trzeba dokonywać *ad casum*, a jego wynik może zmieniać się w zależności od kręgu podmiotów, które mają dostęp do informacji, jak i zmieniać się w czasie w zależności od postępu technicznego. Powoduje to i powodowało będzie w konsekwencji nie tylko krzyżowanie się zakresu przedmiotowego RODO z innymi aktami prawnym w obszarze przetwarzania danych osobowych, ale również niepewność zarówno po stronie podmiotów danych, podmiotów nadzorowanych jak i organów administracji publicznej ustanowionych na podstawie aktów w obszarze przetwarzania danych osobowych do zakresu i treści ich praw i obowiązków oraz kompetencji.

²⁷³ Wyrok TSUE z 5.06.2018 r., C-210/16, Unabhängiges Landeszentrum Für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, ZOTSiSPI 2018, nr 6, poz. I-388, pkt. 137. Por. także trzy oroblemu do tego wyroku: M. Czerniawski, *Odpowiedzialność administratora fanpage'a na Facebooku za przetwarzanie danych osobowych. Glosa do wyroku TS z dnia 5 czerwca 2018 r.*, C-210/16, SIP LEX/el. 2018. M. Rojszczak, *Odpowiedzialność za przetwarzanie danych przez portal społecznościowy. Glosa do wyroku TS z dnia 5 czerwca 2018 r.*, C-210/16, EPS 2018, nr 10, s. 40-46. S. Żyrek, *Pojęcie administratora danych w przypadku wspólnego ich przetwarzania przez portal społecznościowy i podmioty korzystające z jego usług – wprowadzenie i wyrok Trybunału Sprawiedliwości z 5.06.2018 r.*, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH, EPS 2019, nr 7, s. 52-60.

²⁷⁴ Wyrok TSUE z 29.07.2019 r., C-40/17, Fashion Id GmbH & Co. Kg przeciwko Verbraucherzentrale NRW eV., SIP LEX nr 2701708, p. 142.

²⁷⁵ O. Lyskey, *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.), s. 307-311.

2.5. AKTY PRAWNE PRAWA UNIJNEGO I KRAJOWEGO REGULUJĄCE PRZETWARZANIE DANYCH OSOBOWYCH JAKO OBSZAR REFERENCYJNY

Wybór obszaru referencyjnego w celu weryfikacji głównej hipotezy badawczej tej rozprawy stanowił wyzwanie. Wyzwanie to wynikało z tego, jak liczne są akty prawne unijne i krajowe normujące przetwarzanie danych osobowych oraz jak wiele nowych inicjatyw prawodawczych w tym obszarze²⁷⁶ podjęto na poziomie unijnym po roku 2020, w tym w związku z realizacją nowej unijnej strategii cyfrowej²⁷⁷. Pokazuje to analiza ilościowa w wyszukiwarkach EUR-LEX i SIP LEX przeprowadzona na dzień 18 stycznia 2024 r. W wyszukiwarce EUR-LEX²⁷⁸ zidentyfikowano 119²⁷⁹ obowiązujących aktów prawnych prawa unijnego, w których tytule użyto terminu „*personal data*” („dane osobowe”)²⁸⁰, podczas gdy terminu tego użyto w treści aż w 1.717 takich aktów, w tym w 481 rozporządzeniach²⁸¹

²⁷⁶ Obszar, zgodnie ze *Słownikiem języka polskiego PWN*, należy rozumieć jako „miejsce występowania, zasięgu czegoś”, gdzie w odniesieniu do analizowanego problemu badawczego przez „coś” rozumieć należy „przetwarzanie danych osobowych” scharakteryzowane w podrozdziale 2.3. powyżej.

²⁷⁷ Komisja, *Europa na miarę ery cyfrowej*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en (dostęp: 12.09.2024 r.)

²⁷⁸ W odniesieniu do wyszukiwarki w SIP LEX podkreślić należy, że wynik 1.717 rekordów odnosi się do liczby aktów prawnych (dokumentów), w których wyszukiwany termin został użyty, a nie do liczby użyć tego terminu w tych aktach (dokumentach). Ustalono tego po dokonaniu dodatkowego badania sposobu działania wyszukiwarki.

²⁷⁹ Przykładowo: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance); Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.); Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.); Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation; Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications; Regulation (EU, Euratom) 2019/493 of the European Parliament and of the Council of 25 March 2019 amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament.

²⁸⁰ Wyszukania w EUR-LEX dokonano w języku angielskim, aby zminimalizować ryzyko nieprawidłowości tych wyników w języku polskim z uwagi na odmianę fleksyjną.

²⁸¹ Dziesięć przykładowych rozporządzeń z 2023 r.: Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act); Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings; Regulation (EU) 2023/969 of the European Parliament and of the Council of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726; Regulation (EU) 2023/2859 of the European Parliament and of the Council of 13 December 2023 establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability; Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending

i 159 dyrektywach. Z kolei w SIP LEX w krajowych obowiązujących aktach prawnych w Dzienniku Ustaw i Monitorze Polskim zastosowanie terminu „dane osobowe” zidentyfikowano aż w 1.362 aktach, w tym 559 ustawach²⁸² i 484 rozporządzeniach. Łącznie daje to wynik 3.079 obowiązujących aktów prawnych na poziomie krajowym i unijnym, w których użyto terminu „dane osobowe”. Pozwala to przyjąć, że każdy z tych aktów w większym lub mniejszym stopniu wpływa na unormowanie przetwarzania danych osobowych, a zatem wszystkie te akty należy zaliczyć do aktów w obszarze przetwarzania danych osobowych. O liczbie nowoprzyjętych i projektowanych aktów prawnych na poziomie unijnym w tym obszarze świadczą informacje na stronie Parlamentu Europejskiego *Legislative Carriage* („Wagon Legislacyjny”), na której w zakładce dotyczącej priorytetu Komisji „Europa na miarę ery cyfrowej” wskazano na 115 inicjatyw, z czego jako „inicjatywy o charakterze legislacyjnym” zakwalifikowano 89 pozycji. Z tych pozycji 14 jest „ogłoszonych”, 19 jest „procedowanych”, 4 zostały „zablokowane”, 12 jest „bliskich do przyjęcia”, 34 zostały już przyjęte, a 5 wycofano²⁸³. O tej aktywności prawodawcy unijnego świadczy także to, że EIOD

Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance); Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union; Regulation (EU) 2023/1322 of the European Parliament and of the Council of 27 June 2023 on the European Union Drugs Agency (EUDA) and repealing Regulation (EC) No 1920/2006; Regulation (EU) 2023/1804 of the European Parliament and of the Council of 13 September 2023 on the deployment of alternative fuels infrastructure, and repealing Directive 2014/94/EU (Text with EEA relevance); Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance); Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation.

²⁸² Przykładowo: Ochrona danych osobowych (Dz.U.2019.1781) t.j., ustawa z dnia 10 maja 2018 r.; Ochrona danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2023.1206) t.j., ustawa z dnia 14 grudnia 2018 r.; Ratyfikacja Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r. (Dz.U.2019.2284), ustawa z dnia 16 października 2019 r.; Zmiana niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.2019.730), ustawa z dnia 21 lutego 2019 r.; Prawo budowlane (Dz.U.2023.682) t.j., ustawa z dnia 7 lipca 1994 r.; Statystyka publiczna (Dz.U.2023.773) t.j., ustawa z dnia 29 czerwca 1995 r.; Ochrona zabytków i opieka nad zabytkami (Dz.U.2022.840) t.j., ustawa z dnia 23 lipca 2003 r.; Wsparcie gospodarstw domowych w ponoszeniu kosztów związanych ze zmianą standardu nadawania naziemnej telewizji cyfrowej (Dz.U.2022.1399) t.j., ustawa z dnia 24 lutego 2022 r. Polski Bon Turystyczny (Dz.U.2023.35) t.j., ustawa z dnia 15 lipca 2020 r.; Zwalczanie dopingu w sporcie (Dz.U.2022.1258) t.j., ustawa z dnia 21 kwietnia 2017 r.; Zbiorowe zarządzanie prawami autorskimi i prawami pokrewnymi (Dz.U.2023.2207) t.j., ustawa z dnia 15 czerwca 2018 r.; Usługi zaufania oraz identyfikacja elektroniczna (Dz.U.2021.1797) t.j., ustawa z dnia 5 września 2016 r. Krajowa Administracja Skarbowa (Dz.U.2023.615) t.j., ustawa z dnia 16 listopada 2016 r.; Kodeks pracy (Dz.U.2023.1465) t.j., ustawa z dnia 26 czerwca 1974 r.

²⁸³ Na dzień 18 stycznia 2024 r. EP Legislative Carriage, <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age> (dostęp: 12.09.2024 r.).

w 2023 r. wydał aż 54 opinie do unijnych aktów prawnych, które wpływały na przetwarzanie danych osobowych („które mają wpływ na ochronę praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych”²⁸⁴), podczas gdy w 2022 r. było to 28 opinii, a 2021 r. – tylko 12 opinii²⁸⁵. Oznacza to, że prawodawca unijny w ostatnich latach prowadzi intensywne działania nakierowane na przyjęcie lub zmianę aktów prawnych, które wpływają na unormowanie przetwarzania danych osobowych w UE.

Powyższa analiza prowadzi również do wniosku, że akty regulujące ten obszar można podzielić na takie, których podstawowym celem jest unormowanie przetwarzania danych osobowych, i takie, które normują przetwarzanie danych osobowych jedynie incydentalnie, ponieważ ustanowienie szczególnych rozwiązań dotyczących przetwarzania danych osobowych jest uznawane przez prawodawcę za potrzebne, aby całościowo unormować inny, czasami styczny zakresowo, obszar (sektor gospodarki, np. ochronę zdrowia). W odniesieniu do aktów unijnych zidentyfikowanie podstawy prawnej, na której dany akt został przyjęty, mogłoby być pomocne w zaliczeniu do jednego z tych dwóch typów. Innymi słowy, weryfikacja tego, czy akt został przyjęty na podstawie art. 16 ust. 2 TFUE uprawniającego prawodawcę unijnego do określenia „zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych”, czy podstawę stanowił tylko art. 114 TFUE uprawniający do przyjęcia aktów prawnych nakierowanych na „ustanowienie i funkcjonowanie rynku wewnętrznego”.

Jako obszar referencyjny dla prowadzonych badań wybrane zostały unijne i krajowe akty regulujące przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu (Dyrektywa AML IV, Dyrektywa AML V i Dyrektywa AML VI oraz Ustawa o AML), cyberbezpieczeństwo (Dyrektywa NIS, Dyrektywa NIS 2 i UKSC), prawo konkurencji (art. 102 TFUE, Merger Control Regulation, Rozporządzenie 1/2003 i UKK), Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych²⁸⁶, sztuczną inteligencję (AI Act) oraz europejskie przestrzenie danych (Akt w Sprawie Zarządzania Danymi i Akt w Sprawie Danych). Decyzję o wyborze tych, a nie innych aktów prawnych podjęto przy uwzględnieniu szeregu kryteriów. Zarówno wybór określonych aktów prawnych, jak i niewybranie niektórych aktów wyjaśnione zostało poniżej. Niezależnie jednak od tych wyjaśnień, przy tak znacznej liczbie aktów

²⁸⁴ Por. art. 42 ust. 1 EUDPR.

²⁸⁵ EIOD, *Opinie*, https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_en (12.09.2024 r.).

²⁸⁶ Zaliczenie obu tych aktów do prawa konkurencji jest dyskusyjne.

prawnych w tym obszarze spodziewanym i uzasadnionym jest, że możliwe byłoby dokonanie innego, równorzędnego jakościowo wyboru, które również doprowadziłby do weryfikacji głównej hipotezy badawczej.

Wpierw należy uzasadnić, dlaczego porównanie zakresów przedmiotowych RODO i innych aktów jest niezbędne do weryfikacji głównej hipotezy, która dotyczy przecież kompetencji organów, czyli prawa ustrojowego, a nie prawa materialnego. Prawodawca unijny i krajowy ustanowił organy administracji publicznej na podstawie tych aktów i wyposażył je w kompetencje, rozumiane jako całokształt ich uprawnień i obowiązków, w celu osiągnięcia rezultatu, który można określić jako zapewnienie prawidłowej realizacji danego aktu prawnego przez podmioty nadzorowane. Stąd też, istotą kompetencji ogólnej tych organów jest „monitorowanie i egzekwowanie” (por. art. 57 ust. 1 lit a RODO) prawidłowego wykonywania obowiązków nałożonych przez te akty prawne na te podmioty²⁸⁷. W takim wypadku zakres kompetencji tych organów wyznaczony jest przez zakres obowiązków podmiotów nadzorowanych, który z kolei wyznaczony jest przez zakres przedmiotowy tych aktów rozumiany, jak wskazano wyżej, jako „stosunki, które [akt prawny] reguluje”²⁸⁸ (por. § 3 ust. 2 Zasad Techniki Prawodawczej). Tylko w odniesieniu do stosunków, które akty te regulują, podmioty nadzorowane mają obowiązki w nich określone. Jak wskazano we Wprowadzeniu, prawodawca w obszarze referencyjnym preferuje użycie norm-zasad, terminów nieostrych (np. „ryzyko” w podejściu opartym na ryzyku w RODO) i neutralności technologicznej, czego nieuniknioną konsekwencją jest nieostry zakres przedmiotowy i podmiotowy tych aktów (jak wykazano wyżej w odniesieniu do RODO), a zatem także nieostry zakres i treść obowiązków podmiotów nadzorowanych. Skoro zakres i treść obowiązków podmiotów nadzorowanych jest nieostra, a „monitorowanie i egzekwowanie” prawidłowego ich wykonywania jest kompetencją ogólną tych organów, to oznacza, że zakres kompetencji organów wyznaczony jest przez nieostry zakres przedmiotowy tych aktów. Jeżeli zatem ustalono, że zachodzi krzyżowanie się zakresów przedmiotowych tych aktów, to oznacza także, że zachodzi krzyżowanie się kompetencji tych organów.

Wymaga wyjaśnienia, że przez krzyżowanie się (nachodzenie na siebie) zakresów przedmiotowych aktów prawnych należy rozumieć sytuację, w którym co najmniej dwa akty prawne normują ten sam stosunek²⁸⁹, przy czym do spełnienia tej definicji nie jest konieczne,

²⁸⁷ Por. rozdział 3. Rozprawy, gdzie scharakteryzowano kompetencje tych organów.

²⁸⁸ G. Wierczyński [w:] Komentarz do rozporządzenia w sprawie „Zasad techniki prawodawczej” [w:] Redagowanie i ogłaszanie aktów normatywnych. Komentarz, Warszawa 2016, Załącznik 1 § 3, pkt 6.

²⁸⁹ Termin z § 3 ust. 2 Zasad Techniki Prawodawczej

aby ten stosunek unormowany był w tych aktach odmiennie, czyli prowadził do sprzeczności lub przeciwieństwa norm²⁹⁰. Jeżeli jednak doszłoby do takiej sprzeczności lub przeciwieństwa, a jednocześnie w systemie prawnym istniałyby jasne reguły kolizyjne rozstrzygające relację między tymi normami (aktami prawnymi), to sytuacja taka stanowiłaby mniejszy problem z perspektywy kompetencji organów niż sytuacja, w których nie ma jasnych reguł kolizyjnych między normami. W takiej sytuacji wystarczające byłoby bowiem nawiązanie nieformalnej współpracy między tymi organami, w toku której zostałoby potwierdzone, w jaki sposób należy zastosować te jasne reguły kolizyjne. Jak wykazano w rozdziale 4. rozprawy poniżej, między tymi aktami prawnymi nie ma jasnych reguł kolizyjnych, co dodatkowo skomplikowane jest przez fakt, że organom ustanowionym na ich podstawie przyznano (mniejszą lub większą) niezależność od organów administracji rządowej (jak wykazano w rozdziale 3. rozprawy poniżej). Jest to spowodowane przede wszystkim tym, że są to akty prawa unijnego, co wpisuje ich stosowanie i wykładnię w proces europeizacji prawa administracyjnego, której charakterystyczną cechą są właśnie niejasne relacje między normami prawnymi, multicentryczność i brak hierarchii między organami²⁹¹.

Przechodząc do charakterystyki kryteriów wyboru aktów prawnych do obszaru referencyjnego, wskazać należy, że celem było, aby analizie poddać nowe akty prawne (które nie zostały jeszcze dogłębnie i całkowicie omówione w literaturze), a jednocześnie zbadać problem przekrojowo. Stąd też, po pierwsze, wybrano te akty prawne, które ustanawiają lub nakładają obowiązek ustanowienia organów administracji publicznej lub przyznania istniejącym już organom nowych kompetencji. Po drugie, wybrano nowe akty prawa unijnego i akty prawne krajowe stanowiące operacjonalizację albo transpozycję tych aktów prawa unijnego, których zakresy przedmiotowe najbliższe są zakresowi przedmiotowemu RODO. Wyjątek stanowi prawo konkurencji, które zostało wybrane, aby wykazać, że zjawisko krzyżowania się kompetencji organów w obszarze przetwarzania danych osobowych dotyczy także odrębnych kompleksowych gałęzi prawa. Ostatecznie, wybrano te akty prawne, które co do zasady znajdują zastosowanie we wszystkich sektorach gospodarki (przykładowo, możliwa

²⁹⁰ M. Wojciechowski, *Stwierdzane niezgodności norm wyższego i niższego rzędu a pojęcia niezgodności norm*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji” 2016, nr 3718, s. 140-141.

²⁹¹ Por. podrozdziały 3.2. i 5.4. rozprawy.

byłaby charakterystyka aktów prawnych w sektorze ochrony zdrowia²⁹² lub w sektorze finansowym²⁹³).

Poniżej uzasadniono niewłączenie do obszaru referencyjnego Dyrektywy ePrivacy, Prawa Telekomunikacyjnego i projektu Rozporządzenia ePrivacy; Dyrektywy LED i Ustawy LED, aktów prawnych prawa ochrony konsumenta, a także dlaczego badaniem nie objęto organów nadzorczych ustanowionych przez kościoły i związki wyznaniowe (art. 91 ust. 2 RODO). W odniesieniu do Dyrektywy ePrivacy i Prawa Telekomunikacyjnego w zakresie, w jakim dokonuje ono jej implementacji należy wskazać, że w 2017 r. Komisja przyjęła projekt Rozporządzenia ePrivacy, które ma uchylić Dyrektywę ePrivacy. Rozporządzenie ePrivacy nie zostało do dzisiaj przyjęte, a prace nad nim są obecnie wstrzymane²⁹⁴. Projekt Rozporządzenia ePrivacy²⁹⁵ przewiduje wprost, że organami właściwymi będą organy ochrony danych osobowych (art. 18 ust. 1 RODO) i EROD (art. 19 RODO), a nadto rozstrzyga, że Rozporządzenie ePrivacy stanowiło będzie *lex specialis* w stosunku do RODO (motyw 5 i art. 1 ust. 3 Rozporządzenie ePrivacy). Takie samo rozwiązanie przyjęto w RODO rozstrzygając, że wciąż obowiązująca Dyrektywa ePrivacy stanowi *lex specialis* w stosunku do RODO (motyw 173 i art. 95 RODO)²⁹⁶. Chociaż zakres przedmiotowy Dyrektywy ePrivacy i Prawa Telekomunikacyjnego krzyżuje się z zakresem

²⁹² Na przykład w odniesieniu do problemu relacji praw i obowiązków z RODO do udostępniania dokumentacji medycznej unormowanej w art. 26 Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzecznik Praw Pacjenta (t.j. Dz. U. z 2023 r. poz. 1545 z późn. zm.).

²⁹³ W sektorze finansowym, rozumianym także jako działalność banków, przetwarza się znaczne ilości danych osobowych, sektor ten regulowany jest aktami prawnym [przykładowo, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L z 2015 r. nr 337, s. 35 z późn. zm.) i Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2023 r. poz. 2488 z późn. zm)], a podmioty działające w tym sektorze nadzorowane są przez różne podmioty administrujące, w Polsce przede wszystkim przez KNF. Stąd analiza kompetencji organów w obszarze przetwarzania danych osobowych w sektorze finansowym mogłaby stanowić alternatywny, samodzielny obszar referencyjny w niniejszej rozprawie. Wybrane zagadnienia dotyczące krzyżowania się kompetencji podmiotów administrujących w tym sektorze dotyczących przetwarzania danych osobowych scharakteryzowane zostały w dalszej części niniejszej rozprawy.

²⁹⁴ Legislative Train Schedule, Proposal for a regulation on privacy and electronic communications, <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform> (dostęp: 14.09.2024 r.).

²⁹⁵ Zastrzeżenia Grupy Roboczej do projektu Rozporządzenia ePrivacy dotyczyły przede wszystkim ryzyka obniżenia poziomu ochrony danych osobowych ustanowionego przez RODO. Grupa Robocza, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) Adopted on 4 April 2017*, WP247, <https://ec.europa.eu/newsroom/article29/redirection/item/610140>, s. 9-23, (dostęp: 14.09.2024 r.).

²⁹⁶ EROD, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, Adopted on 12 March 2019, https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, s. 12, (dostęp: 14.09.2024 r.).

przedmiotowym RODO²⁹⁷ (na przykład, w kwestii wyrażenia zgody abonenta lub użytkownika wskazanej w art. 5 ust. 3 Dyrektywy ePrivacy, która najczęściej dyskutowana jest w kontekście plików *cookies*²⁹⁸), co oznacza, że dochodzi również do krzyżowania się kompetencji organów ustanowionych do ich stosowania²⁹⁹ (w Polsce jest to Prezes Urzędu Komunikacji Elektronicznej³⁰⁰), to zdecydowano się na wyłączenie tych aktów prawnych z obszaru referencyjnego przede wszystkim z uwagi na wyznaczenie organów ochrony danych jako właściwych w projekcie Rozporządzenia ePrivacy (co ocenić należy pozytywnie jako rozwiązanie, które powinno być zastosowane także w innych aktach), a także z uwagi na ograniczenie objętości tej rozprawy.

Podobnie jest w przypadku Dyrektywy LED i Ustawy LED. W art. 5 Ustawy LED organem nadzorczym ustanowiony został PUODO, co powoduje, że zjawisko krzyżowania się kompetencji organów w Polsce nie występuje. Nie oznacza to jednak, że w literaturze nie zgłaszano uzasadnionych wątpliwości co do krzyżowania się zakresów przedmiotowych Dyrektywy LED (Ustawy LED) i RODO³⁰¹, jak i tego, że zasadnie byłoby, aby zamiast dwóch osobnych aktów prawnych materia ta unormowana była w jednym akcie, do czego istniały podstawy prawne w prawie unijnym³⁰². W odniesieniu do prawa ochrony konsumenta³⁰³

²⁹⁷ Por. przykładowo: Ch. Etteldorf, *Data Protection Authorities Try to Fill the Gap between GDPR and e-Privacy Rules*, EDPL 2018, Vol. 4, No. 2, s. 235-238; W. G. Voss, *First the GDPR, Now the Proposed ePrivacy Regulation*, „Journal of Internet Law” 2017, Vol. 21, No. 1, <https://ssrn.com/abstract=3008765> (dostęp: 20.09.2024 r.), s. 3-11.

²⁹⁸ Por. EROD, *Guidelines 2/2023 on Technical Scope of art. 5(3) of ePrivacy Directive*, Adopted on 14.11.2023, https://edpb.europa.eu/system/files/2023-11/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_en.pdf (dostęp: 14.09.2024 r.). Por. także X. Konarski, *Podstawy prawne korzystania z „ciasteczek” internetowych (cookies) jako przykład wzajemnej relacji przepisów RODO oraz przepisów o ochronie prywatności w sektorze łączności elektronicznej*, MoP 2018, nr 22, s. 10033.

²⁹⁹ Por. EROD, *Opinia 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych*, 12.03.2019, https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_pl.pdf (dostęp: 15.09.2024 r.).

³⁰⁰ Art. 189-190 Prawa Telekomunikacyjnego. Dział 10 Prawa Telekomunikacyjnego uchylony zostanie przez art. 68 ust. 1 ustawy z dnia 12 lipca 2024 r. - Przepisy wprowadzające ustawę - Prawo komunikacji elektronicznej (Dz.U. 2024 poz. 1222) z dniem 10 listopada 2024 r. Organy właściwe w sprawach komunikacji elektronicznej oraz postępowanie przed Prezesem UKE uregulowane zostaną w dziale VIII ustawy z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz.U. 2024 poz. 1221).

³⁰¹ J. Sajfert, T. Quintel, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* <http://dx.doi.org/10.2139/ssrn.3285873>. (dostęp: 20.09.2024 r.), s. 3-4.

³⁰² Por. A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon (October 4, 2021). <http://dx.doi.org/10.2139/ssrn.3935730> (dostęp: 20.09.2024 r.).

³⁰³ Do którego zaliczyć należy co najmniej następujące akty prawa unijnego: Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz. Urz. UE L z 1993 r. nr 95, s. 29 z późn. zm.); Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE i uchylająca dyrektywę 1999/44/WE (Dz. Urz. UE L z 2019 r. nr 136, s. 28 Z późn. zm.); Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk

(którego wyodrębnienie jako kompleksowej gałęzi prawa jest dyskusyjne³⁰⁴) wskazać należy, że z uwagi na zbieżność celu prawa ochrony konsumenta (usuwanie barier na unijnym rynku wewnętrznym przez budowanie zaufania do produktów i usług w oparciu o przejrzystość i dobrą wiarę³⁰⁵) i celu RODO (zapewnienie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przy jednoczesnym umożliwieniu swobodnego przepływu tych danych) ryzyko krzyżowania się zakresu przedmiotowego aktów prawnych, które jednocześnie prowadziłyby do sprzeczności lub przeciwieństwa norm, należy ocenić jako niewielkie³⁰⁶, a zatem występujące skutki krzyżowania się kompetencji organów będą z zasady mniej dotkliwe. Stąd też, mając także na uwadze ograniczenie objętości niniejszej rozprawy, zdecydowano o wyłączeniu prawa ochrony konsumenta z obszaru referencyjnego.

Kościoły i związki wyznaniowe, które stosują szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem danych osobowych zgodnie z art. 91 ust. 1 RODO, mogą ustanowić własne organy nadzorcze. W Polsce skorzystano z tej możliwości m.in. w Kościele Katolickim, Kościele Ewangelicko-Augsburskim i w Kościele Prawosławnym³⁰⁷. Konsekwencją skorzystania z tej możliwości jest wyłączenie jurysdykcji organów ochrony danych w stosunku do tych kościołów³⁰⁸. Oznacza to, że granica między zakresem kompetencji

handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady („Dyrektywa o nieuczciwych praktykach handlowych”) (Dz. Urz. UE L z 2005 r. nr 149, s. 22 z późn. zm.); Dyrektywa 2006/114/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca reklamy wprowadzającej w błąd i reklamy porównawczej (wersja ujednolicona) (Dz. Urz. UE L z 2006 r. nr 376, s. 21). Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniając dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylając dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz. Urz. UE L z 2011 r. nr 304, s. 64 z późn. zm.).

³⁰⁴ A. Doczekalska, *Złożony charakter prawa konsumenckiego [w:] eadem, Język prawny w tworzeniu i transpozycji prawa Unii Europejskiej. Procesy hybrydyzacji*, Warszawa 2021, SIP LEX.

³⁰⁵ Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 16.09.2024 r.), s. 23.

³⁰⁶ Por. Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf, czwarta kolumna tabeli w aneksie (dostęp: 16.09.2024 r.), s. 39-41.

³⁰⁷ P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, art. 91, SIP LEX.

³⁰⁸ P. Litwinski [w:] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, red. P. Litwinski [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwinski, art. 91 RODO, pkt. 7 (nb 7), SIP Legalis.

organów ustanowionych przez kościoły i granica między zakresem kompetencji krajowych organów ochrony danych wyznaczona została możliwie jasno. Stąd też analiza tego zagadnienia nie przybliżałaby do weryfikacji głównej hipotezy badawczego.

2.6. KRZYŻOWANIE SIĘ ZAKRESU PRZEDMIOTOWEGO OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH Z AKTAMI PRAWNYMI PRAWA UNIJNEGO I KRAJOWEGO REGULUJĄCYMI PRZETWARZANIE DANYCH OSOBOWYCH

W tej części rozdziału scharakteryzowano krzyżowanie się zakresu przedmiotowego RODO z wybranymi aktami prawnymi prawa unijnego i krajowego regulującymi przetwarzanie danych osobowych, to jest aktami prawnymi: regulującymi przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu (podrozdział 2.6.1.), cyberbezpieczeństwo (podrozdział 2.6.2.), prawa konkurencji (także Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych; podrozdział 2.6.3.), sztuczną inteligencję (podrozdział 2.6.4.) i europejskie przestrzenie danych (podrozdział 2.6.5.). Każdy z podrozdziałów rozpoczyna się od charakterystyki zakresu przedmiotowego i podmiotowego tych aktów prawnych, aby następnie poddać analizie wybrane przykłady krzyżowania się ich zakresu przedmiotowego z RODO. Celem nie jest kompleksowa charakterystyka wszystkich aktów prawnych, lecz wykazanie, że ich zakres przedmiotowy, czyli stosunki, które one regulują, krzyżuje się z zakresem przedmiotowym RODO.

2.6.1. AKTY PRAWNE REGULUJĄCE PRZECIWDZIAŁANIE PRANIU BRUDNYCH PIENIĘDZY I FINANSOWANIU TERRORYZMU

Relacja między zakresem przedmiotowym aktów prawnych nakierowanych na ochronę danych osobowych (najpierw Dyrektywy ODO, a następnie RODO) a zakresem przedmiotowym aktów prawnych regulujących przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu (AML) w UE była przedmiotem dyskusji od początku wprowadzenia pierwszych tych aktów, czyli od ponad 30 lat³⁰⁹. W dyskusji tej zwracano uwagę, że w rozwiązaniach nakierowanych na AML istotną rolę odgrywa przetwarzanie danych osobowych i zasadnym jest, aby rozwiązania nakierowane na AML były zgodne

³⁰⁹ I. Kindylidi, The Data Protection Implications of the EU AML Framework: A Critical Overview & the Case of AI, [in:] Annual Privacy Forum, edited by A. Gryszczyńska, P. Polański, N. Gruschka et al., Cham 2022, s. 37.

z Dyrektywą ODO, a następnie RODO, oraz art. 7 i 8 KPP³¹⁰. W aktualnym stanie prawnym akty prawne regulujące AML na poziomie unijnym to, co do zasady, Dyrektywa AML IV i V³¹¹, które razem z krajową Ustawą o AML, stanowiącą ich implementację, są przedmiotem analizy w niniejszym podrozdziale. Obowiązująca Dyrektywa AML VI reguluje zasadniczo aspekty prawnokarne prania brudnych pieniędzy i finansowania terroryzmu, zatem nie została objęta obszarem referencyjnym tej rozprawy doktorskiej.

Akty prawne regulujące AML stanowią komponent stabilności systemu finansowego w UE, co identyfikuje prawodawca unijny już w motywie 1 Dyrektywy AML IV, wskazując, że „przepływy pieniędzy pochodzących z nielegalnych źródeł mogą szkodzić integralności, stabilności i wiarygodności sektora finansowego oraz stanowić zagrożenie dla rynku wewnętrznego Unii” Stąd też jej celem „zapobieganie wykorzystywaniu unijnego systemu finansowego do prania pieniędzy³¹² i finansowania terroryzmu³¹³” (art. 1 ust. 1 Dyrektywy AML V), co ma zostać zapewnione przez państwa członkowskie (art. 1 ust. 2 Dyrektywy AML V). Aby zapewnić efektywność realizacji Dyrektywy AML V, jej zakres podmiotowy określony został szeroko w art. 2, obejmując następujące podmioty zobowiązane, m.in. instytucje kredytowe i finansowe; biegłych rewidentów, zewnętrznych księgowych i doradców podatkowych; notariuszy oraz innych przedstawicieli wolnych zawodów prawniczych, gdy uczestniczą, działając w imieniu i na rzecz swojego klienta, w dowolnych transakcjach finansowych lub transakcjach dotyczących nieruchomości lub gdy udzielają klientowi pomocy w planowaniu lub przeprowadzaniu transakcji dotyczących m.in. kupna i sprzedaży nieruchomości lub podmiotów gospodarczych; pośredników w obrocie nieruchomościami.

Dyrektywa składa się z 69 artykułów podzielonych na siedem rozdziałów: 1) Przepisy ogólne; 2) Zasady należytej staranności wobec klienta; 3) Informacje o beneficjentach; 4) Obowiązki zgłaszania; 5) Ochrona danych, przechowywanie dokumentacji i dane statystyczne; 6) Strategie, procedury i nadzór; oraz 7) Przepisy końcowe. Z perspektywy weryfikacji hipotezy badawczej istotny jest rozdział V Ochrona danych, przechowywanie dokumentacji i dane statystyczne. Art. 11 Dyrektywy AML V nakłada obowiązek wdrożenia przez podmioty zobowiązane środków należytej staranności w enumeratywnie wskazanych sytuacjach, przede

³¹⁰ I. Kindylidi, *The Data Protection Implications of the EU AML Framework: A Critical Overview & the Case of AI*, [in:] *Annual Privacy Forum*, edited by A. Gryszczyńska, P. Polański, N. Gruschka et al., Cham 2022I, s. 37-38 i przywołane tam stanowiska organów.

³¹¹ Dyrektywa AML V stanowi nowelizację Dyrektywy AML IV, stąd też dla zachowania przejrzystości wywodu odwołania w tekście odnoszą się do Dyrektywy AML V rozumianej jako tekst skonsolidowany.

³¹² Zdefiniowane w art. 1 ust. 3 Dyrektywy AML 5.

³¹³ Zdefiniowane w art. 1 ust. 5 Dyrektywy AML 5.

wszystkim przy nawiązywaniu stosunków gospodarczych (art. 11 lit. a Dyrektywy AML V), które to środki, unormowane w art. 13 Dyrektywy AML V, winny być realizowane „z uwzględnieniem ryzyka” prania brudnych pieniędzy lub finansowania terroryzmu³¹⁴. W określonych przypadkach instytucje zobowiązane mogą zastosować uproszczone środki należytej staranności wobec klienta (Sekcja 2 Rozdziału II), a w niektórych przypadkach wyższego ryzyka – muszą wykorzystać wzmocnione środki (Sekcja 3 Rozdziału II). Generalnie, środki te obejmują m.in. identyfikację klienta i weryfikację jego tożsamości oraz identyfikację beneficjenta rzeczywistego i podejmowanie uzasadnionych środków weryfikacji jego tożsamości (art. 13 ust. 1 Dyrektywy AML V), zatem wymagają przetwarzania danych osobowych³¹⁵.

Dla unormowania przetwarzania danych osobowych istotny jest rozdział V Dyrektywy AML V zatytułowany „Ochrona danych, przechowywanie dokumentacji i dane statystyczne”, rozstrzygając, że dane te powinny być przetwarzane zgodnie z RODO (art. 41 ust. 1 Dyrektywy AML V)³¹⁶. Art. 41 ust. 2 Dyrektywy AML V normuje wyłączny cel przetwarzania danych przez podmioty zobowiązane, tj. zapobieganie praniu pieniędzy i finansowaniu terroryzmu, zakazując dalszego przetwarzania w sposób niezgodny z tym celem, w tym do celów komercyjnych, natomiast kwestię retencji danych osobowych uregulowano w ust. 1 tego artykułu, wskazując zasadniczo na pięcioletni okres ich przechowywania, liczony od zakończenia stosunków gospodarczych z danym klientem lub od dnia przeprowadzenia sporadycznej transakcji. Pozostałe rozwiązania przyjęte w Dyrektywie AML V istotne dla weryfikacji hipotez sformułowanych w niniejszej rozprawie doktorskiej, w tym jej zakres podmiotowy, omówione zostaną poniżej przy charakterystyce krajowej Ustawy o AML. W motywach 42-43 Dyrektywy AML 5 unormowano, że jej transpozycja i stosowanie musi odbywać się w zgodzie z „unijnymi przepisami i ochronie danych osobowych” (por. także art. 41), a dyrektywa ta nie narusza prawa podstawowego do ochrony danych osobowych (motyw 65).

³¹⁴ Por. I. Kindylidi, *The Data Protection Implications of the EU AML Framework: A Critical Overview & the Case of AI*, [in:] *Annual Privacy Forum*, edited by A. Gryszczyńska, P. Polański, N. Gruschka et al., Cham 2022, s. 38-40.

³¹⁵ Por. Grupa Robocza, *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, 13.06.2011, 01008/2011/EN WP 186 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf (dostęp: 17.09.2024 r.).

³¹⁶ Por. także art. 45 ust. 1 Dyrektywy AML V (Rozdział VI „Strategie, procedury i nadzór”), który przewiduje obowiązek „wdrożenia strategii i procedur obejmujących całą grupę [podmiotów powiązanych], w tym strategii w zakresie ochrony danych (...) do celów przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu.”

Krajowa Ustawa o AML stanowi implementację Dyrektywy AML V. Zgodnie z art. 1, ustawa określa ona zasady i tryb AML oraz warunki wykonywania działalności gospodarczej przez niektóre instytucje obowiązane. Zakres podmiotowy wyznaczony jest przez znaczenie terminu „instytucje obowiązane”, który w Ustawie AML zasadniczo odpowiada omówionemu wyżej w Dyrektywie AML V. Ten zakres podmiotowy – chociaż szeroki – węższy jest od zakresu podmiotowego RODO, a instytucjami obowiązanymi mogą być zarówno administratorzy, jak i podmioty przetwarzające. Instytucje obowiązane zobowiązane są, na podstawie art. 33 ust. 1 Ustawy AML, używać wobec klientów środków bezpieczeństwa finansowego przy uwzględnieniu ryzyka prania brudnych pieniędzy lub finansowania terroryzmu (art. 33 ust. 3 Ustawy o AML). Ustawa AML normuje sytuacje, w których te środki powinny być używane w art. 35 Ustawy, w tym nawiązywanie stosunków gospodarczych, jak i transakcje okazjonalne. Zakres środków bezpieczeństwa, jakie winny wykorzystywać instytucje obowiązane uregulowany został w art. 34 ust. 1 Ustawy AML, obejmując m.in. identyfikację klienta (w tym, zgodnie z art. 36, imię i nazwisko, obywatelstwo, numer PESEL, serię i numer dokumentu tożsamości) i weryfikację tożsamości; identyfikację beneficjenta rzeczywistego (zdefiniowany w art. 2 ust. 2 pkt 1 Ustawy o AML) oraz podejmowanie uzasadnionych czynności w celu: weryfikacji jego tożsamości; bieżące monitorowanie stosunków gospodarczych klienta. Instytucje obowiązane uprawnione są do przetwarzania informacji (w tym danych osobowych) w dokumentach tożsamości i kopiować je (art. 34 ust. 4 Ustawy o AML; por. także art. 37 ust. 1 Ustawy o AML).

Dla przetwarzania danych osobowych istotne jest prowadzenie Centralnego Rejestru Beneficjentów Rzeczywistych (art. 55-71a Ustawy o AML), co stanowi implementację art. 30-31 Dyrektywy AML V. Rejestr ten, prowadzony za pomocą systemu teleinformatycznego, ma na celu gromadzenie i przetwarzanie informacji dotyczących beneficjentów rzeczywistych³¹⁷ (art. 55 Ustawy o AML), a status administratora przypisano ministrowi właściwemu do spraw finansów publicznych (art. 56 Ustawy o AML). Ustawa o AML określa szeroki zakres podmiotów, które są obowiązane do zgłaszania informacji o beneficjentach rzeczywistych (art. 58 Ustawy o AML). Obejmuje to nie tylko podmioty prowadzące działalność gospodarczą w Polsce, ale także podmioty prawa zagranicznego, na przykład trusty. Informacje

³¹⁷ Ustawa o AML definiuje beneficjenta rzeczywistego (art. 2 ust. 2 pkt 1) szeroko jako „każdą osobę fizyczną sprawującą bezpośrednio lub pośrednio kontrolę nad klientem poprzez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych, umożliwiające wywieranie decydującego wpływu na czynności lub działania podejmowane przez klienta, lub każdą osobę fizyczną, w imieniu której są nawiązywane stosunki gospodarcze lub jest przeprowadzana transakcja okazjonalna”.

podlegające zgłoszeniu do rejestru, obejmują informacje identyfikacyjne podmiotów i dane osobowe beneficjentów rzeczywistych (w tym imię i nazwisko, każde posiadane obywatelstwo, państwo zamieszkania, numer PESEL albo datę urodzenia), ze wskazaniem wielkości i charakteru ich uprawnień (art. 59 Ustawy o AML). Zakres tych informacji jest zatem szeroki. Wobec szerokiego zakresu informacji, istotne jest, że rejestr ten jest jawny, to znaczy każdy ma do niego dostęp za pośrednictwem Internetu (art. 67-70 Ustawy o AML).

Wykonywanie obowiązków przez instytucje obowiązane wymaga przetwarzania znacznych ilości danych osobowych³¹⁸. Oznacza to, że zakres przedmiotowy Dyrektywy AML V i Ustawy o AML krzyżuje się z zakresem przedmiotowym RODO, ponieważ oba akty prawne normują przetwarzanie danych osobowych. Intencją prawodawcy unijnego i krajowego było, aby rozwiązania przyjęte w Dyrektywie AML V i Ustawie o AML gwarantowały prawo do ochrony danych osobowych. Zarówno jednak zakres, jak i sposób przetwarzania danych osobowych na podstawie tych przepisów budzą zastrzeżenia w orzecznictwie (np. scharakteryzowany niżej wyrok TSUE dotyczący luksemburskiego rejestru beneficjentów rzeczywistych) i literaturze, gdzie wskazywano na ryzyka dla prawidłowej realizacji zasady ograniczenia celu i minimalizacji danych z RODO³¹⁹.

Analizie poddane zostaną dwa szczegółowe zagadnienia – jawny rejestr beneficjentów rzeczywistych i możliwość kopiowania dokumentów tożsamości (dowodów osobistych) przez podmioty zobowiązane. TSUE w wyroku z 22.11.2022 r. w sprawie o sygn. akt C-37/20 (WM p-ko Luxembourg Business Registers³²⁰) orzekł, że nieważny jest art. 30 ust. 5 akapit pierwszy lit. c Dyrektywy AML V w zakresie w jakim przewiduje, że należy zapewnić, aby informacje o beneficjentach rzeczywistych „były we wszystkich przypadkach udostępniane każdej osobie”³²¹. Sprawa dotyczyła ustanowienia luksemburskiego rejestru beneficjentów rzeczywistych, który umożliwiał publiczny dostęp do informacji o beneficjentach

³¹⁸ M. Brewczyńska, E. Kosta, From the Fight Against Money Laundering and Financing of Terrorism Towards the Fight for Fundamental Rights: Role of Data Protection, „Tilburg Law School Research Paper” 2023, No. 2, <https://ssrn.com/abstract=4328464> (dostęp: 20.09.2024 r.), s. 14-16.

³¹⁹ Przykładowo: M. Gawroński, Rozdział 13 ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu a RODO [w:] Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik, red. W. Kapica, Warszawa 2018; M. Brewczyńska, E. Kosta, From the Fight Against Money Laundering and Financing of Terrorism Towards the Fight for Fundamental Rights: Role of Data Protection, „Tilburg Law School Research Paper” 2023, No. 2, <https://ssrn.com/abstract=4328464> (dostęp: 20.09.2024 r.), s. 17-27; L. M. Landerer, The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention: A Flawed Comparison?, „Eucrim – the European Criminal Law Associations' Forum” 2022, Iss. 01, s. 67-72.

³²⁰ Wyrok TS z 22.11.2022 r., C-37/20, WM przeciwko Luxembourg Business Registers, SIP LEX nr 3433353.

³²¹ Wyrok TS z 22.11.2022 r., C-37/20, WM przeciwko Luxembourg Business Registers, SIP LEX nr 3433353, p. 96.

rzeczywistych zarejestrowanych tam podmiotów³²². TSUE, identyfikując korzyści związane z publicznym dostępem do rejestru, orzekł jednak, że upublicznienie tych informacji stanowiących dane osobowe w ten właśnie sposób stanowi naruszenie niezbędności i proporcjonalności ograniczenia w korzystaniu z praw podstawowych do prywatności i ochrony danych osobowych, a tym samym stanowi naruszenie tych praw³²³, co skutkowało unieważnieniem Dyrektywy AML V we wskazanym wyżej zakresie. Wyrok ten oznacza zakwestionowanie przez europejskie sądy praktyki ustanawiania jawnego dostępu do rejestrów beneficjentów rzeczywistych, który został ustanowiony i dalej obowiązuje³²⁴ także w Polsce. Bardziej odpowiednim byłoby umożliwienie dostępu do informacji o beneficjentach rzeczywistych konkretnym osobom, np. dziennikarzom lub kontrahentom podmiotu wpisanego do rejestru beneficjentów rzeczywistych, po wykazaniu przez nich uzasadnionego interesu w dostępie do konkretnej informacji.

Kolejnym zagadnieniem dotyczącym przetwarzania danych osobowych i obowiązków wynikających z Dyrektywy AML 5 i Ustawy o AML, które wywołuje dyskusję co najmniej od 2019 r., jest możliwość sporządzania kopii (kserowania) dokumentów tożsamości (dowodów osobistych) przez instytucje zobowiązane w ramach wykonywania i dokumentowania środków bezpieczeństwa. Istota tej dyskusji dotyczy wykładni art. 34 ust. 4 Ustawy o AML, zgodnie z którym „instytucje obowiązane na potrzeby stosowania środków bezpieczeństwa finansowego mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie”. W stanowisku z 2019 r. PUODO – w odpowiedzi na zapytanie Związku Banków Polskich dotyczące praktyki weryfikacji tożsamości klientów przez banki w celach AML – wskazał, że sporządzanie kopii dokumentów tożsamości jest zgodne z RODO tylko wówczas, jeżeli jest to niezbędne z perspektywy przesłanek wykorzystania środków bezpieczeństwa finansowego, o których mowa w art. 35 ust. 1-2 Ustawy o AML przy uwzględnieniu ryzyka prania brudnych pieniędzy lub finansowania terroryzmu, co wymaga każdorazowej oceny instytucji zobowiązanych³²⁵. Pomimo wątpliwości co do spójności tego stanowiska zgłaszanych w publikacjach

³²² TSUE, Komunikat Prasowy nr 188/22, 22.10.2022, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188pl.pdf> (dostęp: 15.09.2024 r.).

³²³ TSUE, Komunikat Prasowy nr 188/22, 22.10.2022, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188pl.pdf> (dostęp: 15.09.2024 r.).

³²⁴ M. Sawczuk [w:] Komentarz do ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu [w:] Prawo obrotu pieniężnego. Komentarz, red. P. Zapadka, Warszawa 2023, art. 67, pkt 3, SIP LEX.

³²⁵ Decyzja PUODO, ZSPR.027.306.2019, SIP LEX nr 3285140.

dziennikarskich³²⁶, to stanowisko powtarzane było przez PUODO w kolejnych latach³²⁷. PUODO jeszcze na przełomie lat 2019 i 2020 skierował pismo do GIIF (podmiotu administrującego, krajowej jednostki analityki finansowej) o zajęcie stanowiska, w jaki sposób weryfikacja tożsamość klientów powinna być udokumentowana na potrzeby spełnienia obowiązków przewidzianych przez Ustawę o AML³²⁸. GIIF odpowiedział, że kopiowanie dokumentów tożsamości nie jest obowiązkiem, ale uprawnieniem instytucji zobowiązanych, a GIIF nie wymaga przedłożenia dowodu w postaci kopii dokumentów tożsamości w każdym przypadku; dostępne są inne sposoby dokumentowania weryfikacji, np. przez dokument opatrzone podpisem pracownika, który spisał dane z dokumentu tożsamości³²⁹. PUODO skierował pismo także do KNF, zwracając się o zajęcie stanowiska w tej sprawie wobec podmiotów nadzorowanych. W odpowiedzi KNF podzielił stanowisko GIIF w kwestiach merytorycznych. Wskazał, że nie jest kompetentny do zajmowania stanowiska wobec podmiotów nadzorowanych, ponieważ organem kompetentnym w tej sprawie jest GIIF³³⁰. Efektem tej dyskusji po stronie podmiotów nadzorowanych, które zobowiązane są przestrzegać zarówno RODO (jako administratorzy i podmioty przetwarzające), jak i Ustawy o AML (jako instytucje zobowiązane), było pogłębienie niepewności prawnej w ocenie sytuacji, w których mogą one sporządzać kserokopie dokumentów tożsamości na potrzeby udokumentowania weryfikacji tożsamości klienta (podmiotu danych), pozostając w zgodzie z RODO.

Finalizując analizę dotyczącą aktów prawnych regulujących AML, uzupełnić ją należy przez wskazanie, że w odniesieniu do przetwarzania tych danych osobowych przez jednostki analityki finansowej (art. 32 Dyrektywy AML V) z uwagach na kontekst przetwarzania niejasne jest, w jakim zakresie do tego przetwarzania znajduje zastosowanie RODO, a w jakim Dyrektywa LED i krajowe akty prawne ją implementujące³³¹. To z kolei ma wpływ na zakres

³²⁶ Por. P. Pieńkosz, *Prezes UODO: kopiowanie dowodów osobistych przez instytucje finansowe jest uzasadnione*, „Dziennik Gazeta Prawna” 11.07.2022, <https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8489919,czy-mozna-kopiwac-dowody-osobiste.html> (dostęp: 18.09.2024 r.).

³²⁷ Por. UODO, *Czy instytucje finansowe mogą kopiować dowody osobiste?* 16.08.2022, <https://uodo.gov.pl/pl/138/2476#:~:text=W%20ostatnim%20czasie%20w%20związku,w%20tym%20zakresie%20pozostają%20niezmienne> (dostęp: 18.09.2024 r.).

³²⁸ Por. Pismo GIIF z 4.02.2020 r. nr IF6.701.29.2019 do PUODO, niepubl., przywołanie za: A. Mednis [w:] *Komentarz do ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* [w:] *Prawo obrotu pieniężnego. Komentarz*, red. P. Zapadka, Warszawa 2023, art. 34, pkt 3.

³²⁹ Por. Pismo GIIF z 4.02.2020 r. nr IF6.701.29.2019 do PUODO, niepubl., przywołanie za: A. Mednis [w:] *Komentarz do ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* [w:] *Prawo obrotu pieniężnego. Komentarz*, red. P. Zapadka, Warszawa 2023, art. 34, pkt 3.

³³⁰ *Prezes UODO ws. kopiowania dokumentów tożsamości: konieczne wytyczne dla banków*, „Rzeczpospolita”, <https://www.rp.pl/dane-osobowe/art776041-prezes-uodo-ws-kopiowania-dokumentow-tozsamosci-konieczne-wytyczne-dla-bankow> (dostęp: 18.09.2024 r.).

³³¹ M. Brewczyńska, *Financial Intelligence Units: Reflections on the applicable data protection legal framework*, CLSR 2021, No. 43, s. 8-9.

praw i obowiązków administratorów oraz podmiotów danych³³². Jest to konsekwencja niejasnej granicy między zakresem przedmiotowym RODO i zakresem przedmiotowym LED, które ma zastosowanie w przypadku spełnienia dwóch przesłanek łącznie: 1) przetwarzania danych osobowych przez właściwe organy; 2) „do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom” (art. 2 ust. 1 i art. 1 ust. 1 Dyrektywy LED). Niejasne jest zatem, od którego momentu i wobec jakiego charakteru instytucjonalnego jednostek analityki finansowej możliwe jest przyjęcie, że zastosowanie ma odpowiednio RODO, czy też Dyrektywa LED³³³ (por. np. art. 116b ust. 4 Ustawy o AML).

Prawodawca unijny w 2024 r. przyjął pakiet aktów prawnych, których celem jest dokonanie zmian w unormowaniu AML w UE. Na ten pakiet składały się w szczególności: 1) Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu³³⁴ (wejście w życie zasadniczo 1 lipca 2025 r. zgodnie z art. 108); 2) Rozporządzenie Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu³³⁵ (stosuje się od 36 miesięcy od dnia wejścia w życie zgodnie z art. 90); 3) Dyrektywa Parlamentu Europejskiego i Rady w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić, mających na celu zapobieganie wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz uchylającej dyrektywę (UE) 2015/849³³⁶ (obowiązek transpozycji zasadniczo w ciągu 36 miesięcy od daty wejścia w życie zgodnie z art. 78). Ten pakiet był przedmiotem opinii EIOD³³⁷ i stanowiska EROD,

³³² M. Brewczyńska, Financial Intelligence Units: Reflections on the applicable data protection legal framework, CLSR 2021, No. 43, s. 8-9.

³³³ M. Brewczyńska, Financial Intelligence Units: Reflections on the applicable data protection legal framework, CLSR 2021, No. 43, s. 11-13.

³³⁴ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu i zmieniające rozporządzenia (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010, COM/2021/421 final. Wersja finalna: <https://data.consilium.europa.eu/doc/document/PE-35-2024-REV-1/pl/pdf#page=2.09> (dostęp: 31 maja 2024 r.).

³³⁵ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu, COM/2021/420 final. Wersja finalna: data.consilium.europa.eu/doc/document/PE-36-2024-REV-1/pl/pdf#page=2.18 (dostęp: 31 maja 2024 r.).

³³⁶ Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić, mających na celu zapobieganie wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz uchylająca dyrektywę (UE) 2015/849, COM/2021/423 final. Wersja finalna: <https://data.consilium.europa.eu/doc/document/PE-37-2024-REV-1/pl/pdf#page=91.08> (dostęp: 31 maja 2024 r.).

³³⁷ EIOD, *EDPS Opinion on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals*, 21.09.2022, https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf (dostęp: 31 maja 2024 r.).

gdzie zwrócono uwagę na kwestie dotyczące przetwarzania danych osobowych, krytykując niektóre rozwiązania, m.in. dotyczące partnerstwa publiczno-prawnego w zakresie wymiany informacji, jako potencjalnie sprzeczne z prawami podstawowymi³³⁸. Ten pakiet został przyjęty pod koniec maja 2024 r., dlatego nie został przedmiotem pogłębionej analizy w tej rozprawie doktorskiej, z zastrzeżeniem unormowań dotyczących ustanowienia Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu, które jest przedmiotem analizy w kolejnym rozdziale. Poniżej dokonano jedynie ogólnej charakterystyki tego pakietu zmian legislacyjnych.

Celem zmian jest przede wszystkim ujednolicenie stosowania aktów prawnych regulujących AML w UE³³⁹ i zwiększenie skuteczności, m.in. przez wzmocnienie wymogów tzw. należytej staranności i ujednolicony limit płatności w gotówce w relacjach między podmiotami profesjonalnymi³⁴⁰. Rozporządzenie w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu normuje, m.in.: 1) „środki, które mają być stosowane przez podmioty zobowiązane w celu zapobiegania praniu pieniędzy i finansowaniu terroryzmu;” oraz 2) „wymogi dotyczące przejrzystości w zakresie własności rzeczywistej dla podmiotów prawnych, trustów, które powstały w drodze czynności prawnej, i podobnych porozumień prawnych” (art. 1 lit. a)-b)). W rozporządzeniu RODO wymienione jest 18 razy, w tym w Rozdziale VII „Ochrona danych i przechowywanie dokumentacji” m.in. przy wprowadzaniu obowiązków, które mają w założeniu zapewnić komplementarność względem obowiązków nałożonych przez RODO, np. co do weryfikacji, i przeprowadzania oceny skutków przetwarzania dla ochrony danych (np. art. 75 ust. 2 i ust. 4 lit. h) oraz regulując zasady przetwarzania danych osobowych, w tym szczególnych kategorii danych osobowych i danych osobowych w kontekście wykorzystywania systemów sztucznej inteligencji dla celów AML (art. 76).

Z kolei Dyrektywa w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić, mających na celu zapobieganie wykorzystywaniu systemu finansowego do prania

³³⁸ EROD, EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations, 28.03.2023, https://edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf (dostęp: 31.05.2024 r.). Badanie zasadności tej argumentacji wobec ostatecznego brzmienia tych aktów prawnych nie jest przedmiotem analizy w niniejszym podrozdziale.

³³⁹ Komisja, *Anti-money laundering and countering the financing of terrorism legislative package*, 20.07.2021, https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en?prefLang=pl (dostęp: 07.09.2024 r.).

³⁴⁰ Parlament Europejski, *Walka z praniem pieniędzy: Parlament przyjął nowe przepisy*, <https://www.europarl.europa.eu/news/pl/press-room/20240419IPR20586/walka-z-praniem-pieniedzy-parlament-przyjal-nowe-przepisy> (dostęp: 10.09.2024 r.).

pieniędzy lub finansowania terroryzmu uchyla dyrektywę 2015/849 (analizowaną wyżej jako Dyrektywa AML V) od dnia 10 lipca 2027 r., a jednocześnie reguluje: 1) „środki mające zastosowanie do sektorów narażonych na pranie pieniędzy i finansowanie terroryzmu na poziomie krajowym;” 2) „wymogi w zakresie rejestracji, identyfikacji i kontroli kadry kierowniczej wyższego szczebla i beneficjentów rzeczywistych podmiotów zobowiązanych;” 3) „identyfikację ryzyk prania pieniędzy i finansowania terroryzmu na poziomie Unii i państw członkowskich”; 4) „utworzenie rejestrów beneficjentów rzeczywistych i rachunków bankowych oraz dostępu do nich, a także dostępu do informacji o nieruchomościach;” 5) „obowiązki i zadania jednostek analityki finansowej (FIU);” 6) „obowiązki i zadania organów zaangażowanych w nadzór nad podmiotami zobowiązanymi;” 7) „współpracę między właściwymi organami i współpracy z organami objętymi innymi aktami prawnymi Unii” (art. 1 lit. a)-g)). Dyrektywa dokonuje m.in. modyfikacji dostępu do centralnych rejestrów beneficjentów rzeczywistych przez ograniczenie dostępu podmiotów mających do nich wgląd, co w założeniu stanowić ma uwzględnienie analizowanego powyżej wyroku TSUE w wyroku z 22.11.2022 r. w sprawie o sygn. akt C-37/20³⁴¹ (por. motyw 134; Rozdział II „Rejestry”). RODO przywołane jest w tej Dyrektywie 12 razy, w tym normując, że RODO powinno znaleźć zastosowanie do przetwarzania danych osobowych do jej celów (motyw 56), w tym w zakresie centralnych rejestrów beneficjentów rzeczywistych (art. 12 ust. 4), a także regulując przetwarzanie szczególnych kategorii danych osobowych (Rozdział VI „Ochrona danych”, art. 70).

2.6.2. AKTY PRAWNE REGULUJĄCE CYBERBEZPIECZEŃSTWO

Cyberbezpieczeństwo jest terminem prawnym, zdefiniowanym w UKSC, krajowej implementacji Dyrektywy NIS jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” (art. 2 pkt 4 UKSC). Znaczenie nadane przez tę definicję jest zbliżone do znaczenia nadanego w Dyrektywie NIS określeniu „bezpieczeństwo sieci i systemów informatycznych”³⁴². Zasadniczo odpowiada również rozumieniu tego ostatniego terminu, który występuje także w motywie 49 RODO, gdzie wskazano, że jest to „odporności sieci lub systemu informacyjnego na danym poziomie

³⁴¹ Wyrok TS z 22.11.2022 r., C-37/20, WM przeciwko Luxembourg Business Registers, SIP LEX nr 3433353.

³⁴² Por. *Cyberbezpieczeństwo*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 88.

poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjemne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych”³⁴³. Tak pojmowane cyberbezpieczeństwo jest istotnym elementem zasady integralności i poufności w RODO (art. 5 ust. 1 lit. f) (choć nie wyczerpuje jej) konkretyzowanej przez szereg dalszych obowiązków, w tym ustanowiony w art. 32 RODO obowiązek zapewnienia bezpieczeństwa przetwarzania. W konsekwencji tego funkcjonalnego powiązania, cele aktów prawnych regulujących cyberbezpieczeństwo i RODO są co do zasady zbieżne. Wzmacnianie cyberbezpieczeństwa na podstawie tych aktów prawnych zasadniczo pomaga w realizacji obowiązków z RODO. Świadczy o tym także działalność organów, np. opublikowanie przez ENISA dokumentu „*Handbook on Security of Personal Data Processing*” („Podręcznik bezpieczeństwa przetwarzania danych osobowych”) w 2018 r.³⁴⁴ Pomimo tej zasadniczej zbieżności celów, należy wskazać, że wdrażanie niektórych rozwiązań w celu poprawy tak pojmowanego cyberbezpieczeństwa zarówno w sektorze publicznym, jak prywatnym może oznaczać zagrożenia dla prywatności, na przykład za takie zagrożenie można uznać wdrożenie rozbudowanych systemów śledzenia użytkowników-pracowników aktywności w Internecie przez pracodawcę, aby monitorować występowanie cyberzagrożeń³⁴⁵.

Liczba aktów prawnych regulujących cyberbezpieczeństwo – zarówno horyzontalnych, jak i sektorowych³⁴⁶ – jest znaczna³⁴⁷. Procedowane są także nowe akty prawne³⁴⁸. Na potrzeby tej rozprawy analizie poddana zostanie na poziomie unijnym Dyrektywa NIS 2 (obecnie nieimplementowana jeszcze do krajowego porządku prawnego), a na poziomie krajowym

³⁴³ Por. A. Szkurlat, Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych, iKAR 2020, t. 9, nr 2, s. 54-60.

³⁴⁴ ENISA, *Handbook on Security of Personal Data Processing*, 29.01.2018, <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing> (dostęp: 10.09.2024 r.).

³⁴⁵ Nagranie wideo panelu *Future Trend: The Conflict Between Cybersecurity And Privacy*, który odbył się w czasie konferencji CPDP w Brukseli w roku 2023 r. <https://www.youtube.com/watch?v=LgCWRZYb040> (dostęp: 10.09.2024 r.).

³⁴⁶ Na przykład w sektorze finansowym, co jest trendem wykraczającym poza UE: por. A. N. Didenko, *Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond*, „Uniform Law Review” 2020, Vol. 25, No. 1, <https://ssrn.com/abstract=3533664> (dostęp: 20.09.2024 r.), s. 125-167.

³⁴⁷ Por. R. T. Prabucki, D. Syrociak, *Cyberbezpieczeństwo na fali regulacyjnej*, „ABI Expert: prawne i techniczne aspekty ochrony danych informacji” 2023, nr 1, s.p. 10–13.

³⁴⁸ Np. Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020, COM/2022/454 final; razem z opinią EIOD w przedmiocie tego aktu prawnego: EIOD, *Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*, 9.11.2022, https://edps.europa.eu/system/files/2022-11/2022-0921_d2649_opinion_en.pdf (dostęp: 7.09.2024 r.)

– UKSC (implementująca poprzednią Dyrektywę NIS). Dyrektywa NIS nie zostanie poddana osobnej analizie, ponieważ w październiku 2024 r. uchylona zostanie przez Dyrektywę NIS 2, natomiast jej elementy będą poddane analizie w ramach charakterystyki UKSC, która ją implementuje³⁴⁹. Z uwagi na ograniczenia objętościowe tej rozprawy, analizą nie objęte zostały akty prawne sektorowe regulujące cyberbezpieczeństwo³⁵⁰ ani Akt o Cyberbezpieczeństwie (natomiast w kolejnym rozdziale 3. scharakteryzowano ENISA, która jest organem unormowanym kompleksowo w tym właśnie akcie). Ta fragmentaryczność aktów prawnych regulujących cyberbezpieczeństwo w UE była przedmiotem krytyki w literaturze³⁵¹.

Dyrektywa NIS 2 weszła w życie 16 stycznia 2023 r., uchylając poprzedni akt prawny, Dyrektywę NIS (2016 r.) z dniem 18 października 2024 r. Konieczność przyjęcia nowej dyrektywy umotywowana została nowymi potrzebami wynikającymi z ewolucją cyberzagrożeń spowodowaną transformacją cyfrową (motyw 1-3 Dyrektywy NIS 2)³⁵². Jej celem jest „osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE” (art. 1 ust. 1 Dyrektywy NIS 2). Dyrektywa NIS 2 składa się z 46 artykułów, podzielonych na dziewięć rozdziałów: 1) Przepisy ogólne; 2) Skoordynowane ramy w zakresie cyberbezpieczeństwa; 3) Współpraca na poziomie unijnym i międzynarodowym; 4) Środki zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki dotyczące zgłaszania incydentów; 5) Jurysdykcja i rejestracja; 6) Wymiana informacji; 7) Nadzór i egzekwowanie przepisów; 8) Akty delegowane i wykonawcze; 9) Przepisy końcowe; oraz trzech załączników znajdujących się na końcu aktu prawnego. Przedmiotem charakterystyki w niniejszym podrozdziale są wybrane obowiązki podmiotów nadzorowanych unormowane w rozdziale IV (Środki zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki dotyczące zgłaszania incydentów).

Zakres przedmiotowy Dyrektywy NIS 2 unormowany został w art. 1 ust. 2, obejmując: obowiązki państw członkowskich do przyjęcia krajowych strategii cyberbezpieczeństwa i ustanowienia odpowiednich podmiotów administrujących oraz „egzekwowania przepisów”;

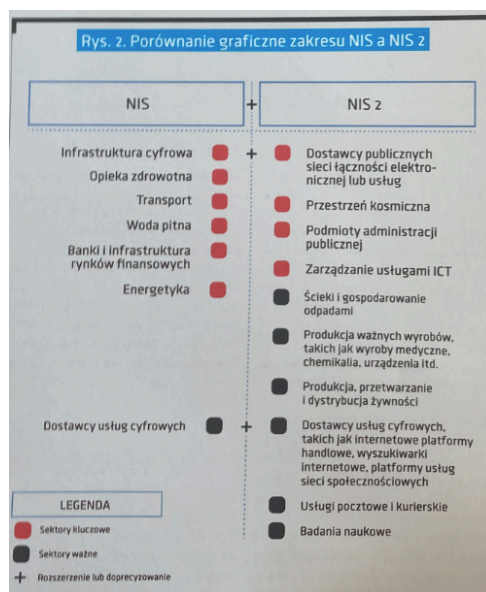
³⁴⁹ Zob. w przedmiocie ewolucji regulacji cyberbezpieczeństwa UE i w Polsce: G. M. Szpor, *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland*, RECoL 2021, Vol. 46, No. 3, <https://doi.org/10.31743/recl.12645> (dostęp: 20.09.2024 r.), s. 219–235.

³⁵⁰ Przykładowo: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L z 2022 r. nr 333, s. 1); Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L z 2022 r. nr 333, s. 164);

³⁵¹ H. Carrapico; A. Barrinha, *The EU as a Coherent (Cyber)Security Actor*, „Journal of Common Market Studies” 2017, Vol. 55, No. 6, s. 1267.

³⁵² Por. także N. Vandezande, *Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor*, CLSR 2024, Vol. 52.

środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów wymianę informacji o cyberbezpieczeństwie. Prawodawca unijny rozszerzył zakres podmiotowy Dyrektywy NIS 2 względem Dyrektywy NIS 1 odchodząc od wyróżniania operatorów usług kluczowych i dostawców usług cyfrowych na rzecz wyróżnienia podmiotów kluczowych i ważnych (por. motyw 6 Dyrektywy NIS 2) zgodnie z rozbudowanym art. 3 ust. 1-6 i załącznikami I („Sektory kluczowe” i II („Sektory ważne”). Podstawowe różnice w zakresie podmiotowymi obrazuje poniższa grafika³⁵³:



Schemat 1 Porównanie graficzne zakresu NIS a NIS 2.

Zasadnicze obowiązki podmiotów kluczowych i ważnych unormowane zostały w rozdziale IV („Środki zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki dotyczące zgłaszania incydentów”), przy czym dalej idące obowiązki spoczywają na podmiotach kluczowych, co wynika już z możliwości użycia „środków nadzoru”, np. wobec podmiotów ważnych nie stosuje się wrywkowych kontroli³⁵⁴. Zgodnie z art. 21 Dyrektywy NIS 2, zarówno podmioty kluczowe, jak i ważne zobowiązane są wprowadzić „odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem” w cyberbezpieczeństwie. Sposób sformułowania tego przepisu prowadzi do wniosku, że to na podmiotach kluczowych i ważnych ciąży obowiązek indywidualnego dostosowania odpowiednich środków do występującego ryzyka, co wymaga przeprowadzenia analizy i monitorowania tego ryzyka (por. art. 21 ust. 3 Dyrektywy NIS). Rozbudowany, otwarty

³⁵³ R. T. Prabucki, D. Syrociak, *Cyberbezpieczeństwo na fali regulacyjnej*, „ABI Expert: prawne i techniczne aspekty ochrony danych informacji” 2023, nr 1, s. 12.

³⁵⁴ R. T. Prabucki, D. Syrociak, *Cyberbezpieczeństwo na fali regulacyjnej*, „ABI Expert: prawne i techniczne aspekty ochrony danych informacji” 2023, nr 1, s. 11 i 13.

katalog tych środków ustanowiono w art. 21 ust. 2 Dyrektywy NIS 2, wskazując m.in. na politykę analizy ryzyka i bezpieczeństwa systemów informatycznych oraz obsługę incydentu. Obowiązkowi wdrożenia środków zarządzania ryzykiem towarzyszy – tak jak w Dyrektywie NIS – obowiązek w zakresie zgłaszania incydentów. Podmioty ważne i kluczowe mają obowiązek zgłosić poważne incydenty (mające istotny wpływ na świadczenie usług zgodnie z art. 23 ust. 3 Dyrektywy NIS 2) do właściwych CSIRT lub organów w terminach i w sposób wskazany w art. 23 ust. 4 Dyrektywy NIS 2, a także powiadomić odbiorców usługi „w stosownych przypadkach”.

Dyrektywa NIS 2 identyfikuje ryzyko krzyżowania się jej zakresu przedmiotowego z RODO, o czym świadczy ponad dwudziestokrotne odwołanie się do RODO w treści Dyrektywy NIS 2 (por. np. motyw 14, 43, 45, 51, 112). Stąd też zawarto w niej przepis, zgodnie z którym stosuje się ją „bez uszczerbku” dla RODO (art. 2 ust. 12 Dyrektywy NIS 2; także motyw 92 w odniesieniu do zgłaszania incydentów), w tym także w odniesieniu do kompetencji organów ochrony danych osobowych (motyw 14 Dyrektywy NIS 2). Unikalnym rozwiązaniem jest art. 35 ust. 1-2 Dyrektywy NIS 2 normujący obowiązki organów właściwych do spraw cyberbezpieczeństwa i kwestie nakładania administracyjnych kar pieniężnych za naruszenia Dyrektywy NIS 2 (art. 21 i 23) pociągające za sobą naruszenie ochrony danych osobowych. Rozwiązanie to scharakteryzowane zostało w niniejszym podrozdziale poniżej w odniesieniu do obowiązku zgłaszania incydentów na podstawie UKSC i zgłaszania naruszeń ochrony danych osobowych na podstawie RODO.

Krajową implementację Dyrektywy NIS stanowi UKSC, która zgodnie z art. 1 ust. 1 UKSC reguluje m.in.: organizację krajowego systemu cyberbezpieczeństwa³⁵⁵ i zadania oraz obowiązki podmiotów wchodzących w jego skład; sposób sprawowania nadzoru i kontroli; oraz zakres Strategii Cyberbezpieczeństwa RP. Zastosowanie UKSC wyłączono do m.in. przedsiębiorców telekomunikacyjnych w rozumieniu Prawa Telekomunikacyjnego w zakresie zgłaszania incydentów. Zakres podmiotowy krajowego systemu cyberbezpieczeństwa wyznaczony jest przez dwadzieścia punktów w art. 4 UKSC, gdzie wskazano m.in. operatorów usług kluczowych i dostawców usług cyfrowych. Celem

³⁵⁵ Rozumianego jako „integralna część krajowego i europejskiego systemu bezpieczeństwa i systemów informacyjnych wyodrębniona w celu efektywnego wykonywania zadań publicznych, usług kluczowych i usług cyfrowych” (Por. *Krajowy system cyberbezpieczeństwa*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 254). Jego celem, zgodnie z art. 3 UKSC, jest „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów”.

systematyzacji tego katalogu w literaturze zaproponowano podział tych podmiotów na trzy typy (których jednoznaczne wyznaczenie jest jednak trudne): 1) administrację systemu; 2) uczestników, czyli przede wszystkim operatorów usług kluczowych i dostawców usług cyfrowych; 3) podmioty wspierające uczestników³⁵⁶. Z powyższego zestawienia wynika, że zakres podmiotowy UKSC jest – podobnie jak w przypadku Ustawy o AML – węższy niż RODO, natomiast podmioty, które objęte są zakresem podmiotowym UKSC są również objęte zakresem podmiotowym RODO.

Dla weryfikacji hipotez badawczych w tej rozprawie znaczenie mają przede wszystkim prawa i obowiązki operatorów usług kluczowych oraz dostawców usług cyfrowych. Są to zasadniczo podmioty prowadzące działalność w sektorze prywatnym i posiadające jednocześnie status administratora lub podmiotu przetwarzającego w rozumieniu RODO. Operatorzy usług kluczowych to, zgodnie z art. 5 ust. 1 UKSC, wybrane podmioty (posiadające jednostkę organizacyjną na polskim terytorium) prowadzące działalność w sektorach zdefiniowanych w załączniku nr 1 do UKSC (energia; transport; bankowość i infrastruktura rynków finansowych; ochrona zdrowia; zaopatrzenie w wodę pitną i jej dystrybucja oraz infrastruktura cyfrowa), wobec których właściwe organy do spraw cyberbezpieczeństwa wydały decyzję o uznaniu ich za takich operatorów, przy uwzględnieniu kryterium istotności skutków potencjalnego incydentu (art. 5 ust. 2 UKSC). Obowiązki operatorów usług kluczowych unormowane zostały w rozdziale 3 UKSC (art. 8-16 UKSC), obejmując m.in. wdrożenie systemu zarządzania bezpieczeństwem, w tym szacowania i zarządzania ryzykiem (art. 8 UKSC), przeprowadzania audytu bezpieczeństwa (art. 15), procedury zgłaszania i postępowania z incydentami oraz obowiązek ich obsługi i zgłaszania incydentów poważnych³⁵⁷ w ciągu 24 godzin od ich wykrycia do właściwego CSIRT (art. 11-13 UKSC). Z kolei dostawcy usług cyfrowych to, zgodnie z art. 17 ust. 1 UKSC, osoby prawne albo jednostki organizacyjnej bez tej osobowości (z zarządem, siedzibą lub przedstawicielem na polskim terytorium) świadczące usługi cyfrowe wskazanych w załączniku nr 2 do UKSC (internetowa platforma handlowa; usługa przetwarzania w chmurze; wyszukiwarka internetowa). Obowiązki spoczywające na dostawcach usług cyfrowych (art. 17-20) są z zasady mniejsze niż obowiązki operatorów usług kluczowych³⁵⁸, obejmując m.in. wdrożenie

³⁵⁶ G. Szpor [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, Warszawa 2019, art. 4, pkt 1.

³⁵⁷ Zdefiniowany w art. 2 ust. 7 UKSC.

³⁵⁸ D. Markopoulou, V. Papakonstantinou, P. de Hert, The new EU cybersecurit' framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, CLSR 2019, Vol. 35, Iss. 6, s. 5.

odpowiednich środków technicznych i organizacyjnych w celu zapewnienia cyberbezpieczeństwa odpowiedniego do ryzyka (art. 17 ust. 2 UKSC), obowiązki dotyczące wykrywania, rejestrowania, analizowania oraz klasyfikowania incydentów (art. 18 UKSC) oraz obowiązek zgłaszania incyduentu istotnego³⁵⁹ w ciągu 24 godzin od momentu wykrycia do właściwego CSIRT (art. 18 ust. 1 pkt 4 w zw. z art. 19 UKSC).

RODO wymienione zostało w UKSC cztery razy, w art. 39 UKSC normującym przetwarzanie danych osobowych w celu realizacji zadań publicznych przez podmioty administrujące ustanowione w UKSC, tworząc tym samym ustawową podstawę do przetwarzania tych danych przez podmioty administrujące. Wobec braku szczegółowych unormowań o relacji UKSC do RODO, w pozostałym zakresie do przetwarzania danych osobowych znajdują zastosowanie przepisy RODO, a wobec zadań i kompetencji CSIRT GOV i organów ścigania oraz jednostek prokuratury – także, w ograniczonym zakresie, Dyrektywy LED i Ustawy o LED³⁶⁰.

Zakres krzyżowania się zakresu przedmiotowego RODO i aktów prawnych regulujących cyberbezpieczeństwo dotyczy dwóch co najmniej obszarów – zgłaszania i obsługi incydentów w zakresie, w jakim stanowią jednocześnie naruszenie ochrony danych oraz wprowadzenie odpowiednich środków technicznych i organizacyjnych w zakresie w jakim jednocześnie zapewniają one zgodność z regułami cyberbezpieczeństwa adekwatnego do ryzyka, a jednocześnie bezpieczne przetwarzanie danych osobowych³⁶¹. Za niesłuszny należy uznać przedstawiony w literaturze przez A. Szkurlata pogląd, że PUODO „ma minimalną możliwość ingerowania w kwestie dotyczące cyberbezpieczeństwa” ograniczoną do monitorowania przestrzegania art. 39 UKSC (przywołanego wyżej)³⁶². Niesłuszność tego poglądu wynika z nieuwzględnienia perspektywy organów nadzorowanych, które jednocześnie zobowiązane są do przestrzegania UKSC i RODO. To oznacza, że w obszarze krzyżowania się zakresów przedmiotowych tych aktów, podlegają one dwóm osobnym obowiązkom zgłoszenia incydentów będących naruszeniami ochrony danych osobowych. Teoretycznie, w obecnym stanie prawnym mogłoby to prowadzić do wszczęcia osobnych postępowań administracyjnych

³⁵⁹ Zdefiniowany w art. 2 ust. 8 UKSC.

³⁶⁰ P. Drobek [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, art. 39, pkt 1.

³⁶¹ Por. także P. de Hert, *Post-GDPR Lawmaking in the Digital Data Society: Mimesis without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law*, [in:] *Data at the Boundaries of European Law*, edited by D. Curtin, M. Catanzariti, Oxford 2023, <https://doi.org/10.1093/oso/9780198874195.003.0004> (dostęp: 30.01.2024 r.), s. 100-104.

³⁶² A. Szkurlat, *Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych*, iKAR 2020, t. 9, nr 2, s. 54-60.

i nałożenia odrębnych administracyjnych kar pieniężnych, a ewentualne akty prawa miękkiego wydane przez organy ochrony danych lub EROD dotyczące prawidłowych środków technicznych i organizacyjnych mogą wpłynąć na wykonywanie przez te podmioty nadzorowane obowiązków wynikających z UKSC. W tym funkcjonalnym ujęciu PUODO ma „istotną możliwość ingerowania w kwestie dotyczące cyberbezpieczeństwa”.

Jako przykład, poniżej scharakteryzowany zostanie obowiązek zgłaszania incydentów w odniesieniu do incydentów istotnych, których obowiązek zgłoszenia spoczywa na dostawcach usług cyfrowych (art. 18 ust. 1 lit. a UKSC) wobec obowiązku zgłaszania do organu ochrony danych (PUODO) naruszenia ochrony danych (art. 32 RODO). Najpierw analiza dokonana zostanie na podstawie UKSC, a potem – z uwagi na zmianę sposobu określenia zakresu podmiotowego w Dyrektywie NIS 2 – scharakteryzowane zostaną zmiany w obowiązku notyfikacyjnym wprowadzone przez Dyrektywę NIS 2, z uwzględnieniem zagadnień dotyczące danych osobowych. Należy wskazać, że obowiązki informowania o incydentach dotyczących cyberbezpieczeństwa lub naruszenia ochrony danych ustanowione zostały także w innych aktach prawnych, w tym sektorowych³⁶³, m.in. Dyrektywa ePrivacy (art. 4 ust. 3); Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym³⁶⁴ (art. 19 ust. 2)³⁶⁵. Skomplikowanie tych różnych chociaż podobnych obowiązków notyfikacyjnych krytykowane jest w literaturze, w której postulowane jest uproszczenie ich wykonywania³⁶⁶.

Celem zgłaszania incydentów w UKSC jest zapewnienie bezpieczeństwa i spójności krajowego systemu cyberbezpieczeństwa, a celem zgłaszania naruszeń ochrony danych do organu ochrony danych jest zwiększenie ochrony danych osobowych. Cele te są zbieżne, ale nie są tożsame. Wpływa to na sposób unormowania zgłaszania incydentów. Zgodnie z art. art. 18 ust. 1 lit. a UKSC, dostawca usługi cyfrowej zgłasza incydent istotny³⁶⁷ nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT. Przy klasyfikacji

³⁶³ Dzieli się je w literaturze na obowiązki: dotyczące incydentów cyberbezpieczeństwa i dotycząc– naruszenia ochrony danych osobowych - Por. M. G. Porcedda, *Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*, CLSR 2018, Vol. 34, No. 5, s. 1079-1080.

³⁶⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L z 2014 r. nr 257, s. 73).

³⁶⁵ Por. M. G. Porcedda, *Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*, CLSR 2018, Vol. 34, No. 5, s. 1079-1081.

³⁶⁶ M. G. Porcedda, *Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*, CLSR 2018, Vol. 34, No. 5, s. 1097-1098.

³⁶⁷ Zdefiniowany w art. 2 ust. 8 UKSC.

incydentu jako istotnego uwzględniane są w szczególności kryteria wskazane w art. 18 ust. 2-3 UKSC, w tym liczba użytkowników, których dotyczy incydent, i zakres wpływu incydentu na działalność gospodarczą i społeczną. Zgłoszenie incydentu istotnego do właściwego CSIRT winno spełniać elementy wskazane w art. 19 UKSC, w tym informacje o podjętych działaniach zapobiegawczych i informacje o podjętych działaniach naprawczych. Zarówno organy właściwe w sprawach cyberbezpieczeństwa (art. 42 ust. 7 UKSC), jak i CSIRT-y (art. 39 ust. 7 UKSC), jak i zobowiązane są do współpracy z PUODO, w tym w szczególności koordynacji obsługi incydentu, który doprowadził do naruszenia ochrony danych osobowych (art. 34 ust. 2 UKSC)³⁶⁸.

Zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych ³⁶⁹, administrator zgłasza je organowi ochrony danych w ciągu 72 godzin po stwierdzeniu naruszenia, „chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych”. Nie każdy incydent istotny w rozumieniu UKSC stanowi naruszenie ochrony danych i nie każde naruszenie ochrony danych stanowi incydent istotny w rozumieniu UKSC. Należy jednak przyjąć, że z większością incydentów istotnych w rozumieniu UKSC związane jest duże prawdopodobieństwo naruszenia ochrony danych, ponieważ zazwyczaj prowadzą one do „przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych” (art. 4 pkt 12 RODO). Oznacza to, że dostawca usługi cyfrowej, który jest jednocześnie administratorem danych w rozumieniu RODO, zobowiązany będzie do dokonania zgłoszenia takiego incydentu istotnego zgodnie z UKSC w ciągu 24 godzin od jego wykrycia i do zgłoszenia naruszenia ochrony danych zgodnie z RODO w ciągu 72 godzin po jego stwierdzeniu.

W Dyrektywie NIS 2 obowiązki w zakresie zgłaszania incydentów przez podmioty kluczowe i ważne unormowane zostały w art. 23 ust. 1-11. Prawodawca unijny zidentyfikował opisane wyżej mankamenty obowiązku zgłaszania incydentów. Stąd też Dyrektywa NIS 2 zawiera postulat uchylenia niektórych przepisów sektorowych nakładających wymogi w zakresie bezpieczeństwa i zgłaszania incydentów (motyw 92 Dyrektywy NIS 2), a w motywie 108 Dyrektywy NIS 2 wyrażono powinność organów właściwych do spraw cyberbezpieczeństwa do współpracy i wymiany informacji „dotyczących wszystkich istotnych kwestii” związanych z incydentami z organami ochrony danych, co skonkretyzowane zostało

³⁶⁸ Por. podrozdział rozprawy 3.5.3. poniżej.

³⁶⁹ Zdefiniowane w art. 4 pkt 12 RODO.

w art. 31 ust. 3 Dyrektywy NIS 2. Ponadto, w motywie 106 Dyrektywy NIS 2 sformułowano zachętę dla państw członkowskich, aby ustanowiły pojedynczy punkt zgłoszenia incydentów, do którego podmiot nadzorowany dokonywał będzie zgłoszeń na podstawie unijnych aktów prawnych przewidujących taki obowiązek, w tym Dyrektywy NIS 2, RODO i Dyrektywy ePrivacy. Należy podkreślić jednak, że prawodawca nie zdecydował się na nałożenie na państwa członkowskie obowiązku ustanowienia takiego punktu, zatem ostateczny kształt przyjętych rozwiązań będzie różnił się w poszczególnych państwach.

Unikalnym rozwiązaniem jest art. 35 ust. 2 Dyrektywy NIS 2, który przewiduje, że, jeżeli organy ochrony danych nałożą na podmiot nadzorowany administracyjną karę pieniężną na podstawie RODO za naruszenie ochrony danych, to organy właściwe do spraw cyberbezpieczeństwa nie mogą nałożyć administracyjnej kary pieniężnej na podstawie Dyrektywy NIS 2 w celu sankcjonowania tego samego zachowania podmiotu nadzorowanego (stanowiącego także naruszenie obowiązków określonych w art. 21 i 23 Dyrektywy NIS 2), przy czym mogą zastosować inne „środki egzekwowania przepisów”. Nie jest jasne czy to ograniczenie w nakładaniu administracyjnej kary pieniężnej przez organy właściwe do spraw cyberbezpieczeństwa dotyczy wszystkich naruszeń art. 21 i 23 Dyrektywy NIS 2, które objęte zostały taką karą przez organy ochrony danych, czy też tylko takich, o których organy właściwe do spraw cyberbezpieczeństwa przekazały uprzednio informację do organów ochrony danych na podstawie art. 35 ust. 1 Dyrektywy NIS 2³⁷⁰.

Podsumowując, zakresy przedmiotowe RODO i aktów prawnych regulujących cyberbezpieczeństwo krzyżują się, a konsekwencją tego krzyżowania jest istnienie równoległych obowiązków do wdrożenia odpowiednich środków technicznych i organizacyjnych oraz do zgłaszania incydentów (naruszeń ochrony danych). W obecnym stanie prawnym zarówno PUODO, jak i organy właściwe do spraw cyberbezpieczeństwa uprawnione są do stosowania ustanowionych w RODO i UKSC administracyjnych kar pieniężnych, które mogą zostać nałożone przez oba te organy niezależnie³⁷¹, natomiast na skutek implementacji Dyrektywy NIS 2 ulegnie to zmianie. Ewolucja unormowań w tej kwestii stanowi ważny przykład zmniejszenia przez prawodawcę unijnego ryzyka wynikających ze zjawiska krzyżowania się kompetencji podmiotów administrujących w obszarze przetwarzania danych osobowych.

³⁷⁰ W przedmiocie możliwości zastosowaniu zasady *ne bis in idem* w prawie administracyjnym por. rozdział 4 niniejszej rozprawy.

³⁷¹ Por. podrozdział 3.5.1. i 3.5.3. poniżej.

2.6.3. AKTY PRAWNE PRAWA KONKURENCJI, AKT O RYNKACH CYFROWYCH I AKT O USŁUGACH CYFROWYCH

W tym podrozdziale analizie poddany został zakres przedmiotowy aktów prawnych prawa konkurencji *sensu stricto*³⁷² w ograniczonym zakresie – prawa unijnego i krajowego dotyczącego kontroli koncentracji i nadużycia pozycji dominującej, oraz Akt o Rynkach Cyfrowych (DMA) i Akt o Usługach Cyfrowych (DSA). Dyskusyjne jest, czy oba te akty należy zaliczyć do prawa konkurencji³⁷³. Z uwagi jednak na bliskość zakresów przedmiotowych tych aktów i celów (zwłaszcza DMA³⁷⁴) z prawem konkurencji, fakt, że ich stosowanie w zasadniczym stopniu jest scentralizowane z kluczową rolą Komisji jako podmiotu administrującego, a także względy redakcyjne podjęto decyzję o omówieniu tych aktów w jednym podrozdziale. Należy wskazać, że również samo wyodrębnienie prawa konkurencji jako samodzielnej kompleksowej gałęzi prawa może być dyskusyjne, jednak w literaturze dokonanie takiego wyodrębnienia, choćby z przyczyn funkcjonalnych, należy uznać aktualnie za powszechne³⁷⁵. Na potrzeby tej rozprawy doktorskiej przyjęto pogląd, że użycie terminu „prawo konkurencji” jest uzasadnione.

2.6.3.1. PRAWO KONKURENCJI – KONTROLA KONCENTRACJI I NADUŻYCIE POZYCJI DOMINUJĄCEJ

RODO i prawo konkurencji różni się zarówno zakresem przedmiotowym (kontrola koncentracji, nadużycie pozycji dominującej i porozumienia oraz praktyki uzgodnione) i zakresem podmiotowym³⁷⁶. Zakres podmiotowy prawa konkurencji obejmuje „przedsiębiorstwa” definiowane w sposób szeroki (co zapewnić ma szeroką realizację prawa konkurencji) jako „każda jednostka zaangażowana w działalność gospodarczą”, przy czym bez znaczenia pozostaje forma organizacyjna, charakter finansowania i czy jest to jednostka

³⁷² Wstęp [w:] *Prawo konkurencji*, red. A. Jurkowska-Gomułka, A. Piszcz, Warszawa 2024.

³⁷³ Por. np. N. Moreno Bellosio, N. Petit, *The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove*, „European Law Review” 2023, Vol. 48, No. 4, <https://ssrn.com/abstract=4411743> (dostęp: 20.09.2024 r.); Komisja, *Keynote of EVP Vestager at the European Competition Law Tuesdays: A Principles Based approach to Competition Policy*, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_6393 (dostęp: 20.09.2024 r.).

³⁷⁴ Por. E. M. Fox, D. Gerard, *EU Competition Law. Cases, Textes and Context*, Cheltenham 2023, s. 325.

³⁷⁵ Przykładowo, wydany w 2024 r. tom Systemu Prawa UE dokonuje takiego wyodrębnienia używając w tytule terminu „prawo konkurencji”, por. *Prawo konkurencji*, red. A. Jurkowska-Gomułka, A. Piszcz, Warszawa 2024, s. 6-7.

³⁷⁶ F. Costa-Cabral, O. Lynskey, *Family ties: the intersection between data protection and competition in EU Law*, „Common Market Law Review” 2017, Vol. 54, No. 11, s. 6.

prywatna czy publiczna³⁷⁷. Kwestia relacji Dyrektywy ODO, a następnie RODO wobec prawa konkurencji od wielu lat jest przedmiotem zainteresowania organów³⁷⁸ i doktryny³⁷⁹, która identyfikuje zarówno możliwości synergii między nimi, jak i potencjalne odmienności, wynikające z relacji między przeważającymi celami aktów prawnych nakierowanych na ochronę danych osobowych i prawa konkurencji, którego to cel określony jest z kolei jako zapewnienie „efektywności rynku wewnętrznego i dobrobytu konsumentów (*consumer welfare*)³⁸⁰”. Wskazuje się, że RODO i prawo konkurencji wpływają „na zachowania rynkowe w innych punktach tego samego spektrum³⁸¹”, a łączy je (razem z prawem ochrony konsumenta) zasada rzetelności (*fairness*) jako podstawa odnosząca się do celów UE (art. 3 TUE)³⁸².

Z uwagi na obszerność i złożoność prawa konkurencji³⁸³, w niniejszym podrozdziale zbadana zostanie kontrola koncentracji uregulowana w Merger Control Regulation i krajowym prawie konkurencji (UKK) oraz unormowania dotyczące nadużycia pozycji dominującej w art. 102 TFUE i krajowym prawie konkurencji (UKK) z ograniczeniem do zagadnień, których analiza pozwoli zweryfikować hipotezę o krzyżowaniu się zakresu przedmiotowego

³⁷⁷ Por. K. Kohutek [w:] *Komentarz do rozporządzenia nr 139/2004 w sprawie kontroli koncentracji przedsiębiorstw*, SIP LEX/el. 2013, art. 1, pkt 2 i przywołany tam Wyrok TS z 23.04.1991 r., C-41/90, Klaus Höfner i Fritz Elser v. Macrotron GmbH, ECR 1991, nr 4, poz. I-1979.

³⁷⁸ Przykładowo: Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 10.09.2024 r.).

³⁷⁹ Przykładowo: F. Costa-Cabral, O. Lynskey, Family ties: the intersection between data protection and competition in EU Law, „Common Market Law Review” 2017, Vol. 54, No. 11; G. Colangelo, M. Maggiolino, Data protection in attention markets: protecting privacy through competition?, „Journal of European Competition Law & Practice” 2017, Vol. 8, No. 6, s. 363-369; B. Kira, V. Sinha, S. Srinivasan, Regulating digital ecosystems: bridging the gap between competition policy and data protection, „Industrial and Corporate Change” 2021, Vol. 30, No. 5, s. 1337-1360; I. Graef, EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility, PhD summary, Kluwer Law International 2016, <https://ssrn.com/abstract=3635378> (dostęp: 08.09.2024 r.); M. Botta, K. Wiedemann, The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey, „The Antitrust Bulletin 64” 2019, No. 3, s. 428-446; K. Majcher, Coherence between Data Protection and Competition Law in Digital Markets, Oxford 2023; K. Singh, S. Mishra, Interplay of Data in Digital Economy and Merger Control Regime: A Conundrum without Solutions, „Law, State and Telecommunications Review” 2022, Vol. 14, No. 2, 17-37.

³⁸⁰ Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf, s. 11 (dostęp: 20.09.2024 r.).

³⁸¹ F. Costa-Cabral, O. Lynskey, *Family ties: the intersection between data protection and competition in EU Law*, „Common Market Law Review” 2017, Vol. 54, No. 11, s. 7.

³⁸² I. Graef, D. Clifford, P. Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, Int. Data Priv. Law 2018, Vol. 8, No. 3, <https://ssrn.com/abstract=3216198> (dostęp: 20.09.2024 r.), s. 200.

³⁸³ Por. np. R. Blicharz, K. Horubski, M. Pawełczyk, *Rozdział XI. Prawo konkurencji w systemie publicznego prawa gospodarczego* [w:] *Publiczne prawo gospodarcze*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2018.

prawa konkurencji z zakresem przedmiotowym RODO. W założeniu jest to zatem uproszczona analiza tych zagadnień prawa konkurencji³⁸⁴.

Kontroli koncentracji rozumiana jest zgodnie z art. 3 Merger Control Regulation rozumiana jako trwała zmiana kontroli wynikająca z łączenia się lub przejęcia przedsiębiorstwa. Merger Control Regulation stosuje się do koncentracji kwalifikowanych jako „wspólnotowe” (art. 1 ust. 1 Merger Control Regulation), gdzie kryterium stanowi z zasady wysokość obrotu zainteresowanych przedsiębiorstw (szczegóły w art. 1 ust. 2-3 Merger Control Regulation). W uproszczeniu można przyjąć, że Merger Control Regulation stosuje się zasadniczo do koncentracji między największymi przedsiębiorstwami, a pozostałe koncentracje badane są przez krajowe organy konkurencji. Podmioty dokonujące koncentracji zobowiązane są do jej uprzedniego zgłoszenia (art. 4 Merger Control Regulation) i nie mogą wprowadzić jej w życie przed uznaniem jej za zgodną ze wspólnym rynkiem (art. 7 Merger Control Regulation). Analogiczny model uprzedniego zgłaszania wybranych koncentracji (art. 13-14 UKK) przyjęto także w krajowym UKK (dział III UKK, art. 13-23).

Kontroli koncentracji, zarówno na poziomie wspólnotowym, jak i na poziomie krajowym, dokonuje się przy użyciu tzw. testu SIEC (test istotnego ograniczenia efektywnej konkurencji)³⁸⁵. Te koncentracje, które „nie przeszkadzałyby znacząco skutecznej konkurencji na wspólnym rynku lub znacznej jego części, w szczególności w wyniku stworzenia lub umocnienia pozycji dominującej”, są zgodne ze wspólnym rynkiem; jeżeli natomiast wynik testu jest przeciwny, takie koncentracje uznaje się za niezgodne (art. 2 ust. 2 i 3 Merger Control Regulation). Proces weryfikacji tego testu przez organy prawa konkurencji jest złożony i wieloelementowy, a Komisja opublikowała wytyczne określające sposób przeprowadzania tej weryfikacji w odniesieniu do poszczególnych typów koncentracji³⁸⁶. Prawodawca unijny normuje, że test ten powinien uwzględniać: „potrzebę zachowania i rozwoju skutecznej konkurencji na wspólnym rynku, z punktu widzenia między innymi struktury wszystkich danych rynków (...)” oraz „pozycję rynkową zainteresowanych przedsiębiorstw oraz ich siłę ekonomiczną i finansową, możliwości dostępne dla dostawców i użytkowników, ich dostęp do

³⁸⁴ Por. publikacje o charakterze podręcznika, np. W. Frenz, *Handbook of EU competition law*, Berlin 2016. C. Banasiński, D. Aziewicz, A. M. Bielecki et al., *Polskie prawo antymonopolowe: zarys wykładu*, Warszawa 2018.

³⁸⁵ M. Kozak, Glosa do wyroku Sądu Ochrony Konkurencji i Konsumentów z 12 maja 2022 r. w sprawie XVII AmA 61/21, iKAR 2022, t. 11, nr 4, s. 106.

³⁸⁶ Przykładowo: Wytyczne w sprawie oceny horyzontalnego połączenia przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw (Dz. U. UE. C. z 2004 r. nr 31, s. 5); Wytyczne w sprawie oceny niehoryzontalnych połączeń przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw (Dz. U. UE. C. z 2008 r. nr 265, s. 6).

zaopatrzenia lub rynków, wszelkie prawne lub inne bariery wejścia na rynek, trendy podaży i popytu w stosunku do właściwych dóbr i usług, interesy konsumentów pośrednich i końcowych oraz rozwój postępu technicznego i gospodarczego, pod warunkiem że dokonuje się on z korzyścią dla konsumentów i nie stanowi przeszkody dla konkurencji”. (art. 2 ust. 1 lit. a-b Merger Control Regulation). Analogiczne kryteria przyjęto w krajowym prawie konkurencji (art. 18-22 UKK)³⁸⁷. Chociaż to ustanowienie lub wzmocnienie pozycji dominującej przedsiębiorstwa (lub wspólnej pozycji dominującej) jest najczęstszą przyczyną uznania, że koncentracja nie spełnia testu SIEC³⁸⁸, to dyskusyjne jest, czy do stwierdzenia, że koncentracja powoduje znaczne utrudnienie skutecznej konkurencji należy brać pod uwagę także kryteria pozaekonomiczne³⁸⁹.

Pozycja dominująca nie została zdefiniowana w prawie unijnym (jej pojęcie jest przedmiotem rozbudowanego orzecznictwa sądów unijnych), natomiast posiada definicję w art. 4 pkt 10 UKK, zgodnie z którą jest to pozycja przedsiębiorcy „umożliwiająca mu zapobieganie skutecznej konkurencji na rynku właściwym przez stworzenie mu możliwości działania w znacznym zakresie niezależnie od konkurentów, kontrahentów oraz konsumentów”, co uzupełnione jest przez wzruszalne³⁹⁰ domniemanie pozycji dominującej w przypadku udział w rynku właściwym przekracza 40%. Na potrzeby tej rozprawy przyjęto, że ta definicja odpowiada pojmowaniu pozycji dominującej w prawie unijnym³⁹¹. Dla dokonania oceny pozycji dominującej zarówno na potrzeby kontroli koncentracji, jak i spraw dotyczących nadużycia pozycji dominującej podstawowym jest ustalenie rynku właściwego, który wyznacza punkt odniesienia dla dokonywanej tej oceny. Podobnie jak w przypadku pojęcia pozycji dominującej, tak również pojęcie rynku właściwego zdefiniowane zostało w prawie krajowym, a definicja ta zasadniczo odpowiada znaczeniu terminu „rynek właściwy”

³⁸⁷ Por. E. Stawicki [w:] *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, red. A. Stawicki, Warszawa 2016, art. 20.

³⁸⁸ Pkt 4 wytycznych w sprawie oceny horyzontalnego połączenia przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw (Dz. U. UE. C. z 2004 r. nr 31, s. 5).

³⁸⁹ Krytycznie w odniesieniu do czynnika pluralizmu mediów w krajowym prawie konkurencji M.K. Derdak; M. K. Derdak, *Problem uwzględniania pozaekonomicznych czynników oceny koncentracji przez Prezesa UOKiK na przykładzie pluralizmu mediów*, IKA 2022, nr 4, s. 32-52. Por. także L. O'Callaghan, *The Intersection between Data Protection and Competition Law: How To Incorporate Data Protection, as a Non-Economic Objective, into EU Competition Analysis*, „Trinity College Law Review” 2018, Vol. 21, s. 109.

³⁹⁰ A. Mała, 4.3. Ocena koncentracji. Rodzaje decyzji kończących postępowanie antymonopolowe w sprawach koncentracji i kryterium ich wydawania [w:] *Prawo konkurencji*, red. A. Bolecki et al., Warszawa 2012, SIP LEX.

³⁹¹ K. Kohutek, [w:] M. Sieradzka, K. Kohutek, *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa 2014, art. 4, 10. Pozycja dominująca – uwagi ogólne oraz przesłanki jej posiadania, SIP LEX. Por. także Komunikat Komisji – wytyczne w sprawie priorytetów, którymi Komisja będzie się kierować przy stosowaniu art. 82 Traktatu WE w odniesieniu do szkodliwych działań o charakterze praktyki wyłączającej, podejmowanych przez przedsiębiorstwa dominujące (Dz. U. UE. C. z 2009 r. nr 45, s. 7 z późn. zm.).

w prawie unijnym³⁹². Zgodnie z art. 4 ust. 9 UKK, rynek właściwy to „rynek towarów, które ze względu na ich przeznaczenie, cenę oraz właściwości, (...), są uznawane przez ich nabywców za substytuty oraz są oferowane na obszarze, na którym, ze względu na ich rodzaj i właściwości, istnienie barier dostępu do rynku, preferencje konsumentów, znaczące różnice cen i koszty transportu, panują zbliżone warunki konkurencji”. Pojęcie rynku właściwego jest fundamentalne dla merytorycznego rozpoznania spraw w prawie konkurencji, a w literaturze prowadzona jest dyskusja w jaki sposób ustalenie rynku właściwego winno się odbywać, w tym do jakiego stopnia pod uwagę winna być brana specyfika poszczególnych sektorów gospodarki³⁹³, w tym przedsiębiorstw, których model biznesowy związany jest z przetwarzaniem danych osobowych³⁹⁴.

Z perspektywy krzyżowania się zakresów przedmiotowych RODO i prawa konkurencji w odniesieniu do kontroli koncentracji kluczowe jest ustalenie czy ocena wpływu koncentracji na ochronę danych osobowych może mieć wpływ na wynik testu SIEC. Zgodnie z przywoływanym w literaturze orzecznictwem sądów unijnych kwestie dotyczące ochrony danych osobowych „nie podlegają, jako takie prawu konkurencji, mogą być rozstrzygnięte na podstawie właściwych przepisów o ochronie tych danych”. Oznacza to, że zarówno organy ochrony konkurencji, jak i unijne sądy wciąż podchodzą z dystansem do uwzględniania tego czynnika,³⁹⁵ chociaż Komisja w niektórych decyzjach wydanych w ostatnich latach (przykładowo, sprawy Facebook/WhatsApp z 2014 r.³⁹⁶ i Microsoft/LinkedIn z 2016 r.³⁹⁷)

³⁹² Por. Obwieszczenie Komisji w sprawie definicji rynku właściwego do celów wspólnotowego prawa konkurencji (Dz. U. UE. C. z 1997 r. nr 372, s. 5).

³⁹³ O definicji rynku właściwego i nieadekwatności tzw. testu SSNiP patrz: W. Herbet, K. Racka, Definiowanie rynku właściwego w sektorze farmaceutycznym w sprawach antymonopolowych – rola Obwieszczenia KE w sprawie definicji rynku właściwego do celów wspólnotowego prawa konkurencji, IKA 2020, nr 5, s. 91-105. Por. także K. Korn, Określanie rynku właściwego w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej w latach 1997-2010, ZNUJ. PPWI 2012, nr 2, s. 114-127.

³⁹⁴ W odniesieniu do „gospodarki cyfrowej”: B. Targański, Definiowanie rynków produktowych w gospodarce cyfrowej w świetle projektu Zawiadomienia Komisji w sprawie definicji rynku właściwego do celów unijnego prawa konkurencji z 8 listopada 2022 roku, IKA 2023, nr 1, s. 74-84.

³⁹⁵ F. Costa-Cabral, O. Lynskey, *Family ties: the intersection between data protection and competition in EU Law*, „Common Market Law Review” 2017, Vol. 54, No. 11, s. 7 i przywołany tam wyrok TS z 23.11.2006 r., C-238/05, Asnef-Equifax, Servicios De Información Sobre Solvencia Y Crédito, S.L. v. Asociación De Usuarios De Servicios Bancarios (AUSBANC), ZOTSIS 2006, nr 11, poz. I-11125, pk– 63.

³⁹⁶ Decyzja Komisji, sprawa COMP/M.7217 - Facebook/ WhatsApp, 03.10.2014, pkt. 87-90, pkt 174. Por. także N. Zingales, *Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law*, CLSR 2017, Vol. 33, No. 4, s. 553-558.

³⁹⁷ Decyzja Komisji, sprawa M.8124 – Microsoft/LinkedIn, 6.12.2016 r. pkt. 177-179, pkt 350. Oba powyższe cytowania za: I. Graef, D. Clifford, P. Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, Int. Data Priv. Law 2018, Vol. 8, No. 3, <https://ssrn.com/abstract=3216198> (dostęp: 20.09.2024 r.), s. 214.

zdaje się rozpoznawać rolę ochrony danych osobowych w ocenie stanu konkurencji³⁹⁸, chociaż robi to niekonsekwentnie³⁹⁹. Z kolei za jego jednoznacznym uwzględnieniem opowiedział się EROD, wskazując, że „poziom ochrony danych (...) należy uwzględniać w ramach każdej oceny potencjalnego nadużycia pozycji dominującej oraz połączeń przedsiębiorstw⁴⁰⁰”, co jeszcze w czasie obowiązywania Dyrektywy ODO podnosił także EIOD⁴⁰¹. W literaturze toczy się spór czy uwzględnienie czynnika ochrony danych osobowych przy ocenie koncentracji w ocenie kontroli koncentracji w unijnym prawie konkurencji należy połączyć pojęciem dobrobytu konsumentów (*consumer welfare*) przez jego rozszerzenie o kryteria pozaekonomiczne⁴⁰². Opowiedzenie się za uwzględnieniem tego czynnika oznacza, że w odniesieniu do koncentracji, których przedmiotem są przedsiębiorstwa przetwarzające dane osobowe (zwłaszcza znaczne ilości tych danych i ich szczególne kategorie), oznacza, że taka koncentracja powinna być oceniana przez organy ochrony konkurencji z perspektywy prawa podstawowego do ochrony danych osobowych i RODO jako element oceny wpływu na dobrobyt konsumentów. Ma to znaczenie zwłaszcza dla przedsiębiorstw będących platformami internetowymi (np. wyszukiwarki i platformy społecznościowe), które wykorzystują dane do poprawy jakości swoich produktów i usług, ale także do ukierunkowanej reklamy (tak zwany rynek wielostronny)⁴⁰³.

Przedsiębiorstwa mogą argumentować, że koncentracja powinna być dopuszczona nawet w sytuacji spełnienia testu SIEC, jeżeli zachodzą okoliczności szczególne, co powinno prowadzić do udzielenia zgody na koncentrację⁴⁰⁴. Nie dokonując pogłębionej charakterystyki zagadnienia zgód szczególnych na koncentrację⁴⁰⁵, wskazać należy, że dotyczy to sytuacji, w których w przypadku braku dokonania koncentracji doszłoby do powstania szkody dla

³⁹⁸ I. Graef, D. Clifford, P. Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, Int. Data Priv. Law 2018, Vol. 8, No. 3, <https://ssrn.com/abstract=3216198> (dostęp: 20.09.2024 r.), s. 214.

³⁹⁹ Por. M. C. Wasastjerna, The implications of big data and privacy on competition analysis in merger control and the controversial competition-data protection interface, „European Business Law Review” 2019, Vol. 30, No. 3, s. 346-376.

⁴⁰⁰ EROD, *Oświadczenie Europejskiej Rady Ochrony Danych w sprawie wpływu koncentracji gospodarczych na ochronę danych*, 27 sierpnia 2018 r., https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_pl.pdf (dostęp: 28.09.2024 r.).

⁴⁰¹ EIOD, *Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (dostęp: 28.09.2024 r.), s. 15.

⁴⁰² F. Costa-Cabral, O. Lynskey, *Family ties: the intersection between data protection and competition in EU Law*, „Common Market Law Review” 2017, Vol. 54, No. 11, s. 3.

⁴⁰³ I. Małobęcka-Szwast, Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi, IKA 2018, nr 8, s. 139-153, s. 142.

⁴⁰⁴ T. Skoczny, *Zgody szczególne w prawie kontroli koncentracji*, Warszawa 2012, s. 35-36.

⁴⁰⁵ Por. wyczerpująca monografia w tym przedmiocie: T. Skoczny, *Zgody szczególne w prawie kontroli koncentracji*, Warszawa 2012.

dobrobytu konsumentów lub też dokonanie koncentracji przynosi szczególne korzyści, które nakazują udzielenie zgody⁴⁰⁶. Przykładowo, zgoda może zostać udzielona, jeżeli koncentracja ma na celu ratunek upadającego przedsiębiorstwa (*failing firm defence*)⁴⁰⁷, lub też, jeżeli przemawiają za tym tzw. korzyści efektywnościowe (*efficiencies*), rozumiane w ten sposób, że powodem dopuszczenia koncentracji jest prognozowane polepszenie dobrobytu ekonomicznego, co jest postulowane zwłaszcza przez badaczy nauk ekonomicznych⁴⁰⁸. Przyjęcie argumentacji korzyści efektywnościowych może stanowić jednak zagrożenie dla prawa podstawowego dla ochrony danych osobowych, jeżeli korzyści efektywnościowe mają polegać na połączeniu lub dzieleniu się zbiorami danych⁴⁰⁹.

Unijne (Komisja) i krajowe organy konkurencji mogą wydać bezwarunkową zgodę na koncentrację, zakaz jej albo też uwarunkować zgodę od spełnienia określonych obowiązków (zwanych środkami zaradczymi; *remedies*⁴¹⁰)⁴¹¹. Katalog środków zaradczych jest otwarty, a polski prawodawca podaje następujące przykłady: zbycie całości lub części majątku jednego lub kilku przedsiębiorców; wyzbycie się kontroli nad określonym przedsiębiorcą; udzielenia licencji praw wyłącznych konkurentowi (por. art. 19 ust. 2 UKK). Skoro katalog tych środków jest otwarty, to w odniesieniu do koncentracji, których przedmiotem są przedsiębiorstwa przetwarzające dane osobowe, możliwe jest wprowadzenie środków zaradczych, które będą dotyczyły bezpośrednio tych danych osobowych. Jeżeli takie rozwiązanie zostanie zastosowane przez organy prawa konkurencji, to powinno ono pozostać w zgodzie z aktami prawnymi nakierowanymi na ochronę danych osobowych. Było to przedmiotem dyskusji w odniesieniu do francuskiej sprawy nadużycia pozycji dominującej przez podmiot GDF Suez, w której to francuski organ ochrony konkurencji nakazał temu przedsiębiorstwu umożliwienie konkurentom dostępu do danych osobowych jego klientów (będących konsumentami), czego ostatecznie dokonano w uzgodnieniu z francuskim organem ochrony danych osobowych⁴¹².

⁴⁰⁶ T. Skoczny, *Zgody szczególne w prawie kontroli koncentracji*, Warszawa 2012, s. 36-37.

⁴⁰⁷ T. Skoczny, *Zgody szczególne w prawie kontroli koncentracji*, Warszawa 2012, s. 37-38.

⁴⁰⁸ Por. M. Danek, *Korzyści efektywnościowe w kontroli koncentracji przedsiębiorstw w systemach ochrony konkurencji Unii Europejskiej i Stanów Zjednoczonych Ameryki – porównanie prawno-ekonomiczne*, ZNUJ. PPWI 2012, nr 3, s. 129-160, s. 131.

⁴⁰⁹ I. Graef, D. Clifford, P. Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, Int. Data Priv. Law 2018, Vol. 8, No. 3, <https://ssrn.com/abstract=3216198> (dostęp: 20.09.2024 r.), s. 222.

⁴¹⁰ M. Błachucki, *System postępowania antymonopolowego w sprawach kontroli koncentracji Przedsiębiorców*, UOKiK, 2012, s. 65.

⁴¹¹ Por. charakterystyka kompetencji organów konkurencji w rozdziale 3. rozprawy.

⁴¹² R. Dacar, *Is the Essential Facilities Doctrine Fit for Access to Data Cases? The Data Protection Aspect*, „Croatian Yearbook of European Law & Policy” 2022, Vol. 18, No. 1, s. 66; I. Graef, D. Clifford, P. Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, Int. Data Priv. Law 2018, Vol. 8, No. 3, <https://ssrn.com/abstract=3216198> (dostęp: 7.09.2024 r.), s. 221-222. W konsekwencji,

Przedmiotem dyskusji pozostaje czy organy ochrony konkurencji mogłyby w toku kontroli koncentracji przyjmować środki zaradcze nakierowane na wzmocnienie ochrony danych osobowych jako elementu dobrobytu konsumentów⁴¹³, na przykład wprowadzenie limitu okresu przechowywania danych osobowych konsumentów⁴¹⁴. Wydaje się, że obecnie nie jest to możliwe, ponieważ wykraczałoby poza cel prawa konkurencji, który wciąż pozostaje nakierowany ekonomicznie. Nie można jednak wykluczyć tego w przyszłości, zwłaszcza w przypadku zmiany polegającej na uwzględnieniu czynnika ochrony danych osobowych jako pozaekonomicznego czynnika w ocenie dobrobytu konsumentów w kontroli koncentracji.

Przechodząc do spraw nadużycia pozycji dominującej, należy wskazać, że mogą one dotyczyć przetwarzania danych osobowych w sytuacjach, w których zachowanie podmiotu dominującego o charakterze nadużycia tej pozycji stanowi jednocześnie naruszenie RODO. Zgodnie z art. 102 TFUE, „zakazane jest nadużywanie (...) pozycji dominującej na rynku wewnętrznym lub na znacznej jego części, w zakresie, w jakim może wpływać na handel między Państwami Członkowskimi”, co uzupełniono przykładami takich zachowań jak „uzależnianie zawarcia kontraktów od przyjęcia przez partnerów zobowiązań dodatkowych, które (...) nie mają związku z przedmiotem tych kontraktów”. Ochrona przed nadużyciem pozycji dominującej ustanowiona w art. 102 TFUE uzupełniona jest przez krajowe przepisy, tj. rozdział 2 „Zakaz nadużywania pozycji dominującej” (art. 9 i 9a UKK) oraz rozdział 3 „Decyzje w sprawach praktyk ograniczających konkurencję” (art. 10-12b UKK), które zakazują „nadużywanie pozycji dominującej na rynku właściwym przez jednego lub kilku przedsiębiorców” (art. 9 ust. 1 UKK). Wyróżniane są zasadniczo dwa typy praktyk stanowiących nadużycie pozycji dominującej: abuzywne praktyki wykluczające (antykonkurencyjne) i abuzywne praktyki eksploatacyjne (wyzysku)⁴¹⁵.

uwagi o zgodności środków zaradczych w kontroli koncentracji mają także zastosowanie do środków zaradczych stosowanych w decyzjach w przedmiocie nadużycia pozycji dominującej, np. art. 10 ust. 4 UKK, w tym w odniesieniu do tzw. doktryny essential facilities.

⁴¹³ I. Graef, D. Clifford, P. Valcke, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, Int. Data Priv. Law 2018, Vol. 8, No. 3, <https://ssrn.com/abstract=3216198> (dostęp: 20.09.2024 r.), s. 219-220.

⁴¹⁴ Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 7.09.2024 r.), s. 32.

⁴¹⁵ T. Skoczny, Komentarz do art. 9, [w:] Ustawa o ochronie konkurencji i konsumentów. Komentarz, red. T. Skoczny, Warszawa 2014, SIP Legalis.

Poniższa analiza dotyczy praktyk eksploatacyjnych, ponieważ to właśnie one związane są najczęściej z operacjami przetwarzania danych osobowych⁴¹⁶. Dokonana zostanie na przykładzie sprawy *Meta/Bundeskartellamt* rozpoznanej przez TSUE w wyroku z 4.07.2023 r., sygn. C-252/21⁴¹⁷. Sąd ten w trybie rozpoznania pytania prejudycjalnego badał czy zachowanie administratora stanowiące naruszenie obowiązków z RODO może być brane pod uwagę przy ocenie, administrator ten, będący przedsiębiorstwem o dominującej pozycji, zachowaniem tym nadużył ten pozycji⁴¹⁸. Sprawa dotyczyła nałożenia przez niemiecki organ ochrony konkurencji ograniczeń na Meta (wcześniej Facebook) dotyczących przetwarzania danych osobowych z uwagi na to, że praktyki te, w ocenie niemieckiego organu, stanowiły abuzywne praktyki eksploatacyjne względem konsumentów⁴¹⁹. Praktyki te polegały na łączeniu danych osobowych użytkowników tej platformy, które Facebook gromadził zarówno na niej, jak i poza nią w Internecie lub w aplikacjach w telefonach komórkowych, wykorzystując postanowienia ogólnych warunków korzystania z platformy internetowej Facebook (jako niezbędnych do wykonania umowy na podstawie art. 6 ust. 1 lit. b RODO)⁴²⁰. Niemiecki organ ochrony konkurencji zakazał tych praktyk, uzależniając ich kontynuację od wyrażenia uprzedniej wyraźnej i odrębnej zgody przez poszczególnych użytkowników⁴²¹. Wskazać należy, że podobny zakaz łączenia danych osobowych między różnymi usługami strażników dostępów

⁴¹⁶ Por. przykłady na s. 9 w EIOD, *Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (dostęp: 7.09.2024 r.); por. także I. Małobęcka-Szwast, *Chapter 4. Data-driven abuse of a dominant position*, [in:] eadem, *Big Data and the Abuse of a Dominant Position by Data-Driven Online Platforms under EU Competition Law*, Warszawa 2021, SIP Legalis.

⁴¹⁷ Wyrok TS z 4.07.2023 r., C-252/21, *Meta Platforms Inc., Anciennement Facebook Inc.* In. przeciwko *Bundeskartellamt*, SIP LEX nr 3576613.

⁴¹⁸ K. Kohutek, *Naruszenie przepisów o ochronie danych osobowych (RODO) a nadużycie pozycji dominującej w rozumieniu art. 102 TFUE – glosa do wyroku Trybunału Sprawiedliwości z 4.07.2023 r., C-252/21, Meta Platforms Inc. (dawniej Facebook Inc.) przeciwko Bundeskartellamt*, EPS 2023, nr 10, s. 33-41, s. 33.

⁴¹⁹ Por. *Bundeskartellamt, Bundeskartellamt prohibits Facebook from combining user data from different sources*, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (dostęp: 24.09.2024 r.).

⁴²⁰ W. Kerber, K. K. Zolna, *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law*, „European Journal of Law and Economics” 2022, Vol. 54, <http://dx.doi.org/10.2139/ssrn.3719098> (dostęp: 7.09.2024 r.), s. 2. Por. także *Bundeskartellamt, Bundeskartellamt prohibits Facebook from combining user data from different sources*, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html oraz M. Volmar, K. Helmdach, *Protecting Consumers and Their Data Through Competition Law? Rethinking Abuse of Dominance in Light of the Federal Cartel Office's Facebook Investigation*, „European Competition Journal”, 2018, Vol. 14, No. 2-3, <https://doi.org/10.1080/17441056.2018.1538033> (dostęp: 20.09.2024 r.), s. 199-200.

⁴²¹ *Bundeskartellamt, Case Summary. Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, 15.02.2019, https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4 (dostęp: 20.09.2024 r.), s. 12.

ustanowiony został w DMA (por. podrozdział 2.6.3.2. poniżej)⁴²². TSUE rozstrzygnął, że organy ochrony konkurencji mogą, badając nadużycie pozycji dominującej, ustalić, że zarówno warunki korzystania z usług, jak i ich wdrażanie w zakresie dotyczące przetwarzania danych osobowych są niezgodne RODO, o ile „to jest konieczne” do wykazania nadużycia⁴²³. Chociaż nie wprowadzono specjalnej procedury współpracy między organami konkurencji a organami ochrony danych osobowych, to te pierwsze zobowiązane są do uprzedniej konsultacji z organami ochrony danych osobowych w zakresie zachowań, które mogą być niezgodne z RODO, na podstawie obowiązku lojalnej współpracy (art. 4 ust. 3 TUE)⁴²⁴. Oznacza to, że TSUE rozstrzygnął, że możliwe jest krzyżowanie się zakresu przedmiotowego RODO i prawa ochrony konkurencji w odniesieniu do praktyk stanowiących nadużycie pozycji dominującej.

Zgodzić się należy, że zarówno unijne prawo konkurencji, jak i unijne prawo ochrony konsumentów oraz RODO wyrastają z tych samych podstawowych celów ustanowionych w traktatach unijnych, w tym przede wszystkim w art. 3 ust. 1-3 TUE, co oznacza, że – nawet jeżeli ich zakres przedmiotowy i sposób obowiązywania się różnią – to podmioty administrujące powinny mieć możliwość stosować je tak, aby zapewnić synergię w kierunku zgodnej ich realizacji⁴²⁵. Ochrona danych osobowych ma szczególną wartość, ponieważ prawo do niej stanowi prawo podstawowe, co nie powinno być obojętne dla organów prawa konkurencji (por. art. 51 KPP). Dane osobowe mają podwójny charakter, ponieważ stanowią nie tylko przedmiot ochrony prawo-człowieczej, ale także kluczowe aktywo niematerialne w gospodarce w czasach transformacji cyfrowej. Stąd też z perspektywy realizacji celów traktatowych zasadne byłoby uwzględnienie ochrony danych osobowych jako elementu dobrobytu konsumenta (*consumer welfare*) w trakcie kontroli koncentracji nie tylko z perspektywy zgodności ewentualnego połączenia zbiorów danych posiadanych przez dwa przedsiębiorstwa czy też oceny czy zastosowanych środków zaradczych z przepisami RODO, ale również z perspektywy prospektywnego wpływu koncentracji na standard ochrony danych

⁴²² Por. I. Małobęcka-Szwast, Komentarz do art. 5, nb. 7 [w:] Akt o rynkach cyfrowych – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828. Komentarz, red. M. Grochowski [w:] Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz, red. M. Grochowski, Warszawa 2024, SIP Legalis.

⁴²³ Wyrok TS z 4.07.2023 r., C-252/21, Meta Platforms Inc., Anciennement Facebook Inc. i In. przeciwko Bundeskartellamt, SIP LEX nr 3576613, pkt 155.

⁴²⁴ Wyrok TS z 4.07.2023 r., C-252/21, Meta Platforms Inc., Anciennement Facebook Inc. i In. przeciwko Bundeskartellamt, SIP LEX nr 3576613, pkt 155.

⁴²⁵ Por. K. Majcher, Coherence between Data Protection and Competition Law in Digital Markets, Oxford 2023, s. 272-274.

osobowych z perspektywy dobrobytu konsumenta. Zasadna jest również współpraca między organami ochrony konkurencji a organami ochrony danych – tak jak w sprawach o nadużycie pozycji dominującej, które dotyczą przetwarzania danych osobowych, jak wynika to z analizowanego powyżej orzecznictwa TSUE.

2.6.3.2. AKT O RYNKACH CYFROWYCH

Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych pomyślane są jako akty prawne będące pakietem, które mają wspólnie osiągnąć cele, określone przez Komisję jak: „1) stworzenie bezpiecznej przestrzeni cyfrowej, w której chronione są prawa podstawowe (...); 2) stworzenie równych warunków działania [na rynku cyfrowym]”⁴²⁶. Nim dokonana zostanie analiza rozporządzenia unijnego Aktu o Rynkach Cyfrowych, należy wskazać, że już w stanowisku EROD dotyczącym Pakietu Usług Cyfrowych i Strategii w sprawie Danych z 2021 r. (obejmującym DMA, DSA, DGA, AI Act i Data Act) zgłoszono trzy zasadnicze uwagi do aktów prawnych procedowanych w ramach tego pakietu i w celu realizacji tej strategii, to jest: osłabienie ochrony podstawowych praw i wolności osób fizycznych; rozdrobnioną strukturę podmiotów administrujących stosujących te akty i ryzyko niespójności między tymi aktami⁴²⁷. Należy zgodzić się z tymi uwagami. Będą one przedmiotem analizy w odniesieniu do poszczególnych aktów.

Akt o Rynkach Cyfrowych zbudowany jest z 54 artykułów podzielonych na sześć rozdziałów i jeden załącznik: Rozdział I – Przedmiot, zakres stosowania i definicje; Rozdział II – Strażnicy dostępu; Rozdział III – Praktyki strażników dostępu, które ograniczają kontestowalność lub są nieuczciwe; Rozdział IV – Badanie Rynku; Rozdział V – Uprawnienia w zakresie prowadzenia badań oraz egzekwowania i monitorowania; Rozdział VI – Przepisy końcowe. Przedmiotem analizy w niniejszym podrozdziale będzie rozdział I, II i III, natomiast rozdziały IV i V zostaną poddane charakterystyce w rozdziale 3 niniejszej rozprawie jako element badania kompetencji Komisji. Ambitny cel DMA ustalony został w art. 1 ust. 1⁴²⁸, zgodnie z którym jest to „zapewnienie wszystkim przedsiębiorstwom kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii, na których działają strażnicy dostępu”

⁴²⁶ Komisja, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (dostęp: 13.09.2024 r.).

⁴²⁷ EROD, *Statement on the Digital Services Package and Data Strategy Adopted on 18 November 2021*, s. 2 https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf (dostęp: 15.09.2024 r.).

⁴²⁸ Por. także U. Czarnomska-Bokowy, Prawo konkurencji a projekt rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym–kto przypilnuje strażników? iKAR 2022, t. 11, nr 1, s. 8-20.

przez obowiązywanie DMA wobec „podstawowych usług platformowych [zdefiniowanych w art. 2 ust. 2 DMA, w tym wyszukiwarek internetowych, internetowych serwisów społecznościowych i usług platformy udostępniania wideo] świadczonych lub oferowanych przez strażników dostępu użytkownikom biznesowym” (z siedzibą w UE) lub użytkownikom końcowym (z siedzibą lub miejscem pobytu w UE), przy czym bez znaczenia pozostaje siedziba lub miejsca pobytu strażników dostępu i przepisy właściwie do świadczenia usług (art. 1 ust. 2 DMA).

Dla ustalenia zakresu obowiązywania DMA kluczowe jest zatem ustalenie znaczenia terminu „strażnicy dostępu”. Termin ten został unormowany w rozbudowanym art. 3 DMA przez wskazanie trzech kryteriów (wywieranie znacznego wpływu na rynek; świadczenia podstawowej usługi platformowej stanowiącej ważny punkt dostępu; ugruntowana i trwała pozycja (...) lub możliwość przewidzenia jej w niedalekiej przyszłości), które musi spełniać przedsiębiorstwo, i ustanowienie domniemań ich spełnienia przez wskazanie m.in. wielomiliardowego progu kwotowych (w odniesieniu do obrotu rocznego i średniej kapitalizacji) oraz ponad 40 milionowego progu liczby użytkowników końcowych. Przedsiębiorstwo spełniające te kryteria jest zobowiązane zgłosić to Komisji, która wskazuje dane przedsiębiorstwo jako strażnika dostępu. Tak unormowane kryteria i domniemania powodują, że tylko niewielka liczba największych przedsiębiorstw w UE je spełnia. Obecnie (na 23 stycznia 2024 r.) status ten posiada sześć podmiotów: Alphabet, Amazon, Apple, ByteDance, Meta, i Microsoft⁴²⁹.

Na strażników dostępu nałożono w rozdziale III obowiązki nakierowane na ograniczenie nieuczciwych praktyk lub praktyk ograniczających kontestowalność (art. 5-7, 14-15 DMA). Mają one różnorodny charakter, w tym: zapewnienie użytkownikom biznesowym (zdefiniowany w art. 2 pkt 221 DMA) współdziałania z usługami świadczonymi przez strażników dostępu bez nadużywania pozycji tych drugich (art. 5 ust. 2-6 DMA); umożliwienie weryfikacji warunków biznesowych usług reklamowych (art. 5 ust. 9 i 10 DMA); zakaz preferencji własnych usług i produktów (art. 5 ust. 7 i 8 DMA); umożliwianie łatwego odinstalowania aplikacji (art. 6 ust. 1 DMA); obowiązek informowania o koncentracjach (art. 14 DMA) i przeprowadzenie niezależnego audytu (art. 15 DMA). Obowiązki te mogą być aktualizowane przez Komisję w aktach delegowanych (art. 12 DMA), zawieszane w szczególnych wypadkach (art. 9 DMA), a nawet Komisja może zwolnić strażnika dostępu od

⁴²⁹ Komisja, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328⁴³⁰ EIOD, *Opinion 2/2021 on the Proposal for a Digital Markets Act*, s. 10, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf (dostęp: 20.09.2024 r.).

wypełniania obowiązków w całości lub w części z powodów zdrowia lub bezpieczeństwa publicznego (art. 10 DMA). Dodatkowo nałożono zakaz obchodzenia tych obowiązków (art. 13 DMA).

Część obowiązków strażników dostępu dotyczy przetwarzania danych, w tym danych osobowych. Po pierwsze, w artykule 5 ust. 2 DMA objęto ich czterema zakazami przetwarzania danych osobowych użytkowników końcowych (zdefiniowani w art. 2 pkt 20 DMA; w tym kontekście to podmioty danych) nakierowanymi na ograniczenie możliwości wykorzystywania pozyskiwanych („nadmiarowych”; por. motyw 36 DMA) danych dla innych celów m.in. danych użytkowników końcowych korzystających z usług osób trzecich wykorzystujących podstawowe usługi platformowe strażnika dostępu w celach usług reklamowych (lit. a) i logowania użytkowników końcowych do innych usług strażnika dostępu, aby dokonać połączenia ich danych (lit. d). Zakazy te nie mają zastosowania, jeżeli użytkownik końcowy wyraził zgodę w sposób zgodny z RODO i „zapewniono mu możliwość dokonania konkretnego wyboru”, przy czym wyłączono (por. motyw 36 DMA) możliwość oparcia się przez strażnika dostępu na podstawie przetwarzania z art. 6 ust. 1 lit. b RODO (wykonywanie umowy) i art. 6 ust. 1 lit. f RODO (tzw. „uzasadniony interes”). EIOD w swojej opinii do projektu DMA sugerował, że zasadne byłoby, aby zobowiązać strażników dostępu do dostarczenia użytkownikom końcowym przyjaznych narzędzi do zarządzania tymi zgodami⁴³⁰. W literaturze poddawano w wątpliwość zasadność użycia zgody jako podstawy przetwarzania, która – wobec sposobu projektowania platform internetowych – daje iluzoryczną ochronę. W zamian proponowano odwołanie tylko do zasad przetwarzania z art. 5 RODO (minimalizacji i ograniczenia przechowywania) oraz zapewnienia odpowiednich środków technicznych dla bezpieczeństwa przetwarzania⁴³¹. Niezależnie od mającej długą historię dyskusji na temat zasadności użycia zgody jako instrumentu dającego faktyczną ochronę podmiotom danych, należy wskazać, że Akt o Rynkach Cyfrowych w motywie 36 wskazuje na potrzebę zapewnienia przez strażników dostępu możliwości decydowania o korzystaniu z praktyk

⁴³⁰ EIOD, *Opinion 2/2021 on the Proposal for a Digital Markets Act*, s. 10, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf (dostęp: 20.09.2024 r.).

⁴³¹ M. Demircan, *The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions* [in:] *Privacy and Identity Management. Privacy and Identity*, red. F. Bieker, J. Meyer, S. Pape, Cham 2022, https://doi.org/10.1007/978-3-031-31971-6_1 (dostęp: 20.09.2024 r.). s. 5-7. Por. także: P. Hacker, J. Cordes, J. Rochon, *Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and Beyond*, <http://dx.doi.org/10.2139/ssrn.4316944> (dostęp: 20.09.2024 r.); A. Davola, G. Malgieri, *Data, Power, and Competition Law: The (Im)possible Mission of the DMA?* [in:] *The Economics and Regulation of Digital Markets*, ed. by F. Fagan, J. Langenfeld, Leeds 2023, <https://doi.org/10.1108/S0193-589520240000031003> (dostęp: 20.09.2024 r.).

zakazanych powyżej, bez konieczności wyrażenia zgody, „oferując mniej spersonalizowane, lecz równoważne rozwiązanie”. Pozostaje niejasne czy mogłyby być te „mniej spersonalizowane, lecz równoważne rozwiązania”, czy ich wdrożenie obejmowałoby także przetwarzanie danych osobowych, a jeżeli tak, to jak miałyby się do podstaw przetwarzania, zważywszy na to, że strażnik dostępu nie może opierać się na art. 6 ust. 1 lit. b i art. 6 ust. 1 lit. f RODO⁴³². Niejasność potęgowana jest przez zakaz obchodzenia obowiązków przez strażników dostępu, którzy – w przypadku braku zgody podmiotów danych – mają obowiązek zapewnienia „przestrzegania unijnych przepisów i zasad w zakresie ochrony danych i prywatności w inny sposób, w tym – w stosownych przypadkach – poprzez dostarczanie użytkownikom biznesowym należycie zanonimizowanych danych” (art. 13 ust. 5 DMA).

Druga grupa obowiązków dotyczy zapewnienia interoperacyjności dla użytkowników biznesowych (art. 6 ust. 7 DMA), dostępu do danych przez użytkowników biznesowych (art. 6 ust. 8, 10-11 DMA) oraz prawa do przenoszenia danych, które rozszerzono względem prawa do przenoszenia danych z art. 20 RODO (art. 6 ust. 9 DMA). Celem jest, aby dostęp do danych przetwarzanych przez strażników dostępu miały także inne podmioty, aby zwiększyć konkurencyjność na rynku. Jednocześnie wprowadzono jednak szereg rozwiązań, które mają chronić dane osobowe, np. obowiązek anonimizacji danych osobowych w formie zapytań, kliknięć i wyświetleń w wyszukiwarkach internetowych w przypadku udzielania dostępu (art. 6 ust. 11 DMA)⁴³³, oraz obowiązek uzyskania zgody użytkowników końcowych na udostępnianie danych osobowych użytkownikom biznesowym produktów, które są im dostarczone lub usług, które są im świadczone (art. 6 ust. 10 DMA). W odniesieniu do tych obowiązków zgłoszono w literaturze wątpliwości co do ograniczenia możliwości wykorzystania przez strażników dostępu środków technicznych wzmacniających bezpieczeństwo przetwarzania, na przykład przez utrudnienie przez wyszukiwarki internetowe dostępu do nieodpowiednio zabezpieczonych stron internetowych podmiotów trzecich⁴³⁴, co mogłoby zostać uznane za obchodzenie obowiązków przez strażników dostępu (art. 13 ust. 5 DMA). Niejasny jest także wybór prawidłowej podstawy przetwarzania danych

⁴³² Por. Sidley Austin LLP, *Unpacking Digital Data Laws Across Europe: Addressing the Digital Markets Act*, <https://datamatters.sidley.com/2023/01/24/unpacking-digital-data-laws-across-europe-addressing-the-digital-markets-act/109> (dostęp: 15.09.2024 r.).

⁴³³ W odniesieniu do problemu należytej anonimizacji por. podrozdział 2.6.5.2. dotyczący Data Act.

⁴³⁴ M. Barcentewicz, *Interpreting the EU Digital Markets Act Consistently With the EU Charter's Rights to Privacy and Protection of Personal Data*, „Bocconi University. MediaLaws.eu” 2023, 3.08.2023, <https://ssrn.com/abstract=4531383> (dostęp: 020.09.2024 r.), s. 10.

osobowych z art. 6 ust. 1 RODO, na której strażnicy dostępu mogą oprzeć, to przetwarzanie w celu wykonania obowiązków wynikających z DMA, w tym również czy podjęcie decyzji o anonimizacji danych osobowych motywowane wątpliwościami co do prawidłowej podstawy przetwarzania (np. spełnienia warunków wyrażenia zgody) może zostać potraktowana jako obejście tych obowiązków.

Jednym z pierwszych przykładów krzyżowania się zakresów podmiotowych DMA i RODO jest wszczęcie przez Komisję postępowania (komunikat z dnia 25 marca 2024 r.) przeciwko Meta „w celu zbadania, czy niedawno wprowadzony model „Płać lub wyrażaj zgodę” dla użytkowników w UE jest zgodny z art. 5 ust. 2 DMA, który wymaga od strażników dostępu uzyskania zgody użytkowników, gdy zamierzają łączyć lub wykorzystywać ich dane w różnych podstawowych usługach platformowych”⁴³⁵. Jednocześnie model ten jest przedmiotem badania przez niektóre organy ochrony danych (np. w Norwegii, Holandii i Hamburgu), a EROD wydała „Opinię 08/2024 w sprawie ważnej zgody w kontekście modeli zgody lub płatności wdrażanych przez duże platformy internetowe” (17 kwietnia 2024 r.)⁴³⁶. To pokazuje, że w krótkim czasie różne organy zarówno na podstawie RODO (organy ochrony danych i EROD), jak i DMA (Komisja Europejska) podejmują równoległe działania dotyczące tego samego zachowania. W takiej sytuacji relacja prawna między tymi działaniami, w tym kwestia uwzględniania (lub ewentualnego związania) wzajemnego stanowiska, możliwość odmiennej wykładni i dublowania sankcji, pozostaje niejasna. Zarówno w RODO, jak i DMA ustanowiono niezależne administracyjne kary pieniężne.⁴³⁷

W DMA dostrzeżono ryzyko krzyżowania się zakresu przedmiotowego tego aktu z zakresem przedmiotowym RODO, normując, że strażnicy dostępu zobowiązani są do wypełnienia ich obowiązków wynikających z RODO, a wypełnianie ich obowiązków wynikających z DMA nie może stanowić zagrożenia dla ochrony danych osobowych (np. art. 8 ust. 1 zdanie 2 DMA i motyw 64 w odniesieniu do interoperacyjności, także motyw 72), przy czym strażnicy dostępu zobowiązani są, aby, na przykład, zapewnić użytkownikom biznesowym możliwość uzyskania zgody podmiotów danych z RODO albo dostarczyć

⁴³⁵ KE, *Akt prawny o usługach cyfrowych: Komisja Europejska przyjmuje pierwszy zestaw aktów delegowanych* (kącik prasowy Komisji Europejskiej, 20 października 2024 r.) https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689 (dostęp: 30.10.2024 r.).

⁴³⁶ Datatilsynet, *Wniosek o opinię EDPB w sprawie zgody lub zapłaty*, <https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/> (dostęp: 15.09.2024 r.).

⁴³⁷ P. de Hert, P. Hajduk, *Governance of Digital Technologies in the EU: Cross-Regime Enforcement, Redundancy Interdependence*.

„należycie zanonimizowane” dane⁴³⁸, jeżeli uzyskanie takiej zgody jest potrzebne (art. 13 ust. 5 DMA). DMA ma pozostawać „bez uszczerbku” dla RODO (por. m.in. motyw 12, 36, 37 DMA), a spójność ma zostać zapewniona m.in. przez bezpośrednio odwołanie do definicji w RODO dla „danych osobowych” (art. 2 pkt 25 DMA); „profilowania” (art. 2 pkt 31 DMA); zgody (art. 2 pkt 32 DMA). Z uwagi na krzyżowanie się zakresu przedmiotowego DMA z zakresem prawa konkurencji, zwłaszcza w odniesieniu do nadużycia pozycji dominującej⁴³⁹, istotne jest także, DMA ma pozostawać „bez uszczerbku” dla unijnego i krajowego prawa konkurencji (art. 1 ust. 6 DMA). Ryzyko krzyżowania się zakresu przedmiotowego i obowiązków wynikających z tego Aktu i RODO zasygnalizował pośrednio także EROD w swoim piśmie z 18 lipca 2024 r. do Komisji dotyczącym wytycznych w sprawie relacji między tymi aktami prawnymi, podkreślając to, że to EROD kompetentny jest do wydania takich wytycznych⁴⁴⁰.

⁴³⁸ W odniesieniu do problemu należytej anonimizacji por. podrozdział 2.6.5.2. dotyczący Data Act.

⁴³⁹ Pojęcie podmiotu o pozycji dominującej nie jest tożsame z pojęciem strażnika dostępu. Mogą być one jednak uznane za zbliżone zakresowo.

⁴⁴⁰ EROD, *EDPB's Letter to the European Commission concerning Guidelines on the Interplay between Digital Markets Act (DMA) and GDPR*, 18 lipca 2024. https://www.edpb.europa.eu/system/files/2024-07/edpb_letter_reply_com_gls_interplay_dma_gdpr_en.pdf (dostęp: 15.09.2024 r.).

2.6.3.3. AKT O USŁUGACH CYFROWYCH

Jak wskazano wyżej, osiągnięcie celów postawionych przed rozporządzeniem unijnym Aktem o Rynkach Cyfrowych w założeniu ma zostać zrealizowane razem z obowiązywaniem Aktu o Usługach Cyfrowych. Jego cele to, zgodnie z art. 1 ust. 1 DSA, „przyczynienie się do właściwego funkcjonowania rynku wewnętrznego usług pośrednich”, które rozumiane jest jako istnienie „bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, które ułatwia innowacje”, przy jednoczesnej efektywnej ochronie praw podstawowych. Stąd też przedmiotem regulacji jest świadczenia usług pośrednich (art. 1 ust. 2 DSA), które zdefiniowane zostały w art. 3 lit. g DSA i obejmują: usługę „zwykłego przekazu”⁴⁴¹, usługę „cachingu”⁴⁴² i usługę „hostingu”⁴⁴³, a DSA znajduje zastosowanie do wszystkich usług pośrednich, które są oferowane odbiorcom usługi (art. 3 lit. b) DSA) przebywających w UE lub z siedzibą w UE, a bez znaczenia jest miejsca siedziby dostawców (art. 2 ust. 1 DSA), co oznacza, że DSA będzie zakres terytorialny obowiązywania DSA wykracza poza terytorium UE. Dodatkowe rozbudowane obowiązki nałożone zostały na największe podmiotów: bardzo duże platformy internetowe (VLOP) i bardzo duże wyszukiwarki internetowe (VLOSE) przede wszystkim w sekcji 5 („Dodatkowe obowiązki spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w zakresie zarządzania ryzykiem systemowym”) rozdziału III (ale także, np. w art. 14 ust. 5 DSA).

DSA złożony jest z 93 artykułów podzielonych na pięć rozdziałów: Rozdział I („Przepisy Ogólne”); Rozdział II („Odpowiedzialność dostawców usług pośrednich”), Rozdział III („Obowiązki w zakresie należytej staranności na potrzeby przejrzystego i bezpiecznego środowiska internetowego”); Rozdział IV („Wdrażanie, współpraca, sankcje i egzekwowanie”) i Rozdział V („Przepisy Końcowe”). Przedmiotem analizy w niniejszym podrozdziale będą niektóre obowiązki ustanowione w rozdziałach II i III z uwzględnieniem obowiązków VLOP oraz VLOSE, ponieważ przetwarzanie przez nich danych osobowych ma potencjalnie największy wpływ na prawa i wolności podmiotów danych⁴⁴⁴. W uproszczeniu, VLOP (bardzo duże platformy internetowe) i VLOSE (bardzo duże wyszukiwarki internetowe) to platformy

⁴⁴¹ „Transmisja w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi lub na zapewnianiu dostępu do sieci telekomunikacyjnej”.

⁴⁴² „Transmisja w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi, obejmującą automatyczne, pośrednie i krótkotrwale przechowywanie tej informacji, dokonywane wyłącznie w celu usprawnienia późniejszej transmisji informacji na żądanie innych odbiorców”.

⁴⁴³ „Przechowywaniu informacji przekazanych przez odbiorcę usługi oraz na jego żądanie”.

⁴⁴⁴ Rozdział IV dotyczący organów ustanowionych w celu stosowania DSA zbadany zostanie w rozdziale rozprawy.

internetowe⁴⁴⁵ i wyszukiwarki internetowe⁴⁴⁶ wskazane przez Komisję w trybie art. 33 ust. 4 DSA, z których miesięcznie korzysta co najmniej 10% ludności UE (obecnie co najmniej 45 mln; por. art. 33 ust. 1 DSA). W praktyce kryteria te spełniają wyłącznie największe podmioty, których lista pokrywa się częściowo z listą strażników dostępu. Aktualnie⁴⁴⁷ status VLOP mają: Alibaba AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Maps; Google Play; Google Shopping; Instagram; LinkedIn; Pinterest; Pornhub; Snapchat; Stripchat; TikTok; Wikipedia; X (Twitter); Xvideos; YouTube i Zalando, status VLOSE mają: Bing i Google Search⁴⁴⁸.

Podobnie jak w przypadku DMA, tak również w DSA część obowiązków dostawców usług pośrednich, w tym VLOP i VLOSE, dotyczy przetwarzania danych, w tym danych osobowych. Komisja na swojej stronie internetowej informującej o DSA wskazuje, że ma ono uzupełniać RODO w ochronie danych osobowych, podając przykład, że dostawcy usług platform internetowych w zakresie przetwarzania danych osobowych do celów reklamowych objęci są zakresem zarówno DSA, jak i RODO⁴⁴⁹. Poniżej zbadane zostaną wybrane przykłady.

DSA normuje zwalczanie nielegalnych treści w Internecie (zdefiniowane w art. 2 lit. h DSA)⁴⁵⁰. Przykładowo, dostawcy usług hostingu (w tym platformy internetowe) zobowiązani są wdrożyć mechanizmy umożliwiające zgłoszenie w ich usłudze informacji rozpoznanych jako nielegalne treści (art. 16 ust. 1 DSA). Dostawcy ci uprawnieni są do użycia środków przeciwko treściom uznany na nielegalne, m.in. ograniczenia w zakresie widoczności określonych informacji, w tym usuwanie treści czy też zawieszenie świadczenia usługi w całości (por. art. 17 ust. 1 DSA)⁴⁵¹. Nielegalne treści mogą obejmować także dane osobowe. W określonych sytuacjach podmiotom danych przysługuje prawo do usunięcia tych

⁴⁴⁵ Art. 2 lit. i) DSA: „usługa hostingu, która na żądanie odbiorcy usługi przechowuje i rozpowszechnia publicznie informacje, chyba że takie działanie jest nieznaczną lub wyłącznie poboczną cechą innej usługi lub nieznaczną funkcją głównej usługi, i ze względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi, a włączenie takiej cechy lub funkcji w taką inną usługę nie jest sposobem na obejście stosowania niniejszego rozporządzenia”.

⁴⁴⁶ Art. 2 lit. j) DSA: „usługa pośrednia, która umożliwia użytkownikom dokonywanie zapytań w celu wyszukiwania – co do zasady – wszystkich stron internetowych lub wszystkich stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, zapytania głosowego, wyrażenia lub innej wartości wejściowej i która podaje wyniki wyszukiwania w dowolnym formacie, w którym można znaleźć informacje związane z zadaniem zapytaniem”.

⁴⁴⁷ Stan na 24 stycznia 2024 r.

⁴⁴⁸ Komisja, <https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers> (dostęp: 15.09.2024 r.).

⁴⁴⁹ Komisja, <https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers> (dostęp: 15.09.2024 r.).

⁴⁵⁰ Por. M. Rojszczak, *The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content*, „Institutiones Administrationis-Journal of Administrative Sciences” 2023, Vol. 3, No. 2, s. 44-59.

⁴⁵¹ Por. inne obowiązki nakierowane na zwalczanie nielegalnych treści, np. art. 9 DSA *Nakaz podjęcia działań przeciwko nielegalnym treściom przez dostawców usług pośrednich*.

danych, zwane prawem do bycia zapomnianym (art. 17 RODO) realizowane względem administratora. Z perspektywy podmiotów danych możliwe będzie zatem w określonych sytuacjach skorzystanie ze zgłoszenia nielegalnych treści (które obejmują dane osobowe ich dotyczące) do dostawcy usługi hostingowej na podstawie DSA i równolegle z żądania wykonania prawa do bycia zapomnianym do administratora, przy czym w literaturze słusznie przyjmuje się, że uprawnienie z DSA stanowi rozszerzenie względem uprawnienia z RODO⁴⁵². Dostawca usługi hostingowej zazwyczaj nie będzie administratorem w rozumieniu RODO, ponieważ z zasady nie decyduje o celach i środkach przetwarzania danych osobowych znajdujących się wśród informacji, które przechowuje na żądania odbiorców usługi hostingowej. Oznacza to, że realizacja obu trybów, która będzie dotyczyła *de facto* tej samej informacji (stanowiącej jednocześnie dane osobowe i nielegalne treści), skierowana będzie z zasady do dwóch różnych podmiotów. Ten dualizm spowoduje niepewność po stronie podmiotów danych co do wyboru trybu i relacji między tymi trybami⁴⁵³.

DSA nakłada na VLOP i VLOSE obowiązek przeprowadzenia oceny „systemowego ryzyka” w UE „wynikającego z projektu lub funkcjonowania swojej usługi i powiązanych z nią systemów (...) lub korzystania” z nich (art. 34 ust. 1 DSA), a następnie wprowadzenie środków zmniejszenia tego ryzyka (art. 35 DSA). Jako jedno z systemowych ryzyk wskazano wystąpienie negatywnych skutków dla praw podstawowych, w tym ochrony danych osobowych (art. 34 ust. 1 lit. b DSA). Ten obowiązek z DSA pokrywa się zatem z obowiązkiem przeprowadzenia oceny skutków przetwarzania dla określonych operacji przetwarzania danych osobowych w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, o którym mowa w art. 35 ust. 1 RODO⁴⁵⁴. Oznacza to, że podmioty o statusie VLOP i VLOSE w zakresie w jakim są administratorami danych osobowych w odniesieniu do operacji przetwarzania objętych hipotezą art. 35 ust. 1 RODO, będą musieli sporządzić jednocześnie ocenę systemowego ryzyka z art. 34 ust. 1 DSA i ocenę skutków przetwarzania z art. 35 ust. 1 RODO, które w zakresie „negatywnych skutków dla praw podstawowych, w tym ochrony danych osobowych” dotyczyły będą tych samych operacji

⁴⁵² P. Polański [w:] *Akt o usługach cyfrowych. Komentarz*, red. J. Gołaczyński, R. Skibicki, Warszawa 2024, art. 17, pkt 11, SIP LEX.

⁴⁵³ Por. V. Rovilos, G. Zafir-Fortuna, *EU's Digital Services Act just became applicable: outlining ten key areas of interplay with the GDPR*, *Future of Privacy Forum*, <https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/> (dostęp: 20.09.2024 r.).

⁴⁵⁴ Por. W. R. Wiewiórowski, *Słowo wstępne* [w:] *Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, Warszawa 2024, SIP LEX.

przetwarzania danych osobowych⁴⁵⁵. Podobna sytuacja istnienia krzyżujących zakresowo obowiązków dotyczy obowiązków związanych z przejrzystością, np. art. 26 (Przejrzystość reklam internetowych)⁴⁵⁶, art. 27 (Przejrzystość systemu rekomendacji) i 39 DSA (Dodatkowe obowiązki dotyczące przejrzystości reklam internetowych nałożone na VLOP i VLOSE), oraz przepisów RODO normujących przejrzystość przetwarzania danych osobowych (np. art. 5 ust. 1 lit. a 12-14 RODO)⁴⁵⁷.

Podobnie jak w DMA, w DSA zidentyfikowano ryzyko krzyżowania się zakresu przedmiotowego tego aktu z zakresem przedmiotowym RODO⁴⁵⁸. RODO wymienione jest w DSA aż 19 razy, w tym w odniesieniu do definicji profilowania w RODO i szczególnych kategorii danych osobowych (art. 26 ust. 3 DSA). DSA wskazuje w art. 2 ust. 4 lit. g, że pozostaje ono „bez uszczerbku” dla „prawa Unii w dziedzinie ochrony danych osobowych, w szczególności” RODO (por. też np. motyw 10, 67, 68). W DSA nie ma jednak przepisu, który stanowiłby, że w przypadku konfliktu między RODO a DSA, „pierwszeństwo” będzie miało RODO (taki przepis znajduje się np. w Data Act scharakteryzowanym niżej). Prawodawca unijny wskazuje natomiast w motywie 10 na „subsidiarny charakter” obowiązywania DSA⁴⁵⁹ wobec RODO w tym znaczeniu, że DSA powinno mieć zastosowanie w odniesieniu do spraw nieuregulowanych w RODO o tyle, o ile RODO „realizuje te same cele” co DSA. Brzmienie tego motywu należy ocenić jako mało pomocne w ustaleniu relacji między DSA a RODO.

2.6.4. AKTY PRAWNE REGULUJĄCE SZTUCZNĄ INTELIGENCJĘ

⁴⁵⁵ Por. EIOD, *Opinion 1/2021 on the Proposal for a Digital Services Act*, s. 13, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf (dostęp: 15.09.2024 r.).

⁴⁵⁶ Dodatkowo, wobec dostawców platform internetowych wprowadzono zakaz prezentowania odbiorcom usługi reklam opartych na profilowaniu zgodnie z definicją w RODO z wykorzystaniem szczególnych kategorii danych osobowych (art. 26 ust. 3 DSA).

⁴⁵⁷ Por. V. Rovilos, G. Zanfir-Fortuna, *EU's Digital Services Act just became applicable: outlining ten key areas of interplay with the GDPR*, *Future of Privacy Forum*, <https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/> (dostęp: 20.09.2024 r.).

⁴⁵⁸ Por. W. R. Wiewiórowski, *Słowo wstępne* [w:] *Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, Warszawa 2024, SIP LEX.

⁴⁵⁹ Por. M. Grochowski, *Komentarz do art. 2, nb. 11* [w:] *Akt o usługach cyfrowych – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE*. Komentarz, red. M. Grochowski [w:] *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, red. M. Grochowski, Warszawa 2024, SIP Legalis.

„Sztuczna inteligencja” („*artificial intelligence*”) to termin używany niekonsekwentnie i niejednoznacznie⁴⁶⁰. W literaturze sformułowano różne jego definicje⁴⁶¹. Definiowana jest m.in. jako „dziedzina informatyki, w której konstruowane są rozwiązania problemów nierozwiązywalnych bądź trudnych do rozwiązania metodami tradycyjnymi”, często przy wykorzystaniu „reguł rządzących działaniami człowieka”⁴⁶², albo też jako „system, który pozwala na wykonywanie zadań wymagających procesu uczenia się i uwzględniania nowych okoliczności w toku rozwiązywania danego problemu, i który może w różnym stopniu – w zależności od konfiguracji – działać autonomicznie oraz wchodzić w interakcję z otoczeniem”⁴⁶³. Zestawienie tych dwóch definicji wskazuje na zasadniczą rozbieżność, bo w pierwszej *genus w definiens* to „dziedzina informatyki”, a w drugiej „system”. Podobne rozbieżności odnaleźć można w definicjach w dokumentach organizacji międzynarodowych⁴⁶⁴. Wydaje się, że różnice te wynikają z zamiennego i niekonsekwentnego posługiwania się terminem „sztucznej inteligencji” na oznaczenie „dziedziny informatyki” albo „systemu”. Zasadne byłoby, aby termin „sztuczna inteligencja” był używany wyłącznie w odniesieniu do tej dziedziny informatyki. Jeżeli natomiast w istocie rzeczy idzie o system, należy wskazać to w *definiendum* przez określenie „system sztucznej inteligencji”. Znaczenie terminu „sztuczna inteligencja” należałoby odróżnić od terminu „uczenie maszynowe” („*machine learning*”)

⁴⁶⁰ Por. *Sztuczna Inteligencja*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 435.

⁴⁶¹ Por. też W. Ertel, *Introduction to artificial intelligence*, Cham 2018, s. 1-5.

⁴⁶² Por. *Sztuczna Inteligencja* [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 435.

⁴⁶³ T. Zalewski, *Rozdział I. Definicja sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa 2020, SIP Legalis. Por. dokonaną tam analizę definicji sztucznej inteligencji.

⁴⁶⁴ Por. *Zalecenia OECD w sprawie Sztucznej Inteligencji*, OECD/LEGAL/0449, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, w których zdefiniowano „system sztucznej inteligencji” w zestawieniu z definicją w słowniczku Rady Europy, <https://www.coe.int/en/web/artificial-intelligence/glossary>, gdzie zdefiniowano sztuczną inteligencję: „Zestaw nauk, teorii i technik, których celem jest odtworzenie przez maszynę zdolności poznawczych człowieka. Obecny rozwój ma na celu powierzenie maszynie złożonych zadań, które wcześniej były powierzane człowiekowi. Termin sztuczna inteligencja jest jednak krytykowany przez ekspertów, którzy rozróżniają „silną” sztuczną inteligencję (która jest w stanie kontekstualizować bardzo różne specjalistyczne problemy całkowicie niezależnie) i „słabą” lub „umiarkowaną” sztuczną inteligencję (która radzi sobie wyjątkowo dobrze w swojej dziedzinie szkolenia). Według niektórych ekspertów „silna” sztuczna inteligencja wymagałaby postępów w badaniach podstawowych, aby móc modelować świat jako całość, a nie tylko poprawy wydajności istniejących systemów”. (w oryginale: „*A set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being. Current developments aim to be able to entrust a machine with complex tasks previously delegated to a human. However, the term artificial intelligence is criticized by experts who distinguish between "strong" AI (who are able to contextualize very different specialized problems completely independently) and "weak" or "moderate" AI (who perform extremely well in their field of training). According to some experts, "strong" AI would require advances in basic research to be able to model the world as a whole and not just improvements in the performance of existing systems*”).

o szerszym znaczeniu, który często używany jest błędnie jako synonim sztucznej inteligencji⁴⁶⁵. Tymczasem uczenie maszynowe „bazuje na algorytmach zdolnych do budowania własnych wniosków na podstawie dostępnych informacji”, a zatem wyróżnia „zdolność do odkrywania wiedzy”, podczas gdy systemy sztucznej inteligencji ma już „zdolność do podejmowania samodzielnych decyzji”⁴⁶⁶.

Sztuczna inteligencja pozostaje przedmiotem wzmożonego zainteresowania opinii publicznej od 2023 r. na skutek udostępnienia przez amerykańskie przedsiębiorstwo OpenAI systemu sztucznej inteligencji o nazwie ChatGPT do szerokiego użytku⁴⁶⁷. Historia sztucznej inteligencji jest znacznej dłuższa i sięga jednak lat 50. ubiegłego wieku, a jej rozwój przechodził etapy zarówno wzmożonego, jak i osłabionego zainteresowania⁴⁶⁸. Sam ChatGPT to przykład systemu generatywnego sztucznej inteligencji opartego na dużym modelu językowym (*large language model*), który ma zdolność do tworzenia nowych treści na podstawie otrzymanych danych wejściowych (generatywna sztuczna inteligencja)⁴⁶⁹, czym zdążył już istotnie wpłynąć na tworzenia internetowych treści⁴⁷⁰. Z zastosowaniem systemów sztucznej inteligencji wiązane są duże nadzieje rozwoju gospodarczego⁴⁷¹ i m.in. usprawnienia funkcjonowania administracji publicznej⁴⁷². Jednocześnie, zidentyfikowano istotne ryzyka, m.in. ryzyko nowych form dyskryminacji⁴⁷³, naruszenia praw własności intelektualnej⁴⁷⁴ i zintensyfikowanego rozpowszechnienia dezinformacji⁴⁷⁵. Stąd też prawodawcy w różnych

⁴⁶⁵ M. Rojszczak, Sztuczna inteligencja w innowacjach finansowych–aspekty prawne i regulacyjne, iKAR 2020, t. 9, nr 2, s. 62-64.

⁴⁶⁶ M. Rojszczak, Prawne aspekty systemów sztucznej inteligencji – zarys problemu, [w:] Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2019, SIP Legalis.

⁴⁶⁷ OpenAI, ChatpGPT, <https://openai.com/blog/chatgpt> (dostęp: 20.09.2024 r.).

⁴⁶⁸ A. Kubiak-Cyruł, *Rekomendacje OECD jako ramy etyczne i prawne dla rozwijaju sztucznej inteligencji*, „Studia Prawnicze: rozprawy i materiały” 2022, t. 26, nr. 1, s. 106.

⁴⁶⁹ A. Piechocki, K. Gorzkowska, Problematyka stosowania prawa autorskiego do dzieł stworzonych przy udziale tzw. generatywnej sztucznej inteligencji, „Prawo Nowych Technologii” 2023, nr 1, s. 25.

⁴⁷⁰ M. Dymitruk, *Akt o usługach cyfrowych w czasach ChatGPT: czy dostawcy generatywnej AI są pośrednikami internetowymi?*, „Prawo Nowych Technologii” 2023, nr 3, s. 37.

⁴⁷¹ Por. Y. He, *The importance of artificial intelligence to economic growth*, „Korea Journal of Artificial Intelligence” 2019, Vol. 7, No. 1, s. 17-22. Por. także Ph. Aghion, B. F. Jones, Ch. I. Jones, *Artificial intelligence and economic growth* [in:] *The economics of artificial intelligence: An agenda*, ed. by A. K. Agrawal, J. Gans, A. Goldfarb, Chicago and London 2019.

⁴⁷² J. Róg-Dyrda, M. Wierzbowski, Szanse, zagrożenia i bariery prawne związane z wykorzystaniem sztucznej inteligencji w kontekście zasad postępowania administracyjnego [w:] *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza*, red. A. Matan, Warszawa 2022, SIP LEX.

⁴⁷³ S. M. West, M. Whittaker, K. Crawford, *Discriminating Systems: Gender, Race and Power in AI*, AI Now Institute 2019, <https://ainowinstitute.org/discriminatingsystems.html> (dostęp: 3.09.2024 r.).

⁴⁷⁴ R. Markiewicz, *ChatGPT i prawo autorskie Unii Europejskiej*, ZNUJ. PPWI 2023, nr 2, s. 142-171.

⁴⁷⁵ Por. N. Bontridder, Y. Pouillet, Y., *The role of artificial intelligence in disinformation*, „Data & Policy” 2021, Vol. 3, No. e32, <https://doi.org/10.1017/dap.2021.20>, (dostęp: 5.09.2024 r.).

jurysdykcjach, w tym także w prawie międzynarodowym⁴⁷⁶, podjęli inicjatywy nakierowane na unormowanie sztucznej inteligencji. W UE przyjęto nie tylko AI Act, ale także procedowane jest przyjęcie innych aktów prawnych bezpośrednio lub pośrednio regulujących (aspekty) zastosowania systemów sztucznej inteligencji, np. Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję)⁴⁷⁷. Przedmiotem analizy w niniejszym podrozdziale nie jest kompleksowe omawianie regulacji sztucznej inteligencji w prawie unijnym, lecz jedynie weryfikacja hipotezy, że zachodzi relacja krzyżowania się zakresów przedmiotowych RODO i AI Act.

Zanim przeanalizowany zostanie zakres przedmiotowy i podmiotowy oraz wybrane obowiązki w AI Act, należy wskazać, że dane, w tym dane osobowe, stanowią kluczowy element w działaniu systemów generatywnej sztucznej inteligencji opartych na dużych modelach językowych, które zyskały na popularności w ostatnich latach.⁴⁷⁸ Dane są bowiem kluczowe zarówno na etapie rozwoju tych systemów, w tym w trakcie ich trenowania, jak i na etapie korzystania z nich przy generowaniu tzw. promptów⁴⁷⁹. Duże modele językowe są zdolne, aby generować wyniki dopiero, jeżeli algorytmy tych modeli przeszły proces uczenia (rozwoju), do którego z kolei niezbędne są dane⁴⁸⁰. W tym celu dane pozyskiwane są najczęściej w procesie tzw. „web scrapping” („zdrapywania sieci”), który w uproszczeniu polega na pobraniu (bezpośrednio lub za pośrednictwem podmiotu trzeciego) publicznie dostępnych informacji zawartych na stronach internetowych, w tym na platformach mediów społecznościowych, w celu uzyskania bogatego zbioru danych⁴⁸¹. Informacje te zasadniczo

⁴⁷⁶ Por. IAPP, *Global AI Legislation Tracker By IAPP Research and Insights*, 25.08.2023, https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf (dostęp: 5.09.2024 r.).

⁴⁷⁷ COM/2022/496 final.

⁴⁷⁸ Elementy tego fragmentu rozprawy inspirowane są niepublikowaną pracą magisterską przygotowaną przez autora tej rozprawy w Uniwersytecie w Tilburgu, Holandia w ramach programu *LL.M. Law and Technology* pod tytułem „*In Search of the Holy Grail. Legal Bases for Processing Publicly Available Personal Data to Train Generative Artificial Intelligence Models in EU Data Protection Law*”. W pracy tej zbadano podstawy prawne do przetwarzania publicznie dostępnych danych osobowych do trenowania modeli generatywnej sztucznej inteligencji ze szczególnym uwzględnieniem uzasadnionego interesu.

⁴⁷⁹ EIOD, *First EDPS Orientations for EUIs using Generative AI*, 3 czerwca 2024, https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en (dostęp: 5.09.2024 r.), s. 4-7.

⁴⁸⁰ CNIL, *AI: CNIL publishes its first recommendations on the development of artificial intelligence systems*, 7 czerwca 2024. <https://www.cnil.fr/en/ai-cnil-publishes-its-first-recommendations-development-artificial-intelligence-systems> (dostęp: 5.09.2024 r.).

⁴⁸¹ S. B. Vale, *Training Large Generative AI Models Based on Publicly Available Personal Data: A GDPR Conundrum that the AI Act Could Solve*, „The Digital Constitutionalist”, 14 kwietnia 2023. <https://digi-con.org/training-large-generative-ai-models-based-on-publicly-available-personal-data-a-gdpr-conundrum-that-the-ai-act-could-solve/> (dostęp: 20.09.2024 r.); por. także C. Gallese, *Web scraping and Generative Models*

zawierają dane osobowe, w tym szczególne kategorie danych osobowych, ponieważ w praktyce nie dokonuje się ich rozróżnienia w tym procesie. W konsekwencji, podmioty rozwijające i korzystające z systemów sztucznej inteligencji stają się – w zależności od okoliczności (tj. środków i celów przetwarzania) – administratorami, współadministratorami lub podmiotami przetwarzającymi tych danych osobowych⁴⁸². Dane osobowe są wykorzystywane także przy wprowadzaniu danych źródłowych (*input data*) w postaci promptów w celu uzyskania danych wyjściowych (*output data*) w postaci odpowiedzi przy wykorzystaniu systemów generatywnej sztucznej inteligencji działających jako chatboxy.

Te operacje przetwarzania danych osobowych wywołują istotne ryzyka dla ich zgodności z RODO. Było to już i pozostaje przedmiotem zainteresowania organów ochrony danych, w tym włoskiego organu ochrony danych Garante⁴⁸³ i grupy roboczej składającej się z przedstawicieli różnych organów ochrony danych prowadzących postępowania w tym zakresie działającej pod auspicjami EROD.⁴⁸⁴ Ryzyka te dotyczą m.in. zapewnienia przejrzystości zgodnie z zasadą przejrzystości, prawidłowości i zgodności z prawem (podstaw przetwarzania). W techniczną specyfikę procesu uczenia się modeli generatywnej sztucznej inteligencji, jak i samego korzystania z nich przez użytkowników końcowych wpisana jest niejasność co do tego, w jaki sposób algorytmy te się uczą i w jaki sposób generują odpowiedzi. Zjawisko to określane jest jako „czarna skrzynka” („*black box*”). W praktyce zasadniczo niemożliwe jest na tym etapie rozwoju tej techniki odtworzenie sposobu działania algorytmu, w tym ustalenie, jakie dane zostały dokładnie wykorzystane do wygenerowania danego wyniku.⁴⁸⁵

training in the Directive 790/19, „Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale” 2023, Vol. 16, No. 2.

⁴⁸² EIOD, *First EDPS Orientations for EUIs using Generative AI*, 3 czerwca 2024, https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en, s. 4-7.

⁴⁸³ Garante per la protezione dei dati personali, 'Provvedimento dell'11 aprile 2023 [9874702]' (Garante per la protezione dei dati personali, 11.04.2023) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702> (dostęp: 20.09.2024 r.). Także francuski organ ochrony danych, CNIL, por. CNIL, 'Restricted Committee Deliberation N° SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI' (17 października 2022) https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf (dostęp: 20.09.2024 r.).

⁴⁸⁴ S. B. Vale, *Training Large Generative AI Models Based on Publicly Available Personal Data: A GDPR Conundrum that the AI Act Could Solve*, „The Digital Constitutionalist”, 14 kwietnia 2023. <https://digi-con.org/training-large-generative-ai-models-based-on-publicly-available-personal-data-a-gdpr-conundrum-that-the-ai-act-could-solve/> (dostęp: 20.09.2024 r.); por. także C. Gallese, *Web scraping and Generative Models training in the Directive 790/19*, „Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale” 2023, Vol. 16, No. 2.

⁴⁸⁵ L. Naudts et al., *Meaningful Transparency through Data Rights: A Multidimensional Analysis*, „Amsterdam Law School Research Paper” 2022, No. 37, <https://dx.doi.org/10.2139/ssrn.3949750> (dostęp: 20.09.2024 r.).

Ma to wpływ na ocenę prawną przestrzegania zasady zgodności z prawem i adekwatności. Największe podmioty wykorzystują tzw. „uzasadniony interes” (art. 6 ust. 1 lit. f RODO) jako podstawę prawną do trenowania modeli generatywnej sztucznej inteligencji. Wykorzystanie tej podstawy – chociaż teoretycznie wydaje się być dopuszczalne – budzi poważne wątpliwości w praktyce działania systemów funkcjonujących na podstawie tych modeli⁴⁸⁶, w tym także czy możliwe jest spełnienie warunków do przetwarzania danych w celu innym niż cel pierwotny (art. 6 ust. 4 RODO). Nadto, należy przypuszczać, że zbiory danych wykorzystywane przez modele generatywnej sztucznej inteligencji zawierają szczególne kategorie danych osobowych⁴⁸⁷, co dodatkowo potęguje problem, gdyż do ich przetwarzania konieczne jest spełnienie jednego z warunków w art. 9 ust. 2 RODO. Kolejnym problem związany jest z zapewnieniem prawidłowości przetwarzania danych osobowych⁴⁸⁸. Zidentyfikowanie, że przy korzystaniu z systemów generatywnej sztucznej inteligencji dochodzi do tzw. „halucynacji” przy udzielaniu odpowiedzi⁴⁸⁹. Przyczyną tego zjawiska jest, że systemy generatywnej sztucznej inteligencji oparte są na statystyce, a zatem prawda (prawidłowość) jako kryterium nie jest dla nich punktem odniesienia⁴⁹⁰. Może prowadzić to do poważnych skutków dla osób fizycznych, w tym naruszenia dobrego imienia i dyskryminacji⁴⁹¹.

Ta analiza prowadzi do wniosku, że jeszcze przed wejściem w życie rozporządzenia unijnego Aktu w sprawie Sztucznej Inteligencji (AI Act) w unijnym porządku prawnym systemy sztucznej inteligencji były przedmiotem regulacji przez RODO, a w konsekwencji organy ochrony danych z perspektywy ochrony danych osobowych i prawa do prywatności. AI Act nie wyłącza stosowania RODO. Przy tak znacznej roli danych osobowych w rozwoju

⁴⁸⁶ Pogłębiona analiza tego problem w: P. T. Kramcsák, Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?, CLSR 2023, Vol. 48.

⁴⁸⁷ EIOD, *First EDPS Orientations for EUIs using Generative AI*, 3 czerwca 2024, https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en (dostęp: 15.09.2024 r.), s. 9.

⁴⁸⁸ Por. F. Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making*, Strasbourg: Council of Europe, Directorate General of Democracy 2018, <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-%20making/1680925d73> (dostęp: 4.11.2024 r.).

⁴⁸⁹ Przykładowo, w wygenerowanej odpowiedzi ChatGPT oskarżył profesora prawa o molestowanie seksualne; por. J Nelson, *ChatGPT Wrongly Accuses Law Professor of Sexual Assault* (Yahoo Finance, 7 April 2023) https://finance.yahoo.com/news/chatgpt-wrongly-accuses-law-professor-184500778.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2x1LmNvbS8&guce_referrer_sig=AQAAAGNAz_Mo-_4Ditq9q0FPgivJrr74PwDjb23HfsDzy7qhphC7XJVskisu-ZHdDaFlIxnWa3MxcHC_pjz2zv2kBV7yGt_VZaUsv2OVzjDIV2CApvmQ5K9AgIW8pIvv2NJyswyvP9sM8jUBfYGc3N5Eo_lgZc4EwBQ9w_izzBHBCc46j (dostęp: 4.09.2024 r.).

⁴⁹⁰ Por. Ji Ziwei et al., *Survey of Hallucination in Natural Language Generation*, „ACM Computing Surveys” 2023, t. 55, nr 12 <https://doi.org/10.1145/3571730>. (dostęp: 20.09.2024 r.).

⁴⁹¹ D. Varona, J. L. Suárez, *Discrimination, Bias, Fairness, and Trustworthy AI*, „Applied Sciences” 2022, Vol. 12, Iss. 12.

i korzystaniu z systemów sztucznej inteligencji (w tym przypadku systemów generatywnej sztucznej inteligencji) jest niemożliwe, że zakres przedmiotowy RODO i AI Act nie będzie się krzyżował.

AI Act, zgodnie z art. 1 ust. 2 (lit. a-g) ustanawia: 1) zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji w UE; 2) zakazy dotyczące określonych praktyk w zakresie sztucznej inteligencji; 3) szczególne wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka oraz obowiązki spoczywające na podmiotach będących operatorami takich systemów; 4) zharmonizowane przepisy dotyczące przejrzystości w przypadku systemów sztucznej inteligencji; 5) zharmonizowane przepisy dotyczące wprowadzania do obrotu modeli AI ogólnego przeznaczenia; 6) przepisy dotyczące monitorowania wprowadzania do obrotu, nadzoru rynku, zarządzania i egzekwowania; 7) środki wspierające innowacje, ze szczególnym uwzględnieniem MŚP, w tym przedsiębiorstw typu start-up.⁴⁹² Celem niniejszego podrozdziału nie jest kompleksowa analiza AI Act, lecz jedynie jego zbadania w zakresie niezbędnym do weryfikacji hipotez badawczych tej rozprawy.

Zasadniczo AI Act stosuje się do systemów AI, przy czym prawodawca unijny ustanowił definicję legalną tego terminu w art. 3 pkt 1 AI Act: „system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne”. Treść tej definicji była przedmiotem intensywnych dyskusji w trakcie procesu prawodawczego⁴⁹³. Definicja ta jest dwuelementowa. Pierwszy element odnosi się do sposobu zaprojektowania systemu maszynowego, przy czym warunkiem koniecznym spełnienia tego elementu przez system maszynowy jest posiadanie poziomu autonomii, natomiast takim warunkiem nie jest zdolność adaptacji po jego wdrożeniu. Z kolei drugim elementem jest czynność wnioskowania jak generować dane wyjściowe. Jedynie łączne

⁴⁹² Cel AI Act określony został w art. 1 ust. 1 z uwzględnieniem praw podstawowych, w tym prawa do ochrony danych osobowych jako: „Celem niniejszego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego i promowanie upowszechniania zorientowanej na człowieka i godnej zaufania sztucznej inteligencji (AI), przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych zapisanych w Karcie, w tym demokracji, praworządności i ochrony środowiska, przed szkodliwymi skutkami systemów AI w Unii oraz wspieraniu innowacji”.

⁴⁹³ Por. motyw 12 do AI Act; Axel Spies, *EU AI Act: Institutions Debate Definition of AI*, Morgan Lewis, September 26, 2023. <https://www.morganlewis.com/pubs/2023/09/eu-ai-act-institutions-debate-definition-of-ai> (dostęp: 23.09.2024 r.).

spełnienie obu elementów powoduje, że system maszynowy jest systemem AI w rozumieniu AI Act. Definicję tę należy uznać za sformułowaną w sposób szeroki, co może powodować w praktyce problemy przy identyfikacji czy określony system maszynowy należy zakwalifikować systemem sztucznej inteligencji w rozumieniu Aktu w sprawie Sztucznej Inteligencji.

Zakres podmiotowy AI Act⁴⁹⁴ unormowany jest przez ustanowienie nowych (względem RODO) kategorii podmiotowych, w tym „dostawca”⁴⁹⁵, „podmiot stosujący”⁴⁹⁶ i „operator”⁴⁹⁷ zdefiniowanych w art. 3 AI Act. Zakres znaczeniowy tych terminów krzyżuje się z zakresem znaczeniowym terminów „administrator”, „współadministrator” i „podmiot przetwarzający”, ale nie jest z nimi tożsamy⁴⁹⁸. Współstosowanie AI Act i RODO powoduje, że na poszczególnych podmiotach spoczywały będą obowiązki wynikające z każdego z tych aktów z osobna w zależności od kwalifikacji tych podmiotów względem powyższych kategorii podmiotowych.

Akt w sprawie Sztucznej Inteligencji przyjęto w oparciu o podejście oparte na analizie ryzyka⁴⁹⁹ (motyw 26-27 AI Act) z uwzględnieniem tzw. nowych ram prawnych („*New Legislative Framework*”⁵⁰⁰) (motyw 9 AI Act) normujących sposób regulowania nadzoru zharmonizowanego rynku wewnętrznego produktów niezwywnościowych, które stanowiły inspirację dla prawodawcy unijnego m.in. w odniesieniu do obowiązków notyfikacyjnych i specyfikacji technicznych w AI Act⁵⁰¹. Niektóre praktyki („wprowadzanie do obrotu, oddawania do użytku lub wykorzystywania systemu AI”) w zakresie AI – zidentyfikowane jako stanowiące największe zagrożenie dla praw podstawowych – zostały wprost zakazane w art. 5 m.in. stosujące techniki podprogowe lub celowe techniki manipulacyjne nakierowane

⁴⁹⁴ Zakres zastosowania uregulowano w art. 2 AI Act.

⁴⁹⁵ Art. 3 pkt 3 AI Act: „dostawca” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które rozwijają system AI lub model AI ogólnego przeznaczenia lub zlecają rozwój systemu AI lub modelu AI ogólnego przeznaczenia oraz które – odpłatnie lub nieodpłatnie – pod własną nazwą lub własnym znakiem towarowym wprowadzają do obrotu lub oddają do użytku system AI”.

⁴⁹⁶ Art. 3 pkt 4 AI Act: „podmiot stosujący” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które wykorzystują system AI, nad którym sprawują kontrolę, z wyjątkiem sytuacji, gdy system AI jest wykorzystywany w ramach osobistej działalności pozazawodowej”.

⁴⁹⁷ Art. 3 pkt 8 AI Act: „operator” oznacza dostawcę, producenta produktu, podmiot stosujący, upoważnionego przedstawiciela, importera lub dystrybutora”.

⁴⁹⁸ D. Lubasz, A. Szkurlat. Relacja aktu o sztucznej inteligencji i ogólnego rozporządzenia o ochronie danych, MoP 2022, nr 21, s. 26-29.

⁴⁹⁹ Termin „ryzyko” zdefiniowano w art. 3 pkt 2 AI Act: „ryzyko” oznacza połączenie prawdopodobieństwa wystąpienia szkody oraz jej dotkliwości”.

⁵⁰⁰ Por. Komisja Europejska, *Nowe ramy legislacyjne*, https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en?prefLang=pl (dostęp: 15.09.2024 r.).

⁵⁰¹ M. Namysłowska, R. Bieda, P. Budrewicz et al., O etycznych, prawnych i społecznych konsekwencjach stosowania systemów sztucznej inteligencji w państwach członkowskich Unii Europejskiej. Uwagi na tle projektu rozporządzenia w sprawie sztucznej inteligencji, „Przegląd Sejmowy” 2023, 6 (179), s. 69.

na ograniczenie świadomego decydowania (art. 5 ust. 1 lit a), wykorzystujące słabości osób fizycznych ze względu m.in. na wiek (art. 5 ust. 1 lit b), dokonujące tzw. *scoringu* społecznego kwalifikowanego negatywnymi skutkami (art. 5 ust. 1 lit. c) lub kategoryzacji biometrycznej (art. 5 ust. 1 lit. g).

Poza zakazanymi praktykami, systemy sztucznej inteligencji zostały w AI Act zaklasyfikowane do jednej z trzech kategorii ryzyka – wysokiego (Rozdział 3 Sekcja 1 „Klasyfikacja systemów AI jako systemów AI wysokiego ryzyka”), średniego i niskiego. Zasady klasyfikacji systemów AI do jednej z trzech kategorii ryzyka są złożone; uzależnione są m.in. od tego, czy system AI stanowi samodzielny produkt, czy też element innego produktu i od kwalifikacji systemu zgodnie z załącznikami do AI Act (w tym Załącznik III określający systemy AI wysokiego ryzyka). Zakres obowiązków uzależniony podmiotów zobowiązanych na podstawie AI Act jest uzależniony od klasyfikacji systemów AI do określonej kategorii ryzyka, przy czym najbardziej wymagające obowiązki związane są z wysokim ryzykiem, np. Sekcja 2 Rozdziału III „Wymogi dotyczące systemów AI wysokiego ryzyka”, np. obowiązek zapewnienia przejrzystości i udostępnianie informacji podmiotom stosującym (art. 13) oraz Sekcja 3 Rozdziału III „Obowiązki dostawców i podmiotów stosujących systemy AI wysokiego ryzyka oraz innych osób”, np. obowiązek wprowadzenia systemów zarządzania jakością (art. 17). Osobno w Rozdziale V AI Act uregulowano modele AI ogólnego przeznaczenia⁵⁰² (por. motyw 105 AI Act), ze szczególnym uwzględnieniem model AI ogólnego przeznaczenia z ryzykiem systemowym, którego kryteria klasyfikacji unormowano w art. 51 ust. 1 AI Act. Generalne obowiązki dostawców modeli AI ogólnego przeznaczenia unormowano w Sekcji 2 Rozdziału V „Obowiązki Dostawców Modeli AI Ogólnego Przeznaczenia”, co obejmuje, na przykład obowiązek sporządzenia dokumentacji technicznej modelu udostępnianej Urzędowi ds. AI i dostawcom systemów AI (art. 53 ust. 1 lit. a-b), podczas gdy szczególne obowiązki dostawców modeli AI ogólnego przeznaczenia z ryzykiem systemowym uregulowano w sekcji 3 Rozdziału V, m.in. w zakresie zgłaszania poważnych incydentów Urzędowi ds. AI (art. 53 ust. 1). Środki ochrony prawnej,

⁵⁰² Zdefiniowany w art. 3 pkt 63 AI Act: „model AI ogólnego przeznaczenia” oznacza model AI, w tym model AI trenowany dużą ilością danych z wykorzystaniem nadzoru własnego na dużą skalę, który wykazuje znaczną ogólność i jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań, niezależnie od sposobu, w jaki model ten jest wprowadzany do obrotu, i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla – z wyłączeniem modeli AI, które są wykorzystywane na potrzeby działań w zakresie badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu”. Podobnie jak w przypadku definicji systemów AI, definicja określenia „model AI ogólnego przeznaczenia” jest szeroka, ponieważ zawiera terminy nieostre, których interpretacja w praktyce spowodować może wątpliwości prowadzące do trudności w kwalifikacji danego modelu AI jako modelu AI ogólnego przeznaczenia. Nadto, nie jest klarowne, dlaczego prawodawca unijny posłużył się terminem „model”, podczas gdy zasadniczo AI Act ma zastosowanie do „systemów” AI.

takie jak prawo do wniesienia skargi przez osoby fizyczne i prawne (art. 85) i prawo do uzyskiwania wyjaśnień na temat procedury podejmowania decyzji (art. 86), uregulowane zostały w Sekcji 4 Rozdziału IX, natomiast reguły dotyczące potencjalnie bardzo wysokich, wielomilionowych (maksymalne wysokości kar podane w euro) administracyjnych kar pieniężnych zawarto w Rozdziale XII „Kary”, które w swojej konstrukcji przypominają unormowanie dotyczących kar pieniężnych w RODO (art. 99 AI Act).

W literaturze zidentyfikowano liczne przypadki krzyżowania się zakresów przedmiotowych (i obowiązków ustanowionych przez) RODO i AI Act⁵⁰³. Przykładowo, G. Zafira-Fortuna⁵⁰⁴ wskazuje, że zarówno niektóre z zakazanych praktyk dotyczą bezpośrednio przetwarzania danych osobowych, jak *social scoring* oparty na tych danych, czy systemy rozpoznawania twarzy, a jednocześnie dostawcy systemów AI wysokiego ryzyka są zobowiązani do przetwarzania szczególnych kategorii danych osobowych, „w zakresie, w jakim jest to bezwzględnie konieczne do celów zapewnienia wykrywania i korygowania stronniczości systemów AI wysokiego ryzyka”, pod warunkiem spełnienia rozbudowanych wymogów nakierowanych na ochronę praw podstawowych i minimalizację przetwarzania danych osobowych, o których mowa w art. 10 ust. 5 AI Act. A. Magiera i J. Wyczyk wskazują na to, że obowiązki dotyczące transparentności w AI Act odnoszą się zasadniczo do systemów AI wysokiego ryzyka, podczas gdy obowiązki wynikające z zasady przejrzystości w RODO mają zastosowanie wobec wszystkich administratorów⁵⁰⁵. Ocenne pozostaje czy spełnienie wymogów przez dostawców systemów AI wysokiego ryzyka i podmiotów stosujących niektóre systemy AI zgodnie z art. 50 AI Act (o ile będą one administratorami lub współadministratorami danych osobowych) dotyczących transparentności z AI Act może być uznane za spełnienie wymogów dotyczących przejrzystości z RODO; a jeżeli tak nie jest, to w jaki sposób należy ocenić relację obu tych równoległych obowiązków. Z kolei K. Sein

⁵⁰³ Por. także P. Hajduk, *AI Act And GDGR: On The Path Towards Overlap Of The Enforcement Structures*, 1.10.2023, <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/?cn-reloaded=1&cn-reloaded=1> (dostęp: 15.09.2024 r.); EROD i EIOD, *EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, 18 czerwca 2021; Grupa Robocza ds. AI, *Analysis of the Relationship of the Act on Artificial Intelligence with Selected and Proposed Regulations*, 3 sierpnia 2023, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjB08fnpNiGAXUjSPEDHea4DEoQFnoECBsQAQ&url=https%3A%2F%2Fwww.gov.pl%2Fattachment%2F8b2bed43-a24c-4d10-b341-a7372e702455&usq=AOvVaw04PjC_uudrNAlYqclDj5BV&opi=89978449 (dostęp: 15.09.2024 r.).

⁵⁰⁴ G. Zafira-Fortuna, *Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package* [in:] *Two decades of personal data protection. What next?*, Brussels: European Data Protection Supervisor 2024, https://www.edps.europa.eu/system/files/2024-06/edps_20thanniversary-book_en.pdf (dostęp: 20.09.2024 r.), s. 6.

⁵⁰⁵ A. Magiera, J. Wyczyk, *Akt o AI w kontekście ochrony danych*, „ABIExpert”, styczeń-marzec 2023, s. 14-16.

I M. Ebers zwracają uwagę na to, że RODO generalnie zakazuje opartych wyłącznie na zautomatyzowanym przetwarzaniu i szczególnych kategoriach danych osobowych (art. 22 ust. 4 RODO), podczas gdy AI Act nakłada obowiązek nadzoru ze strony człowieka zasadniczo dla systemów AI wysokiego ryzyka (art. 14 AI Act)⁵⁰⁶. Finalnie zaś, deklaracja zgodności z UE wydawana dla systemów wysokiego ryzyka (art. 47) ma zawierać informację, że system AI wiążący się z przetwarzaniem danych osobowych jest zgodny z RODO i Dyrektywą LED (zgodnie z pkt 5 Załącznika nr V).

Akt w sprawie Sztucznej Inteligencji identyfikuje ryzyko krzyżowania się zakresów przedmiotowych z RODO, które w AI Act wymieniono wprost 11 razy. Świadczą o tym przepisy rozstrzygające o pozostawianiu AI Act „bez uszczerbku” dla RODO, m.in. art. 2 ust. 7, art. 5 ust. 1 lit. h i motyw (10), art. 10 ust. 5 AI Act, a także przez odwołanie do definicji w RODO, np. art. 3 pkt 37, 50-52 AI Act, przy czym w Akcie w sprawie Sztucznej Inteligencji wprowadzono autonomiczną definicję danych biometrycznych (art. 3 pkt 34 AI Act)⁵⁰⁷. AI Act wybiórczo odnosi się także do interakcji między obowiązkami z RODO a obowiązkami z AI Act (np. motyw (140) AI Act). Dowodem tego, że prawodawca unijny zidentyfikował to ryzyko jest także wyznaczenie EIOD i organów ochrony danych wprost jako organów kompetentnych do stosowania AI Act, jednak tylko w ograniczonym zakresie, co jest przedmiotem analizy w rozdziale 3 rozprawy.

2.6.5. AKTY PRAWNE REGULUJĄCE EUROPEJSKIE PRZESTRZENIE DANYCH

Europejskie przestrzenie danych to koncepcja przedstawiona w Europejskiej Strategii w zakresie Danych przez Komisję w 2020 r.⁵⁰⁸ Termin ten rozumiany jest w tym dokumencie jako „narzędzia i infrastruktura techniczna niezbędna do korzystania z danych i ich wymiany, a także odpowiednich mechanizmów zarządzania” tymi procesami w strategicznych sektorach⁵⁰⁹. Komisja zadeklarowała wsparcie dla rozwoju europejskich przestrzeni danych

⁵⁰⁶ M. Ebers, K. Sein, Data-driven Technologies – Challenges for Privacy and EU Data Protection Law [in:] Privacy, Data Protection and Data-driven Technologies, red. M. Ebers, K. Sein, Abingdon 2024, <https://ssrn.com/abstract=4823823> (dostęp: 20.09.2024 r.), s. 21-22.

⁵⁰⁷ Przy czym w motywie 14 odwołano się do definicji tego terminu w art. 4 pkt 14 RODO; por. także D. Lubasz, A. Szkurlat, *Relacja aktu o sztucznej inteligencji i ogólnego rozporządzenia o ochronie danych*, MoP 2022, nr 21, s. 28-31.

⁵⁰⁸ Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia w zakresie danych COM(2020) 66 final, s. 23.

⁵⁰⁹ Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia w zakresie danych COM(2020) 66 final, s. 23.

w strategicznych sektorach, aby umożliwić dostęp do tych danych (zarówno osobowych, jak i nieosobowych), proponując utworzenie dziesięciu przestrzeni⁵¹⁰: zdrowie, rolnictwo, produkcja (przemysł), energia, mobilność, finanse, administracja publiczna, umiejętności, Europejska Chmura Otwartej Nauki i Wspólny Europejski Zielony Ład⁵¹¹. Strategia ta ma zostać zrealizowana przy „pełnej zgodności” z RODO i standardami cyberbezpieczeństwa⁵¹².

Akt w sprawie Zarządzania Danymi⁵¹³ i Akt w sprawie Danych⁵¹⁴ przyjęte zostały jako ramowe akty prawne ustanawiające rozwiązania dla wszystkich tych przestrzeni, do których to rozwiązań akty prawne ustanawiające poszczególne przestrzenie będą się odwoływały, co – w założeniu – ma pozwolić zachować spójność. Oprócz tych dwóch już przyjętych aktów, w ramach Europejskiej Strategii w zakresie Danych procedowane są obecnie kolejne akty prawne dotyczące finansów (Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych⁵¹⁵), a akt prawny dotyczący przestrzeni zdrowia został już przyjęty (Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia⁵¹⁶) i z uwagi na to, że sektorowe akty te są jeszcze zasadniczo w toku procesu prawodawczego, jak też mając na względzie objętość tej rozprawy, podjęto decyzję o wyłączeniu ich z obszaru referencyjnego⁵¹⁷.

⁵¹⁰ Liczba europejskich przestrzeni danych, jak i klasyfikacja strategicznych sektorów ulegała zmianom po opublikowaniu cytowanej wyżej Strategii.

⁵¹¹ Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia w zakresie danych COM(2020) 66 final, s. 28-36.

⁵¹² Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia w zakresie danych COM(2020) 66 final, s. 23.

⁵¹³ Uzasadnienie, Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) COM/2020/767 final. Komisja Europejska, Komisja z zadowoleniem przyjmuje przyjęcie przez Parlament Europejski europejskiej przestrzeni danych dotyczących zdrowia oraz rozporządzenia w sprawie substancji pochodzenia ludzkiego, [Komunikat prasowy] Bruksela, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2250 (dostęp: 15.09.2024 r.).

⁵¹⁴ Komisja, <https://digital-strategy.ec.europa.eu/pl/policies/strategy-data> (dostęp: 15.09.2024 r.).

⁵¹⁵ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) 1095/2010 i (UE) 2022/2554, COM/2023/360 final.

⁵¹⁶ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia COM/2022/197 final. Por. także opinię EIOD i EROD: Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en.pdf (dostęp: 15.09.2024 r.).

⁵¹⁷ Natomiast autor tej rozprawy jest autorem artykułu *A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research* dotyczącego relacji projektu rozporządzenia o europejskiej przestrzeni danych dotyczących zdrowia, DGA, Data Act i RODO w odniesieniu do prowadzenia badań naukowych z wykorzystaniem danych dotyczących zdrowia. Wybrane wnioski sformułowane w tym artykule zawarto również w tym podrozdziale. Por. P. Hajduk, *A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research* (November 23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 - Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.).

2.6.5.1. AKT W SPRAWIE ZARZĄDZANIA DANYMI (DATA GOVERNANCE ACT)

Przedmiotem unormowania w rozporządzeniu Akt w sprawie Zarządzania Danymi (DGA) są następujące kwestie: 1) ponowne wykorzystywanie niektórych kategorii danych (w tym danych osobowych; por. art. 3 ust. 1 lit. d DGA) w posiadaniu sektora publicznego; 2) zgłaszanie i nadzór w odniesieniu do świadczenia usług pośrednictwa danych; 3) dobrowolna rejestracja uznanych organizacja altruizmu danych (art. 1 ust. 1 DGA). Celem jest poprawa warunków dzielenia się danymi w UE przez utworzenie instrumentów bezpiecznego pośrednictwa (motyw 3 DGA) i dalsze otwarcie danych w posiadaniu sektora publicznego⁵¹⁸.

Akt w sprawie Zarządzania Danymi (DGA) wprowadza nowe (względem RODO) kategorie podmiotów: „posiadacz danych”, „użytkownik danych”, „dostawca usług pośrednictwa danych” i „uznana organizacja altruizmu danych”⁵¹⁹. „Posiadacz danych” (art. 2 pkt 8 DGA) to podmiot inny niż podmiot danych, który ma prawo do udzielania dostępu do niektórych danych osobowych lub nieosobowych lub do dzielenia się nimi (definicja tego ostatniego terminu w art. 2 pkt 10 DGA). Z kolei „użytkownik danych” (art. 2 pkt 10 DGA) jest podmiotem, który ma zgodny z prawem dostęp do niektórych danych osobowych lub nieosobowych, i prawo (w przypadku danych osobowych na podstawie RODO) do ich wykorzystywania w celach komercyjnych lub niekomercyjnych. Dostawcy usług pośrednictwa danych to zaś podmioty (art. 2 pkt 11 DGA w zw. z art. 11 DGA) świadczące usługi nakierowane na ustanowienie relacji handlowych między nieokreśloną liczbą podmiotów danych i posiadaczy danych oraz użytkownikami danych do celów dzielenia się danymi⁵²⁰ (z wyłączeniem co najmniej czterech rodzajów usług wskazanych w art. 2 pkt 11 DGA). Uznane organizacje altruizmu danych to podmioty spełniające formalne wymogi określone w art. 18-21 DGA zarejestrowane w publicznym krajowym rejestrze uznanych organizacji altruizmu danych (art. 17 DGA), które powinny móc gromadzić dane, w tym dane osobowe, bezpośrednio od podmiotów danych i innych podmiotów, jak i danych zebranych przez inne podmioty (motyw 50 DGA) przekazane w ramach altruizmu danych (rozumianego, zgodnie z art. 2 pkt 16 DGA,

⁵¹⁸ W zakresie wykraczającym poza Dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego, L 172/56.

⁵¹⁹ W tej liście pominięto spółdzielnie danych (por. motyw 31 DGA).

⁵²⁰ Por.: w odniesieniu do definicji usług pośrednictwa danych: T. Bobev, V. K. Dessers, Ch. Ducuing et al., *White Paper on the Definition of Data Intermediation Services*, „CiTiP Working Paper Series” 2023, <http://dx.doi.org/10.2139/ssrn.4589987> (dostęp: 20.09.2024 r.).

jako dobrowolne dzielenie się danymi, w tym danymi osobowymi, bez wynagrodzenia przez podmioty danych i odpowiednio posiadaczy danych dla wspólnego dobra⁵²¹). Powyższe zestawienie definicji nowych kategorii podmiotów ustanowionych na podstawie DGA prowadzi do wniosku, że ich liczba jest znaczna. Pomimo prób wyjaśnienia ich relacji względem podmiotów ustanowionych na podstawie RODO, tj. „administratora”, „współadministratora” i „podmiotu przetwarzającego” w motywach DGA (np. 35, 50), relacja ta pozostaje niejasna. Przykładowo, niejasne jest czy dostawcy usług pośrednictwa danych w przypadku przetwarzania danych osobowych posiadali będą status współadministratora razem z użytkownikami danych, a jeżeli tak, to w jaki sposób powinien nastąpić podział obowiązków z RODO zgodnie z uzgodnieniami z art. 26 RODO.

Rozdział II DGA normujący ponowne wykorzystywanie niektórych kategorii chronionych danych (w tym danych osobowych) w posiadaniu sektora publicznego nie kreuje obowiązku podmiotów publicznych do udzielania dostępu w celu ponownego wykorzystywania danych, lecz nakłada obowiązek określenia warunków i procedury umożliwiającej takie ponowne wykorzystywanie (art. 5 ust. 1 DGA). Dane (co do zasady po ich anonimizacji) powinny być przekazywane wnioskodawcy tylko wtedy, gdy pozwala na to podstawa prawna przetwarzania z RODO (motyw 7 i 15 DGA). Oznacza to, że podmioty sektora publicznego lub właściwe podmioty (art. 7 DGA) rozpoznające wnioski o udzielanie dostępu w celu ponownego wykorzystywania danych będą uprawnione do badania podstaw prawnych przetwarzania z RODO (w przypadku takiego zakresu wniosku), a także wyboru techniki anonimizacji i pseudonimizacji tych danych.

Wymogi dotyczące usług pośrednictwa danych uregulowano w rozdziale III DGA, tworząc systemu zgłaszania i nadzoru nad działalnością dostawców usług udostępniania danych (zdefiniowanych wyżej). Podmioty te będą świadczyły usługi pośrednictwa między posiadaczami danych i podmiotami danych z jednej strony, a z drugiej – użytkownikami danych. Dostawcy zobowiązani są do dokonania zgłoszenia świadczonych usług do organu właściwego do spraw usług pośrednictwa danych⁵²² (art. 11 DGA) i przestrzegania warunków ich świadczenia określonych w art. 12 DGA, które obejmują m.in. zakaz wykorzystywania danych do innych celów (art. 12 lit. a DGA), ułatwianie interoperacyjności (art. 12 lit. d DGA) i obowiązki bezpieczeństwa w odniesieniu do przetwarzania danych nieosobowych (art. 12 lit. l DGA). Należy podzielić zastrzeżenia zgłoszone w opinii do projektu DGA przez EIOD

⁵²¹ Uzasadnienie, Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) COM/2020/767 final.

⁵²² Kompetencje tego organu scharakteryzowane w podrozdziale 3.5.6. poniżej.

dotyczące braku pogłębionej procedury weryfikacji podmiotów składających zgłoszenie jako dostawcy usług pośrednictwa danych (podobna uwaga zasadna jest w odniesieniu do rejestracji uznanych organizacji altruizmu danych) – podmiotów, które będą mogły przetwarzać znaczne ilości danych osobowych⁵²³. Ta procedura oparta jest niemal wyłącznie na samych oświadczeniach złożonych przez te podmioty, co nie daje wystarczających gwarancji, że podmioty te spełniać będą warunki określone w art. 12 DGA⁵²⁴. Wskazane byłoby, aby procedura uprzedniej weryfikacji wymagała przynajmniej przedłożenia przez te podmioty opinii biegłego do spraw cyberbezpieczeństwa, że wdrożone przez te podmioty zabezpieczenia są należyte.

Rozdział IV DGA reguluje altruizm danych (zdefiniowany wyżej). Ustanowiono możliwość rejestracji osobnych podmiotów, tzw. „organizacji altruizmu danych” (art. 17 DGA), które winny spełniać wymogi w art. 18-21 DGA, w tym wymóg prowadzenia działalności o charakterze niekomercyjnym (art. 18 lit. c DGA) i prowadzenia dokumentacji dotyczącej przejrzystości (21 DGA) oraz przestrzeganie zbioru zasad przyjętego przez Komisję (zgodnie z art. 22 DGA), które powinny określać m.in. wymogi techniczne, aby zapewnić bezpieczeństwo przetwarzania danych, a także wymogi informacyjne wobec podmiotów danych przed wyrażeniem zgody na altruizm danych. Altruizm danych osobowych opiera się na zgodzie podmiotów danych w rozumieniu art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO, która powinna spełniać warunki jej wyrażenia z RODO (motyw 50 DGA), a jego celem jest wykorzystanie tych danych w interesie ogólnym, którego przykłady wskazane zostały w art. 2 pkt 16 DGA (opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, kształtowanie polityki publicznej). Niejasny pozostaje związek między pojęciem „interesu ogólnego”, który miałby być celem przetwarzania danych osobowych na podstawie zgody, a warunkiem konkretności zgody z RODO (zdefiniowanej w art. 4 pkt 11 RODO; scharakteryzowano powyżej). Pojęcie „interesu ogólnego” w DGA nie jest wystarczająco precyzyjne, aby mogło samodzielnie spełnić warunek konkretności zgody z RODO⁵²⁵. Problem prawidłowego udzielenia zgody w celu altruizmu danych na podstawie DGA i RODO

⁵²³ EROD i EIOD, Wspólna opinia EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu i Rady europejskiego danymi (akt zarządzania danymi), Wersja 1.1, s. 37-41, https://edpb.europa.eu/system/files/2021-09/edpb-edps_joint_opinion_dga_II_0.pdf (dostęp: 15.09.2024 r.).

⁵²⁴ EROD i EIOD, Wspólna opinia EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu i Rady europejskiego danymi (akt zarządzania danymi), Wersja 1.1, s. 37-41, https://edpb.europa.eu/system/files/2021-09/edpb-edps_joint_opinion_dga_pl_0.pdf (dostęp: 15.09.2024 r.).

⁵²⁵ EROD i EIOD, Wspólna opinia EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu i Rady europejskiego danymi (akt zarządzania danymi), Wersja 1.1, s. 44-46, https://edpb.europa.eu/system/files/2021-09/edpb-edps_joint_opinion_dga_pl_0.pdf (dostęp: 15.09.2024 r.).

powiązany jest również z problemem technicznej możliwości jej efektywnego wycofania (art. 7 ust. 3 RODO; przy czym obowiązek zapewnienia odpowiednich rozwiązań spoczywa na uznanych organizacjach altruizmu zgodnie z art. 21 ust. 3 DGA) i należytego wypełnienia obowiązku organizacji altruistycznych do informowania podmiotów danych (art. 21 ust. 1 DGA) o „celach leżących w interesie ogólnym oraz w stosownych przypadkach, o konkretnym, wyraźnym i zgodnym z prawem celu przetwarzania danych osobowych [...]”. Pozostaje niejasne, w jaki sposób należy uzyskać zgody na altruizm danych, jaka jest relacja obowiązku informacyjnego z art. 21 ust. 1 DGA do obowiązku informacyjnego administratora względem podmiotów danych z art. 13 RODO, co dodatkowo skomplikowane jest przez możliwość wydania przez Komisję zbioru zasad wskazanego powyżej w odniesieniu do tych kwestii⁵²⁶.

W DGA zidentyfikowano ryzyko krzyżowania się zakresów przedmiotowych RODO i DGA (art. 1 ust. 3 DGA i motyw 3, 4 DGA), rozstrzygając, że DGA pozostaje „bez uszczerbku” dla RODO i kompetencji organów ochrony danych osobowych (motywy 3, 4, 26, 35 i 44 DGA) oraz odwołując się bezpośrednio do definicji w RODO (np. art. 2 pkt 3,5 i 7 DGA). W sytuacji „kolizji [między DGA] a prawem Unii w dziedzinie ochrony danych osobowych lub prawem krajowym przyjętym zgodnie z takim prawem Unii pierwszeństwo ma odpowiednie prawo [...] w dziedzinie ochrony danych osobowych” (art. 1 ust. 3 DGA). Zgodnie z tym ustępem, DGA nie ustanawia osobnej podstawy prawnej dla przetwarzania danych osobowych i nie zmienia praw i obowiązków określonych w RODO.

2.6.5.2. AKT W SPRAWIE DANYCH (DATA ACT)

Pełna nazwa Aktu w Sprawie Danych (Data Act) to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania⁵²⁷. Akt w sprawie Danych stanowi, obok DGA, drugi z ramowych aktów prawnych dla europejskich przestrzeni danych⁵²⁸. Przywołany pełny tytuł Aktu w sprawie Danych oddaje dwa podstawowe

⁵²⁶ P. Hajduk, A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research (November–23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 – Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.), s. 6. Por. T. Lalova-Spinks, J. Meszaros, I. Huys, The application of data altruism in clinical research through empirical and legal analysis lenses, „Frontiers in Medicine” 2023, Vol. 10.

⁵²⁷ Data Act stosuje się od dnia 12 września 2025 r., zgodnie z art. 50 Data Act.

⁵²⁸ Komisja, <https://digital-strategy.ec.europa.eu/en/news/european-data-act-enters-force-putting-place-new-rules-fair-and-innovative-data-economy> (dostęp: 15.09.2024 r.).

jego cele – zapewnienie dostępu do danych⁵²⁹ (osobowych i nieosobowych), jak i ich wykorzystywania w taki sposób, aby podział tego dostępu i wykorzystywania, a w konsekwencji uzyskiwania wartości ekonomicznej był sprawiedliwy i szeroki, przede wszystkim w kontekście *Internet of Things*⁵³⁰. Możliwość realizacji tych celów przy użyciu instrumentarium zaproponowanego w Data Act jest w literaturze krytykowana, przede wszystkim z uwagi na zbyt silną ochronę posiadaczy danych⁵³¹. Już z drugiego zdania uzasadnienia do Wniosku w sprawie Data Act wynika, że dane normowane są przede wszystkim z perspektywy danych jako aktywa (*resource*)⁵³². Przyjęcie właśnie tej perspektywy uzasadniać ma rozszerzenie prawa do przenoszenia danych osobowych z art. 20 RODO ograniczonego w RODO do określonych podstaw i sposobów przetwarzania (por. motyw 30 Data Act) w taki sposób, aby uczynić z niego komercyjny pożytek⁵³³.

Data Act składa się z 50 artykułów podzielonych na 11 rozdziałów: Rozdział I (Przepisy ogólne; art. 1-2); Rozdział II (Dzielenie się danymi przez przedsiębiorców z konsumentami i z innymi przedsiębiorcami; art. 3-7); Rozdział III (Obowiązki posiadaczy danych zobowiązanych do udostępniania danych zgodnie z prawem UE; art. 8-12); Rozdział IV (Nieuczciwe postanowienia umowne między przedsiębiorstwami dotyczące dostępu do danych i ich wykorzystywania; art. 13); Rozdział V (Udostępnianie danych organom sektora publicznego, Komisji, Europejskiemu Bankowi Centralnemu i organom UE na podstawie wyjątkowej potrzeby; art. 14-22); Rozdział VI (Zmiana dostawcy usług przetwarzania danych; art. 23-31); Rozdział VII (Bezprawny międzynarodowy dostęp administracji rządowej do danych nieosobowych i bezprawne międzynarodowe przekazywanie danych nieosobowych; art. 32); Rozdział VIII (Interoperacyjność; art. 33-36); Rozdział IX (Wdrażanie i egzekwowanie; art. 37-42); Rozdział X (Prawo *sui generis* przewidziane w dyrektywie

⁵²⁹ Art. 2 pkt 1) Data Act: „dane” oznaczają wszelkie cyfrowe odwzorowania działań, faktów lub informacji oraz wszelkie kompilacje takich działań, faktów lub informacji, w tym w formie zapisu dźwiękowego, wizualnego lub audiowizualnego”.

⁵³⁰ Uzasadnienie, Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych) COM/2022/68 final.

⁵³¹ Por. W. Kerber, *Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives*, „GRUR International”, Vol. 72, Iss. 2, <https://doi.org/10.1093/grurint/ikac107> (dostęp: 7.09.2024 r.).

⁵³² Uzasadnienie, Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych) COM/2022/68 final: „Dane są kluczowym elementem gospodarki cyfrowej oraz zasobem niezbędnym do zapewnienia dwójakiej transformacji – ekologicznej i cyfrowej”.

⁵³³ Por. T. Crepax, M. Gaur, B. da Rosa Lazarotto, *Measuring data access and re-use in the European Legal Framework for Data, from the General Data Protection Regulation (GDPR) law to the Proposed Data Act: the case of vehicle data*, „Open Research Europe” 2023, 3:192, <https://doi.org/10.12688/openreseurope.16468.1> (dostęp: 20.09.2024 r.), s. 6.

96/9/WE; art. 43); Rozdział XI (Przepisy końcowe; art. 44-50). Zakres przedmiotowy Data Act określony został w rozbudowanym art. 1, który zasadniczo odpowiada tytułom poszczególnych rozdziałów tego aktu wskazanych powyżej, normując w ustępie 2 jakich rodzajów danych dotyczy. Tak m.in. Rozdział II ma zastosowanie do danych, z wyjątkiem treści, dotyczących działania, wykorzystywania i środowiska produktów skomunikowanych i usług powiązanych, a Rozdział III – do wszelkich danych sektora prywatnego podlegających ustawowym obowiązkom w zakresie dzielenia się danymi. Zakres ten określony został szeroko, obejmując wszystkie sektory gospodarki. Z uwagi na złożony charakter Data Act i ograniczoną objętość tej rozprawy, charakterystyce poddanie zostanie przede wszystkim prawa i obowiązki ustanowione w rozdziale II (Dzielenie się danymi przez przedsiębiorców z konsumentami i z innymi przedsiębiorcami).

Podobnie jak DGA, Akt w sprawie Danych (Data Act) również wprowadza siatkę pojęciową dla ustalenia jego zakresu podmiotowego, która jest nieznana RODO, ale także odmienna od DGA. Sam zakres podmiotowy Data Act unormowano w art. 1 ust. 3 w sposób rozbudowany (wydzielono siedem liter) i szeroki. Akt w Sprawie Danych ma zastosowanie m.in. do producentów produktów skomunikowanych⁵³⁴ wprowadzanych do obrotu w UE i dostawców usług powiązanych⁵³⁵, niezależnie od siedziby (lit. a); znajdujących się w UE ich użytkowników (lit. b); posiadaczy danych udostępniających dane odbiorcom danych w UE, niezależnie od siedziby (lit. c); odbiorców danych w UE (lit. d). Oznacza to, że obowiązywaniem Data Act mogą objęte być, np. podmioty, które nie mają swojej siedziby na terytorium UE, lecz dostarczają usługi powiązane z produktami skomunikowanymi.

Dla ustalenia zakresu podmiotowego, praw i obowiązków poszczególnych podmiotów w Data Act kluczowe jest ustalenie znaczenia trzech terminów: „użytkownik”, „posiadacz danych” i „odbiorca danych”. Każdy z tych terminów zdefiniowany został w art. 2 Data Act. „Użytkownikiem” jest osoba fizyczna (także podmiot danych) lub prawna, która jest właścicielem produktu skomunikowanego lub której przekazane zostały tymczasowe prawa do korzystania z niego, lub która korzysta z usług powiązanych (art. 2 pkt 12 Data Act).

⁵³⁴ Art 2 pkt 5 Data Act: „produkt skomunikowany” oznacza rzecz, która pozyskuje, generuje lub zbiera dostępne dane dotyczące jej wykorzystywania lub jej otoczenia i która jest w stanie komunikować dane z produktu za pomocą usługi łączności elektronicznej, łączy fizycznego lub dostępu na urządzeniu i której podstawową funkcją nie jest przechowywanie, przetwarzanie ani przesyłanie danych w imieniu strony innej niż użytkownik”.

⁵³⁵ Art 2 pkt 6 Data Act: „usługa powiązana” oznacza usługę cyfrową, w tym oprogramowanie, ale z wyłączeniem usług łączności elektronicznej, która podczas zakupu, najmu, dzierżawy lub leasingu jest skomunikowana z produktem w taki sposób, że jej brak uniemożliwiłby produktowi skomunikowanemu wykonywanie co najmniej jednej z jego funkcji, lub która zostaje skomunikowana z produktem przez producenta lub osobę trzecią później, aby dodać, uaktualnić lub zmodyfikować funkcje produktu skomunikowanego”.

„Posiadacz danych” to podmiot, która ma prawo lub obowiązek (zgodnie z Data Act lub innym prawem UE lub krajowym) wykorzystywać i udostępniać dane (art. 2 pkt 13 Data Act). „Odbiorca danych” oznacza podmiot działający w celach związanych z własną działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, (niebędący jednocześnie użytkownikiem produktu lub usługi), któremu to podmiotowi posiadacz danych udostępnia je (art. 2 pkt 14 Data Act). Z zestawienia powyższych definicji wynika, że kategorie podmiotów są podobne do tych w DGA z nazw, ale odmienne materialnie⁵³⁶. Podmioty danych będą z zasady użytkownikami, przy czym nie każdy użytkownik będzie podmiotem danych. Przykładowo, jeżeli użytkownikiem (właścicielem) produktu skomunikowanego (urządzenia *Internet of Things* do monitoringu ryzyka zawału serca wszczepionego w organizm pacjenta) byłby podmiot leczniczy, to wobec pacjenta byłby on na podstawie RODO administratorem (lub współadministratorem), będąc użytkownikiem na podstawie Data Act (por. motyw 34 Data Act). Gdyby jednak pacjent samodzielnie zakupił urządzenie *Internet of Things*, które zewnętrznie monitorowałoby to ryzyko, to wówczas ten pacjent byłby jednocześnie użytkownikiem na podstawie Data Act i podmiotem danych na podstawie RODO⁵³⁷. Jak wskazane zostało w DGA, liczba nowych kategorii podmiotów, które ustanowione zostały na podstawie Data Act i DGA, powoduje niepewność co do kwalifikacji ich statusu na podstawie RODO, a w konsekwencji ich praw oraz obowiązków⁵³⁸.

Rozdział II reguluje dzielenie się danymi przez przedsiębiorców z innymi przedsiębiorcami, ustanawiając w art. 3 generalny obowiązek projektowania, produkowania i świadczenia produktów skomunikowanych i usług powiązanych tak, aby dane z nich były domyślnie możliwe do łatwego odczytu maszynowego, a o ile to technicznie możliwe, także bezpośrednio dostępne dla użytkownika (ust. 1), a nadto nakłada na te podmioty rozbudowane obowiązki informacyjne względem użytkowników (ust. 2-3), obejmujące m.in. informację o charakterze i częstotliwości zbierania danych z produktu (ust. 3 lit. a). Jeżeli użytkownik nie ma bezpośredniego dostępu do danych, ma prawo żądać nieodpłatnego udostępnienia tych danych (art. 4 ust. 1), przy nie może ich wykorzystywać do opracowania produktu lub usługi

⁵³⁶ Jest to odmienna definicja od definicji terminu „użytkownik danych” w DGA analizowanej powyżej. W DGA termin „użytkownik danych” odnosi się do podmiotu, który dopiero uzyskuje dostęp do danych.

⁵³⁷ Por. EROD i EIOD, Wspólna opinia EROD i EIOD 2/2022 na temat wniosku Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych), s. 14, pkt. 39, https://edpb.europa.eu/system/files/2023-03/edpb-edps_Jointopinion_2022-02_data_act_proposal_pl.pdf (dostęp: 15.09.2024 r.).

⁵³⁸ Por. też P. Hajduk, A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research (November 23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 – Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.), s. 8-10.

konkurencyjnej (art. 4 ust. 10), a prawo to podlega ograniczeniu w szczególnych przypadkach dotyczących przede wszystkim ochrony tajemnicy przedsiębiorstwa (art. 4 ust. 2-8). Użytkownik nie tylko ma prawo do uzyskania danych samodzielnie, ale może także upoważnić osobę trzecią (odbiorcę danych) do wystąpienia z wnioskiem do posiadacza danych (art. 5), której obowiązki określono w art. 6 Data Act. Wprowadzono dodatkowe instrumenty ochrony tajemnicy przedsiębiorstwa (art. 5 ust. 9-11). Powyższe obowiązki nie dotyczą z zasady mikroprzedsiębiorców i małych przedsiębiorstw (art. 7). Jeżeli udostępniane są dane osobowe, użytkownik lub osoba trzecia (odbiorca danych) wykazać musi podstawę przetwarzania zgodnie z art. 6 RODO i spełnienie warunków z art. 9 RODO (art. 4 ust. 12 i art. 5 ust. 7 Data Act). Oznacza to, że to posiadacz danych (por. motyw 30), rozpoznając wnioski o udostępnienie danych, będzie dokonywał oceny czy użytkownik lub osoba trzecia dysponuje odpowiednią podstawą przetwarzania z art. 6 RODO i spełnia warunki z art. 9 RODO, a w przypadku negatywnej oceny może odmówić wykonania wniosku⁵³⁹. Zasadniczo, tą podstawą będzie zgoda⁵⁴⁰ (art. 6 ust. 1 lit. a RODO). Błędne uznanie, że warunki zostały spełnione i udostępnienie danych osobowych stanowiło będzie naruszenie ochrony danych osobowych i będzie mogło stanowić podstawę odpowiedzialności posiadacza danych jako administratora na podstawie RODO (o ile, rzecz jasna, w danej sytuacji przysługiwał mu będzie taki status administratora).

Jako istotne zabezpieczenie dla przetwarzania danych osobowych i nieosobowych w Data Act (i DGA) ustanowiono anonimizację i pseudonimizację. Data Act i DGA wprowadza instrumenty umożliwiające i mające na celu zachęcić do przetwarzania danych w zbiorach danych, które zawierają nierozzerwalnie ze sobą związane dane osobowe i nieosobowe (por. motyw 34 Data Act). Wprowadzenie technik anonimizacji wpływa nie tylko na wyższy poziom bezpieczeństwa przetwarzania danych, ale także na zakres obowiązywania RODO w odniesieniu do tego przetwarzania. Dane zanonimizowane (będąc danymi nieosobowymi) nie podlegają bowiem RODO (por. podrozdział 2.3. powyżej)⁵⁴¹. Przykładowo, w Data Act określeń „anonimizacja” lub „anonimizować” użyto 7 razy, np. w motywie

⁵³⁹ P. Hajduk, A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research (November 23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 - Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.), s. 6-7.

⁵⁴⁰ Por A. T. I. K. Can, Horizontal intervention, sectoral challenges: Evaluating the data act's impact on agricultural data access puzzle in the emerging digital agriculture sector, CLSR 2023, Vol. 51, s. 21. Wskazać dodatkowo należy, Data Act nie tworzy odrębnej podstawy dla użytkownika niebędącego podmiotem danych do przetwarzania danych (por. motyw 7 Data Act in fine).

⁵⁴¹ Dane osobowe pseudonimizowane podlegają RODO.

7 („posiadacz danych może stosować się do wniosków m.in. przez zastosowanie anonimizacji danych osobowych”), a także w odniesieniu do udostępnienie danych organowi sektora publicznego w przypadkach wyjątkowej potrzeby (art. 15 Data Act), jeżeli wymagane jest ujawnienie taki danych posiadacz danych „odpowiednio je anonimizuje”, a gdy wniosek wymaga danych osobowych – pseudonimizuje je (art. 18 ust. 4 Data Act). Terminu „pseudonimizacja” użyto w Data Act 5 razy, w tym w motywie 8 łącząc go z zasadą minimalizacji i obowiązkami *privacy by design* i oraz *privacy be default* ustanowionymi w RODO. Z kolei w DGA określeń „anonimizacja” użyto 9 razy, w tym w motywie 8 i 9 w odniesieniu do tego, że RODO nie ma zastosowania do informacji anonimowych, czyli „informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować”, oraz w art. 12 lit. e DGA określającym dodatkowe usługi ułatwiające wymianę danych w toku świadczenia usług pośrednictwa danych.

Data Act (i DGA) zdaje się traktować anonimizację jako skuteczną technikę oddzielającą takie przetwarzanie, które nie podlega RODO od przetwarzania, które RODO podlega. Tymczasem wyznaczenie granicy między danymi osobowymi a danymi nieosobowymi (granicy zakresu przedmiotowego RODO) jest trudne i obarczone ryzykiem deanonimizacji (ponownej identyfikacji podmiotów danych, której to ryzyka prawodawca unijny jednak dostrzega, np. w motywie 8 DGA). Chociaż prawidłowa anonimizacja prowadzi do uczynienia informacji danymi nie-osobowymi i wyłączenia zakresu obowiązywania RODO, to – jak scharakteryzowano w podrozdziale 2.3. powyżej – przeprowadzenie skutecznej anonimizacji jest uważane za trudne, a wobec trwających przemian technicznych może okazać się zupełnie nieskuteczne. Stąd też wybór i wdrożenie odpowiednich technik anonimizacji jest objęte zakresem przedmiotowym nie tylko Data Act i DGA, ale także RODO i Rozporządzenia Dane Nieosobowe. Kwestia ta stanowiła będzie przedmiot zainteresowania wszystkich organów administracji publicznej ustanowionych na podstawie tych aktów prawnych na poziomie krajowym i unijnym. W aktach ustanawiających europejskie wspólnoty danych prawodawca unijny łączy z deanonimizacją dodatkowe obowiązki, np. w przypadku ponownego wykorzystania danych będących w posiadaniu sektora publicznego zgodnie z Rozdziałem II DGA, deanonimizacja podmiotów danych prowadzi do dodatkowego obowiązku notyfikacyjnego nałożonego na użytkownika takich danych do poinformowania odpowiedniego podmiotu sektora publicznego o przypadku deanonimizacji (art. 5 ust. 5 DGA i motyw 15 DGA). Oparcie modelu ponownego wykorzystania danych sektora publicznego,

pośrednictwa danych i dostępu do danych *Internet of Things* (czego konsekwencją może być utworzenie bardzo obszernych zbiorów danych nie-osobowych, które stały się nimi na skutek anonimizacji) powoduje zwiększenia skali ryzyka deanonimizacji danych nie-osobowych w przypadku znacznej ilości zgromadzonych danych w tych zbiorach.

W odniesieniu do relacji Data Act względem RODO, w Data Act dostrzeżono ryzyko krzyżowania się zakresów przedmiotowych (por. motyw 7 Data Act), wprowadzając zastrzeżenie o pozostawianiu Data Act „bez uszczerbku” dla aktów prawnych dotyczących „ochrony danych osobowych, prywatności i poufności komunikacji oraz integralności urządzeń końcowych”, wskazując przykładowo na RODO, w tym w odniesieniu do kompetencji organów ochrony danych osobowych (art. 1 ust. 5 Data Act). Dodatkowo, unormowano, że w przypadku kolizji między Data Act a wskazanymi wyżej aktami prawnymi, „pierwszeństwo” będą miały te akty prawne. Nadto, organy ochrony danych osobowych ustanowione zostały jako „odpowiedzialne za monitorowanie stosowania [Data Act] w zakresie ochrony danych osobowych”, co zostanie scharakteryzowane w podrozdziale 3.5.7. dotyczącym organów właściwych w Akcie w sprawie Danych.

2.7. PODSUMOWANIE

W rozdziale 2. wykazano, że zakres przedmiotowy i podmiotowy RODO jest szeroki i nieostry. Wynika to z brzmienia samego RODO, przede wszystkim szerokiego i nieostrego zakresu znaczeniowego terminu „dane osobowe”, poprzedzającej ją Dyrektywy ODO oraz orzecznictwa powoduje, że nie można jednoznacznie z góry ustalić, do jakich stosunków i do jakich podmiotów RODO ma zastosowanie. Konsekwencją powyższego jest to, że zachodzi krzyżowanie zakresów przedmiotowych RODO i wybranych aktów prawnych w obszarze przetwarzania danych osobowych (regulujących przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu; cyberbezpieczeństwo; prawa konkurencji, w tym DMA i DSA; regulujących sztuczną inteligencję, w tym AI Act; oraz regulujących europejskie przestrzenie danych), których wybór jako obszaru referencyjnego został także uzasadniony. W tym rozdziale scharakteryzowano przykłady tego krzyżowania się. Jak wynika z tej charakterystyki, dotyczą one m.in.: 1) niejasnej relacji podstaw prawnych do przetwarzania danych określonych w tych aktach z podstawami przetwarzania z art. 6 ust. 1 RODO i warunkami przetwarzania z art. 9 ust. 2 RODO; 2) niejasnej relacji między kategoriami podmiotów w RODO („administrator”, „współadministrator”, „podmiot przetwarzający”) względem nowych kategorii podmiotów (jak „posiadacz danych”, „użytkownik danych”, „dostawca usług

pośrednictwa danych” i „uznana organizacja altruizmu danych”); 3) zabezpieczeń przetwarzania danych, zwłaszcza anonimizacji, której wdrożenie wpływa na ustalenie, czy przetwarzanie podlega RODO czy też nie.

Krzyżowanie się tych zakresów przedmiotowych powoduje, że podmioty nadzorowane (w zakresie podmiotowym obowiązywania tych aktów) podlegają obowiązkom ze wszystkich tych aktów prawnych łącznie. Jak zostało wskazane wyżej, skoro zatem zakres obowiązków podmiotów nadzorowanych jest nieostry, a „monitorowanie i egzekwowanie” prawidłowego ich wykonywania jest kompetencją ogólną organów administracji publicznych ustanowionych na podstawie tych aktów, to oznacza, że zakres kompetencji organów wyznaczony jest przez nieostry zakres przedmiotowy tych aktów. Jeżeli zatem ustalono, że zachodzi krzyżowanie się zakresów przedmiotowych tych aktów, to oznacza także, że zachodzi krzyżowanie się kompetencji tych organów. Stąd też, aby zweryfikować główną hipotezę badawczą, w kolejnym rozdziale trzecim analizie poddane zostaną kompetencje wybranych organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych (w ustalonym w tym rozdziale obszarze referencyjnym).

3. ROZDZIAŁ 3 – KOMPETENCJE WYBRANYCH ORGANÓW ADMINISTRACJI PUBLICZNEJ STOSUJĄCYCH AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

3.1. WSTĘP

Przedmiotem tego rozdziału jest analiza kompetencji wybranych organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych, które wybrane zostały jako obszar referencyjny. W obszarze referencyjnym (zgodnie z podrozdziałem 2.5. rozprawy) zidentyfikowane zostały następujące organy administracji publicznej na poziomie unijnym stosujące akty prawne w obszarze przetwarzania danych osobowych, których kompetencje zostały zbadane: Europejska Rada Ochrony Danych, Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Komisja Europejska jako organ unijnego prawa konkurencji, Grupa Wysokiego Szczebla, Europejska Rada ds. Usług Cyfrowych, Europejska Rada ds. Innowacji w zakresie Danych i Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji. Z kolei na poziomie krajowym zidentyfikowane następujące organy: Prezes Urzędu Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej, organy właściwe do spraw cyberbezpieczeństwa, Prezes Urzędu Ochrony Konkurencji i Konsumenta jako organ krajowego prawa konkurencji, organy właściwe w Akcie o usługach cyfrowych, organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych, organy właściwe w Akcie w sprawie danych i organy właściwe w Akcie w sprawie Sztucznej Inteligencji.

Ponadto, w rozdziale analizie poddano czy możliwe jest wyróżnienie cech wspólnych dla tych organów administracji publicznej, co pozwoliło dokonać umiejscowienia tych organów w strukturze administracji unijnej i krajowej. Nadto, dokonano wyróżnienia typów kompetencji tych organów, co z kolei umożliwia porównanie tych typów pomiędzy poszczególnymi organami, zwłaszcza w odniesieniu do skutków wobec podmiotów nadzorowanych. W odniesieniu do typów kompetencji weryfikacji podlega hipoteza, że zasadne jest wyróżnienie następujących typów kompetencji: proceduralne w toku prowadzonych postępowań w celu wyjaśnienia sprawy lub wobec podmiotów nadzorowanych, naprawcze, współpracy i doradcze, informacyjne oraz edukacyjne. Kierując się potrzebą ograniczenia objętości tej rozprawy i mając na względzie zmieniający się kształt projektów aktów prawnych, podjęto decyzję, aby z zakresu niniejszej pracy wyłączyć analizę konkretnych rozwiązań w zakresie krajowych (polskich) organów administracji publicznej, które zostały albo zostaną

ustanowione na skutek operacjonalizacji w krajowym porządku prawnym następujących aktów prawnych: Aktu o usługach cyfrowych, Aktu w sprawie danych, Aktu w sprawie zarządzania danymi i Aktu w sprawie Sztucznej Inteligencji. W odniesieniu do tych aktów dokonano analizy ich przepisów w zakresie, w jakim nakładają na prawodawcę krajowego obowiązek ustanowienia określonych organów.

3.2. CECHY WSPÓLNE ORGANÓW ADMINISTRACJI PUBLICZNEJ STOSUJĄCYCH AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

W tym rozdziale analizie poddano łącznie 16 organów – 7 organów na poziomie unijnym i 9 organów na poziomie krajowym. Poza sytuacją, w której to Komisja jest organem unijnym ustanowionym na podstawie aktów prawnych regulujących unijne prawo konkurencji, Akt w sprawie Usług Cyfrowych i Aktu w sprawie Rynków Cyfrowych, wszystkie inne struktury organów ustanowione zostały w taki sposób, że w zasadniczej części stosowanie tych aktów przekazano organom krajowym, podczas gdy organy na poziomie unijnym wyposażone zostały w kompetencje doradcze, informacyjne i edukacyjne, aby umożliwić współpracę i zapewnić spójności stosowania tych aktów w całej UE. Te organy unijne w niektórych przypadkach wyposażone zostały we władcze kompetencje w procedurach kompozytowych (np. mechanizm spójności w sekcji 2 rozdziału VII RODO), których celem jest także zapewnienie spójności. Taka struktura organów w obszarze przetwarzania danych osobowych, którego unormowanie należy zaliczyć do europejskiego prawa administracyjnego⁵⁴², nie jest zjawiskiem nowym, ani ograniczonym tylko do tego obszaru. Stanowi typową strukturę, jaką wybiera prawodawca unijny w regulacjach sektorowych (np. bankowości i energetyce)⁵⁴³, przy uwzględnieniu ograniczeń prawa unijnego. W tym podrozdziale zbadane zostaną cechy wspólne organów administracji unijnej (Europejska Rada Ochrony Danych, Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Grupa Wysokiego Szczebla, Europejska Rada ds. Usług Cyfrowych,

⁵⁴² Proces europeizacji prawa administracyjnego scharakteryzowany został szczegółowo w podrozdziale 5.6. rozprawy.

⁵⁴³ Przykładowo, sektor bankowy (Komisja Nadzoru Finansowego i Europejski Urząd Nadzoru Bankowego na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylecia decyzji Komisji 2009/78/WE), czy sektor energetyczny (Prezes Urzędu Regulacji Energetyki i Agencja ds. Współpracy Organów Regulacji Energetyki na podstawie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/942 z dnia 5 czerwca 2019 r. ustanawiające Agencję Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki (przekształcenie) (Tekst mający znaczenie dla EOG.) PE/83/2018/REV/1 OJ L 158, 14.6.2019, p. 22–53)

Europejska Rada ds. Innowacji w zakresie Danych i Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji; z wyłączeniem Komisja Europejska jako rodzajowo odrębnej) i organów administracji krajowej ustanowionych do stosowania analizowanych aktów prawnych prawa UE jako elementu dwupoziomowych struktur organów stosujących unijne prawo administracyjne w kontekście europeizacji prawa administracyjnego⁵⁴⁴.

Abstrahując od dyskusji o pojęciu europejskiego prawa administracyjnego, należy wskazać, że jego stosowanie jest złożonym, wielopoziomowym (co najmniej dualistycznym, unijnym i krajowym) procesem charakteryzującym się mnogością zdecentralizowanych i niepodporządkowanych struktur oraz procedur (określanym jako „zarządzaniem administracyjnym w UE”), co czyni je przedmiotem szczególnie trudnym do analizy⁵⁴⁵. To skomplikowanie jest konsekwencją natury samego prawa unijnego, która z kolei wynika z ustroju UE opartego o zasadę kompetencji powierzonych (art. 2-6 TFUE)⁵⁴⁶, proporcjonalności i pomocniczości (art. 5 TEU)⁵⁴⁷. Z perspektywy traktatowej to zasadniczo na państwach członkowskich spoczywa obowiązek stosowania administracyjnego prawa unijnego, przy czym państwa te mogą wybrać instytucje i procedury (zasada autonomii instytucjonalnej i proceduralnej), będąc ograniczonymi koniecznością zapewnienia efektywności i ekwiwalentności⁵⁴⁸ (art. 291 ust. 1 TFEU i art. 298 TFUE). Należy przez to rozumieć, że w przypadku nieustanowienia rozwiązań instytucjonalnych i proceduralnych w prawie unijnym, to na państwach członkowskich ciąży ustanowienie organów oraz procedur, które zapewnią skuteczne wykonywanie tego prawa⁵⁴⁹. W ostatnich latach obserwowana jest tendencja przełamująca ten model, którą można scharakteryzować jako dążenie do centralizacji stosowania prawa unijnego⁵⁵⁰. W pewnym uproszczeniu, w takim właśnie kontekście

⁵⁴⁴ Proces europeizacji prawa administracyjnego zbadany został w podrozdziale 5.4. rozprawy.

⁵⁴⁵ M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et al. [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 556-558.

⁵⁴⁶ Zobacz więcej: P. Saganek [w:] *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1 (art. 1-89), red. D. Miąsik, N. Półtorak, A. Wróbel, Warszawa 2012, art. 2, SIP LEX.

⁵⁴⁷ Zobacz więcej: R. Grzeszczak [w:] *Traktat o Unii Europejskiej. Komentarz*, red. D. Kornobis-Romanowska, Warszawa 2023, art. 5, SIP LEX.

⁵⁴⁸ *Law of Administrative Procedure of the European Union: European Added Value Assessment (+ Annexes I-III)*, (2012), s. II-49, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/dv/eav_lawofadminprocedure_/EAV_LawofAdminprocedure_EN.pdf (dostęp: 15.09.2024 r.).

⁵⁴⁹ D.U. Galetta, *Procedural autonomy of EU Member States: paradise lost?: a study on the „functionalized procedural competence” of EU Member States*, Cham 2010., s. 7-9.

⁵⁵⁰ M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et al. [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 569.

prawnym⁵⁵¹, prawodawca unijny przyjmuje akty prawne w obszarze przetwarzania danych osobowych, które stanowią obszar referencyjny badań w tej rozprawie.

Organy administracji na poziomie UE wymienione wyżej zaklasyfikować można jako tak zwane unijne agencje, które odróżnić należy od instytucji UE⁵⁵². Te agencje to niejednorodne podmioty administrujące UE, których status prawny i podstawy do ustanowienia budzą w literaturze dyskusje⁵⁵³. Celem ich ustanowienia jest wspólne wykonywanie tak zwanej administracji dzielonej (*shared administration*) przez stworzenie struktur umożliwiających koordynację i współpracę oraz w niektórych przypadkach, także wspólne podejmowanie decyzji⁵⁵⁴. Do realizacji tych celów dobrane zostały formy działania – instrumenty współpracy i spójności, wydawanie aktów prawa miękkiego oraz udział w procedurach kompozytowych. Z uwagi na charakter kompetencji agencji, w literaturze wyróżniane są następujące typy agencji: 1) ustanowione w celu wymiany informacji; 2) opracowujące i koordynujące sieci podmiotów w określonym sektorze; 3) przygotowujące ekspertyzy na potrzeby podejmowania decyzji; 4) wyposażone w kompetencje o charakterze decyzyjnym⁵⁵⁵.

W wielopoziomowym modelu zarządzania administracyjnego w UE zasadniczą rolę wciąż odgrywają organy krajowe, które, stanowiąc element struktury administracji państw członkowskich, stosują prawo unijne i przestrzegają jego zasad, w tym KPP jako prawa pierwotnego UE⁵⁵⁶. Te organy charakteryzuje niejednorodność⁵⁵⁷, spowodowana przede wszystkim odmiennymi wyborami prawodawców krajowych w procesie operacjonalizacji prawa unijnego, przy czym jednocześnie prawodawca unijny ustanawia zwykle w unijnym prawie wtórnym instrumenty współpracy horyzontalnej (z organami innych państw członkowskich dla spraw transgranicznych i dla zachowania spójności, w tym przez sieci

⁵⁵¹ Por. też H. C. H. Hofmann, *Mapping the European administrative space*, „West European Politics” 2008, Vol. 31, Iss. 4, <https://doi.org/10.1080/01402380801905918> (dostęp: 20.09.2024 r.), s. 662-676.

⁵⁵² L. Jančiūtė, European data protection board: nascent EU agency or an 'intergovernmental club'?, *Int. Data Priv. Law* 2020, 10(1), s. 57.

⁵⁵³ Por. E. Maciariello, *EU Agencies and the Issue of Delegation: Conferral, Implied Powers and the State of Exception*, „European Papers-A Journal on Law and Integration” 2019, Vol. 4, No. 3, s. 723-751.

⁵⁵⁴ M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et al. [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 568-569.

⁵⁵⁵ M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et al. [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 574-575.

⁵⁵⁶ M. Szpyrka, Znaczenie niezależności Prezesa UKE dla realizacji unijnych praw podstawowych na przykładzie postępowania karowego prowadzonego na podstawie prawa telekomunikacyjnego, *iKAR* 2023, t. 12, nr 4., s. 64-65.

⁵⁵⁷ Por. K. Yesilkagit, J. Jordana, *Entangled agencies and embedded preferences: National Regulatory Agencies in multi-level European governance*, *J. Eur. Public Policy* 2022, Vol. 29, No. 10, <https://doi.org/10.1080/13501763.2022.2103170> (dostęp: 20.09.2024 r.), s. 1679-1680.

organów⁵⁵⁸) i wertykalnej (najczęściej z unijnym agencjami regulacyjnymi), które obejmują przede wszystkim nie-władcze, ale także coraz częściej władcze formy działania, np. współdecydowanie⁵⁵⁹. Analizowane organy krajowe zaliczyć należy właśnie do takiego typu organów. Wobec multicentryczności struktury europejskiego prawa administracyjnego i ciągłej ewolucji tej struktury, stanowiącej refleks procesów wykraczających poza prawo administracyjne⁵⁶⁰, nieuniknionym jest, że kompetencje ustanowionych w takiej strukturze organów zarówno na poziomie unijnym, jak i krajowym oraz relacje między nimi pozostają i pozostawać będą zagmatwane.

3.3. TYPOLOGIA KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ STOSUJĄCYCH AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Jak zostało wskazane, w tym rozdziale analizie poddano 16 organów. Część organów ustanowiona została na poziomie unijnym, a część na poziomie krajowym. Chociaż organy te różnią się od siebie, mają pewne cechy wspólne. Podobnie jest z ich kompetencjami. Aby ułatwić porównanie tych kompetencji i je uporządkować, zasadne jest zaproponowanie ich typologii. Nim jednak przedstawiona zostanie propozycja typologii, konieczne jest poczynienie podstawowych uwag metodologicznych. Typologia to procedura podziału określonych przedmiotów na rodzaje na podstawie wspólnej cechy lub ich zestawu, które tworzą typ⁵⁶¹. Polega to na zorganizowaniu tych przedmiotów w grupy w oparciu o stopień wzajemnego podobieństwa, który badacz ustala arbitralnie⁵⁶². Typologię jako procedurę bardziej elastyczną należy odróżnić od klasyfikacji, która winna być wyczerpująca i rozłączna⁵⁶³.

⁵⁵⁸ Por. D. S. Martinsen, E. Mastenbroek, R. Schrama, The power of 'weak' institutions: assessing the EU's emerging institutional architecture for improving the implementation and enforcement of joint policies, J. Eur. Public Policy 2022, Vol. 29, No. 10, <https://doi.org/10.1080/13501763.2022.2125046> (dostęp: 20.09.2024 r.), s. 1530-1531.

⁵⁵⁹ Por. T. A. Börzel, K. Heard-Lauréote, Networks in EU multi-level governance: concepts and contributions, „Journal of Public Policy” 2009, No. 29(2), s. 135-151; H. C. H. Hofmann, Multi-Jurisdictional Composite Procedures - The Backbone to the EU's Single Regulatory Space, „University of Luxembourg. Law Working Paper” 2019 No. 003-2019, <https://ssrn.com/abstract=3399042> (dostęp: 20.09.2024 r.).

⁵⁶⁰ Por. P. L. Lindseth, *What's in a Label? The EU as 'Administrative' and 'Constitutional'* [in:] *Comparative Administrative Law*, ed. by S. Rose-Ackerman, P. L. Lindseth, B. Emerson, Cheltenham 2017, s. 680-698.

⁵⁶¹ M. Prokop, Typologia reżimów hybrydalnych. Ujęcie teoretyczno-metodologiczne, „Historia i Polityka” 2017, t. 28, nr 21, s. 30.

⁵⁶² T. Rzepiński, *Konstruowanie typologii i klasyfikacji wielowymiarowych dla potrzeb*, „Zagadnienia Naukoznawstwa” 2016, t. 2, nr 208, s. 207.

⁵⁶³ M. Prokop, Typologia reżimów hybrydalnych. Ujęcie teoretyczno-metodologiczne, „Historia i Polityka” 2017, t. 28, nr 21, s. 29.

W literaturze dotyczącej przetwarzania danych osobowych zaproponowano dwie typologie kompetencji organów; w pierwszym przypadku w odniesieniu do organów nadzorczych ustanowionych na podstawie RODO (P. Litwiński⁵⁶⁴), a w drugim w odniesieniu do EROD (A. Grzelak⁵⁶⁵). Pierwszą z nich zaproponował P. Litwiński w odniesieniu do uprawnień organów nadzorczych ustanowionych na podstawie RODO, stosując podział zaproponowany przez samego prawodawcę unijnego w art. 58 RODO, to jest: „1) uprawnienia, z których organ nadzorczy może korzystać w trakcie prowadzonego postępowania; 2) katalog nakazów organu nadzorczego wydawanych w wyniku przeprowadzonego postępowania; 3) katalog uprawnień związanych z wydawaniem zezwoleń; 4) katalog uprawnień doradczych”. Jest to propozycja wartościowa poznawczo, ponieważ jest wyczerpująca i zasadniczo rozłączna. Na potrzeby tej rozprawy musi zostać jednak uzupełniona o konieczność objęcia typologią także kompetencji organów unijnych, z uwzględnieniem znaczenia kompetencji współpracy dla zjawiska krzyżowania się kompetencji tych organów.

Odminną typologię, w odniesieniu do samych uprawnień EROD, zaproponowała A. Grzelak, wskazując na pięć typów: „1) uprawnienia wykonywane w ramach mechanizmu spójności; 2) uprawnienia doradcze i opiniodawcze; 3) uprawnienia do wydawania wytycznych, zaleceń i określania najlepszej praktyki; 4) uprawnienia w zakresie procedury certyfikacji; 5) uprawnienia edukacyjno-informacyjne”⁵⁶⁶. Wydaje się, że zarówno uprawnienia doradcze i opiniodawcze (2), jak i do wydawania wytycznych, zaleceń i określania najlepszej praktyki (3), oraz (5) uprawnienia edukacyjno-informacyjne zaliczyć można do jednego typu kompetencji doradczych, informacyjnych i edukacyjnych, ponieważ są to kompetencje, które nie wywołują bezpośrednich skutków prawnych. W odniesieniu do mechanizmu spójności (1) należy wskazać natomiast, że w istocie rzeczy stanowi on po prostu specyficzny instrument współpracy między organami w toku procedury kompozytowej.

Chociaż te typologie zaproponowano w odniesieniu do konkretnych organów, można uznać je za mogące znaleźć zastosowanie także dla innych organów, co umożliwia zaproponowanie typologii w niniejszej rozprawie zasadniczo na ich podstawie, po dokonaniu

⁵⁶⁴ Artykuł 58 RODO, red. P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, SIP Legalis, nb 1.

⁵⁶⁵ A. Grzelak, *Charakter prawny zaleceń i wytycznych Europejskiej Rady Ochrony Danych* [w:] *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych – Aktualne problemy ochrony danych osobowych*, dodatek MoP 2021, nr 23.

⁵⁶⁶ A. Grzelak, *Charakter prawny zaleceń i wytycznych Europejskiej Rady Ochrony Danych* [w:] *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych – Aktualne problemy ochrony danych osobowych*, dodatek MoP 2021, nr 23, s. 5.

modyfikacji uwzględniających to, że ma ona obejmować zarówno kompetencje organów na poziomie krajowym, jak i unijnym.

Kryterium podziału, które należy uznać za porządkujące w dostatecznym stopniu, to charakter kompetencji organów. Należy mieć na względzie, że analizowane organy, chociaż podobne, pozostają różne, przede wszystkim część z nich ustanowiona została na poziomie unijnym, a część na poziomie krajowym, co powoduje, że mają one inne cele i zostały wyposażone w odmienne kompetencje do ich osiągnięcia. W konsekwencji, wydzielenie ich wspólnych cech może prowadzić do sytuacji, w których poszczególne kompetencje zaliczyć będzie można do więcej niż jednego typu, np. kompetencje EROD w mechanizmie spójności można zaliczyć jednocześnie do kompetencji współpracy (ponieważ jest to obligatoryjny element procedury wydania decyzji *one-stop shop*, w której bierze udział więcej niż jeden organ) i kompetencji naprawczych (ponieważ przedmiotem tej decyzji może być nałożenie sankcji, w tym administracyjnej kary pieniężnej). Z tego powodu, poniższa typologia nie rości sobie miana kompletnej. Jej celem jest bowiem, jak zostało wskazane, możliwe uporządkowanie tych kompetencji w celu porównania. Mając to na względzie, zasadne jest wyróżnienie następujących typów kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych:

- (a) proceduralne w toku prowadzonych postępowań w celu wyjaśnienia sprawy lub wobec podmiotów nadzorowanych – obejmują w szczególności kompetencje do wszczęcia i prowadzenia postępowań, prowadzenia czynności kontrolnych, żądania uzyskania informacji i dokumentów;
- (b) naprawcze, w tym do nakładania administracyjnych kar pieniężnych – obejmują kompetencje do nakładania sankcji wobec podmiotów nadzorowanych, w szczególności nakładania administracyjnych kar pieniężnych, udzielania upomnień i wydawania ostrzeżeń lub kompetencje w procedurze ich nakładania;
- (c) współpracy – obejmują kompetencje do fakultatywnego lub obligatoryjnego nawiązania współpracy z innymi organami administracji publicznej lub kompetencje, których celem jest osiągnięcie spójności w stosowaniu aktów prawnych lub wzmacnianie współpracy przez ustanowione do tego organy tak w ramach tych aktów, jak i strukturach równoległych, między tymi aktami (to istotne dla organów na poziomie unijnym);
- (d) do wydawania zezwoleń – obejmują kompetencje w procedurze wydawania zezwoleń rozumianych jako udzielenie przez organ administracji publicznej zgody na uchylenie

- przeszkody w legalnym podejmowaniu albo niepodejmowaniu określonego działania⁵⁶⁷, np. akredytowanie podmiotów certyfikujących na podstawie art. 43 RODO i zatwierdzanie wiążących reguł korporacyjnych na podstawie art. 47 RODO;
- (e) doradcze, informacyjne i edukacyjne, w tym do wydawania rekomendacji – obejmują kompetencje do podejmowania wszelkich działań organów administracji publicznej wyjaśniających akty prawne, w tym do wydawania rekomendacji, opinii, najlepszych praktyk, które nie mają jednak skutku prawnego, czy to abstrakcyjnego i generalnego, czy to indywidualnego i konkretnego⁵⁶⁸.

3.4. CHARAKTERYSTYKA WYBRANYCH ORGANÓW ADMINISTRACJI PUBLICZNEJ NA POZIOMIE UNIJNYM

W niniejszym podrozdziale charakterystyce poddano wybrane organy administracji publicznej na poziomie unijnym w obszarze referencyjnym. Są to: Europejska Rada Ochrony Danych, Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Komisja Europejska jako organ unijnego prawa konkurencji, Grupa Wysokiego Szczebla, Europejska Rada ds. Usług Cyfrowych, Europejska Rada ds. Innowacji w zakresie Danych i Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji. W odniesieniu do każdego z organów zbadano ich status prawny, strukturę i kompetencje, z uwzględnieniem kompetencji współpracy (i mechanizmów spójności).

3.4.1. EUROPEJSKA RADA OCHRONY DANYCH

EROD ustanowiony został na podstawie art. 68 ust. 1 RODO umieszczonego w rozdziale VII „Współpraca i spójność” jako niezależny organ wyposażony w osobowość prawną, który co do zasady „nie zwraca się do nikogo o instrukcje ani ich od nikogo nie przyjmuje” podczas wykonywania swoich kompetencji (art. 69 ust. 2 RODO). EROD scharakteryzowany zostanie w odniesieniu do RODO, z wyłączeniem przepisów Dyrektywy LED (artykuł 51).

⁵⁶⁷ *Prawo handlowe – część ogólna. System prawa handlowego*, t. 1: red S. Włodyka, Warszawa 2009, s. 504. Należy odróżnić takie rozumienie terminu „zezwoenie” na potrzeby tej typologii od pojęcia zezwolenia w publicznym prawie gospodarczym.

⁵⁶⁸ Artykuł 68 RODO, red. P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, SIP Legalis, Nb 4.

EROD jest kontynuatorem działalności prowadzonej przez Grupę Roboczą Art. 29 ustanowioną na podstawie Art. 29 Dyrektywy ODO. Zarówno status prawny jak i kompetencje EROD należy ocenić jako silniejsze w porównaniu do kompetencji Grupy (art. 30 Dyrektywy ODO), która nie miała ani osobowości prawnej, ani kompetencji podobnych do kompetencji EROD w mechanizmie spójności (sekcja 2. rozdziału VII RODO)⁵⁶⁹. Przyznanie EROD osobowości prawnej było zasadne, aby umożliwić wydawanie wiążących decyzji w ramach mechanizmu spójności, ponieważ daje to EROD możliwości występowania przez sądami unijnymi⁵⁷⁰.

W skład EROD wchodzi przewodniczący jednego organu nadzorczego każdego państwa członkowskiego i EIOD, a Komisja ma prawo do udziału w pracach, jednak bez głosu (art. 68 ust. 4 RODO). Członkowie EROD mogą być reprezentowani przez swoich przedstawicieli. Pracami EROD kieruje przewodniczący (art. 74 RODO) wybierany na pięcioletnią kadencję (art. 73 RODO), który reprezentuje EROD (art. 68 ust. 2 RODO). EROD działa na podstawie regulaminu wewnętrznego przyjętego większością dwóch trzecich głosów (art. 72 ust. 2 RODO)⁵⁷¹, przy czym decyzje EROD podejmowane są zasadniczo zwykłą większością głosów (art. 72 ust. 1 RODO). Ważną rolę w bieżącym funkcjonowaniu EROD odgrywa sekretariat, który udziela analitycznego, administracyjnego i logistycznego wsparcia (art. 75 ust. 1, 5 i 6 RODO). Obsługa sekretariatu dostarczana jest przez EIOD (art. 75 ust. 1 RODO), przy czym wprowadzone zostały instrumenty, aby uniezależnić organizacyjnie sekretariat EROD od EIOD (art. 75 ust. 2-4 RODO).

Przed przystąpieniem do dalszych rozważań, należy pokrótce przedstawić status prawny EIOD jako organu, który pełni istotną funkcję w działaniach EROD. EIOD ustanowiony jest na podstawie art. 52 EUDPR jako niezależny organ w celu zapewnienia przestrzegania podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucje i organy Unii. Stąd też EIOD jest odpowiedzialny za „za monitorowanie i zapewnienie stosowania przepisów każdego [...] aktu Unii odnoszącego się do podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucje i organy Unii oraz za doradzanie instytucjom i organom Unii

⁵⁶⁹ Por. *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 2.01.2024 r.).

⁵⁷⁰ Artykuł 68 RODO, red. P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, SIP Legalis, SIP Legalis, Nb 4.

⁵⁷¹ Regulamin wewnętrzny EROD przyjęty w dniu 25 maja 2018 r. (wersja 8; ostatnio zmieniony i przyjęty w dniu 6 kwietnia 2022 r.). https://edpb.europa.eu/system/files/2022-08/edpb_rules_of_procedure_version_8_adopted_20220406_pl.pdf (dostęp: 10.09.2024 r.).

i osobom, których dane dotyczą” w sprawach z tym związanych (art. 52 ust. 3 EUDPR). EIOD powoływany jest przez Parlament Europejski i Radę UE (art. 53 EUDPR), a jego kompetencje określone zostały zasadniczo w art. 57 (zadania, z uwzględnieniem „upowszechniania wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem”) i 58 (uprawnienia w zakresie prowadzonych postępowań, naprawcze, zatwierdzające i doradcze) EUDPR. Podzielić je można na cztery pola aktywności EIOD: 1) nadzór na instytucjami i organami Unii w odniesieniu do przetwarzania danych osobowych; 2) doradztwo Komisji, Parlamentowi Europejskiemu i Radzie UE w procesie prawodawczym i w innych kwestiach dotyczących tego obszaru; 3) monitorowanie zmian technicznych wpływających na przetwarzanie danych osobowych; 4) współpraca z krajowymi organami nadzorczymi⁵⁷².

Celem ustanowienia EROD jest wsparcie spójnego stosowania RODO (art. 70 ust. 1 RODO i motyw 139 RODO)⁵⁷³. Odzwierciedla to art. 2 Regulaminu Wewnętrznego EROD, który wskazuje, że misją EROD jest spójne stosowanie RODO⁵⁷⁴. W tym celu EROD wyposażony został w otwarty katalog dwudziestu pięciu kompetencji w art. 70 lit. od a) do y) RODO. Wymaga wskazania, że artykuł 70 RODO zatytułowany został „Zadania”, podczas gdy nie ma osobnego artykułu zatytułowanego „Uprawnienia”, który odnosiłby się do EROD, inaczej niż jest to w przypadku organów nadzorczych ustanowionych przez RODO (odpowiednio art. 57 i 58 RODO). Artykuł 70 RODO, pomimo swojego tytułu, zawiera nie tylko zadania, ale także uprawnienia. Dla ustalenia kompetencji EROD znaczenie ma także art. 35 ust. 4 i 5 RODO (Ocena skutków dla ochrony danych), art. 40 RODO (Kodeksy postępowania), art. 41 RODO (Monitorowanie zatwierdzonych kodeksów postępowania), art. 42 RODO (Certyfikacja), art. 43 RODO (Podmiot certyfikujący) i sekcje 1. i 2. rozdziału VII RODO o współpracy i spójności między krajowymi organami nadzorczymi, przy czym argumentować można, że nowatorski charakter ma mechanizm spójności, omawiany w art. 64-66 RODO. Wskazać należy, że na poziomie EROD podejmowane są inicjatywy nakierowane na koordynację stosowania RODO, np. w ramach inicjatywy „Coordinated Enforcement Framework” („Ramy skoordynowanego egzekwowania prawa”), która nakierowana jest na

⁵⁷² P. Fajgielski, Rola Europejskiego Inspektora Ochrony Danych w kształtowaniu i wykładni przepisów o ochronie danych osobowych [w:] Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych – Aktualne problemy ochrony danych osobowych, dodatek MoP 2021, nr 23, s. 12.

⁵⁷³ Por. także U. Góral, Europejska Rada Ochrony Danych – proces transformacji Grupy Roboczej Art. 29, MoP 2017, nr 20, Dodatek, s. 13.

⁵⁷⁴ Regulamin wewnętrzny EROD przyjęty w dniu 25 maja 2018 r. (wersja 8; ostatnio zmieniony i przyjęty w dniu 6 kwietnia 2022 r.). https://edpb.europa.eu/system/files/2022-08/edpb_rules_of_procedure_version_8_adopted_20220406_pl.pdf (dostęp: 15.09.2024 r.).

koordynację czynności podejmowanych przez poszczególne organy ochrony danych osobowych w państwach członkowskich⁵⁷⁵.

W zasadniczej części kompetencje EROD mają charakter doradczy, informacyjny i edukacyjny. EROD doradza Komisji we wszelkich „sprawach związanych z ochroną danych osobowych w Unii” („*any issue related to the protection of personal data in the Union*”; art. 70 ust. 1 lit. b RODO), zatem zakres doradztwa jest sformułowany szeroko (uszczegółowiony w art. 70 ust. 1. lit. c, q-s, x RODO), w tym obejmuje opinie na temat odpowiedniego stopnia ochrony na potrzeby decyzji Komisji na podstawie art. 45 RODO w przedmiocie przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych (lit. s). Ponadto, w odniesieniu do podobnie szerokiego zakresu kwestii („wszelkie kwestie dotyczące stosowania” RODO) EROD może wydawać wytyczne, zalecenia i najlepsze praktyki, zarówno z własnej inicjatywy, jak na wniosek jednego z członków lub Komisji (art. 70 ust. 1 lit. e RODO). Takie kwestie wskazane zostały w literach od f do m, obejmując zagadnienia materialne i proceduralne, m.in., profilowanie (lit. f), naruszenia ochrony danych osobowych (lit. g i h), wysokość kar administracyjnych (lit. k) oraz procedury w przypadkach naruszeń RODO zgłaszanych przez osoby fizyczne (lit. m). Kompetencje o charakterze informacyjnym i edukacyjnym skierowane do krajowych organów nadzorczych obejmują m.in. upowszechnianie współpracy, wymiany informacji i dobrych praktyk (lit. u). EROD podaje opinie, wytyczne, zalecenia i najlepsze praktyki do publicznej wiadomości (art. 70 ust. 3 RODO) oraz sporządza roczne sprawozdania (art. 71 ust. 1 RODO).

Nowością względem Dyrektywy ODO jest przyznanie EROD – obok kompetencji doradczych, informacyjnych i edukacyjnych – kompetencji w procedurze wydawania opinii i wiążących decyzji w ramach mechanizmu spójności (art. 63-66 RODO). Część tych kompetencji zaliczyć można do kompetencji do wydawania zezwoleń (art. 64 ust. 1 RODO), a część do kompetencji naprawczych (art. 65 RODO), w zakresie, w jakim mogą służyć do nakładania administracyjnych kar pieniężnych lub innych rozstrzygnięć o charakterze naprawczym, ale jednocześnie wszystkie te kompetencje zaliczyć należy do kompetencji współpracy, ponieważ mechanizm spójności całościowo służy ujednoliceniu stosowania RODO w UE. Istotą mechanizmu spójności jest, że to EROD zajmuje stanowisko w konkretnej sprawie przy współudziale określonych organów nadzorczych. Ten mechanizm jest

⁵⁷⁵ EROD, Dokument EROD w sprawie ram skoordynowanego egzekwowania prawa na mocy rozporządzenia 2016/679 (przyjęty 20 października 2020 r.), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_documents_20201020_coordinatedenforcementframework_pl.pdf (dostęp: 10.09.2024 r.).

komplementarny z mechanizmem współpracy między krajowymi organami nadzorczymi z sekcji 1. rozdziału VII RODO i tworzy tzw. procedurę *one-stop shop*⁵⁷⁶. Stanowi przykład procedury kompozytowej charakterystycznej dla procesu Europeizacji prawa administracyjnego w wymiarze proceduralnym⁵⁷⁷. Z osobna należy zbadać zarówno przesłanki i skutki mechanizmu spójności w odniesieniu do trybu z art. 64 ust. 1 i ust. 2 RODO, art. 65 RODO i art. 66 RODO⁵⁷⁸.

W trybie art. 64 ust. 1 RODO krajowy organ nadzorczy zobowiązany jest zgłosić do EROD projekt decyzji w celu wydania przez EROD opinii w jednym z sześciu przypadków: 1) przyjęcia wykazu operacji przetwarzania, które wymagają oceny skutków dla ochrony danych; 2) stwierdzenia, czy projekt kodeksu postępowania, jego zmiana lub rozszerzenie jego zakresu są zgodne z RODO; 3) zatwierdzenia kryteriów akredytacji podmiotu monitorującego przestrzeganie kodeksu postępowania lub podmiotu certyfikującego; 4) określenia standardowych klauzul ochrony danych; 5) zezwolenie na klauzule umowne, o których mowa w art. 46 ust. 3 RODO; 6) zatwierdzenia wiążących reguł korporacyjnych. Chociaż zastosowanie procedury z art. 64 ust. 1 RODO jest obligatoryjne i wywołuje określone skutki proceduralne, np. obowiązek wstrzymania się organu nadzorczego z wydaniem decyzji do czasu wydania opinii przez EROD (art. 64 ust. 6 RODO), to jednak opinia EROD nie jest wiążąca, chociaż organ jest zobowiązany uwzględnić ją w możliwie największym stopniu przy wydawaniu decyzji (art. 64 ust. 4 RODO)⁵⁷⁹. Niezastosowanie się do opinii EROD może spowodować uruchomienie postępowania w przedmiocie rozstrzygania sporów przez EROD z art. 65 ust. 1 lit. (c) RODO, który omówiony zostanie niżej.

Z kolei art. 64 ust. 2 RODO pozwala krajowym organom nadzorczym, przewodniczącemu EROD lub Komisji wystąpić do EROD o opinię w sprawie o „charakterze ogólnym lub wywołującej skutki w więcej niż jednym państwie członkowskim”. W literaturze słusznie wskazuje się, że ten przepis nie jest klarowny. Po pierwsze, niejasne jest samo pojęcie

⁵⁷⁶ K. Mojzesowicz, Refleksje po ponad trzech latach stosowania RODO [w:] Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych – Aktualne problemy ochrony danych osobowych, dodatek MoP 2021, nr 23, s. 17.

⁵⁷⁷ J. Supernat, Restatements – koncepcja i zastosowanie [w:] Administracja publiczna pod rządami prawa: księga pamiątkowa z okazji 70-lecia urodzin prof. zw. dra hab. Adama Błasia, red. J. Korczak, Wrocław 2016, s. 461. Proces Europeizacji prawa administracyjnego w kontekście analizowanego obszaru zbadany został w podrozdziale 5.6. niniejszej rozprawy.

⁵⁷⁸ *Consistency mechanism: opinions and binding decisions* [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 2.01.2024 r.).

⁵⁷⁹ Artykuł 64 RODO, red. P. Litwiński [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021, SIP Legalis, SIP Legalis, nb 12.

„sprawy mającej ogólny charakter”. Podnosi się, że chodzi o sprawy o takim charakterze, który mogą wpłynąć na przetwarzanie danych w innych państwach członkowskich, jednak nie wywołują bezpośrednich skutków⁵⁸⁰. Po drugie, nie jest wyjaśniony jaki skutek (w więcej niż jednym państwie członkowskim) musi wystąpić, aby sprawa mogła spełnić drugą z przesłanek z art. 64 ust. 2 RODO. Doktryna prawidłowo sugeruje, że nie chodzi o każdy skutek, ale o taki, który ma „realny wpływ” na podmiot danych⁵⁸¹. W ustępie tym *in fine* wskazano przykładowo, że chodzi o sytuacje, w których właściwy organ nadzorczy nie wypełnia obowiązków wzajemnej pomocy (art. 61 RODO) lub wspólnych operacji (art. 62 RODO), co może sugerować, że chodzi o sprawy, które pozostają sporne między organami nadzorczymi, dlatego w literaturze proponowane jest zawężające rozumienie tego przepisu wyłącznie do tego rodzaju spraw⁵⁸².

Artykuł 65 ust. 1 RODO „Rozstrzyganie sporów przez EROD” normuje trzy przypadki sporów między krajowymi organami nadzorczymi, w których EROD może wydać wiążące decyzje: 1) kiedy występuje istotny i uzasadniony sprzeciw organu nadzorczego, którego sprawa dotyczy zgłoszony w procedurze *one-stop shop*⁵⁸³; 2) w przypadku sporu, który z organów nadzorczych jest wiodącym organem; 3) kiedy organ nadzorczy naruszył art. 64 RODO (zgłoszenia może dokonać Komisja lub organ, którego sprawa dotyczy). Ustęp 2-4 art. 65 RODO określają kluczowe aspekty proceduralne, które podlegają uszczegółowieniu w Tytule III – „Przyjmowanie dokumentów i procedura” Regulaminu wewnętrznego EROD (Artykuł 11 – „Wiążąca decyzja Rady”). Wiążący charakter decyzji EROD powoduje, że odpowiedni organ nadzorczy podejmuje ostateczną decyzję na podstawie decyzji EROD, jednocześnie dokonując odesłania do niej w treści tej ostatecznej decyzji, w terminie miesiąca po notyfikacji przez EROD o swojej decyzji (art. 65 ust. 6 RODO). W konsekwencji, z uwagi na istnienie w obrocie prawnym odrębnej decyzji EROD, podmioty uprawnione, w tym administratorzy danych osobowych, na podstawie art. 263 TFUE mogą zaskarżyć decyzję

⁵⁸⁰ Artykuł 64 RODO, red. P. Litwiński [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021, SIP Legalis, SIP Legalis, nb 3.

⁵⁸¹ Artykuł 64 RODO, red. P. Litwiński [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021, SIP Legalis, SIP Legalis, nb 3.

⁵⁸² P. Van Eecke, A.Šimkus, *Article 64 Opinion of the Board* [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 2.01.2024 r).

⁵⁸³ Mechanizm one-stop shop scharakteryzowany został w podrozdziale 3.5.1. „Prezes Urzędu Ochrony Danych Osobowych”.

EROD do TSUE, niezależnie od środków ochrony prawnej przysługujących przed sądami krajowymi (motyw 143 RODO).

Artykuł 66 RODO wprowadza tryb pilny podejmowania decyzji, który zastosowanie znajduje w wyjątkowych okolicznościach. Pojęcie „wyjątkowych okoliczności” nie zostało zdefiniowane. W ust. 1 pojęcie to kwantyfikowane jest ogólnym określeniem „pilnej potrzeby podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą,” co oznacza, że należy dokonywać oceny *ad casum*. W przypadku wystąpienia tych okoliczności, krajowy organ nadzorczy może zastosować środki tymczasowe na terytorium swojego państwa członkowskiego na czas oznaczony do trzech miesięcy z pominięciem procedury współpracy lub mechanizmu spójności, przy czym zobowiązany jest poinformować o tym organy nadzorcze, których sprawa dotyczy, Komisję i EROD (art. 66 ust. 1 RODO). Z kolei w ust. 2 wprowadzono tryb przyjmowania środków ostatecznych w takich okolicznościach. Jeżeli jednak organ nadzorczy w tych okolicznościach nie skorzystał ze środków tymczasowych, może zwrócić się do EROD o wydanie opinii albo decyzji w przyspieszonym trybie określonym w art. 66 ust. 3 RODO. Tryb pilny, który ma zastosowanie zarówno do ust. 2 i 3, powoduje, że EROD dokonuje tych czynności zwykłą większością głosów w terminie dwóch tygodni, co stanowi znaczne skrócenie terminów (art. 66 ust. 4 RODO)⁵⁸⁴.

Z perspektywy ponad pięciu lat obowiązywania RODO, w literaturze toczy się dyskusja na temat skuteczności mechanizmu spójności i *one-stop shop*. Punktem odniesienia dla tej dyskusji może być fakt, że do stycznia 2024 r. w ramach *one-stop shop* organy nadzorcze wydały aż 425 decyzji, przy czym aż 301 decyzji w latach 2021-2023⁵⁸⁵, natomiast EROD wydał 11 wiążących decyzji w trybie art. 65 albo art. 66 RODO, przy czym aż 8 z nich wydanych zostało w 2022 i 2023 r.⁵⁸⁶ To zrozumiałe, zważywszy, że tego typu postępowania kompozytowe muszą zająć czas zanim sprawa trafi do organu unijnego. Część autorów (np. K. Mojzesowicz) stoi na stanowisku, że ten mechanizm i ta procedura odgrywają swoją rolę należycie, co dodatkowo wzmocnione jest orzecnictwem TSUE, które nie zakwestionowało

⁵⁸⁴ P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2022, art. 66, pkt 5.

⁵⁸⁵ EROD, *Final One Stop Shop Decisions*, https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en (dostęp: 15.09.2024 r.).

⁵⁸⁶ EROD, *Binding Decisions*, https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_en?page=0 (dostęp: 15.09.2024 r.).

tych rozwiązań (np. wyrok TSUE z 27.10.2022 r., C-129/21, Proximus NV)⁵⁸⁷. Z kolei inni przedstawiciele doktryny (np. F.B. Bastos i P. Pałka, G. Gentile i O. Lynskey⁵⁸⁸, M. Magierska) wskazują na wady, na przykład zbyt dużą rolę wiodących organów nadzorczych względem organów, których sprawa dotyczy, w odniesieniu do inicjowania działań nakierowanych na ochronę danych osobowych⁵⁸⁹, ryzyko *forum shopping*⁵⁹⁰, czy brak wpływu EROD na problemy natury proceduralnej, na przykład zbyt długo trwające postępowanie czy język, w jakim postępowanie jest prowadzone⁵⁹¹.

3.4.2. URZĄD DS. PRZECIWDZIAŁANIA PRANIU PIENIĘDZY I FINANSOWANIU TERRORYZMU

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu⁵⁹² przyjęto w 2024 r. Stanowi element szerszego pakietu zmian regulacji AML w UE⁵⁹³. Będzie miało zastosowanie od 1 lipca 2025 r. (art. 108). Rozporządzenie ustanawia nowy unijny organ, Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (art. 1 ust. 1) z siedzibą we Frankfurcie nad Menem, który wyposażony jest w osobowość i zdolność prawną (art. 3). Jego celem jest m.in. „ochrona stabilności i integralności systemu finansowego Unii” (art. 1 ust. 3) przez „przyczynianie się do identyfikacji i oceny ryzyka oraz zagrożeń związanych z” AML (art. 1 ust. 3 lit. b), a także zapewnienie harmonizacji stosowania unijnych unormowań AML w UE oraz współpraca między jednostkami analityki finansowej i organami nadzorczymi z innymi organami (art. 1 ust. 3 lit. d-f). Zgodnie z Rozdziałem III regulującym strukturę organizacyjną Urzędu, składał się on będzie z pięciu elementów: Rady Generalnej; Rady Wykonawczej; przewodniczącego Urzędu, dyrektora wykonawczego i Administracyjnej Rady

⁵⁸⁷ K. Mojzesowicz, Refleksje po ponad trzech latach stosowania RODO [w:] Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych – Aktualne problemy ochrony danych osobowych, dodatek MoP 2021, nr 23, s. 17-18.

⁵⁸⁸ Por. G. Gentile, O. Lynskey, *Deficient by Design? The Transnational Enforcement of the GDPR*, „International and Comparative Law Quarterly” 2022, No.71(4). Autorzy cytowani przez F.B. Bastos i P. Pałka.

⁵⁸⁹ F. Brito Bastos, P. Pałka, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?*, „European Constitutional Law Review” 2023.

⁵⁹⁰ F. Brito Bastos, P. Pałka, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?*, „European Constitutional Law Review” 2023.

⁵⁹¹ M. Magierska, *Three EDPB Binding Decisions in the Art. 65 GDPR Procedure and Two Major Questions for the Future*, EDPL 2023, Vol. 9, No. 1, s. 60.

⁵⁹² Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu i zmieniające rozporządzenia (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010 COM/2021/421 final. Wersja finalna: <https://data.consilium.europa.eu/doc/document/PE-35-2024-REV-1/pl/pdf#page=2.09> (31 maja 2024 r.).

⁵⁹³ Scharakteryzowano w końcowym fragmencie podrozdziału 2.6.1. rozprawy.

Odwoławczej (art. 56). Kluczowa decyzyjność spoczywa na Radzie Generalnej (art. 60), która może działać w dwóch składach: nadzorczym i właściwym dla jednostek analityki finansowej (art. 57). W skład pierwszego wchodzi: przewodniczący AMLA z prawem głosu, szefowie organów nadzorczych z każdego z państw członkowskich i przedstawiciel KE bez prawa głosu (art. 57 ust. 1), a skład drugiego różni się tym, że w miejsce szefów organów nadzorczych wchodzi szefowie jednostek analityki finansowej (art. 57 ust. 3). Działania Rady Generalnej winny być niezależne, w tym nie powinna ona ani się zwracać, ani przyjmować instrukcji od innych „instytucji, organów ani jednostek organizacyjnych Unii” (art. 59), stąd też do współpracy, np. z EIOD konieczne jest ustanowienie odrębnej podstawy prawnej (o czym niżej). Rozdział IV zawiera przepisy finansowe, w tym dotyczące budżetu AMLA (art. 75), a Rozdział V Sekcja 1 dotyczy personelu organu.

Rozdział II zatytułowany „Zadania i uprawnienia Urzędu” w sposób kompleksowy normuje zadania (art. 5) i kompetencje tego organu, mającego wraz z krajowymi organami stworzyć spójny i zintegrowany system nadzorczy, który w założeniu ma skuteczniej walczyć ze zjawiskiem prania brudnych pieniędzy i finansowania terroryzmu mającym często charakter transgraniczny.⁵⁹⁴ W tym podrozdziale scharakteryzowane zostaną wybrane zadania i kompetencje AMLA. Zadania AMLA podzielono na: 1) zadania w odniesieniu do ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, na jakie narażony jest rynek wewnętrzny (art. 5 ust. 1); 2)) w odniesieniu do wybranych podmiotów zobowiązanych (art. 5 ust. 2); 3)) w odniesieniu do podmiotów sprawujących nadzór finansowy (art. 5 ust. 3); 4)) w odniesieniu do podmiotów sprawujących nadzór niefinansowy (art. 5 ust. 4); w odniesieniu do jednostek analityki finansowej i ich działalności w państwach członkowskich (art. 5 ust. 5).

Zadania AMLA sformułowano zatem w sposób szeroki i, oprócz zadań typowych dla organów na poziomie unijnym nakierowanych na zapewnienie spójności stosowania prawa unijnego i wspierania współpracy transgranicznej, obejmują także zadania bezpośredniego nadzoru nad niektórymi podmiotami. AMLA wyposażona została we własne kompleksowe kompetencje proceduralne i naprawcze (art. 6), w tym do nakładania kar pieniężnych (art. 22-23), w ramach sprawowania bezpośredniego nadzoru nad wybranymi (niektórymi) podmiotami zobowiązanymi z sektora finansowego (Rozdział II Sekcja 3), które definiowane są jako „instytucje kredytowe, finansowe lub grupy instytucji kredytowych lub finansowych

⁵⁹⁴ Rada UE, *Przeciwdziałanie praniu pieniędzy: Rada przyjmuje pakiet przepisów* (30 maja 2024) <https://www.consilium.europa.eu/pl/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/pdf/> (dostęp: 15.09.2024 r.).

o najwyższym poziomie konsolidacji w Unii zgodnie z obowiązującymi standardami rachunkowości” (art. 2 ust. 1) i umieszczone zostały w wykazie wybranych podmiotów zobowiązanych (art. 13) po klasyfikacji ich profilu ryzyka szacunkowego jako wysokiego (zgodnie z art. 12). W istocie, ten bezpośredni nadzór obejmował będzie największe podmioty, które prowadzą rozbudowaną działalność transgraniczną („w co najmniej sześciu państwach członkowskich” zgodnie z art. 12 ust. 1). Stanowi to wyraz woli prawodawcy unijnego, aby dokonać częściowej centralizacji stosowania prawa unijnego, co kierowane jest potrzebą zwiększenia efektywności i spójności wobec wyzwań ze strony samego przedmiotu regulacji.⁵⁹⁵ Jest to charakterystyczne także dla innych aktów unijnych przyjętych po 2020 r. w obszarze cyfrowym, w tym DSA, DMA i Aktu w sprawie Sztucznej Inteligencji.

Ponadto, AMLA przyznano kompetencje w zakresie pośredniego nadzoru nad niewybranymi podmiotami zobowiązanymi (Rozdział II Sekcja 4), w tym przez koordynację i ułatwianie pracy kolegiów organów nadzoru ds. AML (art. 31) oraz rozbudowane kompetencje współpracy w zakresie wsparcia oraz koordynacji spójnej współpracy transgranicznej między organami nadzorczymi (np. zwłaszcza art. 7 i 10; Rozdział II Sekcja 2), w tym w ramach nadzoru zwierzchniego nad sektorem niefinansowym (Rozdział II Sekcja 5), oraz między jednostkami analityki finansowej (Rozdział II Sekcja 6). AMLA przyznano także kompetencje współpracy z wybranymi organami spoza obszaru AML (art. 92), co nie obejmuje jednak organów ochrony danych, ani EROD, ani EIOD), Europejskim Urzędem Nadzoru (art. 91) i OLAF-em, Europol, Eurojustem i Prokuraturą Europejską (art. 94).

AMLA przyznano rozbudowane kompetencje doradcze, informacyjne i edukacyjne, w tym w zakresie opracowywania projektów regulacyjnych standardów technicznych w określonych przypadkach (art. 49) i do wydawania wytycznych i zaleceń w celu „ustanowienia spójnych, wydajnych i skutecznych praktyk nadzorczych oraz praktyk dotyczących jednostek analityki finansowej oraz zapewnienia wspólnego, jednolitego i spójnego stosowania prawa” (art. 54).

Rozporządzenie ustanawiające AMLA odnosi się do RODO wprost jedynie 4 razy, jednak w rozporządzeniu zidentyfikowano potrzebę zachowania zgodności z RODO, w tym w art. 98 normującym ochronę danych osobowych, gdzie uregulowane podstawę prawną do przetwarzania danych osobowych na potrzeby AML na podstawie rozporządzenia, przede wszystkim przez samą AMLA. Natomiast w odniesieniu do współpracy między AMLA

⁵⁹⁵ G. Pavlidis, *The birth of the new anti-money laundering authority: harnessing the power of EU-wide supervision*, „Journal of Financial Crime” 2024, Vol. 31 No. 2, <https://doi.org/10.1108/JFC-03-2023-0059>. (dostęp: 20.09.2024 r.), s. 322-324.

i organami ochrony danych, EROD i EIOD (art. 98 ust. 2) przewiduje, że w przypadku wydawania wytycznych i zaleceń, które mają istotny wpływ na ochronę danych osobowych, AMLA winna nawiązać ścisłą współpracę z EROD, a także może nawiązać współpracę z EIOD (lecz, co pozostaje niejasne, po upoważnieniu przez KE), jak również krajowymi organami ochrony danych (w tym przypadku jako obserwatorów). Celem takiego rozwiązania jest, aby uniknąć „powielania zadań, niespójności i braku pewności prawa w dziedzinie ochrony danych”, co znaczy, że prawodawca unijny dostrzega krzyżowanie się zakresów przedmiotowych między aktami prawnymi regulującymi AML a RODO, jak i krzyżowania się kompetencji organów w tym obszarze, prawidłowo identyfikując ryzyko w postaci niespójności i niepewności wykładni prawa. Zważywszy jednak na szeroki zakres przetwarzania danych osobowych, w tym szczególnych kategorii danych osobowych, przy stosowaniu aktów normujących AML, dyskusyjne pozostaje, czy takie rozwiązanie jest wystarczające, aby wyczerpać postulat zgłoszony EIOD dotyczący precyzyjnego wyznaczenia zadań i kompetencji wszystkich organów w strukturze stosowania tych aktów prawnych względem przetwarzania danych osobowych⁵⁹⁶, zwłaszcza, że ani EROD, ani EIOD, ani organy ochrony danych nie są zasadniczo wyposażone w kompetencje w bezpośrednim i pośrednim nadzorze.

3.4.3. AGENCJA UNII EUROPEJSKIEJ DS. CYBERBEZPIECZEŃSTWA

Struktura podmiotów na poziomie unijnym, które wyposażone zostały w kompetencje w obszarze cyberbezpieczeństwa, jest rozbudowana. Na stronie internetowej ENISA w zakładce „Instytucjonalna mapa cyberbezpieczeństwa” wskazano ponad 20 podmiotów, które odgrywają rolę w unijnym cyberbezpieczeństwie⁵⁹⁷. Jest to konsekwencja kilku

⁵⁹⁶ EIOD, Opinia EIOD 12/2021 w sprawie pakietu legislacyjnego dotyczącego przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (AML/CFT) (22 września 2021), https://www.edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf#page=7.57 (dostęp: 15.09.2024 r.).

⁵⁹⁷ ENISA, *Cybersecurity Institutional Map*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=actors> (dostęp: 15.09.2024 r.). Te podmioty to: 1. CEPOL - European Union Agency for Law Enforcement Training; 2. CERT-EU; 3. Council, European Union Military Committee (EUMC); 4. Council, Horizontal Working Party on Cyber Issues (HWP); 5. CSIRTS Network; 6. Europol, European Cybercrime Centre (EC3); 7. European Commission, Directorate-General for Communications Networks, Content and Technology (DG CONNECT); 8. European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW); 9. European Commission, Directorate-General for International Cooperation and Development (DG DEVCO); 10. European Commission, Directorate-General for Migration and Home Affairs (DG HOME); 11. European Commission, Directorate-General for Research and Innovation (DG RTD); 12. European Commission, European Anti-Fraud Office (OLAF); 13. European Commission, Joint Research Centre (JRC); 14. European Defence Agency (EDA); 15. European External Action Service (EEAS); 16. European External Action Service (EEAS), EU Hybrid Fusion Cell; 17. European Judicial Cybercrime Network (EJC�); 18.

czynników. Po pierwsze, już samo pojęcie cyberbezpieczeństwa jest niejednoznaczne, pomimo tego, że doczekało się definicji legalnej w art. 2 pkt 1 Aktu o Cyberbezpieczeństwie (2019 r.), zgodnie z którym są to: „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”. Przyjmując takie rozumienie cyberbezpieczeństwa, należy wskazać, że odnosi się zarówno do wszystkich sektorów gospodarki, jak i do bezpieczeństwa państwa, zatem zrozumiałe jest, że różne podmioty – nakierowane tak na sektor prywatny, jak i publiczny – wyposażone zostały w kompetencje tego dotyczące⁵⁹⁸. Po drugie, jest to skutek historii rozwoju regulacji cyberbezpieczeństwa na poziomie unijnym sięgającej początku XXI wieku, w której istotną rolę odgrywała wola państw członkowskich, aby obszar ten w możliwie szerokim zakresie pozostawał w ich kompetencji, także z uwagi na jego powiązanie z bezpieczeństwem państwa⁵⁹⁹. Nadto, zapewnienie cyberbezpieczeństwa znalazło się na liście priorytetów politycznych (które determinują inicjatywę prawodawczą) dopiero w ostatniej dekadzie z powodu dynamiki przebiegu transformacji cyfrowej⁶⁰⁰. Konsekwencją tego było przyjęcie Dyrektywy NIS w 2016 r. i Aktu o Cyberbezpieczeństwie, a następnie Dyrektywy NIS 2. Historia tych zmian pokazuje stopniową centralizację regulacji cyberbezpieczeństwa w UE. Proces ten wydaje się pozostawać niezakończony.

Stąd też na potrzeby niniejszej rozprawy analizie poddane zostanie jeden organ unijny, tj. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), z uwzględnieniem dwóch aktów prawnych – Aktu o Cyberbezpieczeństwie i Dyrektywy NIS 2. Nie ulega wątpliwości, że z uwagi na przedstawioną wyżej wielość podmiotów na poziomie unijnym w połączeniu z organami administracji publicznej na poziomie krajowym, podstawowym celem ENISA jest zapewnienie spójnego stosowania aktów prawnych w tym obszarze.

Historia ENISA sięga 2004 r. (motyw 14 Aktu o Cyberbezpieczeństwie), jednak obecny, wzmocniony⁶⁰¹ status prawny uzyskała dopiero na podstawie Aktu o Cyberbezpieczeństwie z 2019 r. (w tym podrozdziale Akt o Cyberbezpieczeństwie

European Parliament, Committee on Industry, Research and Energy (ITRE); 19. European Union Agency for Cybersecurity - ENISA; 20. Eurojust; 21. NIS Cooperation Group; 22. European Judicial Network (EJN).

⁵⁹⁸ Bardziej obszernie na temat tej kwestii w podrozdziale 2.6.2. Krzyżowanie się zakresu przedmiotowego RODO z aktami prawnymi prawa unijnego i krajowego regulującymi cyberbezpieczeństwo.

⁵⁹⁹ M. Cavelty, M. Smeets, Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority, J. Eur. Public Policy 2023, No. 30(7), s. 1338.

⁶⁰⁰ D. Markopoulou, V. Papakonstantinou, P. de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, CLSR 2019, Vol. 35, Iss. 6, s. 2.

⁶⁰¹ M. Adamczyk, Rozdział 16. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Jej rola w cyberbezpieczeństwie i ochronie danych, 3. Podsumowanie [w:] Internet. Globalne gry. Global Games, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2022.

definiowany będzie jako „CSA”), który określa jej cele, zadania ENISA i kwestie organizacyjne jej dotyczące (art. 1 ust. 1 lit. a) CSA). ENISA jest organem unijnym z osobowością prawną (art. 38 ust. 1 CSA), który działa niezależnie (art. 3 ust. 3 CSA). ENISA składa się z Zarządu, Rady Wykonawczej, Dyrektora Wykonawczego, Grupy Doradczej ENISA i Sieci Krajowych Urzędników Łącznikowych (art. 13 CSA). W skład Grupy Doradczej ENISA wchodzi eksperci z różnych środowisk, w tym sektor ITC, przedstawiciele konsumentów, akademicy i przedstawiciele organów nadzorczych ustanowionych na podstawie RODO (art. 21 ust. 1 CSA). Z kolei Sieć Krajowych Urzędników Łącznikowych, która to sieć ma stanowić punkt kontaktowy między ENISA a poziomem krajowym oraz ułatwiać wymianę informacji (art. 23 CSA), tworzą przedstawiciele wszystkich państw członkowskich

Celem ENISA jest osiągnięcie „wysokiego wspólnego poziomu cyberbezpieczeństwa w całej” UE (art. 3 ust. 1 CSA). Do realizacji tego celu ENISA wyposażona została przede wszystkim w kompetencje współpracy i doradcze, informacyjne oraz edukacyjne (art. 3 ust. 1 CSA i Rozdział II CSA). Realizując ten cel, ENISA powinna przyczyniać się do „zmniejszenia rozdrobnienia” rynku wewnętrznego (art. 3 ust. 1 CSA), w tym przez promocję korzystania z europejskiej certyfikacji cyberbezpieczeństwa (art. 4 ust. 6 CSA). ENISA ma stanowić ośrodek wiedzy fachowej o cyberbezpieczeństwie (art. 4 ust. 1 CSA) i wsparcie dla instytucji UE i państw członkowskich we wdrażaniu polityk dotyczących cyberbezpieczeństwa (art. 4 ust. 2 CSA); powinna budować potencjału i gotowości do odpowiedzi na cyberzagrożenia (art. 4 ust. 3 CSA) oraz promować współpracę między państwami członkowskimi, organami i innymi interesariuszami (art. 4 ust. 4 CSA) i wiedzę na temat cyberbezpieczeństwa, a także podejmować działania zwiększające cyberbezpieczeństwo na poziomie unijnym, w tym w odniesieniu do incydentów transgranicznych (art. 4 ust. 5 CSA).

Kompetencje ENISA w CSA zostały zasadniczo umieszczone w Rozdziale II zatytułowanym „Zadania”, jednak w tym rozdziale, oprócz zadań, znalazły się także uprawnienia. Jak zostało to już wskazane, zasadnicza część kompetencji ENISA to kompetencje współpracy i kompetencje doradcze, informacyjne i edukacyjne⁶⁰². Kompetencje ENISA w CSA wydzielone zostały do ośmiu artykułów. Są to: pomoc w opracowywaniu i wdrażaniu polityki i prawa Unii (art. 5 CSA) dla cyberbezpieczeństwa przez m.in. doradztwo na rzecz instytucji i organów unijnych oraz państw członkowskich, w tym dla badań i innowacji

⁶⁰² Por. D. Markopoulou, V. Papakonstantinou, P. de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, CLSR 2019, Vol. 35, Iss. 6, s. 8.

(art. 11 CSA); budowanie zdolności (art. 6 CSA) państw członkowskich i instytucji oraz organów unijnych przez pomoc w zapobieganiu, wykrywaniu i reagowaniu na cyberzagrożenia; wspieranie certyfikacji i ustanowienia norm dla cyberbezpieczeństwa (art. 8 CSA); analiza cyberzagrożeń i cyberbezpieczeństwa (art. 9 CSA), propagowanie wiedzy na te tematy (art. 10 CSA); współpraca międzynarodowa z państwami trzecimi i organizacjami międzynarodowymi (art. 12). Istotne jest, że ENISA zobowiązana jest pomagać państwom członkowskim i doradzać EROD przy wdrażaniu polityki i prawa związanego z cyberbezpieczeństwem, ochroną danych osobowych i prywatnością (art. 5 pkt 5 CSA). Obowiązek współpracy z EROD wynika także z motywu 44 CSA. Ponadto, ENISA zajmuje się wspieraniem współpracy operacyjnej między państwami członkowskimi i pozostałymi instytucjami, organami i jednostkami organizacyjnymi UE oraz interesariuszami (art. 7 ust. 1 CSA). Jest to realizowane m.in. przez wymianę know-how i wydawanie wytycznych (art. 7 ust. 2 CSA). Jednym ze sposobów pogłębiania tej współpracy jest zapewnianie przez ENISA sekretariatu sieci CSIRT (*Computer Security Incident Response Team*) (art. 7 ust. 3 CSA) i wsparcie państw w ramach tej sieci, w tym przez przygotowywanie wspólnej odpowiedzi na istotne transgraniczne incydenty (art. 7 ust. 4 CSA).

ENISA wyposażona została także w kompetencje na podstawie Dyrektywy NIS 2 (w dalszej części tego podrozdziału Dyrektywy NIS 2 definiowany będzie jako „NIS 2”). Są one komplementarne z kompetencjami ENISA w CSA. Wskazane zostaną te z nich, które sama ENISA identyfikuje jako kluczowe⁶⁰³, to jest: opracowanie i prowadzenie europejskiej bazy danych dotyczącej podatności (art. 12 ust. 2 NIS 2); zapewnienie obsługi sekretariatu dla Europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe)⁶⁰⁴ (art. 16 ust. 2 NIS 2); przyjmowanie sprawozdanie o stanie cyberbezpieczeństwa w UE raz na dwa lata (art. 18 ust. 1 NIS 2); stworzenie i prowadzenie rejestru dostawców usług transgranicznych, m.in. usług DNS, rejestrów nazw TLD, usług chmurowych (art. 27 ust. 1 NIS 2). Podobnie jak w Dyrektywie NIS, również zgodnie z NIS 2 ENISA bierze udział w pracach Grupy Współpracy (art. 14 ust. 3 ENISA 2), składającej się z przedstawicieli ENISA, państw członkowskich i Komisji. Kompetencje tej Grupy w art. 14 ust. 4 NIS 2 są kompetencjami doradczymi, informacyjnymi i edukacyjnymi, które ze

⁶⁰³ ENISA, *NIS Directive*, <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new> (dostęp: 15.09.2024 r.).

⁶⁰⁴ Ta sieć składa się z przedstawicieli organów państw członkowskich do spraw zarządzania kryzysowego w cyberbezpieczeństwie, aby pomagać w skoordynowanym zarządzaniu (art. 16 ust. 1 i 2 NIS 2).

względu na swój cel i zachowanie spójności mogą być także zaliczone do kompetencji współpracy.

W odniesieniu do obszaru przetwarzania danych istotnym jest, że EIOD zawarł z ENISA dokument „Memorandum of Understanding” z 30 listopada 2022 r.⁶⁰⁵ w celu ustalenia ustrukturyzowanych ram współpracy w obszarach wspólnego zainteresowania, przede wszystkim kwestii cyberbezpieczeństwa w ochronie danych osobowych (pkt. 4 i 6). Obejmuje to m.in. wspólny strategiczny plan w kwestii cyberbezpieczeństwa w ochronie danych osobowych w instytucjach i organach unijnych (pkt. 7), wspólne inicjatywy edukacyjne (pkt. 8), coroczne spotkania dotyczące obszarów wspólnego zainteresowania (w pkt 9 wymieniono: bezpieczeństwo przetwarzania i zarządzanie incydentami, ochronę danych *by design* i *by default*, technologie zwiększające ochronę prywatności, a także analizy innowacji technicznych), wzajemne informowanie o planowanych strategicznych i programowych dokumentach oraz wytycznych dotyczących obszarów wspólnego zainteresowania (pkt 13 i 14).

3.4.4. EUROPEJSKA RADA DS. INNOWACJI W ZAKRESIE DANYCH

Europejska Rada ds. Innowacji w zakresie Danych ustanowiona została na podstawie Aktu w sprawie zarządzania danymi (w dalszej części tego podrozdziału ten akt definiowany będzie jako „DGA”) jako grupa ekspercka, w skład której wchodzi przedstawiciele organów właściwych do spraw rejestracji organizacji altruizmu danych i do spraw usług pośrednictwa danych ze wszystkich państw członkowskich, EROD, EIOD, ENISA, Komisji, pełnomocnika UE ds. MŚP lub jego przedstawiciela, z innych przedstawicieli podmiotów sektorowych i podmiotów posiadających odpowiednią ekspertyzę (art. 29 ust. 1 DGA). Posiedzeniom Rady przewodniczy Komisja, która także tworzy jej sekretariat (art. 29 ust. 3-4 DGA). Stały udział EROD, EIOD i ENISA w pracach Rady, przeciwnie do rozwiązania przyjętego w Europejskiej Radzie ds. Usług Cyfrowych, należy ocenić pozytywnie, ponieważ powinno przyczynić się to do zwiększenia spójności i współpracy z organami unijnymi wyposażonymi w kompetencje w obszarze przetwarzania danych osobowych.

Kompetencje Rady, określone w art. 30 DGA, są kompetencjami doradczymi, informacyjnymi i edukacyjnymi, a ze względu na swój cel, czyli skuteczne wdrożenie DGA (motyw 54 DGA), w tym przez zapewnienie współpracy i spójności – także kompetencjami

⁶⁰⁵ https://edps.europa.eu/system/files/2022-11/22-11-30_edps_enisa_mou_en.pdf (dostęp: 15.09.2024 r.).

współpracy. Ta Rada m.in. doradza Komisji w opracowaniu spójnych praktyk i wytycznych dotyczących wniosków o ponowne wykorzystywanie danych przez podmioty sektora publicznego, usług pośrednictwa danych i altruizmu danych (art. 30 lit. a)-c) DGA), w niektórych przypadkach konsultując uprzednio EROD (art. 25 ust. 1 DGA z motywem 54 DGA), wymogów cyberbezpieczeństwa i interoperacyjności w zakresie wymiany i przechowywania danych (art. 30 lit. e) DGA), wytyczne dotyczące wspólnych europejskich przestrzeni danych (art. 30 lit. h) DGA) oraz wspiera współpracę między państwami członkowskimi i organami właściwymi (art. 30 lit. i) DGA). Ponadto, zgodnie z motywami 109 i 110, art. 9 ust. 5 i art. 42 Aktu w sprawie Danych (który nie powołuje odrębnego organu na poziomie prawa unijnego), Rada ta może wydawać zalecenia w zakresie ustanawiania i stosowania kar przewidzianych w Akcie o Danych, a także powinna doradzać Komisji w odniesieniu do zapewnienia spójności, interoperacyjności i normalizacji, a także służyć jako forum do wymiany informacji między organami właściwymi ustanowionymi na podstawie Aktu w sprawie Danych.

3.4.5. EUROPEJSKA RADA DS. SZTUCZNEJ INTELIGENCJI I EUROPEJSKI URZĄD DS. SZTUCZNEJ INTELIGENCJI

W AI Act prawodawca unijny wprowadził najbardziej skomplikowaną (z analizowanych w rozprawie) strukturę organów zarówno na poziomie unijnym, jak i krajowym. Na poziomie unijnym w ostatecznym brzmieniu rozporządzenia (przede wszystkim Rozdział VII „Zarządzanie”) ustanowiono Urząd do spraw AI (art. 64 ust. 1 AI Act), który – na podstawie decyzji Komisji⁶⁰⁶ – stanowi część Komisji w strukturze Dyrekcji Generalnej ds. Sieci Komunikacyjnych, Treści i Technologii (art. 1 decyzji), a także Europejską Radę ds. Sztucznej Inteligencji (art. 65 AI Act). Dodatkowo, w AI Act ustanowiono także podmioty doradcze w postaci Forum doradczego złożonego z przedstawicieli różnych sektorów, a także Agencji Praw Podstawowych i ENISA (art. 67 AI Act) oraz panel naukowy niezależnych ekspertów, który ma zostać powołany przez Komisję przez akt wykonawczy (art. 68 AI Act). Nadto, EIOD jest kompetentny jako „organ odpowiedzialny za sprawowanie nadzoru” w sytuacji, w której „instytucje, organy i jednostki organizacyjne Unii są objęte zakresem” AI Act (art. 70 ust. 9 AI Act).

⁶⁰⁶ Decyzja Komisji z dnia 24 stycznia 2024 r. ustanawiająca Europejski Urząd ds. Sztucznej Inteligencji, Bruksela, 24.1.2024, C(2024) 390 final.

W modelu przyjętym w AI Act Urząd ds. AI (w istocie jest to Komisja⁶⁰⁷) wyposażony jest w ograniczone, ale istotne kompetencje. Można argumentować, że jest to model zbliżony do DSA, w którym nastąpił podział kompetencji proceduralnych i sankcyjnych między organy na poziomie unijnym a organy na poziomie krajowym. Przede wszystkim, Urząd ds. AI jest wyłącznie kompetentny do „nadzorowania i egzekwowania” rozdziału V AI Act w odniesieniu do modeli AI ogólnego przeznaczenia (art. 88 ust. 1 AI Act)⁶⁰⁸, co obejmuje możliwość monitorowania wdrożenia AI Act przez dostawców modeli AI ogólnego przeznaczenia (art. 89), w tym przez żądanie przedstawienia dokumentacji i udzielenie wyjaśnień (art. 91), przeprowadzanie oceny ryzyka systemowego tych modeli (art. 92), w tym także dostęp do kodu źródłowego modelu (art. 92 ust. 3)⁶⁰⁹, żądanie podjęcia środków od dostawców, w tym także wycofanie modelu z rynku (art. 93 ust. 1), a także nakładanie kar pieniężnych zgodnie z Rozdziałem XII Rozporządzenia (art. 101). Oprócz tych kompetencji proceduralnych i naprawczych, zarówno z treści AI Act, jak i z przywołanej wyżej decyzji Komisji ustanawiającej Urząd ds. AI wynikają kompetencje doradcze, w tym do rozwoju narzędzi do oceny zdolności modeli AI ogólnego przeznaczenia (art. 3 ust. 1 lit. a przywołanej wyżej decyzji), co uzupełnia kompetencje Komisji do opracowywania wytycznych w przedmiocie wdrożenia AI Act (art. 96 AI Act). W zakresie kompetencji współpracy decyzja ta reguluje, że przy wykonywaniu swoich kompetencji powinien współpracować ze wszystkimi właściwymi podmiotami na poziomie unijnym (zatem także EROD i EIOD) i krajowym w imieniu Komisji (art. 2 ust. 3, art. 3 ust. 1 lit. f, art. 6 decyzji), a także zapewniać spójność w stosowaniu innych aktów unijnych, w których Komisja została ustanowiona jako kompetentna, na przykład DSA i DMA (art. 3 ust. 1 lit. e decyzji, a także art. 5). Nadto, Urząd ds. AI powinien przyczyniać się do spójnego stosowania samego Aktu w Sprawie Sztucznej Inteligencji w UE (m.in. art. 3 ust. 2 lit. b decyzji), w tym także przez wspieranie współpracy między interesariuszami z rynku AI i środowiskami akademickimi oraz społeczeństwa obywatelskiego (art. 4 ust. 1 decyzji).

⁶⁰⁷ Artykuł 3(47): „Urząd ds. AI” oznacza zadanie Komisji polegające na przyczynianiu się do wdrażania, monitorowania i nadzorowania systemów AI i modeli AI ogólnego przeznaczenia oraz zarządzania AI, określone w decyzji Komisji z dnia 24 stycznia 2024 r.; zawarte w niniejszym rozporządzeniu odesłania do Urzędu ds. AI odczytuje się jako odesłania do Komisji”. Zdaniem Autora, niejasna pozostaje relacja kompetencji Urzędu ds. AI (stanowiącego przecież „zadanie Komisji”) do kompetencji Komisji, które zostały z osobna wskazane w treści AI Act, co wydaje się być spowodowane przede wszystkim dynamiczną historią procesu legislacyjnego tego aktu prawnego.

⁶⁰⁸ Zdefiniowanych w art. 3(3) AI Act, których klasyfikacja dokonana jest na podstawie art. 51 AI Act.

⁶⁰⁹ Przy czym w tym przepisie literalnie jako kompetentna wskazana została Komisja.

Z kolei Europejska Rada ds. Sztucznej Inteligencji swoim charakterem i kompetencjami przypomina inne kolegialne podmioty ustanowione na poziomie unijnym. Zgodnie z art. 65 ust. 2, Radę stanowią przedstawiciele (po jednym) z każdego państw członkowskich, z których wybierany jest przewodniczący. EIOD jest obserwatorem prac Rady, a w posiedzeniach uczestniczy także Urząd ds. AI (jednak bez prawa głosu), który także zapewnia sekretariat dla działalności Rady. Działalność Rady regulowana jest regulaminem wewnętrznym przyjętym kwalifikowaną większością głosów (art. 65 ust. 5), przy czym już w treści samego AI Act unormowano, że w Radzie ustanowione zostaną dwie stałe podgrupy – współpracy między organami nadzoru rynku i powiadamiające w sprawach nadzoru rynku i jednostek notyfikujących (art. 65 ust. 6). W art. 66 uregulowano kompetencje Rady (określając je zadaniami), przy czym wprost wskazano kompetencję ogólną, to jest doradzanie Komisji i państwom członkowskim w celu spójnego i skutecznego stosowania AI Act (ust. 1), uzupełniając ją o rozbudowany, otwarty katalog kompetencje szczególnych (ust. 2), w tym m.in. przyczynianie się do koordynacji działań między organami odpowiedzialnymi za stosowanie AI Act (art. 66 ust. 2 lit. a) i harmonizacji praktyk administracyjnych w państwach członkowskich (ust. 2 lit. d); wydawanie zaleceń i opinii (ust. 2 lit. e); ułatwianie wspólnego rozumienia koncepcji w AI Act przez inne organy i podmioty gospodarcze (ust. 2 lit. g); współpraca z innymi organami i sieciami na poziomie unijnym, w tym w dziedzinie cyberbezpieczeństwa, usług cyfrowych, ochrony danych i praw podstawowych (ust. 2 lit. h).

Kompetencje Europejskiej Rady ds. AI nakierowane są przede wszystkim na zapewnienie spójności stosowania AI Act w UE, a pomocniczo także na zapewnienie spójności stosowania tego aktu z innymi aktami prawnymi, w tym RODO, związane są zatem przede wszystkim z kompetencjami doradczymi, co ma zostać w odniesieniu do RODO wzmocnione przez udział EIOD w pracach tej Rady jako obserwatora.

3.4.6. KOMISJA EUROPEJSKA JAKO ORGAN UNIJNEGO PRAWA KONKURENCJI I GRUPA WYSOKIEGO SZCZEBŁA

W niniejszym podrozdziale przeanalizowany zostanie status prawny i kompetencje Komisji jako unijnego organu prawa konkurencji⁶¹⁰, organu stosującego Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych w zakresie, w jakim stosowanie tych aktów przyznane

⁶¹⁰ Por. J. Supernat, Komisja europejska jako administracja publiczna [w:] Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza, red. A. Matan, Warszawa 2022.

jest Komisji. Dodatkowo, w tym podrozdziale krótko omówiona zostanie także Grupa Wysokiego Szczebla ustanowiona na podstawie Aktu o Rynkach Cyfrowych.

3.4.6.1. PRAWO KONKURENCJI

Komisja, kolegalna instytucja UE (art. 13 ust. 1 TUE) kluczowa w sprawowaniu władzy wykonawczej w UE⁶¹¹, jest także organem prawa konkurencji w UE zarówno w odniesieniu do kontroli koncentracji, jak i zakazanych porozumień między przedsiębiorcami (art. 101 TFUE), jak i nadużycia pozycji dominującej (art. 102 TFUE). Departamentem odpowiedzialnym za stosowanie prawa konkurencji jest Dyrekcja Generalna (DG) ds. Konkurencji (DG COMP)⁶¹². W tym podrozdziale kompetencje Komisji scharakteryzowane zostały w odniesieniu do kontroli koncentracji i nadużycia pozycji dominującej zgodnie z obszarem referencyjnym (podrozdział 2.6.3. powyżej). Kompetencje Komisji w odniesieniu do tych kwestii uregulowane zostały odpowiednio w Merger Control Regulation i Rozporządzeniu nr 1/2003. Ze względu na obszerność i złożoność prawa konkurencji, analizie poddane zostały wybrane kompetencje Komisji istotne z perspektywy celu badawczego tej rozprawy. Status prawny i kompetencje Komisji zostaną scharakteryzowane najpierw w odniesieniu do nadużycia pozycji dominującej, a następnie kontroli koncentracji. W obu przypadkach analizę rozpocznie ustalenie relacji kompetencji Komisji do kompetencji krajowych organów.

W UE, oprócz Komisji, prawo konkurencji stosują także krajowe organy konkurencji, które, w ramach Europejskiej Sieci Konkurencji, ściśle współpracują z Komisją⁶¹³. Celem takiego rozwiązania jest odciążenie działalności Komisji od spraw mniejszej wagi i zwiększenie efektywności stosowania unijnego prawa konkurencji przy jednoczesnym zachowaniu jego spójności⁶¹⁴. W tej rozprawie jako krajowy organ konkurencji analizie

⁶¹¹ Jej pozycja ustrojowa i podstawowe kompetencje wynikają z art. 17 TUE. Art. 17 ust. 1 TUE: „Komisja wspiera ogólny interes Unii i podejmuje w tym celu odpowiednie inicjatywy. Czuwa ona nad stosowaniem Traktatów i środków przyjmowanych przez instytucje na ich podstawie. Nadzoruje stosowanie prawa Unii pod kontrolą Trybunału Sprawiedliwości Unii Europejskiej. Wykonuje budżet i zarządza programami. Pełni funkcje koordynacyjne, wykonawcze i zarządzające, zgodnie z warunkami przewidzianymi w Traktatach. Z wyjątkiem wspólnej polityki zagranicznej i bezpieczeństwa oraz innych przypadków przewidzianych w Traktatach, zapewnia reprezentację Unii na zewnątrz. Podejmuje inicjatywy w zakresie rocznego i wieloletniego programowania Unii w celu osiągnięcia porozumień międzyinstytucjonalnych”. Por. także Dyl, Paczkowska-Tomaszewska, Stankiewicz, Wierzbowski, *Rozdział IX. Zarys systemu podmiotów administrujących w Unii Europejskiej* [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 562.

⁶¹² Komisja, Konkurencja, https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/competition_pl (dostęp: 15.09.2024 r.).

⁶¹³ Por. Europejska Sieć Konkurencji (ECN), <https://eur-lex.europa.eu/pl/legal-content/summary/european-competition-network-ecn.html> (dostęp: 15.09.2024 r.).

⁶¹⁴ Por. E. M. Fox, D. Gerard, *EU Competition Law. Cases, Textes and Context*, Cheltenham 2023, s. 18-19.

poddano Prezesa Urzędu Ochrony Konkurencji i Konsumenta w podrozdziale 3.5.4. niżej. Status i kompetencje krajowych organów kompetencji uległy w ostatnich latach wzmocnieniu na skutek implementacji Dyrektywy ECN+ z grudnia 2018 r.⁶¹⁵

W kwestii relacji kompetencji Komisji do kompetencji organów krajowych w sprawach dotyczących nadużycia pozycji dominującej kluczowy jest art. 3 Rozporządzenia nr 1/2003, który nakłada na organy i sądy krajowe obowiązek stosowania art. 102 TFUE bezpośrednio, co oznacza ustanowienie systemu równoległych uprawnień dla organów krajowych⁶¹⁶, przy czym państwa członkowskie mogą przyjąć bardziej restrykcyjne prawo dotyczące tego typu praktyk. Komisja zachowuje kompetencję do wszczęcia postępowania w sprawach, które mogą wpływać na handel między państwami członkowskimi⁶¹⁷, co oznacza, że w przypadku wszczęcia takiego postępowania przez Komisję, krajowe organy ochrony konkurencji zostają pozbawione kompetencji w tych sprawach (art. 11 ust. 6 Rozporządzenia nr 1/2003).

Kompetencje Komisji należy ocenić jako rozbudowane i kompleksowe. Obejmują kompetencje proceduralne, naprawcze i współpracy. Komisja może wszcząć dochodzenie, żądać informacji i przesłuchiwać wszelkie osoby fizyczne i prawne, które wyrażą zgodę (art. 17-19 Rozporządzenia nr 1/2003), a także przeprowadzać kontrole (art. 20-21 Rozporządzenia nr 1/2003), korzystając przy tym i innych czynnościach ze wsparcia krajowych organów prawa konkurencji (art. 22 Rozporządzenia nr 1/2003). Komisja może decyzją stwierdzić naruszenie i nakazać jego kontynuowanie, używając w tym celu proporcjonalnych i koniecznych środków naprawczych o charakterze behawioralnym lub strukturalnym (art. 7 Rozporządzenia nr 1/2003), a także zastosować środki tymczasowe w wyjątkowych okolicznościach (art. 8 Rozporządzenia nr 1/2003). Zainteresowane przedsiębiorstwo może w toku postępowania zaproponować podjęcie zobowiązań uwzględniających wstępne zastrzeżenia Komisji, które Komisja może uznać za wiążące i zakończyć sprawę (art. 9 Rozporządzenia nr 1/2003). Detale prowadzenia postępowania przez Komisję zostały uregulowane w Rozporządzeniu Komisji (WE) nr 773/2004 z dnia 7 kwietnia 2004 r. odnoszące się do prowadzenia przez Komisję postępowań zgodnie z art. 81 i art. 82 Traktatu WE⁶¹⁸. W założeniu, spójność między organami krajowymi i Komisją ma zostać osiągnięta

⁶¹⁵ Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1 z dnia 11 grudnia 2018 r. mająca na celu nadanie organom ochrony konkurencji państw członkowskich uprawnień w celu skuteczniejszego egzekwowania prawa i zapewnienia należytego funkcjonowania rynku wewnętrznego (Tekst mający znaczenie dla EOG.) PE/42/2018/REV/1 OJ L 11, 14.1.2019, p. 3–33.

⁶¹⁶ Por. Europejska Sieć Konkurencji (ECN), <https://eur-lex.europa.eu/pl/legal-content/summary/european-competition-network-ecn.html> (dostęp: 15.09.2024 r.).

⁶¹⁷ E. M. Fox, D. Gerard, *EU Competition Law. Cases, Textes and Context*, Cheltenham 2023, s. 20.

⁶¹⁸ Dz. Urz. UE L 123, 27.4.2004, s. 18–24.

przez ścisłą współpracę między nimi. Instrumenty współpracy obejmują m.in. wymianę dokumentów i informacji (art. 11 ust. 1 i art. 12 ust. 1 Rozporządzenia nr 1/2003), zawieszenie postępowania w przypadku, jeżeli jeden z organów już zajmuje się daną sprawą (art. 13 Rozporządzenia nr 1/2003), utworzenie Komitetu Doradczego ds. Praktyk Ograniczających Konkurencję i Pozycji Dominujących (art. 14 Rozporządzenia nr 1/2003) i współpracę z sądami krajowymi ukierunkowaną na jednolite stosowanie unijnego prawa konkurencji (art. 15 i 16 Rozporządzenia nr 1/2003). Istotną rolę w zachowaniu spójności odgrywa także orzecznictwo samego TSUE wydawane w odpowiedzi na pytania prejudycjalne sądów krajowych⁶¹⁹.

Z kolei w kwestii relacji kompetencji Komisji względem kompetencji krajowych organów dla kontroli koncentracji należy wskazać zgodnie z podrozdziałem 2.6.3.1. powyżej, że Merger Control Regulation stosuje się do koncentracji kwalifikowanych jako „wspólnotowe” (art. 1 ust. 1 w zw. z art. 21 ust. 1-3 Merger Control Regulation), gdzie kryterium stanowi z zasady wysokość obrotu zainteresowanych przedsiębiorstw (szczegóły w art. 1 ust. 2-3 Merger Control Regulation). Wyjątek od tej reguły stanowią tzw. klauzula niemiecka (art. 9 Merger Control Regulation) i tzw. klauzula holenderska (art. 22 Merger Control Regulation). Pierwsza pozwala na skierowanie przez Komisję konkretnej sprawy do zbadania przez krajowy organ konkurencji w przypadku szczególnego zagrożenia dla rynku danego państwa członkowskiego (art. 9 ust. 1-2 Merger Control Regulation). Druga, klauzula holenderska, pozwala na odesłanie w odwrotnym kierunku. Państwo członkowskie może złożyć do Komisji wniosek o zbadanie koncentracji, która nie ma wymiaru wspólnotowego, ale spełnia dwie przesłanki: „ma wpływ na handel pomiędzy Państwami Członkowskimi i zagraża w sposób znaczący konkurencji na terytorium Państwa Członkowskiego” (art. 22 ust. 1 Merger Control Regulation).

Jak wskazano w podrozdziale 2.6.3.1. powyżej, podmioty dokonujące koncentracji zobowiązane są do jej uprzedniego zgłoszenia (art. 4 Merger Control Regulation) i nie mogą wprowadzić jej w życie przed uznaniem jej za zgodną ze wspólnym rynkiem (art. 7 Merger Control Regulation). Komisja ma uprawnienie do żądania informacji (art. 11 Merger Control Regulation) i przeprowadzania inspekcji (art. 13 Merger Control Regulation), w tym może korzystać ze wsparcia krajowych organów konkurencji (art. 12 Merger Control Regulation). W wydaniu decyzji w przedmiocie oceny zgodności koncentracji ze wspólnym rynkiem Komisja może – w uproszczeniu – stwierdzić taką zgodność rozwiązania (zgodnie

⁶¹⁹ E. M. Fox, D. Gerard, *EU Competition Law. Cases, Textes and Context*, Cheltenham 2023, s. 17.

z art. 8 Merger Control Regulation) bezwarunkowo, uzależnić tę zgodność od spełnienia przez zainteresowane przedsiębiorstwa określonych zmian albo stwierdzić brak takiej zgodności. W przypadku, jeżeli koncentracja niezgodna ze wspólnym rynkiem została już dokonana, Komisja może w decyzji wymagać od zainteresowanych przedsiębiorstw jej rozwiązania (art. 8 ust. 4 Merger Control Regulation). Komisja może także nałożyć na przedsiębiorstwa lub związki przedsiębiorstw kary pieniężne zgodnie z art. 13 Merger Control Regulation, w tym zwłaszcza za niezgłoszenie koncentracji i dokonanie koncentracji przez uznanie jej za zgodną ze wspólnym rynkiem, ale także za naruszenia proceduralne w postępowaniu przed Komisją.

W praktyce spraw dotyczących jak nadużycia pozycji dominującej, jak i kontroli koncentracji, istotne są obwieszczenia Komisji (np. w zakresie dostępu do akt ⁶²⁰ i niewiążących wytyczne, np. *Wytyczne w sprawie oceny horyzontalnego połączenia przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw* (2004/C 31/03)⁶²¹, *Wytyczne w sprawie oceny niehoryzontalnych połączeń przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw*⁶²², czy *Wytyczne dotyczące stosowania mechanizmu odsyłania spraw przewidzianego w art. 22 rozporządzenia w sprawie kontroli łączenia przedsiębiorstw w odniesieniu do określonych kategorii spraw* 2021/C ⁶²³). Niektóre z tych wytycznych, zarówno dotyczących nadużycia pozycji dominującej⁶²⁴, jak i kontroli koncentracji⁶²⁵ są obecnie zmieniane.

3.4.6.2. AKT O RYNKACH CYFROWYCH I GRUPA WYSOKIEGO SZCZEBŁA

Model stosowania DMA jest odmienny od najczęściej wybieranego przez prawodawcę unijnego w obszarze przetwarzania danych osobowych. Jest to bowiem scentralizowany model, w którym zasadnicze kompetencje przyznane zostały Komisji, a krajowe organy prawa konkurencji i Grupa Wysokiego Szczębla (scharakteryzowana niżej) pełnią funkcję tylko subsydiarną, której istotą jest współpraca z Komisją w stosowaniu DMA, zarówno w odniesieniu do prowadzonych postępowań w ramach Europejskiej Sieci Konkurencji przez

⁶²⁰ Obwieszczenie Komisji dotyczące zasad dostępu do akt Komisji w sprawach na mocy art. 81 i 82 Traktatu WE, art. 53, 54 i 57 Porozumienia EOG oraz rozporządzeniem Rady (WE) nr 139/2004 (Tekst mający znaczenie dla EOG OJ C 325, 22.12.2005, s. 7–15.

⁶²¹ Dz. Urz. UE C 31, 5.2.2004, s. 5–18.

⁶²² Dz. Urz. UE C 265, 18.10.2008, s. 6–25.

⁶²³ C/2021/1959 OJ C 113, 31.3.2021, s. 1–6.

⁶²⁴ Competition Policy, Application of Article 102 TFEU, https://competition-policy.ec.europa.eu/antitrust-and-cartels/legislation/application-article-102-tfeu_en

⁶²⁵ Competition Policy, Antitrust: Commission adopts new Horizontal Block Exemption Regulations and Horizontal Guidelines, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2990 (dostęp: 15.09.2024 r.).

krajowe organy prawa konkurencji (art. 38 DMA), jak i innych organów (art. 37 DMA), oraz kompetencji doradczych (art. 40 ust. 5 DMA). Dodatkowo, krajowe organy prawa konkurencji zobowiązane są informować Komisję o dochodzeniach wszczętych (art. 38 ust. 2 DMA) i obowiązkach nałożonych (art. 38 ust. 3 DMA) na strażników dostępu w celu koordynacji stosowania DMA i krajowego prawa konkurencji (art. 38 ust. 5 DMA), wobec którego DMA pozostaje bez uszczerbku w zakresie wskazanymi w art. 1 ust. 6 DMA, oraz o uzasadnionym podejrzeniu naruszenia DMA (art. 27 ust. 3 DMA).

Kompetencje Komisji określone zostały jednak szeroko w celu zapewnienia skuteczności stosowania DMA (motyw 80 DMA) przede wszystkim w rozdziale IV (Badanie rynku w celu wskazania strażników dostępu, dotyczące systematycznego niewypełnienia obowiązków i nowych usług oraz praktyk) i V (Uprawnienia w zakresie prowadzenia badań oraz egzekwowania i monitorowania). Na podstawie przepisów rozdziału V Komisja może wszczynać i prowadzić postępowania w celu weryfikacji realizacji obowiązków przez strażników dostępu oraz badania rynku (art. 20 DMA i art. 8 ust. 2-9 DMA), w tym żądać informacji (art. 21 i 27 DMA, także art. 13 ust. 2 DMA), prowadzić przesłuchania (art. 22 DMA) i kontrole (art. 23 DMA), stosować środki tymczasowe (art. 24 DMA) oraz monitorować obowiązki strażników dostępu (art. 26 DMA). Strażnik dostępu może w toku postępowania zaproponować podjęcie zobowiązań, które Komisja może uznać za wiążące i zakończyć postępowanie (art. 25 ust. 1 DMA). Wreszcie, Komisja stwierdza niewypełnienie obowiązków przez strażnika dostępu (art. 29 DMA) i może nałożyć na niego kary pieniężne do wysokości 10% łącznego światowego obrotu w poprzednim roku obrotowym w przypadku stwierdzenia naruszenia obowiązków, o których mowa w art. 30 ust. 1 DMA (w tym także okresowe kary pieniężne), a w kwalifikowanych przypadkach wskazanych w art. 30 ust. 2 DMA – do wysokości 20% tego wskaźnika. Komisja może także nałożyć kary pieniężne do wysokości 1% wskaźnika przedstawionego wyżej za inne zaniedbania, o których mowa w art. 30 ust. 3 DMA dotyczące obowiązków proceduralnych strażników dostępu w postępowaniu przed Komisją. Istotne kompetencje naprawcze przewidziane zostały w art. 18 DMA dotyczącym badania rynku w celu weryfikacji systematycznego niewypełniania obowiązków, które umożliwiają nałożenie przez Komisję koniecznych i proporcjonalnych środków zaradczych o charakterze strukturalnym i behawioralnym w celu zapewnienia skutecznego stosowania DMA (art. 18 ust. 1 DMA).

Te rozdziały IV i V, w odniesieniu do kompetencji Komisji inspirowane unijnym prawem konkurencji ⁶²⁶, należy ocenić jako wyczerpujący, ponieważ zawiera także przepisy proceduralne dotyczące terminów przedawnienia w nakładaniu (art. 32 DMA) i wykonaniu (art. 33 DMA) sankcji oraz gwarancje procesowe, np. prawo do bycia wysłuchanym i prawo dostępu do akt (art. 34 DMA). Komisja ma nadto uprawnienie do przyjmowania aktów delegowanych w celu uzupełnienia DMA w odniesieniu do obowiązków strażników dostępu w art. 5, 6 DMA (art. 12 ust. 1 DMA) i w art. 7 DMA (dotyczącym interoperacyjności usług łączności interpersonalnej niewykorzystujących numerów; art. 12 ust. 3-4 DMA) w zakresie ograniczonym i w sposób przewidziany w art. 12 i 49 DMA. Komisja może także zawiesić wykonywanie lub zwolnić strażnika dostępu z części obowiązków w wyjątkowych okolicznościach, w tym ze względu zdrowia i bezpieczeństwa publicznego (art. 9-10 DMA). Komisji przyznano także rozbudowane kompetencje doradcze, informacyjne i edukacyjne w przedmiocie przyjmowania wytycznych dotyczących wszelkich aspektów DMA (art. 47 DMA) i upoważnianie europejskich organów normalizacyjnych do opracowania norm, które mają uczynić wypełnianie obowiązków określonych DMA łatwiejszym.

Grupa Wysokiego Szczebla ustanowiona została na podstawie art. 40 DMA jako grupa doradcza i ekspercka dla Komisji (art. 40 ust. 5 DMA), która zapewnia obsługę jej sekretariatu (art. 40 ust. 4 DMA). W jej skład wchodzi Organ Europejskich Regulatorów Łączności Elektronicznej, EIOD i EROD, Europejska Sieć Konkurencji, sieć współpracy w zakresie ochrony konsumenta oraz Europejska Grupa Regulatorów ds. Audiowizualnych Usług Medialnych (art. 40 ust. 2 DMA). Grupa ta nie została wyposażona w instrumenty, które mogą dawać jej możliwość formalnego wpływu na działania podejmowane przez Komisję. Ze wszystkich podmiotów scharakteryzowanych na poziomie unijnym w tym rozdziale, Grupa ta ma najsłabszą pozycję. Jej kompetencje są doradcze z uwzględnieniem ogólnych kwestii dotyczących stosowania DMA i identyfikacji krzyżowania się zakresu przedmiotowego DMA z innymi aktami prawnymi oraz kompetencjami organów ustanowionymi na podstawie tych aktów (art. 40 ust. 5 lit. b) DMA i ust. 6 DMA), z czego Grupa Wysokiego Szczebla sporządza coroczne sprawozdanie przedkładane Parlamentowi Europejskiemu i Radzie (art. 40

⁶²⁶ Keynote of EVP Vestager at the European Competition Law Tuesdays: A Principles Based approach to Competition Policy, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_6393 (dostęp: 15.09.2024 r.).

ust. 6 DMA). Grupa Wysokiego Szczębla powołana została decyzją Komisji z 23.03.2023 r., gdzie uszczegółowiono zagadnienia proceduralne⁶²⁷.

Nie wprowadzono bezpośrednio instrumentów współpracy z organami ochrony danych, ani EROD, ani EIOD, poza tymi wprowadzonymi w odniesieniu do Grupy Wysokiego Szczębla przedstawionymi wyżej i obowiązkiem przekazywania poddanego audytowi opisu technik profilowania konsumentów przez strażnika dostępu do ERIOD (art. 15 ust. 1 DMA), którego metodyka oraz procedura sporządzania podlegają opracowaniu w porozumieniu z EROD i EIOD (motyw 72 DMA i art. 46 ust. 1 lit. (g) DMA). Należy jednak zwrócić uwagę na art. 37 ust. 2 DMA, który daje podstawę Komisji do konsultowania z organami krajowymi „wszelkich spraw związanych ze stosowaniem” DMA w celu „spójnego i komplementarnego egzekwowania dostępnych instrumentów prawnych” (art. 37 ust. 1 DMA). Z uwagi na krzyżowanie się zakresów przedmiotowych DMA i RODO oraz brzmienie motywu 12 do DMA, takimi organami będą także organy ochrony danych, co pozostawia prawodawcy krajowemu możliwość i obowiązek ukształtowania instrumentów współpracy tych organów z Komisją⁶²⁸. W literaturze zidentyfikowano zresztą ryzyko niespójności stosowania DMA z uwagi na inicjatywy prawodawcze podejmowane przez prawodawców krajowych przy implementacji art. 37-38 DMA do krajowych porządków prawnych⁶²⁹.

3.4.6.3. AKT O USŁUGACH CYFROWYCH

Komisja jest z zasady odpowiedzialna za stosowanie DSA wobec VLOPs i VLOSEs, czyli największych podmiotów nadzorowanych zgodnie z DSA. Sposób podziału kompetencji między Komisję a państwa członkowskie w odniesieniu do Aktu o Usługach Cyfrowych scharakteryzowany został w podrozdziale 3.5.5. poniżej. Jest to model stosowania mniej scentralizowany niż w DMA, ale bardziej, niż w RODO.

Katalog kompetencji Komisji wobec nadzorowanych podmiotów zawarty został w sekcji 4 „Nadzór, czynności sprawdzające, egzekwowanie i monitorowanie w odniesieniu do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych” rozdziału IV „Wdrażanie, współpraca, sankcje i egzekwowanie”. Podobnie jak

⁶²⁷ Komisja, Decision of 23.3.2023 on setting up the High-Level Group for the Digital Markets Act, 23.3.2023 C(2023) 1833 final, https://competition-policy.ec.europa.eu/system/files/2023-03/High_Level_Group_on_the_DMA_0.pdf (dostęp: 15.09.2024 r.).

⁶²⁸

⁶²⁹ A. Ribera Martínez, *The Decentralisation of the DMA's System of Enforcement*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4857232 (dostęp: 15.09.2024 r.).

w przypadku DMA, sekcję tę, inspirowaną kompetencjami Komisji w prawie konkurencji ⁶³⁰, należy ocenić jako wyczerpującą, ponieważ zawiera także przepisy proceduralne dotyczące terminów przedawnienia w nakładaniu (art. 77 DSA) i wykonaniu (art. 78 DSA) sankcji oraz gwarancje procesowe, np. prawo do bycia wysłuchanym i prawo dostępu do akt (art. 79 DSA). Oprócz kompetencji proceduralnych, naprawczych i współpracy Komisji w tej sekcji, Komisja przyznano także kompetencje doradcze, np. wydawanie wytycznych (we współpracy z koordynatorami ds. usług cyfrowych) dotyczących zalecanych środków zmniejszających konkretne rodzaje ryzyk systemowych (art. 35 ust. 3 DSA), czy promowanie przyjęcia dobrowolnych norm technicznych przez podmioty nadzorowane (art. 44 DSA) i zachęcanie ich do przyjęcia dobrowolnych kodeksów postępowania (art. 45-47 DSA). Działania Komisji finansowane są z opłat nadzorczych pobieranych od VLOPs i VLOSEs zgodnie z art. 43 DSA⁶³¹.

Komisja, prowadząc czynności sprawdzające, może żądać wsparcia od krajowych koordynatorów ds. usług krajowych (art. 66 ust. 3 DSA), których, razem z Europejską Radą ds. Usług Cyfrowych, zobowiązana jest poinformować o wszczęciu postępowania w odniesieniu do praktyki VLOPs i VLOSEs. Komisja może żądać informacji i wyjaśnień od podmiotów, które mogą dysponować informacjami związanymi ze sprawą (art. 67 i 68 DSA), a także przeprowadzać niezbędne kontrole zgodnie ze szczegółowym unormowaniem w art. 69 DSA oraz stosować środki tymczasowe (art. 70 DSA). VLOPs i VLOSEs mogą zaproponować zobowiązania mitygujące naruszenia obowiązków w DSA, które Komisja może uczynić wiążącymi (art. 71 DSA), co stanowi sposób na wcześniejsze zakończenie postępowania. Komisja, w celu weryfikacji przestrzegania DSA przez VLOPs i VLOSEs, może monitorować działania tych podmiotów, w tym m.in. przez dostęp do ich baz danych i algorytmów (art. 72 ust. 1 DSA). Wreszcie, Komisja jest kompetentna do wydawania decyzji o stwierdzeniu naruszenia DSA (art. 73 DSA), w tym nakładania kar pieniężnych, których wysokość nie może przekraczać 6 % łącznego światowego rocznego obrotu danego podmiotu uzyskanego w poprzednim roku obrotowym (art. 74 DSA; patrz także art. 76 DSA dotyczący okresowych kar pieniężnych), a także, w wyjątkowych przypadkach uporczywego i szczególnie szkodliwego działania, do wnioskowania do koordynatora ds. usług cyfrowych dla miejsca siedziby VLOPs i VLOSEs o zawniaskowanie do właściwego sądu krajowego o tymczasowe zawieszenie usługi (art. 82 ust. 1 DSA). W przypadku wydania decyzji o stwierdzenie

⁶³⁰ Q&A: Digital Services Act, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (dostęp: 15.09.2024 r.).

⁶³¹ Por. motyw 101 DSA.

naruszenia DSA któregośkolwiek z przepisów rozdziału III sekcja 5 DSA, Komisja, we współpracy z Europejską Radą ds. Usług Cyfrowych, stosuje wzmożony nadzór nad środkami zaradczymi, w związku z planem działania przygotowanego przez VLOP lub VLOSE zgodnie z decyzją w celu wyeliminowania tych naruszeń (art. 75 DSA).

3.4.7. EUROPEJSKA RADA DS. USŁUG CYFROWYCH

Europejska Rada ds. Usług Cyfrowych ustanowiona została na podstawie Aktu o Usługach Cyfrowych (w dalszej części tego podrozdziału ten akt definiowany będzie jako „DSA”) jako niezależna grupa doradcza (art. 61 ust. 1 DSA) z trzema celami: spójność stosowania DSA i zapewnienie współpracy; koordynacja sporządzania wytycznych; udzielania wsparcia organom właściwym ustanowionym w DSA na poziomie krajowym (koordynatorzy ds. usług cyfrowych) i Komisji w nadzorowaniu VLOP (art. 61 ust. 2 DSA). W skład Rady wchodzi co do zasady koordynatorzy ds. usług cyfrowych, a przewodniczy jej Komisja (art. 62 ust. 1 i 2 DSA). Rada, działając na podstawie regulaminu wewnętrznego (który jest przez nią uchwalany; art. 62 ust. 2 DSA), przyjmuje akty zwykłą większością głosów, przy czym każdemu państwu przysługuje jeden głos, a Komisja nie ma prawa głosu (art. 62 ust. 3 DSA).

Katalog kompetencji tej Rady sformułowany został w sposób otwarty, przy czym w art. 63 ust.1 DSA wskazane zostało pięć tych kompetencji: koordynacja wspólnych czynności sprawdzających; wsparcie w badaniu sprawozdań i wyników audytów VLOPs i VLOEs; opiniowanie, doradzanie i wydawanie zaleceń koordynatorom ds. usług cyfrowych zgodnie z DSA; doradztwo na rzecz Komisji w procedurze z art. 66 DSA (wszczęcie postępowania przez Komisję i współpraca w ramach czynności sprawdzających); wydawanie wytycznych, opinii i zaleceń (np. na podstawie art. 35 ust. 2 DSA we współpracy z Komisją). Kompetencje te należy zaliczyć do kompetencji współpracy lub kompetencji lub doradczych, informacyjnych i edukacyjnych. Kompetencje Rady należy interpretować z uwzględnieniem celów ustanowienia Rady, które przedstawione zostały wyżej.

W skład Rady nie wchodzi przedstawiciele EROD ani EIOD. Brak partycypacji przedstawicieli tych organów należy ocenić negatywnie, ponieważ oznacza to, że w toku obrad nie będzie reprezentantów perspektywy ochrony danych osobowych. W motywie 134 DSA wskazane jest jedynie, że Rada powinna współpracować z innymi organami unijnymi, których obowiązki dotyczą m.in. ochrony danych z uwagi na ryzyko istnienia rozwiązań krzyżujących się z innymi unijnymi aktami prawnymi (*In view of possible cross-cutting elements that may be of relevance for other regulatory frameworks at Union level*). Nie oznacza to jednak obowiązku nawiązania takiej współpracy, lecz jedynie taką możliwość i zachętę prawodawcy, aby taką inicjatywę podjąć.

Interesujące jest, że w rozdziale IV „Wdrażanie, współpraca, sankcje i egzekwowanie” sekcja 2 „Kompetencje, skoordynowane czynności sprawdzające i mechanizmy spójności” wprowadzona została procedura skierowania spraw do Komisji, w której Rada bierze udział.

Celem tej procedury jest zapewnienie skutecznej współpracy transgranicznej między koordynatorami ds. usług cyfrowych (art. 58 DSA) i wspólnych czynnościach sprawdzających (*joint investigations*) (art. 60 DSA). Koordynatorzy ds. usług cyfrowych właściwych dla miejsca siedziby dostawcy usług pośrednich zobowiązani są w określonych terminach podjąć czynności procesowe zmierzające czy doszło do naruszenia DSA na uzasadniony wniosek koordynatora ds. usług cyfrowych właściwego dla miejsca przeznaczenia lub zalecenie Rady (art. 58 ust. 1-2 i art. 60 ust. 1-2 DSA). Brak podjęcia działań przez tego koordynatora lub niewystarczające działania (art. 59 ust. 1 i art. 60 ust. 3 DSA) powodują, że Rada może skierować sprawę do Komisji. Wówczas Komisja dokonuje własnej oceny sprawy i może wnieść do tego koordynatora o przegląd sprawy (art. 59 ust. 3 DSA), przy czym koordynator nie jest związany stanowiskiem Komisji, przy czym zobowiązany jest uwzględnić je w możliwie największym stopniu. Ten instrument, którego celem jest zachowanie spójności, należy ocenić jako mniej efektywny niż mechanizm spójności w RODO. Rada nie ma, w przeciwieństwie do EROD, możliwości wydania decyzji w sprawie. Jest to zrozumiałe z racji statusu Rady jako grupy doradczej, jednak odbiera jej sprawczość, czyniąc z niej organ o słabszych kompetencjach niż EROD.

3.5. CHARAKTERYSTYKA WYBRANYCH ORGANÓW NA POZIOMIE KRAJOWYM

W tym podrozdziale zbadano wybrane organy administracji publicznej na poziomie krajowym w obszarze referencyjnym: Prezes Urzędu Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej, organy właściwe do spraw cyberbezpieczeństwa, Prezes Urzędu Ochrony Konkurencji i Konsumenta jako organ krajowego prawa konkurencji, organy właściwe w Akcie o usługach cyfrowych, organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych, organy właściwe w Akcie w sprawie danych i organy właściwe w Akcie w sprawie Sztucznej Inteligencji. Podobnie jak w przypadku organów na poziomie unijnym, analizie poddano ich status prawny, strukturę i kompetencje, z uwzględnieniem kompetencji współpracy.

3.5.1. PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH

Struktura organów administracji publicznej stosujących RODO jest dwupoziomowa⁶³². Zasadniczy ciężar stosowania RODO spoczywa na krajowych organach nadzorczych (w Polsce jest to Prezes Urzędu Ochrony Danych Osobowych), podczas gdy (analizowany wyżej) EROD na poziomie unijnym ma kompetencje doradcze, innowacyjne i edukacyjne, a także istotne kompetencje współpracy w postaci mechanizmu spójności. W tym podrozdziale zbadany zostanie organ krajowy, Prezes Urzędu Ochrony Danych Osobowych, przy czym opisanie jego statusu i kompetencji wymaga analizy zarówno RODO (które zostanie scharakteryzowane jako pierwsze), jak i UODO.

Historia organów ochrony danych osobowych ma początek w połowie lat siedemdziesiątych XX wieku. Ponad dwie dekady przed wejściem w życie Dyrektywy ODO niektóre państwa członkowskie, na przykład Szwecja (1973), Niemcy (1977) i Francja (1978), przyjęły akty prawne, których celem była ochrona danych osobowych⁶³³. Aby stosować te akty, konieczne było ustanowienie odpowiednich organów. Za pierwszy niezależny organ ochrony danych uznawany jest w literaturze francuski organ, *Commission Nationale Informatique et Libertés* (CNIL),⁶³⁴ który, przykładowo, nie mógł otrzymywać instrukcji od innych organów (zgodnie z art. 13 *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), a jego niezależność wynikała wprost z brzmienia aktu prawnego, który go ustanawiał (art. 8 przywołanego wyżej aktu). W prawie Rady Europy, w pierwotnej wersji Konwencji 108 (sporządzona w 1981 r.), pierwszego prawnie wiążącego aktu prawa międzynarodowego dotyczącego ochrony danych osobowych⁶³⁵, nie nałożono obowiązku ustanowienia niezależnych organów ochrony danych osobowych. Obowiązek ten dodany został w modyfikacji tego aktu, w art. 1 ust. 1-3 Protokołu Dodatkowego (2001 r.) do Konwencji 108. W prawie unijnym obowiązek ustanowienia krajowych organów ochrony danych osobowych wynikał z art. 28 ust. 1 Dyrektywy ODO (1995 r.) obowiązującej do wejścia w życie RODO. Zgodnie z Dyrektywą ODO, każde państwo członkowskie miało zapewnić, że jeden lub więcej organów władzy publicznej będzie odpowiedzialny za kontrolę przestrzegania przepisów przyjętych na mocy Dyrektywy ODO i wprowadzone zostaną rozwiązania, które zapewnią jego

⁶³² Autor tej rozprawy obronił w kwietniu 2018 r. pracę magisterską zatytułowaną „Pozycja organów nadzorczych w ogólnym rozporządzeniu o ochronie danych osobowych” (niepublikowana). Część twierdzeń w tym podrozdziale odpowiada twierdzeniom sformułowanym w tej pracy magisterskiej, bowiem zachowały one aktualność.

⁶³³ G. G: Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Cham 2014, s. 70-71.

⁶³⁴ G. G: Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Cham 2014, s. 65.

⁶³⁵ H. Hijmans, *Article 51 Supervisory authority* [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 2.01.2024 r.), s. 866.

całkowitą niezależność. W Polsce organem ochrony danych osobowych był GODO na podstawie art. 8 ust. 1 UODO⁹⁷ do wejścia w życie UODO.

W prawie UE status niezależnych organów ochrony danych jest w aktualnym stanie prawnym wyjątkowy, ponieważ obowiązek ich ustanowienia wynika wprost z prawa pierwotnego UE, tj. art. 8 ust. 3 KPP (prawo podstawowe do ochrony danych osobowych), art. 16 ust. 2 TFUE i art. 39 TUE. Zgodnie z art. 8 ust. 3 KPP, przestrzeganie zasad dotyczących ochrony danych osobowych ustanowionych w art. 8 ust. 1-2 KPP podlega kontroli niezależnego organu. Jest to jedyny przepis w KPP, który wprost wskazuje na konieczność ustanowienia niezależnego organu w celu kontroli prawa podstawowego⁶³⁶. Oznacza to, że ustanowienie przez państwa członkowskie takiego organu stanowi immanentną część prawa do ochrony danych osobowych w aspekcie instytucjonalnym⁶³⁷.

3.5.1.1. RODO

W tej części przedmiotem analizy będzie status prawny i kompetencje organów nadzorczych zgodnie z Rozdziałem VI „Niezależne organy nadzorcze” i sekcją 1 „Współpraca” Rozdziału VII „Współpraca i spójność” RODO. Wywód oparty jest zasadniczo o systematykę przepisów wprowadzoną przez RODO. Najpierw scharakteryzowane zostaną zasady ustanowienia organów i ich niezależność (art. 51-54 w Sekcji 1 „Niezależny status”), następnie zasady ich właściwości (art. 55 RODO), w tym właściwość wiodącego organu (art. 56 RODO) i kompetencje (art. 57-58 RODO), kończąc na współpracy horyzontalnej między krajowymi organami nadzorczymi (art. 60-62 RODO).

Prawodawca unijny zobowiązuje państwa członkowskie do ustanowienia „niezależnego organu publicznego [który monitorował będzie przestrzeganie RODO] w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii” (art. 51 ust. 1 RODO), które mają przyczyniać się do spójnego stosowania RODO w UE (art. 51 ust. 2 RODO). Organy nadzorcze mają zatem dwa cele. Pierwszym jest ochrona podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych w UE, a drugim ułatwianie swobodnego przepływu tych danych. Odpowiada to pełnemu tytułowi RODO („w sprawie ochrony osób

⁶³⁶ Article 8 [in:] *The EU Charter of Fundamental Rights: A Commentary*, ed. by S. Peers, T. Hervey, J. Kenner et al. Oxford 2021, Nb 08.186.

⁶³⁷ K. Rokita, Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych, EPS 2016, nr 7, s. 6.

fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych”) i przedmiotowi oraz celom RODO w art. 1 ust. 1-2 RODO. Tak szerokie sformułowanie celu działalności organów nadzorczych wpływa na pojmowanie ich kompetencji, które powinny być wykładane w taki sposób, aby umożliwić pełną realizację tych celów.

Państwa członkowskie, zgodnie z zasadą autonomii instytucjonalnej i przy uwzględnieniu zapewnienia efektywności prawa UE, mają swobodę w wyborze rozwiązań ustrojowych (motyw 120 RODO), np. mogą ustanowić więcej niż jeden organ na terytorium jednego państwa członkowskiego (np. Niemcy⁶³⁸), lub też organ nadzorczy może być organem jednoosobowym (np. PUODO w Polsce) lub kolegialnym (np. Francja⁶³⁹). Aby zagwarantować niezależność organów nadzorczych (o której niżej), prawodawca unijny w pewnym stopniu limituje jednak tę swobodę. W art. 54 ust. 1 RODO, wskazując niezbędne elementy, które musi zawierać prawodawstwo krajowe ustanawiające organy nadzorcze, w tym: określenie kwalifikacji i warunków wyboru na stanowisko członka organów nadzorczych; zasady i procedury powoływania członka tych organów i okres kadencji nie krótszy niż cztery lata; określenie liczby kadencji, przez jaką ten członek może sprawować funkcję; oraz obowiązki członka i personelu organu, w tym dotyczące konfliktu interesów i ustania stosunku pracy. W RODO (art. 53) uszczegółowiono także elementy procedury wyboru członka organu, konieczność posiadania przez niego odpowiednich kwalifikacji, doświadczenia i umiejętności oraz trzy przypadki zakańczania pełnienia przez niego funkcji (upływ kadencji, rezygnacja i przymusowe pozbawienie funkcji). Procedura wyboru powinna być możliwie transparentna, czemu może służyć, np. udział opinii publicznej w konsultowaniu kandydatur w jej toku⁶⁴⁰. Wyboru członków, zgodnie z ust. 1 art. 53 RODO, powinien dokonywać parlament, rząd, głowa państwa lub niezależny organ, któremu zadanie to powierzono w prawie państwa członkowskiego (por. także motyw 121 RODO). W odniesieniu natomiast do zakończenia funkcji członka organu, przymiot niezależności organu nadzorczego wzmocniony jest przez ograniczenie przymusowego pozbawienia funkcji tylko do dwóch przypadków: gdy członek

⁶³⁸ *Commission Nationale Informatique et Libertés*. CNIL, Status & Composition, <https://www.cnil.fr/en/cnil/status-composition>

⁶³⁹ Na poziomie federalnym – jeden organ *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*. BfDI, https://www.bfdi.bund.de/EN/DerBfDI/UeberUns/ueberuns_node.html (dostęp: 15.09.2024 r.). Na poziomie krajów związkowych (landów) – 16 organów ochrony danych dla każdego z landów z osobna, BfDI, Data protection authorities of the federal states (Länder), <https://www.bfdi.bund.de/EN/Service/Anschriften/Laender/Laender-node.html> (dostęp: 15.09.2024 r.).

⁶⁴⁰ U. Góral, P. Makowski [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 53, pkt 2, SIP LEX.

dopuszczył się poważnego uchybienia lub jeżeli przestał spełniać warunki niezbędne do pełnienia obowiązków⁶⁴¹ (art. 53 ust. 4 RODO).

Jak zostało wskazane, niezależność organów nadzorczych wpisana jest do prawa pierwotnego UE i stanowi instytucjonalny aspekt prawa do ochrony danych osobowych. Stąd też prawodawca unijny w RODO, określając niezależność organów jako „zasadniczym element” ochrony danych osobowych (motyw 117 RODO), wprowadza rozwiązania, które mają zapewnić ją w państwach członkowskich. Najpierw jednoznacznie rozstrzyga w art. 52 ust. 1 RODO, że, „każdy organ nadzorczy [...] działa w sposób w pełni niezależny”. Zanim scharakteryzowane zostaną rozwiązania przyjęte w RODO, omówiona zostanie historia pojmowania niezależności tych organów.

Przekonanie o potrzebie niezależności organów ochrony danych osobowych w europejskim modelu ochrony danych osobowych sięga, jak wskazano wyżej, początku historii tych organów, czyli lat siedemdziesiątych ubiegłego wieku. Uzasadnieniem dla tej potrzeby było i jest postrzeganie tej niezależności jako podstawowego warunku umożliwiającego jednostkom realizację praw w stosunku do władzy publicznej i jej nadużyć⁶⁴². Sąd też już Dyrektywa ODO (1995 r.) wprowadzała obowiązek zapewnienia niezależności działania tych organów przez państwa członkowskie (art. 28 ust. 1 Dyrektywy ODO). Wypełnienie tego obowiązku stało się przedmiotem szeregu sporów między Komisją a państwami członkowskimi (np. Niemcy i Austria), czego konsekwencją było wyrokowanie przez TSUE w tej kwestii⁶⁴³. To właśnie orzecznictwo TSUE ukształtowało rozumienie niezależności organów ochrony danych, co znalazło odzwierciedlenie w treści RODO⁶⁴⁴. Jego istotą jest szerokie rozumienie (pełnej) niezależności jako „wykluczenie jakiegokolwiek zewnętrznego wpływu” – nie tylko pośredniego i bezpośredniego od podmiotów

⁶⁴¹ P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2022, art. 53, pkt 7, SIP LEX.

⁶⁴² M. Rojszczak, Reforma Krajowych Przepisów o Ochronie Danych a Kwestia Niezależności Organów Nadzorczych na Tle Rozporządzenia 2016/679 i Dyrektywy 2002/58–Uwagi Krytyczne, iKAR 2018, t. 7, nr 4, s. 71.

⁶⁴³ Np. wyrok TSUE C-518/07, Komisja przeciwko Niemcom; wyrok TSUE C-614/10, Komisja przeciwko Austrii; wyrok TSUE C-288/12, Komisja przeciwko Węgrom. Należy wskazać, że na pojęcie niezależności organów ochrony danych wpłynęło również orzecznictwo dotyczące transferów danych do państw trzecich, np. wyrok TSUE C-362/14, Schrems I.

⁶⁴⁴ *Article 8 [in:] The EU Charter of Fundamental Rights: A Commentary*, ed. by S. Peers, T. Hervey, J. Kenner et al. Oxford 2021, Nb 08.192. Inny podział proponowała M. Sakowska-Baryła, wyodrębniając element kadencyjności: 1) niezależność funkcjonalna; 2) niezależność organizacyjna; 3) niezależność kadrowa; 4) niezależność finansową i budżetową; 5) niezależność wynikająca z kadencyjności; por. *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, Nb 4.

nadzorowanych, ale także pośredniego i bezpośredniego od innych organów administracji publicznej, w tym przez nadzór lub kontrolę administracji rządowej⁶⁴⁵. Chociaż rozwiązania przyjęte w RODO stanowią próbę zagwarantowania tak pojmowanej niezależności, to jednak do państw członkowskich należy ustanowienie konkretnych rozwiązań ustrojowych i proceduralnych, aby ją wdrożyć. Ocena spełnienia przymiotu niezależności przez poszczególne organy nadzorcze powinna być dokonywana dla każdego z państw członkowskich z osobna przy uwzględnieniu pozycji ustrojowej tych organów ochrony danych, ponieważ wpływ na tę ocenę może mieć sposób ukształtowania struktury administracji publicznej i relacji między organami w strukturze oraz model kontroli sądowej nad działalnością administracji publicznej.

W literaturze wyróżniono cztery elementy gwarantujące niezależność organu zgodnie z art. 52 RODO: wolność od jakiegokolwiek zewnętrznego wpływu, w tym niezwracanie się o instrukcje ani ich nieprzyjmowanie (art. 52 ust. 2 RODO), zakaz podejmowania przez członków organu niewłaściwych czynności, które mogłyby doprowadzić zwłaszcza do konfliktu interesów (art. 52 ust. 3 RODO), konieczność zapewnienia odpowiednich co do wysokości i sposobu wydzielenia zasobów finansowych i osobowych (art. 52 ust. 4-5 RODO) w połączeniu z ustaleniem granic finansowej kontroli i obowiązku ustanowienia odrębnego budżetu rocznego dla organu (art. 52 ust. 6 RODO)⁶⁴⁶. Element wolności od zewnętrznych wpływów został przedstawiony wyżej. Kwestią fundamentalną dla tej wolności jest ustanowienie transparentnej procedury wyboru członków organów, stąd też prawodawca unijny dokonał analizowanego powyżej ograniczenia swobody prawodawcy krajowego w tym zakresie, w tym także w odniesieniu do minimalnej, czteroletniej kadencji i zawężenia przyczyn przymusowego pozbawienia funkcji.

Istotnym praktycznym wyzwaniem zapewnienia niezależności organów jest obowiązek zapewnienia przez państwa członkowskie, aby organy te dysponowały „zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień, w tym w zakresie wzajemnej pomocy, współpracy i uczestnictwa w pracach” EROD (art. 52 ust. 4 RODO). Jeszcze przed wejściem w życie RODO problem głębokiego niedofinansowania organów ochrony danych był

⁶⁴⁵ Wyrok TSUE C-518/07, Komisja przeciwko Niemcom, p. 30.

⁶⁴⁶ T. Zerdick, *Article 52 Independence* [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Ch. Kuner et al., by Oxford 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 2.01.2024 r), s. 880.

sygnalizowany w literaturze⁶⁴⁷. Po wejściu w życie RODO ta sytuacja uległa nieznacznej poprawie⁶⁴⁸. Natomiast z analizy raportu przygotowanego przez EROD „Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities” („Przegląd zasobów udostępnionych organom ochrony danych przez państwa członkowskie oraz działań organów ochrony danych w zakresie egzekwowania przepisów”)⁶⁴⁹ (sierpień 2021 r.) wynika, że tylko 5 organów krajowych (18%) jest zdania, że przyznany budżet jest wystarczający do realizacji ich kompetencji, a tylko 4 organy (14%), że posiadane zasoby ludzkie są wystarczające. Oznacza to, że zapewnienie przez państwa członkowskie elementu finansowej i osobowej niezależności nie jest w pełni realizowane. Ma to wpływ nie tylko na przymiot niezależności tych organów, ale także na efektywność, z jaką organy te mogą realizować swoje kompetencje.

Tymczasem te kompetencje unormowane zostały szeroko w RODO (por. motyw 129 RODO). Już art. 51 RODO przyznaje organom kompetencję ogólną, to jest: monitorowanie stosowania RODO w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwianie swobodnego przepływu danych osobowych w UE (powtórzoną z uzupełnieniem o „egzekwowanie” jako zadanie tych organów w art. 57 ust. 1 lit. a RODO). U. Góral i P. Makowski słusznie twierdzą, że termin „monitorowanie” należy odnosić do aktywnego podejmowania działań przez organ, co zasadniczo wynika również z określeń w innych wersjach językowych RODO, np. termin *surveiller* w wersji francuskiej oznaczający „czuwanie”, ale także „przeprowadzanie inspekcji”⁶⁵⁰. Natomiast szczególne kompetencje organów nadzorczych ustanowione zostały w dwóch (niewyczerpujących) jednostkach redakcyjnych – uprawnienia w art. 58 RODO⁶⁵¹, a zadania w art. 57 RODO. Prawodawca unijny wprowadził podział uprawnień na dotyczące postępowań (art. 58 ust. 1 RODO), naprawcze (art. 58 ust. 2 RODO) i w zakresie wydawania zezwoleń

⁶⁴⁷ Por. A. Dmochowska, M. Zadrożny, *Rozdział IX, pkt 1* [w:] A. Dmochowska, M. Zadrożny, *Unijna reforma ochrony danych osobowych. Analiza zmian*, SIP Legalis.

⁶⁴⁸ P. Litwiński, *Krajowy, czy europejski organ nadzorczy w sprawach ochrony danych osobowych?*, dodatek MoP 2020, nr 28 (23), s. 54, SIP Legalis.

⁶⁴⁹ EROD, *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities*, 5.08.2021, https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf (dostęp: 15.09.2024 r.). Znaleźnienie tego źródła inspirowane było artykułem: P. Litwiński, *Krajowy, czy europejski organ nadzorczy w sprawach ochrony danych osobowych?*, dodatek MoP 2020, nr 28 (23), s. 54-59, SIP Legalis.

⁶⁵⁰ Podobnie w wersji niemieckiej, angielskiej i hiszpańskiej. Por. U. Góral, P. Makowski [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 51, pkt 5, SIP LEX.

⁶⁵¹ Por. P. Hajduk, *The Powers of the Supervisory Body in the GDPR as a Basis for Shaping the Practices of Personal Data Processing*. RECoL 2021, Vol. 45, No. 2, <https://doi.org/10.31743/recl.10733> (dostęp: 7.09.2024 r.), s. 45-57.

i doradcze (art. 58 ust. 3 RODO), pozostawiając prawodawcy krajowemu możliwość przyznania innych uprawnień (art. 58 ust. 6 RODO), a także zobowiązując go do ustanowienia zabezpieczeń (w tym prawa do środka ochrony prawnej przed sądem) oraz instrumentów umożliwiających efektywne ich stosowanie (art. 58 ust. 4-6 RODO). Dwadzieścia dwa zadania organów nadzorczych unormowano w art. 57 RODO, w podobnie szeroki sposób jak uprawnienia, nie dokonując jednak ich podziału. Podział taki zaproponowany został w literaturze przez P. Fajgielskiego, który wyróżnia: 1) zadania nadzorcze; 2) zadania doradcze; 3) zadania edukacyjne; 4) zadania w zakresie współpracy z innymi organami nadzorczymi i Europejską Radą Ochrony Danych; 5) inne zadania⁶⁵². Charakterystyka uprawnień i zadań organów nadzorczych, rozumianych razem jako kompetencje tych organów, dokonana zostanie z wykorzystaniem typologii tych kompetencji sformułowanej w podrozdziale 3.3. Celem nie jest jednak dokonanie wyczerpującej analizy wszystkich kompetencji, lecz dokonanie syntezy w taki sposób, aby przybliżyło to do weryfikacji głównej hipotezy badawczej niniejszej rozprawy.

Kompetencje proceduralne obejmują prowadzenie postępowań w sprawie stosowania RODO (art. 57 ust. 1 lit. h RODO), w tym żądanie dostarczenia informacji od administratorów i podmiotów przetwarzających (art. 58 ust. 1 lit. a RODO) i prowadzenie audytów ochrony danych (art. 58 ust. 1 lit. b RODO) oraz kontroli (art. 58 ust. 1 lit. e-f RODO), przegląd certyfikacji (art. 58 ust. 1 lit. c RODO), a także zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia RODO (art. 58 ust. 1 lit. d RODO). Wykonywanie kompetencji proceduralnych prowadzi do możliwości zastosowania kompetencji naprawczych wobec administratorów i podmiotów przetwarzających, które obejmują m.in. wydawanie ostrzeżeń i upomnień (art. 58 ust. 2 lit. a i b RODO); nakazanie spełnienia żądań podmiotów danych (art. 58 ust. 2 lit. c RODO), dostosowania operacji przetwarzania (art. 58 ust. 2 lit. d RODO) i zawiadomienia o naruszeniu ochrony danych (art. 58 ust. 2 lit. e RODO); wprowadzanie czasowych lub całkowitych ograniczeń w przetwarzaniu (art. 58 ust. 2 lit. f RODO); cofnięcie certyfikacji (art. 58 ust. 2 lit. h RODO), nakazanie zawieszenia przepływu danych do państwa trzeciego (art. 58 ust. 2 lit. j RODO) i nakładanie

⁶⁵² P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2022, art. 57, pkt 3. Inny, bardziej rozbudowany podział na 10 typów proponuje M. Sakowska-Baryła w M. Sakowska-Baryła, Komentarz do art. 57 [w:] Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018, nb 2, SIP Legalis.

administracyjnych kar pieniężnych (art. 58 ust. 2 lit. i RODO). Warunki tej ostatniej kompetencji doprecyzowane są w art. 83 RODO przez unormowanie indywidualizacji kary, przesłanek jej kalkulacji, czynności współukaranych i potencjalnie wielomilionowych kar maksymalnych, kalkulowanych w odniesieniu do przedsiębiorstw w sposób alternatywny – jako określona kwota, albo jako procent całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, przy czym nakłada się karę wyższą⁶⁵³.

Osobny typ kompetencji stanowią kompetencje do wydawania zezwoleń. Dotyczą one przede wszystkim instrumentów prawnych, jak kodeksy postępowania i certyfikacja, które wprowadzone zostały do RODO, aby zmniejszyć niepewność prawną po stronie administratorów i podmiotów przetwarzających działających w różnych sektorach gospodarki (por. motywy 81 i 98 RODO), ułatwiając im zapewnienie zgodności ich działalności z RODO. Funkcją tych kompetencji organów jest najczęściej zatwierdzenie dokumentu (np. kodeksu postępowania zgodnie z art. 40 ust. 5 RODO), czego konsekwencją jest nabranie przez te dokumenty określonej mocy prawnej, która wynika dla niego z RODO. Do tych kompetencji, oprócz przykładu kodeksów postępowania, zaliczyć można m.in. akredytowanie na mocy art. 43 RODO podmiotów certyfikujących (art. 58 ust. 3 lit. e RODO i art. 57 ust. 1 pkt p RODO), udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji na mocy art. 42 ust. 5 RODO (art. 58 ust. 3 lit. f RODO art. 57 ust. 1 pkt n RODO) i zatwierdzanie wiążących reguł korporacyjnych (art. 58 ust. 3 lit. j RODO i art. 57 ust. 1 pkt s RODO).

Organy nadzorcze dysponują rozbudowanymi kompetencjami doradczymi, informacyjnymi i edukacyjnymi. Obejmują one m.in. wydawanie opinii dla organów prawodawczych, wykonawczych i społeczeństwa w sprawach związanych z ochroną danych osobowych (art. 58 ust. 3 lit. a RODO), w tym w sprawie aktów prawnych (art. 57 ust. 1 lit. c RODO), udzielanie porad podmiotom danych o ich prawach (art. 57 ust. 1 lit. e RODO) i administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 36 RODO (art. 58 ust. 3 lit. a RODO), monitorowanie rozwój technik informacyjno-komunikacyjnych i praktyk handlowych, które mają wpływ na ochronę danych osobowych (art. 57 ust. 1 lit. i RODO), a także upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o ich obowiązkach wynikających z RODO (art. 57 ust. 1 lit. d RODO). Uwagę zwraca, że ten typ kompetencji jest rozbudowany, a sposób sformułowania przepisów pozwala organom

⁶⁵³ M. Sakowska-Baryła [w:] M. Sakowska-Baryła, *Komentarz do art. 83 [w:] Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, nb. 2-6, SIP Legalis.

nadzorczym na wydawanie opinii w sprawach, które są tylko „związane” z ochroną danych osobowych, zatem wystarczające jest, aby sprawy te miały „element łączący”⁶⁵⁴ je z tą ochroną.

W ostatniej części tego podrozdziału analizie poddana zostanie właściwość organów nadzorczych (art. 55 RODO) i właściwość wiodącego organu nadzorczego w sprawach transgranicznych (art. 56 RODO) omówione zostaną poniżej. Pozwoli to także na omówienie kompetencji współpracy między organami nadzorczymi, na które prawodawca unijny nałożył obowiązek przyczyniania się do spójnego stosowania RODO (art. 51 ust. 2 RODO i art. 57 ust. 1 lit. g RODO). Art. 55 RODO wprowadza regułę, zgodnie z którą organy nadzorcze właściwe są „do wypełniania zadań i wykonywania uprawnień” (kompetencji) na terytorium swojego państwa członkowskiego, co decyduje o wyznaczeniu właściwości miejscową. Wyjątkiem od tej reguły jest art. 56 RODO ustanawiający właściwość wiodącego organu nadzorczego (organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego) dla działań względem transgranicznego przetwarzania danych w ramach instrumentu *one-stop shop* (analiza tego zagadnienia niżej). Zgodnie jednak z art. 55 ust. 2 RODO, art. 56 RODO nie ma zastosowania (co oznacza wyłączną właściwość organów nadzorczych na terytorium swojego państwa członkowskiego) w przypadku, gdy przetwarzanie dokonywane jest organy publiczne danego państwa członkowskiego, albo podmioty prywatne, a przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na takim administratorze lub w ramach sprawowania władzy publicznej powierzonej takiemu administratorowi (art. 6 ust. 1 lit. c i e RODO).

Wyjaśnienia wymaga pojęcie wiodącego organu nadzorczego. Intencją prawodawcy unijnego wobec zintensyfikowanego transgranicznego przetwarzania danych było ustanowienie w RODO takich rozwiązań proceduralnych, które ułatwiałyby transgraniczną działalność administratorów i podmiotów przetwarzających, jednocześnie wzmacniając spójność stosowania RODO⁶⁵⁵. Dlatego też wprowadzony został instrument *one-stop shop* (kompleksowa obsługa). Jego istotą jest, że administrator i podmiot przetwarzający transgranicznie przetwarzający dane są zasadniczo nadzorowani przez jeden organ nadzorczy w całej UE – organ nadzorczy ich głównej lub pojedynczej jednostki organizacyjnej. Rozbudowana definicja legalna głównej jednostki organizacyjnej zawarta została w art. 4 pkt 16 RODO, a pojęcie to jest przedmiotem wytycznych EROD „Wytyczne 8/2022

⁶⁵⁴ Związywać, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/slowniki/zwiazany.html> (dostęp: 15.09.2024 r.).

⁶⁵⁵ M. Piech, One stop shop. Mechanizmy podejmowana decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE, MoP 2016, nr 20, s. 82.

dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego” z marca 2023 r.⁶⁵⁶. W uproszczeniu, główna jednostka organizacyjna administratora i podmiotu przetwarzającego znajduje się w państwie, w którym znajduje się ich centralna administracja w UE, chyba że decyzje co do celów i sposobów przetwarzania zapadają w innej jednostce w UE⁶⁵⁷. Jeżeli podmiot przetwarzający nie ma centralnej administracji w UE, to jego główna jednostka organizacyjna jest tam, gdzie jednostka organizacyjna tego podmiotu, w której odbywają się główne czynności przetwarzania.

Do transgranicznego przetwarzania danych osobowych dochodzi w dwóch przypadkach zgodnie z art. 4 pkt 23 RODO. Pierwszy, kiedy przetwarzanie odbywa się w ramach działalności jednostek organizacyjnych administratora lub podmiotu przetwarzającego posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim, jest najczęstszy. Drugi ma miejsce, kiedy przetwarzanie odbywa się w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w UE, ale znacznie wpływa lub może znacznie wpłynąć na podmioty danych w więcej niż jednym państwie. RODO nie precyzuje znaczenia określeń „znacznie wpływa” i „może znacznie wpłynąć”. Są one natomiast przedmiotem analizy w wytycznych EROD, które wskazują, że sama skala przetwarzania (liczba podmiotów danych, których dane są przetwarzane) nie decyduje jeszcze o spełnieniu tej przesłanki. Do jej oceny należy brać pod uwagę kontekst przetwarzania, rodzaj danych, cel przetwarzania danych i, przede wszystkim, ryzyka dla praw i wolności osób fizycznych związane z konkretnym przetwarzaniem⁶⁵⁸.

Istotą procedury *one-stop shop* jest to, że w odniesieniu do transgranicznego przetwarzania danych tylko wiodący organ nadzorczy stosuje RODO w odniesieniu do administratora i podmiotu przetwarzającego dokonującego takie przetwarzania, jednak przy współpracy z krajowymi organami, których sprawach dotyczy (art. 60 ust. 1-11 RODO)⁶⁵⁹. Definicja tych organów w art. 4 ust. 22 RODO wskazuje na trzy przypadki, w których sprawa

⁶⁵⁶ EROD, *Wytyczne 8/2022 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego*, https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202208_identifying_lsa_targeted_update_pl.pdf (dostęp: 15.09.2024 r.).

⁶⁵⁷ Por. także Wyrok TSUE, C-230/14, Weltimmo s.r.o.

⁶⁵⁸ Więcej na s. 5-6 przywołanych wytycznych. EROD, *Wytyczne 8/2022 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego*, https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202208_identifying_lsa_targeted_update_pl.pdf, (dostęp: 15.09.2024 r.).

⁶⁵⁹ EROD, *Wytyczne 02/2022 w sprawie stosowania art. 60 RODO*, https://www.edpb.europa.eu/system/files/2022-10/guidelines_202202_on_the_application_of_article_60_gdpr_pl.pdf (dostęp: 15.09.2024 r.), s. 1.

dotyczy organu: 1) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium danego państwa; 2) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na podmioty danych na terytorium danego państwa; 3) wniesiono do tych organów skargę⁶⁶⁰. W uproszczeniu, organy te biorą udział w procedurze wydawania decyzji przez wiodący organ. W przypadku uzasadnionego sprzeciwu organu, którego sprawa dotyczy wobec projektu decyzji wiodącego organu, organ ten przekazuje sprawę do EROD w ramach mechanizmu spójności (który poddany został analizie w pkt 3.4.1. powyżej), aby EROD rozstrzygnął spór między organami co do treści decyzji⁶⁶¹ (art. 60 ust. 4 RODO). Procedura *one-stop shop*, będąca *novum* względem Dyrektywy ODO, była przedmiotem krytyki w literaturze w ostatnich latach z uwagi, zwłaszcza z perspektywy ryzyka występowania zjawiska *forum shopping*⁶⁶².

RODO przewiduje także inne, oprócz procedury *one-stop shop*, instrumenty współpracy horyzontalnej między krajowymi organami nadzorczymi. Unormowane zostały w art. 61 RODO (Wzajemna pomoc) i art. 62 RODO (Wspólne operacje organów nadzorczych), które przewidują także skutki braku tej współpracy w odpowiednim terminie, np. zastosowanie środka tymczasowego zgodnie z art. 55 RODO przez organ, który zwrócił się z pierwotnym wnioskiem. Wzajemna pomoc obejmuje m.in. wymianę informacji i stosowanie środków nadzorczych, takich jak przeprowadzenie uprzednich konsultacji oraz wnioski o przeprowadzenie kontroli i postępowań wyjaśniających (art. 61 ust. 1 RODO). Z kolei wspólne operacje to możliwość przeprowadzania wspólnych postępowań i działań egzekucyjnych, w których bierze udział personel organów nadzorczych kilku państw członkowskich (art. 62 ust. 1-5 RODO). Te instrumenty współpracy horyzontalnej między krajowymi organami nadzorczymi należy ocenić jako rozbudowane i względnie szczegółowe w porównaniu do instrumentów takiej współpracy poddanej analizie w tym rozdziale.

3.5.1.2. UODO

⁶⁶⁰ Por. L. Chemlali, The competence of non-lead supervisory authority under the EU GDPR'S one-stop-shop mechanism: CJEU judgment in Facebook and Others (C-645/19), „Journal of Media Law” 2022, Vol. 14, No. 2, <https://doi.org/10.1080/17577632.2022.2109852> (dostęp: 20.09.2024 r.), s. 208-217.

⁶⁶¹ Por. A. Giurgiu, T. A. Larsen, Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?, EDPL 2016, Vol. 2, No. 3., s. 349-350.

⁶⁶² Krytyka ta scharakteryzowana została w podrozdziale 3.4.1. w kontekście mechanizmu spójności, który stanowi część procedury *one-stop shop*.

Krajowy organ nadzorczy w rozumieniu RODO ustanowiony został w Polsce na podstawie UODO. Zgodnie z art. 34 ust. 1 i 2 UODO jest nim Prezes Urzędu Ochrony Danych Osobowych (PUODO), który jest także organem właściwym „w sprawie ochrony danych osobowych” oraz m.in. Dyrektywy LED. PUODO jest jednoosobowym i centralnym organem administracji publicznej, co jest zasadniczo powszechnie przyjmowane w doktrynie⁶⁶³. W literaturze dyskutowane jest natomiast czy PUODO jest niezależnym organem regulacyjnym podobnym do organów regulacyjnych w sektorze transportu kolejowego czy energetycznym⁶⁶⁴. Abstrahując od dyskusji na temat zasadności wyodrębnienia i cech charakterystycznych niezależnych organów nadzorczych, wydaje się, że chociaż PUODO jako organowi nadzorcemu przysługuje szczególna niezależność wynikająca z pierwotnego i wtórnego prawa UE (scharakteryzowana powyżej), to jednak fakt, że zakres przedmiotowy RODO ma horyzontalny charakter obejmujący nie tylko cały sektor prywatny, ale i sektor publiczny powoduje, że nie można kwalifikować PUODO jako organu regulacyjnego. Jego niezależność powinna być raczej łączona ze szczególną rolą, jaką odgrywa jako element instytucjonalny prawa do ochrony danych osobowych w powiązaniu z prawem prywatności. Dlatego też zasadnie byłoby zaliczyć PUODO jako organ ochrony prawnej, chociaż i to kwestionowane jest w literaturze⁶⁶⁵.

UODO dokonuje operacjonalizacji RODO do polskiego porządku prawnego, przy czym, jak wskazano powyżej, zasadniczo pozycja i kompetencje organu nadzorczego określone zostały bezpośrednio w RODO⁶⁶⁶. PUODO, zgodnie z art. 34 ust. 3 UODO, jest powoływany i odwoływany Sejm za zgodą Senatu Rzeczypospolitej Polskiej na czteroletnią kadencję (art. 34 ust. 6 UODO), a ta sama osoba nie może być PUODO przez więcej niż dwie kadencje (art. 34 ust. 7 UODO). Zgodnie z art. 34 ust. 5 UODO, Prezes Urzędu w zakresie wykonywania swoich zadań podlega tylko ustawie, co oznacza, że inne organy nie mogą mieć żadnego wpływu na

⁶⁶³ E. Kuczma, *Generalny Inspektor Ochrony Danych Osobowych jako organ ochrony prawa do prywatności*, 2017. Rozprawa doktorska niepublikowana. https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/5975/1/E_Kuczma_Generalny_Inspektor_Ochrony_Danych_Osobowych_jako_organ_ochrony_prawa_do_prywatnosci.pdf (dostęp: 15.09.2024 r.), s. 207-208 i przywołana tam literatura.

⁶⁶⁴ K. Rokita, Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych, EPS 2016, nr 7, s. 5-6.

⁶⁶⁵ E. Kuczma, P. Kuczma, *Generalny Inspektor Ochrony Danych Osobowych jako organ kontroli i ochrony prawa*, Zeszyty Naukowe DWSPiT. Studia z Nauk Społecznych, 2013, nr 6, s. 211-212.

⁶⁶⁶ Rozdział I. Ochrona danych osobowych obywateli jako zadanie państwa w dziedzinie bezpieczeństwa. 4. Status ustrojowy PUODO [w:] J. Kurek, J. Taczowska-Olszewska, *Ochrona danych osobowych jako realizacja zadań w obszarze bezpieczeństwa państwa*, Warszawa 2020, SIP Legalis.

wykonywanie kompetencji przez PUODO⁶⁶⁷. Powody odwołania przed upływem kadencji ograniczone zostały do zamkniętego katalogu pięciu przypadków: 1) zrzeczenia się stanowiska; 2) trwałej niezdolności do pełnienia obowiązków na skutek choroby stwierdzonej orzeczeniem lekarskim; 3) sprzeniewierzenia się ślubowaniu; 4) skazanie prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego; 5) pozbawienia praw publicznych. Do rozwiązań stanowiących gwarancję niezależności PUODO zaliczają w literaturze także: samodzielność w doborze zastępców (art. 36 OchrDanychU), zakaz podejmowania aktywności wymienionej w art. 37 UODO, która mogłaby spowodować zwłaszcza konflikt interesów, przyznanie PUODO immunitetu (art. 38-44 UODO)⁶⁶⁸ i kompetencji do nadawania Urzędowi Ochrony Danych Osobowych statutu, określającego m.in. organizację wewnętrzną Urzędu (art. 45 ust. 3 UODO).

Przy PUODO powinna zostać, zgodnie z art. 48 UODO, ustanowiona 8-osobowa Rada do Spraw Ochrony Danych Osobowych, która byłaby organem opiniodawczo-doradczym. Do zadań Rady powinno należeć m.in. opiniowanie projektów dokumentów organów i instytucji UE, krajowych aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych; opracowywanie propozycji rekomendacji określających środki techniczne i organizacyjne wykorzystywane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Do dnia złożenia rozprawy rada ta nie została powołana. Niepowołanie jej należy ocenić negatywnie, ponieważ jej działalność mogłaby wzmocnić spójne stosowanie RODO i UODO w Polsce. Jednak od czerwca 2024 r. powołany został i działa opiniodawczy i doradczy Społeczny Zespół Ekspertów przy PUODO, którego zadania zbliżone są do zadań Rady do Spraw Ochrony Danych Osobowych⁶⁶⁹. Z tym zespołem wiązać można zatem oczekiwania dotyczące zwiększenia spójności stosowania RODO, jakie wiązać można byłoby z tą radą.

PUODO na podstawie art. 50 UODO zobowiązany jest sporządzić coroczne sprawozdanie z działalności, które przedstawia Sejmowi, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka i Prokuratorowi Generalnemu. Sprawozdanie

⁶⁶⁷ Ustawa o ochronie danych osobowych. Komentarz, Komentarz do art. 34, red. P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe*. Komentarz, red. P. Litwiński, pkt 17, SIP Legalis.

⁶⁶⁸ Por. K. Jabłonka-Jankowska, *Komentarz do art. 34* [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. M. Czerniawski, M. Kawecki, Warszawa 2019, pkt 6, SIP Legalis.

⁶⁶⁹ Zarządzenie nr 13/2024 Prezesa Urzędu Ochrony Danych Osobowych z dnia 4 czerwca 2024 r. w sprawie: ustanowienia Społecznego Zespołu Ekspertów przy Prezesie Urzędu Ochrony Danych Osobowych, <https://uodo.gov.pl/583#:~:text=Spo%C5%82eczny%20Zesp%C3%B3%C5%82%20Ekspert%C3%B3w%20przy%20Prezesie%20Ur%C4%99du%20Ochrony%20Danych%20Osobowych%20zosta%C5%82,cia%C5%82em%20opiniodawczo%2Ddoradczym%20Prezesa%20Ur%C4%99du> (dostęp: 15.09.2024 r.).

to stanowi istotne źródło informacji o działalności organu. Przykładowo, ze sprawozdania za rok 2022 wynika, że liczba skarg wniesionych do WSA na decyzje PUODO wzrosła do 194 w porównaniu z 177 skargami wniesionymi w 2021 r.⁶⁷⁰, a PUODO wszczął 59 postępowań administracyjnych z urzędu⁶⁷¹ i wydał 25 decyzji w związku ze stwierdzeniem naruszenia ochrony danych, w większości udzielając (16) upomnienia. PUODO nałożył także 9 administracyjnych kar pieniężnych⁶⁷² w łącznej kwocie ponad 7,5 miliona złotych, co stanowi ponad 3-krotny wzrost względem roku 2021⁶⁷³.

Kompetencje szczególne PUODO w kontekście kompetencji ogólnej organu nadzorczego z art. 51 ust. 1 RODO zostały doprecyzowane przez ustawodawcę w art. 51-52 UODO. Do tych kompetencji PUODO należy zaliczyć m.in. opiniowanie założeń i projektów aktów prawnych dotyczące danych osobowych (art. 51 UODO), kierowanie wystąpień do wszelkich podmiotów zmierzające do zapewnienia skutecznej ochrony danych osobowych, w tym także kierowanie wniosków o podjęcie inicjatywy ustawodawczej w sprawach dotyczących ochrony danych osobowych (art. 52 UODO), przy czym do wystąpień tych nie stosuje się KPA⁶⁷⁴. Z kolei na podstawie art. 53 ust. 1 pkt 4 UODO, PUODO zobowiązany jest udostępniać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, gdy projekty wymagają uprzedniej konsultacji podmiotami, których działalności mają dotyczyć.

Jak wskazano wyżej, UODO dokonuje operacjonalizacji RODO do polskiego porządku prawnego zarówno przez wprowadzenie norm administracyjnego prawa ustrojowego, jak i prawa procesowego. Postępowanie przed PUODO jest jednoinstancyjne, co w literaturze oceniono jako uzasadniony wyjątek od zasady dwuinstancyjności postępowań wyrażonej w art. 78 Konstytucji RP⁶⁷⁵. Zasadniczo do postępowań administracyjnych przed PUODO stosuje się przez odesłanie KPA (art. 7 ust. 1 UODO) w sprawach nieuregulowanych

⁶⁷⁰ Sprawozdanie z działalności Prezesa UODO w roku 2022, <https://uodo.gov.pl/pl/file/4404>, s. 22 (dostęp: 15.09.2024 r.).

⁶⁷¹ Sprawozdanie z działalności Prezesa UODO w roku 2022, <https://uodo.gov.pl/pl/file/4404>, s. 134 (dostęp: 15.09.2024 r.).

⁶⁷² Sprawozdanie z działalności Prezesa UODO w roku 2022, <https://uodo.gov.pl/pl/file/4404>, s. 134 (dostęp: 15.09.2024 r.).

⁶⁷³ Sprawozdanie z działalności Prezesa UODO w roku 2022, <https://uodo.gov.pl/pl/file/4404>, s. 138 (dostęp: 15.09.2024 r.).

⁶⁷⁴ O. Legat [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Warszawa 2018, art. 52, pkt 4, SIP LEX.

⁶⁷⁵ I. Bogucka [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, art. 7, pkt 6 SIP LEX.

w UODO, zatem subsydiarnie⁶⁷⁶. Znajduje to zastosowanie do postępowań w sprawie: certyfikacji (art. 42-43 RODO); kodeksów postępowań (art. 40-41 RODO); wiążących reguł korporacyjnych (art. 47 RODO); zezwoleń na transfery danych do państw trzecich zgodnie z art. 46 ust. 3 RODO; naruszeń ochrony danych osobowych i nakładania administracyjnych kar pieniężnych⁶⁷⁷.

Niektóre elementy procedury uregulowane zostały odrębnie przez UODO. W rozdział 7 unormowano postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. Następnie, w rozdziale 8 ustanowiono przepisy dotyczące europejskiej współpracy administracyjnej, w tym możliwość stosowania środków tymczasowych zgodnie z rozdział VII RODO „Współpraca i spójność” (art. 75 ust. 1 UODO), a w rozdziale 9 uregulowano procedurę kontroli prowadzonych przez PUODO. Z perspektywy kompetencji naprawczych kluczowy jest rozdział 11 UODO normujący nakładanie administracyjnych kar pieniężnych. Administracyjne kary pieniężne nakładane są w drodze decyzji administracyjnej (art. 101 i art. 123 UODO). UODO wyłącza zastosowanie art. 189d-189f i art. 189k KPA (dyrektywy wymiaru, podstawy odstąpienia i ulgi w wykonaniu administracyjnej kary pieniężnej oraz siłę wyższą), ponieważ te zagadnienia unormowane są bezpośrednio w RODO. Zastosowanie mają natomiast pozostałe przepisy działu IVa KPA (Administracyjne kary pieniężne), w tym dotyczące definicji administracyjnej kary pieniężnej, przedawnienia i przerwania oraz zawieszenia terminu przedawnienia⁶⁷⁸.

3.5.2. GENERALNY INSPEKTOR INFORMACJI FINANSOWEJ

Na poziomie unijnym kwestie kompetencji organów administracji publicznej w obszarze AML są uregulowane przede wszystkim w Dyrektywie AML IV i V⁶⁷⁹, które scharakteryzowane zostanie jedynie w ograniczonym zakresie. Dyrektywy AML V nakłada na państwa członkowskie w rozdziale IV (Obowiązki zgłaszania) sekcji 1 obowiązek ustanowienia jednostek analityki finansowej (*Financial Intelligence Units*), których celem jest „zapobieganie przypadkom prania pieniędzy i finansowania terroryzmu, wykrywania takich

⁶⁷⁶ I. Bogucka [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, art. 7, pkt 1-2 SIP LEX.

⁶⁷⁷ Por. A. Dmochowska [w:] A. Dmochowska, A. Piotrowska, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, art. 7, pkt 1 SIP Legalis; I. Bogucka [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, art. 7, pkt 3 SIP LEX.

⁶⁷⁸ L. Staniszevska, 3. Postępowanie administracyjne zmierzające do nałożenia administracyjnej kary pieniężnej [w:] *Ochrona danych osobowych w prawie publicznym*, red. M. Jędrzejczak, Warszawa 2021, SIP LEX.

⁶⁷⁹ Dyrektywa AML V stanowi nowelizację Dyrektywy AML IV, stąd też dla zachowania przejrzystości przy analizie przyjęto odwołania do Dyrektywy AML V.

przypadków oraz ich skutecznego zwalczania” (art. 32 ust. 1 Dyrektywy AML V), a nadto do ustanowienia organów nadzorczych do „skutecznego monitorowania i podejmowania niezbędnych środków” z adekwatnymi kompetencjami (art. 48 Dyrektywy AML V). Jednostki analityki finansowej odpowiadają m.in. za przyjmowanie i analizowanie zgłoszeń dotyczących takich przypadków oraz informowanie o wynikach analiz właściwym organom (art. 32 ust. 3 Dyrektywy AML V). Aby realizować te kompetencje, jednostki te powinny być niezależne i odpowiednio wyposażone (art. 32 ust. 3 Dyrektywy AML V). Dodatkowo, na poziomie unijnym wprowadzono ograniczone kompetencje doradcze, informacyjne i edukacyjne (np. art. 17 Dyrektywy AML V w przedmiocie wydawania wytycznych dotyczące czynników ryzyka, które należy uwzględnić, oraz środków, które należy podjąć, w sytuacjach, gdy właściwe są uproszczone środki należytej staranności wobec klienta) oraz współpracy (np. art. 45 ust. 4 Dyrektywy AML V nakładający obowiązek wzajemnego informowania się o przypadkach, w których prawo państwa trzeciego nie pozwala na wdrożenie strategii i procedur obejmujących całą grupę zgodnie z art. 45 ust. 1; art. 49 i art. 50a) przyznane zostały Europejskiemu Urzędowi Nadzoru Bankowego (EUNB), który jest niezależnym organem UE stanowiącym część części Europejskiego Systemu Nadzoru Finansowego (ESNF)⁶⁸⁰. Celem ich przyznania jest wzmocnienie współpracy między organami w państwach członkowskich i zapewnienie spójności stosowania przepisów AML na poziomie unijnym. Kolejna z dyrektyw przyjętych w tym obszarze, Dyrektywa AML VI, nie wpływa zasadniczo na kompetencje organów właściwych w sprawach AML, ponieważ reguluje aspekty prawnokarne prania brudnych pieniędzy i finansowania terroryzmu w celu poprawy wymiany i dostępu do informacji między jednostkami analityki finansowej i podmiotami zapobiegającymi i zwalczającymi przestępczość (motyw 2 Dyrektywy AML VI).

Można spodziewać się, że pakiet zmian w unormowaniu AML w UE przyjęty w 2023 r. wpłynie na pozycję ustrojową i kompetencje jednostek analityki finansowej i organów nadzorczych na poziomie krajowym przez ich wzmocnienie, w tym przez bardziej precyzyjne uregulowanie współpracy transgranicznej. Te kwestie zostały unormowane przede wszystkim w Dyrektywie Parlamentu Europejskiego i Rady w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić, mających na celu zapobieganie wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu⁶⁸¹. Nie będzie ona przedmiotem

⁶⁸⁰ European Banking Authority, <https://www.eba.europa.eu/polski> (dostęp: 15.09.2024 r.).

⁶⁸¹ Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić, mających na celu zapobieganie wykorzystywaniu systemu finansowego do prania pieniędzy

szczegółowej analizie. Wskazane zostaną jedynie podstawowe informacje. Powołanie i działanie jednostek analityki finansowej unormowane zostało w Rozdziale III tej dyrektywy, a nadzór nad przeciwdziałaniem praniu pieniędzy, który powinien być oparty na analizie ryzyka (art. 40 tej dyrektywy), uregulowano z kolei w Rozdziale IV. Przykładowo, w tej dyrektywie wprowadzono instytucję kolegów podmiotów sprawujących nadzór ds. AML oraz odpowiednikami z państw trzecich dla nadzoru nad instytucjami kredytowymi lub finansowymi, które m.in. utworzyły zakłady w więcej niż jednym państwie członkowskim (art. 49 tej dyrektywy), co ma zastosowanie dopiero wtedy, gdy AMLA nie jest kompetentna do sprawowania tego nadzoru (art. 49 ust. 3 tej dyrektywy). Uzupełnione jest to o przepisy Rozdziału V – „Współpraca”, który dotyczy zarówno współpracy w zakresie AML (Sekcja 1 tej dyrektywy), w tym z AMLA (art. 63 tej dyrektywy), jak i współpracy z innymi organami (Sekcja 2 tej dyrektywy).

Rozwiązania przyjęte w krajowej Ustawie o AML stanowią co do zasady transpozycję Dyrektywy AML V. Zgodnie z art. 10 ust. 1 Ustawy o AML, organami administracji rządowej właściwymi w sprawach AML są jednoosobowy organ – Generalny Inspektor Informacji Finansowej (GIIF) i minister właściwy do spraw finansów publicznych jako naczelny organ informacji finansowej, którego rolą jest inicjatywa legislacyjna dotycząca AML i nadzór nad GIIF⁶⁸², a nadto jest on organem właściwym w sprawach Centralnego Rejestru Beneficjentów Rzeczywistych (art. 56 Ustawy o AML). GIIF, odgrywający w stosowaniu Ustawy o AML nadrzędną rolę wykonawczą⁶⁸³, powołuje i odwołuje Prezes Rady Ministrów na wniosek ministra właściwego do spraw finansów publicznych (art. 10 ust. 2 Ustawy o AML) na 6-letnią kadencję, przy czym ta sama osoba może być GIIF tylko przez dwie kolejne kadencje (art. 11a Ustawy o AML). GIIF jest wspomagany przez Departament Informacji Finansowej Ministerstwa, który razem z GIIF stanowi krajową jednostkę analityki finansowej⁶⁸⁴. Finansów Przesłanki odwołania GIIF przed upływem kadencji są ograniczone (art. 11b Ustawy o AML). Dodatkowo, przy GIIF działa Komitet Bezpieczeństwa Finansowego, pełniący funkcję opiniodawczą i doradczą w zakresie AML (art. 19 ust. 1 Ustawy o AML), którego członkowie

lub finansowania terroryzmu oraz uchylająca dyrektywę (UE) 2015/849. COM/2021/423 final. Wersja finalna: <https://data.consilium.europa.eu/doc/document/PE-37-2024-REV-1/pl/pdf#page=91.08> (dostęp: 31 maja 2024 r.).

⁶⁸² J. Grynfelder [w:] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, M. Nowakowski, Warszawa 2023, art. 10, pkt 2, SIP LEX.

⁶⁸³ S. Juszczak [w:] *Komentarz do ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* [w:] *Prawo obrotu pieniężnego. Komentarz*, P. Zapadka, Warszawa 2023, art. 11, pk. 1, SIP LEX.

⁶⁸⁴ Ministerstwo Finansów, Generalny Inspektor Informacji Finansowej, <https://www.gov.pl/web/finanse/generalny-inspektor-informacji-finansowej> (dostęp: 15.09.2024 r.).

obejmują szeroki krąg przedstawicieli organów administracji publicznej (art. 20 ust. 1 pkt. 3 Ustawy o AML), przy czym bez przedstawiciela PUODO.

Podstawowe kompetencje GIIF ustanowione zostały w art. 12 ust. 1 Ustawy o AML przez wskazanie ogólnej kompetencji do podejmowania działań w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, która uszczegółowiona jest następnie przez otwarty katalog kompetencji szczególnych. Te szczególne kompetencje obejmują m.in.: analizowanie informacji dotyczących wartości majątkowych, co do których GIIF powziął podejrzenie, że mają związek z przestępstwem prania pieniędzy lub finansowania terroryzmu (art. 12 ust. 1 pkt 1 Ustawy o AML); przeprowadzenie wstrzymania transakcji lub blokady rachunku (art. 12 ust. 1 pkt 2 Ustawy o AML); żądanie przekazania informacji o transakcjach i ich udostępnianie (art. 12 ust. 1 pkt 3 Ustawy o AML); przekazywanie uprawnionym organom informacji i dokumentów uzasadniających podejrzenie popełnienia przestępstwa (art. 12 ust. 1 pkt 4 Ustawy o AML); sporządzanie krajowej oceny ryzyka prania pieniędzy i finansowania terroryzmu oraz strategii przeciwdziałania tym przestępstwom (art. 12 ust. 1 pkt 6 Ustawy o AML), która obejmuje identyfikację zagadnień dotyczących ochrony danych osobowych związanych z AML (art. 29 ust. 1 pkt 6 Ustawy o AML); sprawowanie kontroli nad przestrzeganiem przepisów dotyczących AML (art. 12 ust. 1 pkt 7 Ustawy o AML); współpraca z organami innych państw i międzynarodowymi organizacjami, przede wszystkim z zagranicznymi jednostkami analityki finansowej (art. 12 ust. 1 pkt 9 Ustawy o AML); nakładanie kar administracyjnych zgodnie z Ustawą o AML (art. 12 ust. 1 pkt 10 Ustawy o AML); udostępnianie wiedzy i informacji z zakresu przepisów o AML (art. 12 ust. 1 pkt 11 Ustawy o AML) oraz przetwarzanie informacji, w tym danych osobowych, w trybie określonym w Ustawie o AML (art. 12 ust. 1 pkt 10 Ustawy o AML). Nadto, GIIF jest administratorem systemu teleinformatycznego służącego przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (art. 12 ust. 4 Ustawy o AML) niezbędnego w realizacji jego szerokich kompetencji przy uwzględnieniu znacznej liczby informacji, które są przez niego otrzymywane, przede wszystkim, od podmiotów obowiązanych na podstawie Ustawy o AML. GIIF przedstawia Prezesowi Rady Ministrów roczne sprawozdanie z działalności (art. 14 Ustawy o AML). Te kompetencje GIIF wykonuje w urzędzie ministra właściwego do spraw finansów publicznych przy pomocy wyodrębnionej komórki organizacyjnej (art. 12 ust. 2 i art. 12b Ustawy o AML).

W literaturze proponowano różne typologie tych rozbudowanych kompetencji, przyjmując kryterium ich charakteru. W. Filipkowski zaproponował wyróżnienie dwóch

typów: czynności badawczo-analityczne i czynności prewencyjne,⁶⁸⁵ którą to typologię W. Ługowski uważa za najbardziej adekwatną⁶⁸⁶. Inną typologię zaproponował A. Golonka, który dokonał podziału na trzy typy: 1) zadania związane z badaniem przebiegu transakcji; 2) uprawnienia i obowiązki związane z udostępnianiem wiedzy i informacji; 3) zadania, które są wykonywane w zakresie kontroli, oraz kompetencje w zakresie współpracy z właściwymi organami innych państw⁶⁸⁷.

Kluczowe kompetencje proceduralne i naprawcze GIIF ustanowione zostały w rozdziale 12 (Kontrolowanie instytucji obowiązanych) i w rozdziale 13 (Kary administracyjne). Zakres przedmiotowy kontroli określony został w art. 130 ust. 1 Ustawy o AML szeroko, obejmując kontrolę wykonywania przez instytucje obowiązane obowiązków w zakresie AML. Z kolei tryb i zasady nakładania kar administracyjnych uregulowane zostały w rozdziale 13 Ustawy o AML. Art. 147 Ustawy o AML wskazuje dwadzieścia obowiązków, których niedopełnienie przez instytucje obowiązków stanowi podstawę do nałożenia takiej kary. Jest to m.in.: brak wyznaczenia osoby odpowiedzialnej za wykonanie obowiązków określonych w Ustawie o AML (art. 147 pkt. 1 Ustawy o AML); brak sporządzania oceny ryzyka i jej aktualizacji (art. 147 pkt. 2 Ustawy o AML); niezastosowanie środków bezpieczeństwa finansowego, o których mowa w Ustawie o AML (art. 147 pkt. 3 Ustawy o AML); brak dokumentowania zastosowanych środków bezpieczeństwa finansowego oraz wyników bieżącej analizy przeprowadzanych transakcji i brak wykazania na żądanie organów zastosowania odpowiednich środków bezpieczeństwa (art. 147 pkt. 5 Ustawy o AML); wprowadzenia wewnętrznych procedur dla instytucji obowiązanej i grupy (art. 147 pkt. 7, 8 i 10 Ustawy o AML). Z kolei artykuł 148 i 149 Ustawy o AML w sposób szczegółowy przewiduje możliwość nałożenia kary administracyjnej za niedopełnienie przez instytucje obowiązków wynikających z rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/847 z dnia 20 maja 2015 r. w sprawie informacji towarzyszących transferom środków pieniężnych i uchylenia rozporządzenia (WE) nr 1781/2006⁶⁸⁸ (art. 148 Ustawy o AML) oraz obowiązków w zakresie użycia szczególnych środków ograniczających (art. 149 Ustawy o AML). Katalog

⁶⁸⁵ W. Filipkowski, *Zwalczanie przestępczości zorganizowanej w aspekcie finansowym*, Kraków 2004, s. 283. Cytowanie za: W. Ługowski [w:] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu*. Komentarz, W. Kapica, Warszawa 2020, art. 12, SIP LEX.

⁶⁸⁶ W. Ługowski [w:] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu*. Komentarz, W. Kapica, Warszawa 2020, art. 12, SIP LEX.

⁶⁸⁷ A. Golonka, *Prawnokarne zagadnienia wprowadzania do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł*, Rzeszów 2008, s. 133. Cyt. za: Krzywka [w:] *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*. Komentarz, red. M. Dyl, M. Królikowski, Warszawa 2021, art. 12, SIP Legalis.

⁶⁸⁸ Dz. Urz. UE L 141, 5.6.2015, p. 1–18.

kar administracyjnych przyjęty w art. 150 ust. 1 Ustawy o AML obejmuje 5 form kary, m.in. nakaz zaprzestania podejmowania przez instytucję obowiązaną określonych czynności; cofnięcie koncesji lub zezwolenia i kary pieniężne. Kara pieniężna może zostać nałożona co do zasady do wysokości dwukrotności kwoty korzyści osiągniętej lub straty unikniętej przez instytucję obowiązaną w wyniku naruszenia (art. 150 ust. 2 Ustawy o AML), natomiast w odniesieniu do niektórych instytucji obowiązanych (można w uproszczeniu określić je jako najważniejsze), kara może sięgnąć nawet do wysokości równowartości kwoty 5 mln euro albo do wysokości 10% obrotu (art. 150 ust. 3 Ustawy o AML).

Dodatkowo, wymaga wskazania, że kompetencje proceduralne (kontrolowanie instytucji obowiązanych) i naprawcze (nakładanie kar administracyjnych) mają w odniesieniu do sektorowych instytucji obowiązanych sektorowe organy administracji publicznej w ramach sprawowanego nadzoru lub kontroli, to jest: Prezes Narodowego Banku Polskiego (NBP) w odniesieniu do podmiotów prowadzących działalność kantorową; Komisja Nadzoru Finansowego (KNF) – do instytucji przez nią nadzorowanych; Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa (KSKOK) – do spółdzielczych kas oszczędnościowo-kredytowych; prezesi sądów apelacyjnych – do notariuszy i naczelnicy urzędów celno-skarbowych – do kontrolowanych przez nich instytucji obowiązanych (art. 130 ust. 2 i art. 151 ust. 1-3 Ustawy o AML).

Pomimo że w Ustawie o AML termin „dane osobowe” (w mianowniku lub w deklinacji) użyty został 39 razy⁶⁸⁹, to na możliwość współpracy między GIIF i PUODO wskazano wprost w ograniczonym zakresie, tj. w art. 116b ust. 4 Ustawy o AML. Zgodnie z nim, w związku z weryfikacją zgodności przetwarzania danych osobowych z prawem, PUODO może wnioskować do GIIF o wgląd do danych zgromadzonych w rejestrze wniosków składanych do GIIF przez podmioty zapobiegające i zwalczające przestępczość. Kompetencja ta dotyczy zatem co do zasady ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz kompetencji PUODO wynikających z Ustawy LED. Brak rozbudowanych kompetencji współpracy między GIIF i PUODO nie jest rozwiązaniem pożądanym, zważywszy, że Ustawa o AML wprowadza szereg obowiązków instytucji obowiązanych, które bezpośrednio związane są z przetwarzaniem danych osobowych, np. obowiązek identyfikować i weryfikować tożsamość klientów i beneficjentów rzeczywistych (art. 34 ust. 2 Ustawy o AML)⁶⁹⁰. Negatywnie należy ocenić także to, że przedstawiciel

⁶⁸⁹ Na przykład: art. 70c; art. 80 ust. 2; art. 96 ust. 2; art. 100; art. 102; art. 105b i art. 111 ust. 7 Ustawy o AML.

⁶⁹⁰ Analiza krzyżowania się zakresu przedmiotowego RODO i Ustawy o AML dokonana została w podrozdziale rozprawy. Por. także M. Gawroński, *Rozdział 13. Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu*

PUODO nie jest członkiem Komitetu Bezpieczeństwa Finansowego, mając na względzie już chociażby to, że Komitet opiniuje krajową ocenę ryzyka prania pieniędzy oraz finansowania terroryzmu (art. 19 ust. 2 pkt 1 Ustawy o AML), która z kolei zawiera identyfikację zagadnień dotyczących ochrony danych osobowych związanych z AML (art. 29 ust. 1 pkt 6 Ustawy o AML). Skoro ta ocena ryzyka zawiera identyfikację zagadnień dotyczących ochrony danych osobowych, co z kolei objęte jest kompetencją PUODO, wskazane byłoby, aby przedstawiciel PUODO brał udział w jej opiniowaniu dla zachowania spójności między stosowaniem Ustawy o AML i RODO.

3.5.3. KRAJOWE ORGANY WŁAŚCIWE DO SPRAW CYBERBEZPIECZEŃSTWA I CSIRT-Y

Krajowy system cyberbezpieczeństwa ustanowiony w UKSC, stanowiącej implementację Dyrektywy NIS, jest szczególnie skomplikowany. W niniejszym podrozdziale na poziomie unijnym scharakteryzowane zostaną kompetencje organów, które mają zostać ustanowione zgodnie z nieimplementowaną jeszcze Dyrektywą NIS 2 uchylającą Dyrektywę NIS, a na poziomie krajowym – kompetencje krajowych organów właściwych do spraw cyberbezpieczeństwa (rozdział 8 UKSC) i zespołów CSIRT MON, CSIRT NASK i CSIRT GOV (Rozdział 6 UKSC) ustanowione na podstawie UKSC, która, jak zostało wskazane, transponuje wcześniejszą Dyrektywę NIS.

Dyrektywa NIS 2, która weszła w życie 16 stycznia 2023 r., winna być implementowana przez państwa członkowskie do 17 października 2024 r. Państwa członkowskie zobowiązane są zapewnić, aby ustanowić skuteczny system monitorowania i stosowania niezbędnych środków do przestrzegania Dyrektywy NIS 2 (art. 31 ust. 1 Dyrektywy NIS 2), wprowadzając rozwiązania umożliwiające niezależność operacyjną od nadzorowanych przez nie podmiotów administracji publicznej, przy czym państwa członkowskie mogą wprowadzić, uwzględniając analizę ryzyka, hierarchię priorytetów zadań nadzorczych (art. 31 ust. 2 Dyrektywy NIS 2). W tym celu w każdym państwie powinien zostać wyznaczony co najmniej jeden właściwy organ odpowiedzialny za cyberbezpieczeństwo i zadania nadzorcze (art. 8 ust. 1 Dyrektywy NIS 2) oraz pojedynczy punkt kontaktowy (art. 8 ust. 3 Dyrektywy NIS 2). Dyrektywa NIS 2 rozróżnia katalog środków nadzoru i egzekwowania przepisów dla podmiotów kluczowych w nadzorze *ex ante* (art. 32 Dyrektywy NIS 2) i podmiotów ważnych w nadzorze *ex post*

terroryzmu a RODO [w:] Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik, red. W. Kapica, Warszawa 2018.

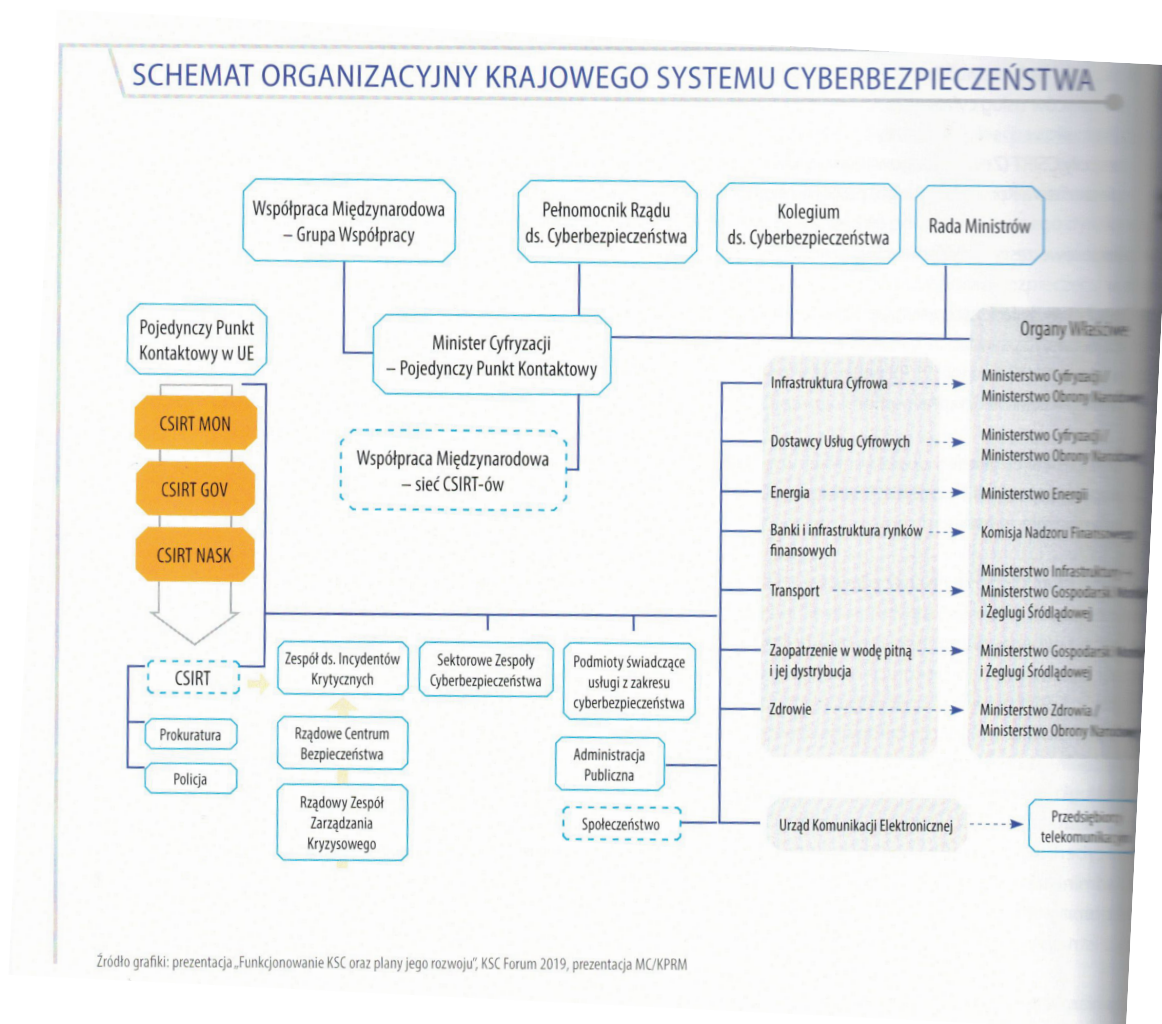
w przypadku powzięcia informacji o niewykonywaniu obowiązków przez te podmioty (art. 33 Dyrektywy NIS 2)⁶⁹¹. W obu katalogach środki te (które winny być „skuteczne, proporcjonalne i odstraszające”) unormowano szeroko (art. 32 ust. 2-8 Dyrektywy NIS 2 i art. 33 ust. 2-8 Dyrektywy NIS 2), obejmując m.in. kontrole na miejscu i nadzór zdalny, audyty bezpieczeństwa, wnioski o udzielenie informacji i przekazanie dokumentów, wydawanie ostrzeżeń, wiążących poleceń i kar administracyjnych opiewających do wielomilionowych kwot (zgodnie z ogólnymi warunkami ich nakładania unormowanymi w art. 34 Dyrektywy NIS 2). Unikalnym rozwiązaniem jest art. 35 ust. 1-2 Dyrektywy NIS 2, ustanawiający obowiązek właściwych organów odpowiedzialnych za cyberbezpieczeństwo do informowania organów ochrony danych o naruszeniach Dyrektywy NIS 2, które „mogą pociągać za sobą naruszenie ochrony danych osobowych” w rozumieniu RODO, a jeżeli organy ochrony danych osobowych nałożą administracyjną karę pieniężną na podstawie RODO za naruszenie wynikające „z tego samego zachowania”, organy odpowiedzialny za cyberbezpieczeństwo nie mogą nałożyć administracyjnej kary pieniężnej na podstawie Dyrektywy NIS 2, przy czym mogą zastosować „inne środki egzekwowania przepisów”⁶⁹².

Wzajemna pomoc między organami właściwymi w państwach członkowskich uregulowana jest w art. 37 Dyrektywy NIS 2, obejmując m.in. informowanie o zastosowanych środkach nadzoru lub egzekwowania przepisów i zwracanie się z wnioskami o zastosowanie takich odpowiednich środków. Artykuł 13 ust. 3 Dyrektywy NIS 2 nakłada na CSIRT-y i organy właściwe, w celu skutecznego wykonywania ich kompetencji, obowiązek współpracy m.in. z organami nadzorczymi ustanowionymi na podstawie RODO. Dodatkowo, prawodawca unijny zachęca prawodawcę krajowego do ustanowienia pojedynczych punktów zgłaszania incydentów na podstawie zarówno Dyrektywy NIS 2, jak i RODO oraz Dyrektywy ePrivacy, przy czym ustanowienie takich punktów nie powinno wpływać na stosowanie RODO oraz Dyrektywy ePrivacy, zwłaszcza na niezależność organów (motyw 106 Dyrektywy NIS 2). W Dyrektywie NIS 2 nałożono na organy właściwe prawnych obowiązek współpracy i wymiany informacji z organami ustanowionymi na podstawie RODO, zwłaszcza w odniesieniu do naruszeń, których konsekwencją mogłoby być naruszenie ochrony danych (art. 31 ust. 3, art. 35 ust. 1 oraz motyw 108 i 136 Dyrektywy NIS 2).

⁶⁹¹ Por. Uzasadnienie do Wniosku Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148, COM/2020/823 final.

⁶⁹² Por. podrozdział 2.6.2. powyżej.

W Polsce implementacja poprzedniej Dyrektywy NIS dokonana została przez UKSC, która normuje krajowy system cyberbezpieczeństwa. Definiowany jest w literaturze jako integralna część krajowego i europejskiego systemu bezpieczeństwa i sieci i systemów informacyjnych, którą wydzielono, aby zapewnić efektywność jej działania⁶⁹³. Jak wskazano wyżej, system ten jest szczególnie złożony podmiotowo. Tę złożoność obrazuje poniższa grafika z 2019 r.⁶⁹⁴



Schemat 2. Schemat organizacyjny krajowego systemu cyberbezpieczeństwa

Złożoność ta jest konsekwencją decyzji polskiego ustawodawcy, aby w zakresie autonomii instytucjonalnej wybrać zdecentralizowany, rozproszony sektorowo model dla organu właściwego dla cyberbezpieczeństwa podobnie jak, np. Finlandia czy Królestwo

⁶⁹³ Por. *Krajowy system cyberbezpieczeństwa*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 254.

⁶⁹⁴ Prezentacja *Funkcjonowanie KSC oraz plany jego rozwoju*, KSC Forum 2019, prezentacja MC/KPRM. Cytowanie za: A. Bartosiewicz J. Bieniasz, K. Szczypiorski, *Poradnik cyberbezpieczeństwa dla środowisk edukacyjnych i przedsiębiorstw*, Warszawa 2023, s. 14.

Niderlandów, w odróżnieniu od jurysdykcji, które wybrały bardziej scentralizowany model np. Niemcy, Francja i Dania⁶⁹⁵. Stąd też w niniejszym podrozdziale przedstawione zostaną kompetencje zespołów CSIRT MON, CSIRT NASK i CSIRT GOV i ośmiu krajowych organów właściwych do spraw cyberbezpieczeństwa. Należy wskazać, że odmienne kompetencje ustanowiono w rozdziale IX dla ministra właściwego do spraw informatyzacji, a w rozdziale 10 – dla Ministra Obrony Narodowej, przy czym oba te organy są również organami właściwymi w rozumieniu art. 41 UKSC. Wszystkie podmioty krajowego systemu cyberbezpieczeństwa są zobowiązane do współpracy w celu zapewnienia spójnego i kompleksowego systemu zarządzania ryzykiem na poziomie krajowym (art. 26 ust. 1 UKSC).

Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), chociaż nie stanowią odrębnych organów administracji publicznej, są w praktyce kluczowymi podmiotami w koordynacji reagowania na incydenty, a także mogą zapewniać wsparcie w obsłudze incydentów (art. 26 ust. 2 UKSC). Wszystkie CSIRT-y działają na poziomie krajowym (art. 2 pkt. 1-3 UKSC). CSIRT MON jest prowadzony przez Ministra Obrony Narodowej przede wszystkim dla podmiotów podległych i nadzorowanych przez Ministra Obrony Narodowej, (art. 26 ust. 5 UKSC), CSIRT GOV – przez Szefa Agencji Bezpieczeństwa Wewnętrznego dla administracji publicznej rządowej i infrastruktury krytycznej⁶⁹⁶ (art. 26 ust. 7 UKSC), CSIRT NASK – przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy dla pozostałych podmiotów, których katalog zwarto w art. 26 ust. 6 UKSC. Dla każdego z CSIRT ustanowiono zarówno odrębne (np. w odniesieniu do CSIRT NAS – art. 26 ust. 6 UKSC), jak i wspólne dla nich kompetencje unormowane w Rozdziale 6 UKSC. J. Dysarz wprowadza typologię kompetencji CSIRT, wyróżniając kompetencje dotyczące: wsparcia obsługi incydentu (art. 26 ust. 3 pkt 5–9 i 15 UKSC), np. reagowanie na zgłoszone incydenty (ust. 3 pkt. 5 UKSC); współpracy z podmiotami w krajowym systemie cyberbezpieczeństwa i z CSIRT-ami w innych państwach członkowskich; oraz innych usług CSIRT (najszerszego rodzajowo typu), m.in. monitoringu zagrożeń i szacowania ryzyka (art. 26 ust. 3 pkt 1–2 UKSC)⁶⁹⁷. UKSC wprowadza także możliwość zawierania porozumień między CSIRT-ami w przedmiocie powierzania sobie wykonywania zadań (art. 26 ust. 10 UKSC). W rozbudowanym art. 39 UKSC w rozdziale 7 (Zasady

⁶⁹⁵ J. Dysarz, *Komentarz do Art. 41*, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska, Warszawa 2019, pkt. 1, SIP Legalis.

⁶⁹⁶ M. Nowilkowska, *Komentarz do art. 26* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, pkt. 16, SIP Legalis.

⁶⁹⁷ J. Dysarz, *Komentarz do Art. 26* [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska, Warszawa 2019, pkt. 7, SIP Legalis.

udostępniania informacji i przetwarzania danych osobowych) uregulowano przetwarzanie danych osobowych, w tym szczególnych kategorii tych danych, zgodnie z RODO przez CSIRT-y (i sektorowe zespoły bezpieczeństwa) w celu wykonywania kompetencji. Przetwarzanie danych osobowych może być bowiem do tego niezbędne. Ustawodawca unormował m.in. reguły anonimizacji tych danych (art. 39 ust. 8 UKSC), okres ich retencji danych i możliwość wzajemnego ich przekazywania (art. 39 ust. 6 UKSC), obowiązek współpracy z PUODO (art. 39 ust. 7 UKSC), a także ograniczenie części obowiązków z RODO (np. art. 39 ust. 8 UKSC). Wymaga wskazania, że unormowania dotyczące CSIRT GOV różnią się od pozostałych CSIRT-ów z uwagi na wyłączenie stosowania RODO do przetwarzania danych osobowych w zakresie koniecznym do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego i podmiotowego wyłączenia tego stosowania wobec m.in. Agencji Bezpieczeństwa Wewnętrznego (art. 6 pkt 1 i 2 UODO)⁶⁹⁸.

Organy właściwe w obszarze cyberbezpieczeństwa uregulowane zostały w rozdziale 8 UKSC. Zostały nimi, zgodnie z art. 41 UKSC, ustanowione naczelne organy administracji rządowej – ośmiu ministrów właściwych zgodnie z Ustawą o Działach dla sektorów objętych UKSC (m.in. dla energii, transportu i ochrony zdrowia) oraz Komisja Nadzoru Finansowego dla sektora bankowego i infrastruktury rynków finansowych. Stanowi to potwierdzenie, że prawodawca krajowy wybrał zdecentralizowany model systemu cyberbezpieczeństwa. Kluczowym przepisem normującym rozbudowane kompetencje tych organów jest art. 42 UKSC. W literaturze wyróżnia się typologię kompetencji, dzieląc je na: związane z wyznaczaniem operatorów, związane z nadzorem i inne⁶⁹⁹. Każdy z organów m.in.: prowadzi analizę podmiotów pod kątem uznania ich za operatora usługi kluczowej (art. 42 ust. 1 pkt 1 UKSC) i decyduje o przyznaniu albo wygaśnięciu tego statusu (art. 42 ust. 1 pkt 2-3 UKSC); przygotowuje (we współpracy z CSIRT-ami i sektorowymi zespołami cyberbezpieczeństwa) rekomendacje dotyczące cyberbezpieczeństwa, w tym zgłaszania incydentów (art. 42 ust. 1 pkt 5 UKSC); monitoruje przestrzeganie przepisów UKSC i przeprowadza kontrole (art. 42 ust. 1 pkt 6 i 8 UKSC); współpracuje z organami państw członkowskich UE (art. 42 ust. 1 pkt 9 UKSC) oraz przetwarza dane osobowe w niezbędnym zakresie (art. 42 ust. 1 pkt 10 UKSC). Organy te mogą także ustanawiać sektorowe zespoły cyberbezpieczeństwa na podstawie art. 44 UKSC, a także nakładać kary pieniężne na

⁶⁹⁸ P. Drobek [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019, art. 39, pkt 2, SIP LEX.

⁶⁹⁹ J. Dysarz, *Komentarz do Art. 26 [w:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. A. Besiekierska, Warszawa 2019, pkt. 1, SIP Legalis.

operatorów usług kluczowych i dostawców usług cyfrowych (art. 53 ust. 2 UKSC) w ramach nadzoru, o którym mowa w art. 53 ust. 1 UKSC.

W kwestii współpracy między organami nadzorczymi ustanowionymi na podstawie RODO i organami właściwymi w sprawach cyberbezpieczeństwa istotne jest, że organy te zobowiązane są w uzasadnionych przypadkach współpracować z „organem właściwym do spraw ochrony danych osobowych”, czyli PUODO (art. 42 ust. 7 UKSC). Podobnie CSIRT-y. zobowiązane są do współpracy z PUODO (art. 39 ust. 7 UKSC), zwłaszcza przy koordynacji obsługi incydentu, który doprowadził do naruszenia ochrony danych osobowych (art. 34 ust. 2 UKSC). Pomimo że sprawy objęte zakresem przedmiotowym Dyrektywy NIS i UKSC krzyżują się z RODO, np. w odniesieniu do obowiązku zgłaszania incydentów stanowiących naruszenia ochrony danych i zapewnienia bezpieczeństwa przetwarzania (art. 32 RODO), to instrumenty współpracy między PUODO a organami właściwymi w sprawach cyberbezpieczeństwa i CSIRT należy ocenić jako ogólne. Nie precyzują one bowiem ani zakresu zagadnień i spraw, które powinny być objęte współpracą w celu zapewnienia spójności, ani tego, na ile ta współpraca jest obligatoryjna oraz w jakich formach ta współpraca miałyby się odbywać. Należy ocenić je zatem jako niewystarczające.

3.5.4. PREZES URZĘDU OCHRONY KONKURENCJI I KONSUMENTÓW JAKO ORGAN PRAWA KONKURENCJI

Przedmiotem analizy w tym podrozdziale są kompetencje Prezesa Urzędu Ochrony Konkurencji i Konsumentów (Prezes UOKiK) jako polskiego organu prawa konkurencji w odniesieniu do kontroli koncentracji (dział III UKK Koncentracje przedsiębiorców) i nadużywania pozycji dominującej (rozdział II działu II UKK Zakaz praktyk ograniczających konkurencję). Relacja kompetencji Komisji wobec UOKiK dla tych dwóch kwestii w kontekście równoległych uprawnień przyznanych Komisji i organom krajowym dokonana została powyżej⁷⁰⁰.

Prezes UOKiK jest – zgodnie z art. 29 ust. 1 UKK – jednoosobowym, centralnym organem administracji rządowej właściwym w sprawach ochrony konkurencji i konsumentów, którego działalność, wykonywana przy pomocy Urzędu Ochrony Konkurencji i Konsumentów, nadzorowana jest przez Prezesa Rady Ministrów. To właśnie ten organ powołuje Prezesa

⁷⁰⁰ Por. także C. Banasiński, M. Bychowska, Kompetencje decyzyjne Komisji Europejskiej i Prezesa UOKiK wynikające z rozporządzenia Rady UE nr 1/2003 w świetle zasady równoległego stosowania wspólnotowego i krajowego prawa antymonopolowego, PPH 2009, nr 3, s. 4-9.

UOKiK na pięcioletnią kadencję (art. 29 ust. 3 UKK), natomiast przyczyny odwołania Prezesa UOKiK są ograniczone do wskazanych w art. 29 ust. 4 UKK. W literaturze przedmiotem dyskusji jest czy Prezesa UOKiK można zaliczyć do niezależnych organów regulacyjnych, na przykład R. Wasilewski opowiadał się w 2020 r. przeciwko takiemu stanowisku, kwestionując przymioty niezależności organu i nieuwzględnienie Prezesa UOKiK w definicji legalnej organów regulacyjnych w art. 73 ust. 3 UKK⁷⁰¹. Niezależność Prezesa UOKiK została wzmocniona na skutek implementacji przywołanej już Dyrektywy ECN+ z grudnia 2018 r.⁷⁰² Między innymi, wprowadzono art. 34a ust. 1 pkt 1-2 UKK, zgodnie z którym Prezes UOKiK działa niezależnie, co oznacza, że wykonuje kompetencje niezależnie od wpływów zewnętrznych, w tym politycznych, ani nie może zwracać się o instrukcje do organów administracji rządowej, innego podmiotu publicznego, zatem także PUODO, oraz przyjmować od tych organów i podmiotów instrukcje. Nawet jednak po dokonaniu tej implementacji, która zresztą ocenione zostały w literaturze krytycznie⁷⁰³, pozycję ustrojową Prezesa UOKiK należy ocenić jako charakteryzującą się mniejszą niezależnością niż, na przykład, pozycję PUODO, który powoływany jest przez Sejm, a Prezes Rady Ministrów nie sprawuje nad nim nadzoru.

Zakres działania Prezesa UOKiK jest szczególnie szeroki. Należy wyjaśnić, że ustawodawca w art. 31 UKK posłużył się terminem „zakres działania”, chociaż zasadne byłoby posłużenie się terminem „kompetencje”, który przyjmowany jest w literaturze do tego przepisu jako odpowiedni⁷⁰⁴. Ustawodawca wskazuje w katalogu o charakterze otwartym⁷⁰⁵ siedemnaście kompetencji (art. 31 UKK), m.in. sprawowanie kontroli przestrzegania przez przedsiębiorców przepisów UKK (pkt 1); wydawanie decyzji w sprawach praktyk ograniczających konkurencję i w sprawach koncentracji przedsiębiorców (pkt 2); współpraca z krajowymi i międzynarodowymi organami i organizacjami, do których zakresu działania

⁷⁰¹ II. Prezes UOKiK jako organ administracji publicznej 1. Umiejscowienie w strukturze władzy publicznej [w:] R. R. Wasilewski, *Postępowanie dowodowe przed Prezesem Urzędu Ochrony Konkurencji i Konsumentów*, Warszawa 2020, SIP Legalis; patrz także: przywołany tam w przypisie nr 32 przegląd stanowisk w odniesieniu do tej kwestii w doktrynie.

⁷⁰² Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1 z dnia 11 grudnia 2018 r. mająca na celu nadanie organom ochrony konkurencji państw członkowskich uprawnień w celu skuteczniejszego egzekwowania prawa i zapewnienia należytego funkcjonowania rynku wewnętrznego (Tekst mający znaczenie dla EOG.) PE/42/2018/REV/1 OJ L 11, 14.1.2019, p. 3–33.

⁷⁰³ Por. A. Piszcz, *Niezależność Prezesa Urzędu Ochrony Konkurencji i Konsumentów a dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1*, PUG 2022, nr 10, s. 11-19; także M. Kozak, Raz, dwa, trzy, niezależny będziesz ty... O konieczności szerszego spojrzenia na niezależność polskiego organu antymonopolowego w świetle dyrektywy ECN+, IKA 2019, nr 6, s. 23-38.

⁷⁰⁴ Por. J. Baehr, T. Feliszewski [w:] *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, red. A. Stawicki, E. Stawicki, Warszawa 2016, art. 31.

⁷⁰⁵ K. Jaroszyński, *Komentarz do art. 31 [w:] Ustawa o ochronie konkurencji i konsumentów. Komentarz*, red. K. Skoczny, Warszawa 2014, pkt 1, SIP Legalis.

należy ochrona konkurencji i konsumentów (pkt 5); wykonywanie zadań i kompetencji organu ochrony konkurencji państwa członkowskiego (pkt 6); opracowywanie i wydawanie publikacji oraz programów edukacyjnych popularyzujących wiedzę o ochronie konkurencji i konsumentów (pkt 12); występowanie do przedsiębiorców w sprawach z zakresu ochrony konkurencji i konsumentów (pkt 13). Prezesowi UOKiK przyznano szerokie kompetencje, w tym kompetencje proceduralne do wszczęcia prowadzenia postępowań (np. art. 48 UKK dotyczący wszczęcia postępowanie wyjaśniającego i art. 49 dotyczący wszczęcia postępowań antymonopolowych przed Prezesem UOKiK), w tym przeprowadzania kontroli (np. Dział VI Postępowanie przed Prezesem Urzędu Rozdział 5 Kontrola i przeszukiwanie w toku postępowania przed Prezesem Urzędu), współpracy krajowej i międzynarodowej (np. art. 31a pkt. 16a UKK i art. 73 ust. 3 UKK – współpraca z organami regulacyjnymi w sektorze energetyki, telekomunikacji i rynku finansowego oraz rozdział VIIIa – wzajemna pomoc w sprawach powiadomień lub egzekucji kar pieniężnych lub okresowych kar pieniężnych w sprawach dotyczących naruszeń art. 101 i art. 102 TFUE). W UKK brak jest unormowań nakładających współpracę Prezesa UOKiK z organami nadzorczymi ustanowionymi na podstawie RODO. Z informacji publicznie dostępnych wynika, że organy te podejmowały wspólne inicjatywy dotyczące m.in. walki ze zjawiskiem niezamówionego telemarketingu (razem z Prezesem Urzędu Komunikacji Elektronicznej)⁷⁰⁶ i organizowały konferencje naukowe⁷⁰⁷. Nadto, zgodnie z komunikatem na stronie UODO z dnia 28 sierpnia 2023 r., PUODO, wyjaśniając sposób przetwarzania danych osobowych w procedurze weryfikacji pasażerów jednego z przewoźników lotniczych, zwrócił się do Prezesa UOKiK o zbadanie praktyk tego przewoźnika z perspektywy naruszenia zbiorowych interesów konsumentów⁷⁰⁸, co pozwala przypuszczać, że organy te współpracują w indywidualnych sprawach.

W praktyce istotne są także kompetencje doradcze, informacyjne i edukacyjne Prezesa UOKiK, w tym wydawanie wyjaśnień i interpretacji mających istotne znaczenie dla przestrzegania prawa (art. 31a UKK) w celu zwiększenia przewidywalności jego stosowania, które jednak jako takie nie są wiążące, ani nie mogą być przedmiotem abstrakcyjnej kontroli

⁷⁰⁶ *Uciążliwe telefony od telemarketerów. Jest nowy pomysł jak z nimi walczyć*, „Business Insider” 12.11.2019. <https://businessinsider.com.pl/walka-z-telefonami-od-telemarketerow-dzialania-uke-uokik-i-uodo/23pbryg> (dostęp: 15.09.2024 r.).

⁷⁰⁷ *O ochronie danych osobowych. Między teorią a praktyką*, UODO 31.03.2023, <https://uodo.gov.pl/pl/138/2652> (dostęp: 15.09.2024 r.).

⁷⁰⁸ *Procedura weryfikacji pasażerów linii Ryanair. UODO reaguje*, UODO 28.08.2023, <https://uodo.gov.pl/pl/138/2815> (dostęp: 15.09.2024 r.).

przez sądy⁷⁰⁹. W odniesieniu do kompetencji naprawczych, wydawanie decyzji w sprawach praktyk ograniczających konkurencję, w tym praktyki nadużywania pozycji dominującej, uregulowane zostało w rozdziale 3 „Decyzje w sprawach praktyk ograniczających konkurencję” działu II UKK. W szczególności, Prezes UOKiK może w szczególności nakazać umożliwienie dostępu do określonej infrastruktury na niedyskryminacyjnych warunkach (art. 10 ust. 4 pkt 2 UKK) i zapewnienie innym podmiotom dostawy określonych produktów lub świadczenia określonych usług na niedyskryminacyjnych warunkach (art. 10 ust. 4 pkt 4 UKK). Natomiast wydawanie decyzji w sprawach kontroli koncentracji uregulowane jest w rozdziale 2 „Decyzje w sprawach koncentracji” działu III UKK. Podobnie jak Komisja, Prezes UOKiK może wyrazić zgodę (art. 18 UKK), warunkową zgodę (art. 19 UKK), albo zakazać dokonania koncentracji (art. 20 UKK). Z kolei rozbudowane unormowania w przedmiocie nakładania kar pieniężnych i odstąpienia od ich wymierzenia lub ich obniżenia zamieszczono w dziale VIII UKK „Kary pieniężne”.

3.5.5. KRAJOWE ORGANY WŁAŚCIWE W AKCIE O USŁUGACH CYFROWYCH

Akt o Usługach Cyfrowych (w dalszej części tego podrozdziału zdefiniowany jako „DSA”) wprowadza dużo bardziej scentralizowany model stosowania niż RODO. W tym modelu to Komisja ma wyłączne kompetencje wobec VLOPs i VLOSEs, czyli największych podmiotów nadzorowanych, w zakresie dodatkowych obowiązków tych podmiotów w odniesieniu do zarządzania ryzykiem systemowym określonych w sekcji 5 rozdziału III DSA (art. 56 ust. 1 DSA), przy czym krajowe organy właściwe mogą przesłać Komisji informację o podejrzeniu naruszenia tych obowiązków (art. 65 ust. 2 DSA). W pozostałym zakresie stosowania DSA wobec tych podmiotów – Komisja ma również kompetencje, które jednak dzielone są z państwami członkowskimi (art. 56 ust. 3 DSA) i powinny być wykonywane w ścisłej współpracy (art. 56 ust. 4 DSA). Kompetencje Komisji scharakteryzowane zostały w podrozdziale 3.4.6. powyżej. Przedmiotem analizy w tym podrozdziale jest status prawny i kompetencje organów właściwych w DSA na poziomie krajowym.

Państwa członkowskie, zgodnie z zasadą autonomii instytucjonalnej, mają swobodę w ustanowieniu organów właściwych organów (art. 49 ust. 1 DSA). W przypadku

⁷⁰⁹ J. Affre, K. Witek, Soft law Prezesa UOKiK na przykładzie „Informacji o sposobie składania wniosków o ograniczenie prawa wglądu w postępowaniach”, IKA 2020, nr 5, s. 78; patrz także: przywołany tam literatura, zwłaszcza Ustawa o ochronie konkurencji i konsumentów. Komentarz, red. A. Stawicki, E. Stawicki, Warszawa 2016.

ustanowienia więcej niż jednego organu, konieczne jest – ze względu na transgraniczny charakter spraw – ustanowienie koordynatorów ds. usług cyfrowych, którzy odpowiadają za wszystkie kwestie związane ze stosowaniem DSA w państwie członkowskim, w tym za koordynację w przypadku, jeżeli ustanowiono więcej niż jeden organ, w tym organy sektorowe (art. 49 ust. 2 DSA). Właściwe organy powinny działać w sposób niezależny (art. 50 ust. 2 DSA), bezstronnie, przejrzysto i terminowo (art. 50 ust. 1 DSA). Nie ma przeszkód, aby organami właściwymi w DSA wyznaczone zostały organy nadzorcze ustanowione na podstawie RODO.

Krajowe organy właściwe nadzorują i egzekwują DSA wobec wszystkich podmiotów poza VLOPs i VLOSEs w całości, a wobec tych podmiotów – w odniesieniu do obowiązków innych niż zastrzeżone wyłącznie dla Komisji, o ile Komisja nie wszczęła już postępowania w sprawie tego samego naruszenia (art. 56 ust. 4 DSA). Krajowe organy są właściwe wobec tych podmiotów, których główne miejsce prowadzenia działalności znajduje się na terytorium ich państwa członkowskiego (art. 56 ust. 1 DSA). Pomimo zatem brzmienia art. 56 ust. 1 DSA sugerującego, że to organy krajowe będą w zasadniczej mierze stosowały DSA, to właśnie Komisja odgrywa kluczową rolę w stosowaniu DSA, a organy krajowe pełnią funkcję, którą można określić jako subsydiarną (pomocniczą), ponieważ, w pewnym uproszczeniu, mogą wykonywać swoje kompetencje wtedy, kiedy Komisja nie podejmuje działań.

Kompetencje organów właściwych uregulowane zostały w sposób kompleksowy i szeroki (art. 51 DSA). Obejmują kompetencje proceduralne (w tym żądanie informacji i przeprowadzenie kontroli), naprawcze (zatwierdzanie zobowiązań proponowanych przez dostawców, nakazanie zaprzestania naruszeń, nakładanie sankcji, w tym kar pieniężnych, przyjmowania środków tymczasowych aż po wnioskowanie do właściwych sądów krajowych o tymczasowe zawieszenie usługi w kwalifikowanych przypadkach zgodnie z art. 51 ust. 3 DSA) i współpracy (z innymi właściwymi organami, Komisją i Europejską Radę Usług Cyfrowych). Na państwach członkowskich spoczywa obowiązek przyjęcia przepisów, które będą zapewniały skuteczne, proporcjonalne i odstraszające sankcje (art. 52 ust. 1-2 DSA), przy czym maksymalna wysokość kar pieniężnych ustalona została w art. 52 ust. 3 DSA (co do zasady maksymalnie jest to 6% rocznego światowego obrotu danego dostawcy usług pośrednich w poprzednim roku obrotowym).

Reguły wzajemnej pomocy między Komisją i koordynatorami ds. usług cyfrowych i współpracy transgranicznej określono w art. 57 DSA i art. 58 DSA w celu spójnego i efektywnego stosowania DSA, w szczególności zaś koordynator ds. usług cyfrowych właściwy dla miejsca siedziby zobowiązanych jest wszystkich koordynatorów ds. usług

cyfrowych właściwych dla miejsca przeznaczenia, Europejską Radę Usług Cyfrowych i Komisję o prowadzeniu czynności sprawdzających i zamiarze wydania decyzji (art. 57 ust. 1 DSA), a koordynator ds. usług cyfrowych właściwy dla miejsca przeznaczenia może wnioskować do koordynatora właściwego dla miejsca siedziby o podjęcie czynności sprawdzających lub przyjęcie niezbędnych środków w celu egzekwowania DSA (art. 58 ust. 1 DSA). Procedura wspólnych czynnościach sprawdzających (*joint investigations*) (art. 60 DSA) i przekazania spraw do Komisji (art. 59 DSA), realizowana z udziałem Europejskiej Rady ds. Usług Cyfrowych, scharakteryzowana została w podrozdziale 3.4.7. dotyczącym tej Rady. W DSA, w odróżnieniu od Aktu w sprawie Zarządzania Danymi i Aktu w sprawie Danych, nie ma bezpośrednio ustanowionego obowiązku współpracy z organami nadzorczymi ustanowionymi na podstawie RODO, natomiast prawodawca unijny wskazał prawodawcy krajowemu na możliwość ustanowienia osobnego instrumentarium współpracy między koordynatorami ds. usług cyfrowych i innymi organami administracji publicznej (art. 49 ust. 2 DSA), a taki ogólnie sformułowany obowiązek współpracy między organami można wywieść z brzmienia art. 49 ust. 2 DSA i motywów 109-117 do DSA.

3.5.6. ORGANY WŁAŚCIWE DO SPRAW USŁUG POŚREDNICTWA DANYCH I ORGANY WŁAŚCIWE DO SPRAW REJESTRACJI ORGANIZACJI ALTRUIZMU DANYCH (AKT W SPRAWIE ZARZĄDZANIA DANYMI)

Podobnie jak w przypadku organów nadzorczych ustanowionych na podstawie RODO, prawodawca unijny w Akcie w sprawie Zarządzania Danymi (w dalszej części tego podrozdziału ten akt zdefiniowany jako „DGA”) zdecydował, że kwestie ustrojowe dotyczące organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych zostaną pozostawione prawodawcom krajowym zgodnie z zasadą autonomii instytucjonalnej.

Struktura organów stosujących DGA jest dwupoziomowa, przy czym zasadniczy ciężar stosowania DGA spoczywa na organach krajowych (organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych, którymi mogą być wyznaczone także organy ochrony danych) z doradczymi kompetencjami Europejskiej Rady ds. Innowacji w zakresie Danych (scharakteryzowanej w podrozdziale 3.4.4. powyżej). Dodatkowo, Komisji powierzono w ramach procedury komitetowej przyjmowanie aktów delegowanych w art. 5 ust. 13 DGA (dotyczących ustanowienia przekazywania warunków szczególnych kategorii danych nieosobowych do państw trzecich)

i art. 22 ust. 1 DGA (zbiór zasad dotyczący altruizmu danych w zakresie wymogów informacyjnych i technicznych, standardów interoperacyjności oraz sposobu komunikacji do podmiotów, których dane dotyczą i posiadaczy danych). Nadto, Komisji przyznano kompetencje dotyczące, np. opracowania i przyjęcia, po odpowiednich konsultacjach, europejskiego formularza zgody do celów altruizmu danych (art. 25 DGA).

Obok wskazanych powyżej organów, w art. 7 DGA zobowiązano państwa członkowskie do wyznaczenia podmiotu, który udzielał będzie pomocy podmiotom sektora publicznego udzielającym dostępu lub odmawiającym jego udzielenia do celów ponownego wykorzystywania kategorii danych. Nierozstrzygnięty jest status prawny tych podmiotów na poziomie krajowym. Zakres pomocy, jakiej mają one udzielać, obejmujący wsparcie techniczne i prawne dla tych podmiotów sektora publicznego, określony został m.in. w art. 7 ust. 4 DGA, w szczególności dotyczy „pseudonimizacji oraz zapewnienie przetwarzania danych w sposób skutecznie chroniący prywatność, poufność, integralność i dostępność informacji”. Oznacza to, że ten zakres pomocy obejmuje także kwestie, które są w zakresie kompetencji organów nadzorczych ustanowionych na podstawie RODO.

Organy właściwe do spraw usług pośrednictwa danych mają być ustanowione przez prawodawców krajowych, aby wykonywać kompetencje związane z procedurą zgłaszania usług pośrednictwa danych (art. 13 ust. 1 DGA). Art. 13 ust. 3 DGA przewiduje, że kompetencje tych organów nie naruszają kompetencji „organów ochrony danych, krajowych organów ochrony konkurencji, organów odpowiedzialnych za cyberbezpieczeństwo oraz innych odpowiednich organów sektorowych”. Jednocześnie, wszystkie te organy zobowiązane zostały do prowadzenia ścisłej współpracy i zapewniania spójności podejmowanych przez nie działań (art. 13 ust. 3 DGA). Kompetencje tych organów ustanowione zostały w art. 14 DGA i art. 34 DGA (kary opisane niżej). Kluczową kompetencją jest monitorowanie i nadzorowanie spełniania wymogów przewidzianych w DGA dla dostawców usług pośrednictwa danych i dla uznanych organizacji altruizmu danych. W tym celu organy mogą żądać informacji od podmiotów nadzorowanych (art. 14 ust. 2 DGA), a w przypadku stwierdzenia naruszeń żądać zaprzestania naruszeń lub nakładać administracyjnych kar pieniężnych, lub inne sankcje, np. żądanie zawieszenia lub zaprzestania świadczenia usług pośrednictwa danych (art. 14 ust. 3 DGA).

Organy właściwe do spraw rejestracji organizacji altruizmu danych powinny być ustanowione przez każde z państw członkowskich, aby prowadzić publiczny krajowy rejestr uznanych organizacji altruizmu danych (art. 23 ust. 1 DGA). W wykonywaniu swoich kompetencji są one zobowiązane współpracować z innymi organami, w tym niezależnymi

organami nadzorczymi ustanowionymi na podstawie RODO (art. 23 ust. 3 DGA). Kompetencje tych organów określone zostały w art. 24 i 34 DGA (kary opisane niżej). Podobnie jak wyżej, kluczową kompetencją jest monitorowanie i nadzorowanie spełniania wymogów przewidzianych w DGA dla uznanych organizacji altruizmu danych. Aby to zrealizować, organy mogą żądać informacji od nadzorowanych podmiotów (art. 24 ust. 2 DGA). Chociaż organy te w art. 24 ust. 5 DGA nie mają wprost przyznanej kompetencji do nakładania kar pieniężnych, a sankcje za naruszenie obowiązków obejmują utratę prawa do posługiwania się oznakowaniem „uznana w Unii organizacja altruizmu danych” lub usunięcie z rejestru uznanych organizacji altruizmu danych, to możliwość nakładania kar pieniężnych za naruszenie obowiązków przewidzianych w DGA wynika wprost z art. 34 ust. 1 DGA. Oba organy zobowiązane są do współpracy, w tym zwłaszcza wymiany informacji, między sobą i Komisją (art. 26 ust. 5 DGA) z organami w innych państwach członkowskich w sprawach z elementem transgranicznym przewidziany (art. 14 ust. 7 i art. 24 ust. 6 DGA).

Prawodawca unijny w art. 34 ust. 1 DGA pozostawił państwom członkowskim swobodę co do ustanowienia kar za naruszenie DGA, sugerując jedynie kryteria co do charakteru i wysokości tych kar (ust. 2), w zakresie obowiązków dotyczących: przekazywania danych nieosobowych do państw trzecich przy ponownym wykorzystywaniu danych, które są w posiadaniu podmiotów sektora publicznego, obowiązku dostawców usług pośrednictwa danych dotyczącego zgłoszenia świadczenia tych usług, warunków świadczenia tych usług pośrednictwa i warunków rejestracji podmiotu jako uznana organizacja altruizmu danych.

Chociaż, jak zostało wskazane, prawodawca unijny pozostawił państwom członkowskim swobodę w ukształtowaniu pozycji ustrojowej organów w DGA, to jednak w art. 26 DGA wprowadził określone wymogi dotyczące tych organów. Obejmują one m.in. zachowanie formalnej odrębności i funkcjonalnej niezależności od dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych (art. 26 ust. 1 DGA), obowiązek wykonywania kompetencji bezstronnie, przejrzystie, spójnie, wiarygodnie i terminowo (art. 26 ust. 2 DGA), unikając konfliktu interesów (art. 26 ust. 3 DGA). Organów te powinny mieć zapewnione odpowiednie środki finansowe i osobowe (art. 26 ust. 5 DGA). Państwa członkowskie mogą przyznać kompetencje obu tych organów dla jednego organu, mogą także powołać więcej organów albo wykorzystać ustanowione już organy (art. 26 ust. 1 DGA). Również niezależne organy nadzorcze ustanowione na podstawie RODO mogą zostać ustanowione jako oba organy właściwe w DGA albo też jako jeden z nich (motyw 4 DGA). W sytuacji, w której ustanowione zostały inne organy, to ich kompetencje powinny pozostawać bez uszczerbku dla kompetencji niezależnych organów nadzorczych

ustanowionych na podstawie RODO (motyw 4 DGA *in fine*, motyw 35 DGA i art. 1 ust. 3 DGA). Każdy z tych organów w przypadku kwestii wymagających oceny zgodności z RODO powinny zwrócić się o opinię lub decyzję do organu nadzorczego ustanowionego na podstawie RODO (motyw 44, jak i motyw 51 DGA).

3.5.7. ORGANY WŁAŚCIWE W AKCIE W SPRAWIE DANYCH

Tak jak w przypadku Aktu w sprawie Zarządzania Danymi, Akt w sprawie Danych (w dalszej części tego podrozdziału ten akt zdefiniowany jako „Data Act”) ustanawia dwupoziomową strukturę organów – właściwe organy na poziomie krajowym z kluczowymi kompetencjami (art. 37 Data Act) i Europejską Radę ds. Innowacji w zakresie Danych z ograniczonymi kompetencjami doradczymi (jak analizowano wyżej). Ponownie, państwom członkowskim pozostawiono ustanowienie właściwych organów na poziomie krajowym w taki sposób, aby zapewnić skuteczne stosowanie Data Act (art. 37 ust. 1 Data Act). Mogą to być zarówno istniejące organy, w tym organy nadzorcze ustanowione na podstawie RODO, jak i nowe organy. W przypadku większej liczby organów w jednym państwie członkowskim należy wskazać jeden organ, który pełnił będzie rolę tak zwanego koordynatora danych, a także z osobna wskazać krajowy organ do spraw współpracy międzynarodowej w kwestiach prawnych (art. 32 ust. 3 Data Act). Ograniczone kompetencje polegające na przyjmowaniu aktów delegowanych ma także Komisja (art. 45 ust. 1 Data Act). Dotyczą one m.in. interoperacyjności (art. 33 ust. 2 Data Act), np. środków technicznych zapewniających ciągły dostęp do danych (art. 33 ust. 1. lit. c Data Act), i monitorowania prawidłowego nakładania opłat przez dostawców usług przetwarzania danych art. 29 ust. 7 (Data Act).

Istotne jest, że organy ochrony danych osobowych zostały wprost na mocy art. 37 ust. 3 Data Act jako „odpowiedzialne za monitorowanie stosowania [Data Act] w zakresie ochrony danych osobowych” (*„insofar as the protection of personal data is concerned”*). Na marginesie należy wskazać, że EIOD został odpowiedzialny za monitorowanie stosowania Data Act w zakresie, w jakim dotyczy ono organów i instytucji UE (art. 37 ust. 3 Data Act). Celem przyjęcia tego rozwiązania jest zapewnienie spójności stosowania RODO i Data Act⁷¹⁰. Państwa członkowskie zostały zobowiązane do jasnego określenia kompetencji właściwych organów (art. 37 ust. 5 Data Act), przy czym kompetencje organów sektorowych powinny być „respektowane” (art. 37 ust. 4 lit. a Data Act).

⁷¹⁰ Dalsza analiza tej kwestii w podrozdziale 4.4. rozprawy.

Kompetencje organów właściwych (art. 37 ust. 5 Data Act) obejmują promowanie umiejętności danych wśród podmiotów objętych zakresem Data Act, rozpatrywanie skarg i prowadzenie postępowań w przedmiocie stosowania Data Act, nakładania kar pieniężnych, monitorowanie rozwoju technicznego i ekonomicznego istotnego dla udostępniania i wykorzystywania danych, współpracę z innymi organami, w tym organami nadzorczymi ustanowionymi na podstawie RODO, organami właściwymi do spraw usług opartych na danych i usług łączności elektronicznej, właściwymi organami innych państw członkowskich i Komisją. Jednocześnie, przy wykonywaniu swoich kompetencji właściwe organy powinny pozostawać bezstronne ani nie mogą zwracać się „o instrukcje w indywidualnych sprawach do [...] innego organu publicznego [...] ani nie przyjmują takich instrukcji” (art. 37 ust. 8 Data Act), co – literalnie interpretując – ogranicza prawodawcę krajowego w wyborze form wykonywania współpracy między organami właściwymi i innymi organami, uniemożliwiając wprowadzenie procedury współdecydowania w indywidualnych sprawach należących do kompetencji organów właściwych, np. przez uzależnienie wydania decyzji przez organy właściwe od wiążącej albo niewiążącej opinii od organów nadzorczych ustanowionych na podstawie RODO.

O ustaleniu właściwych organów w przypadkach o charakterze transgranicznym rozstrzygnięto w art. 37 ust. 10-16 Data Act. Podmioty objęte zakresem obowiązywania Data Act podlegają kompetencji organów w państwie członkowskim, w którym mają siedzibę lub główną siedzibę (siedziba zarządu lub siedziba statutowa, z której wykonywane są podstawowe funkcje finansowe i kontrola operacyjna) (ust. 10). Oznacza to brak rozwiązania podobnego do mechanizmu spójności w RODO i zwiększa ryzyko zjawiska *forum shopping*.

Państwom Członkowskim pozostawiono, na podstawie art. 40 Data Act, swobodę w ustanowieniu skutecznych, proporcjonalnych i odstraszaających kar. Organom nadzorczym ustanowionym na podstawie RODO w art. 40 ust. 4 Data Act przyznano kompetencję do nakładania administracyjnych kar pieniężnych za naruszenie obowiązków z ograniczeniem do obowiązków ustanowionych w rozdziałach II (Dzielenie się danymi przez przedsiębiorców z konsumentami i z innymi przedsiębiorcami), III (Obowiązki posiadaczy danych zobowiązanych do udostępniania danych zgodnie z prawem unii) i V (Udostępnianie danych organom sektora publicznego, komisji, Europejskiemu Bankowi Centralnemu i organom Unii na podstawie wyjątkowej potrzeby) Data Act. Relacja art. 40 ust. 4 Data Act do omówionego wyżej art. 37 ust. 3 Data Act jest niejasna. Po pierwsze, nie jest klarowne, czy to ograniczenie możliwości nakładania administracyjnych kar pieniężnych oznacza, że organy nadzorcze ustanowione na podstawie RODO nie będą mogły nałożyć takiej kary w przypadku, jeżeli

dojdzie do naruszenia obowiązków wynikających z innych rozdziałów Data Act, które jednocześnie stanowiły będą naruszenie RODO. Po drugie, nie jest także jasne czy art. 40 ust. 4 Data Act ogranicza możliwość monitorowania stosowania Data Act w odniesieniu do rozdziałów innych niż II, III i V, czyli, na przykład, w odniesieniu do rozdziału VI dotyczącego zmiany dostawcy usług przetwarzania danych; czy też raczej oznacza, że możliwe jest jak monitorowanie, tak i nałożenie innych sankcji niż administracyjne kary pieniężne. Wobec tego braku klarowności – w połączeniu z niejasnym zakresem odpowiedzialności organów nadzorczych ustanowionych na podstawie RODO i zakazem otrzymywania lub żądania instrukcji w sprawach indywidualnych – wyzwaniem będzie zrealizowanie przez prawodawców krajowych jasnego określenia kompetencji właściwych organów (art. 37 ust. 5 Data Act). Już samo wprowadzenie tego rozwiązania oznacza, że prawodawca unijny dostrzega ryzyko krzyżowania się kompetencji organów nadzorczych ustanowionych na podstawie RODO i organów właściwych ustanowionych na podstawie Data Act.

3.5.8. ORGANY WŁAŚCIWE W AKCIE W SPRAWIE SZTUCZNEJ INTELIGENCJI

Prawodawca unijny pozostawił prawodawcy krajowemu znaczną swobodę w ustanowieniu struktury organów administracji publicznej („właściwych organów krajowych”) stosujących Akt w sprawie Sztucznej Inteligencji⁷¹¹, normując przy tym, że należy ustanowić co najmniej jeden organ notyfikujący i jeden organ nadzoru rynku (art. 70 ust. 1 AI Act), o których informacje winny być przekazane Komisji (art. 70 ust. 2 AI Act), zapewniając ich niezależność oraz wyposażając w odpowiednie zasoby, w tym zasoby ludzkie posiadające wiedzę z zakresu ochrony danych osobowych (art. 70 ust. 3 AI Act). Możliwie jest zatem, przykładowo, ustanowienie tylko jednego organu nadzoru rynku w kraju, albo też ustanowienie organów nadzoru rynku dla każdego z sektorów z osobna, przy czym konieczne jest ustanowienie jednego punktu kontaktowego na poziomie krajowym (art. 70 ust. 1 AI Act). EROD zajął stanowisko, że kompetencje w odniesieniu do AI Act na poziomie krajowym powinny zostać zasadniczo przyznane organom ochrony danych osobowych, podkreślając

⁷¹¹ Fragmenty tego podrozdziału inspirowane są publikacją autora niniejszej rozprawy: P. Hajduk, *AI Act And GDPR: On The Path Towards Overlap Of The Enforcement Structures*, 1.10.2023, <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/?cn-reloaded=1&cn-reloaded=1> (dostęp: 15.09.2024 r.).

konieczność zapewnienia efektywnych instrumentów współpracy między kompetentnymi organami⁷¹².

Swoboda prawodawcy krajowego w kształtowaniu struktury jest do pewnego stopnia ograniczona sektorowo, np. przez art. 74 ust. 6 AI Act⁷¹³, zgodnie z którym systemy AI wysokiego ryzyka wykorzystywane przez instytucje finansowe nadzorowane są przez organ krajowy odpowiedzialny za nadzór finansowy (w zakresie „bezpośrednio związanym” ze świadczeniem usług finansowych). Ponadto, organy ochrony danych (co do zasady) zostały wskazane jako organy nadzorcze do systemów AI wysokiego ryzyka (wyszczególnione w załączniku III pkt 1 AI Act), „w zakresie, w jakim systemy te są wykorzystywane do celów ścigania przestępstw, kontroli granicznej oraz w kontekście wymiaru sprawiedliwości i demokracji, oraz w odniesieniu do systemów AI wysokiego ryzyka wymienionych w załączniku III pkt 6, 7 i 8 AI Act” (art. 74 ust. 8 AI Act), czyli zasadniczo systemów AI wysokiego ryzyka w jednym z trzech wymienionych wyżej obszarów. Chociaż organy ochrony danych mogłyby zostać wyznaczone jako organy właściwe do stosowania Aktu w sprawie Sztucznej Inteligencji, to należy przypuszczać, że najprawdopodobniej tak się nie stanie. Alternatywnie – co wydaje się nawet bardziej prawdopodobne – w poszczególnych państwach wdrożone zostaną odmienne rozwiązania, co pogłębi złożoność struktury organów z perspektywy unijnej.

AI Act wymienia wprost organy notyfikujące i organy nadzoru rynku na poziomie krajowym (art. 70 ust. 1 AI Act). Organy notyfikujące – których założenia ukształtowano zgodnie z tzw. nowymi ramami prawnymi („*New Legislative Framework*”) – są kompetentne do opracowania, stosowania i monitorowania procedur oceny, wyznaczania i notyfikowania jednostek oceniających zgodność systemów AI (w tym także wycofania notyfikacji), które to procedury mają być przygotowywane przez organy poszczególnych państw członkowskich w porozumieniu (art. 28 ust. 1 AI Act). Organy te rozpoznają wnioski jednostek oceniających o notyfikację po spełnieniu wymogów unormowanych w art. 31 AI Act (art. 29 ust. 1 AI Act) zgodnie z procedurą notyfikacyjną w art. 30 AI Act. Stosownie do proponowanej w tej rozprawie typologii kompetencji, kompetencje organów notyfikujących zaliczyć należy do kompetencji do wydawania zezwoleń.

Krajowe organy nadzoru rynku wykonują kluczowe kompetencje proceduralne i naprawcze w AI Act. Ich kompetencje te nie są wydzielone do jednej (kilku sąsiadujących)

⁷¹² EROD, *EDPB Statement 2024/03 on DPAs Role in AI Act*, https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf (dostęp: 15.09.2024 r.), p. 9-15.

⁷¹³ Jednak z wyjątkiem w art. 74 ust. 7 AI Act.

jednostki redakcyjnej AI Act, lecz rozproszone są w różnych rozdziałach i sekcjach rozporządzenia. Istotna ich część uregulowana jest natomiast w Rozdziale IX – „Monitorowanie po wprowadzeniu do obrotu, wymiana informacji oraz nadzór rynku”, Sekcja 3 „Egzekwowanie”. Krajowe organu nadzoru rynku sprawują nadzór i kontrolę systemów AI, w tym systemów AI wysokiego ryzyka, w poszczególnych państwach członkowskich (art. 74 AI Act)

Organy nadzoru rynku wyposażone zostały w rozbudowane kompetencje proceduralne i naprawcze dla realizacji swoich zadań⁷¹⁴. Są uprawnione m.in. do prowadzenia postępowań wyjaśniających, kontroli i uzyskiwania niezbędnych informacji⁷¹⁵, w tym dostępu do kodu źródłowego systemu AI wysokiego ryzyka na uzasadniony wniosek organu (art. 74 ust. 13). W ramach kompetencji naprawczych organy te mogą także m.in. zakończyć testy na systemach AI w warunkach rzeczywistych (art. 76 ust. 3 AI Act), zobowiązać do podjęcia wszelkich odpowiednich działań (art. 79 ust. 2 i art. 82 AI Act), wycofać system AI z ryzyka (art. 79 ust. 2 AI Act) i podejmować środki tymczasowe (art. 79 ust. 2 AI Act) a również nakładać wielomilionowe kary pieniężne, co zostało unormowane w Rozdziale XII (art. 99). Ponadto, organy nadzoru rynku rozpoznają skargi osób fizycznych i prawnych dotyczące naruszeń AI Act (art. 85 AI Act), a także uprawnione są do weryfikacji prawidłowej klasyfikacji ryzyka systemów AI przez dostawców (art. 80 AI Act). W zakresie kompetencji doradczych, informacyjnych i edukacyjnych, organy nadzoru rynku (jako właściwe organy krajowe) uprawnione są do wydawania aktów *soft law* (art. 70 ust. 8 AI Act). Wydaje się także, że to te organy na poziomie krajowym będą odpowiedzialne za wspieranie przyjmowania kodeksów postępowania (art. 95 AI Act).

W zakresie kompetencji współpracy, AI Act normuje możliwość m.in. fakultatywnych wspólnych postępowań organów nadzoru rynku i Komisją (art. 74 ust. 11 AI Act), współpracy w odniesieniu do nadzoru nad systemami AI ogólnego przeznaczenia wykorzystywanym do celów zakwalifikowanych jako wysokie ryzyko między krajowymi organami nadzoru rynku i Urzędem ds. AI oraz Radą ds. AI (art. 75 ust. 2-3 AI Act), informowania o podjętych środkach tymczasowych i niezgodności systemów AI na terytorium innego państwa członkowskiego (art. 79 ust. 3 i 5 AI Act). W ramach zwiększenia spójności w stosowaniu rozporządzenia, AI

⁷¹⁴ Por C. Novelli, P. Hacker, J. Morley et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, Eur. J. Risk Regul. 2024, <https://ssrn.com/abstract=4817755>. (dostęp: 7.09.2024 r.), s. 21-23.

⁷¹⁵ Por. L. Pliauskaite, *EU AI Act Stakeholder Map*, IAPP AI Governance Center, May 2024. https://iapp.org/media/pdf/resource_center/eu_ai_act_stakeholder_map.pdf (dostęp: 7.09.2024 r.).

Act normuje specjalną procedurę „Unijną procedurę ochronną” (art. 81 AI Act), którą można określić jako procedurę kompozytową, w której czynności procesowe podejmowane są zarówno przez organy krajowe, jak i przez organy unijne (Komisję). Celem tej procedury jest możliwość weryfikacji na poziomie unijnym środków przyjętych przez poszczególne organy nadzoru rynku przez inne takie organy lub Komisję. Centralnym podmiotem w tej procedurze jest Komisja, która uprawniona jest (po wypełnieniu czynności proceduralnych) do rozstrzygnięcia, czy nałożony środek krajowy jest uzasadniony (art. 81 ust. 1 AI Act). W przypadku pozytywnej decyzji pozostałe państwa członkowskie zobowiązane są do podjęcia adekwatnych działań w odniesieniu do danego systemu AI; zaś w przypadku decyzji negatywnej, krajowy organ nadzoru winien wycofać zastosowany środek (art. 81 ust. 2 AI Act). Za kompetencje współpracy mogą być także uznane obowiązki informacyjne wobec Komisji nałożone na krajowe organy nadzoru takie jak przewidziany w art. 81 ust. 1 Aktu w sprawie Sztucznej Inteligencji.

W AI Act wprowadzono instrumenty współpracy między organami administracji publicznej ustanowionymi na podstawie innych aktów. Prawodawcy krajowi mogą rozbudować lub wprowadzić nowe instrumenty współpracy między organami przy implementacji tego rozporządzenia. W założeniu AI Act nie powinien wpływać na kompetencje organów ochrony danych osobowych zgodnie z motywem 10 AI Act. Kluczowy instrument współpracy między organami unormowany został przez odniesienie do kategorii „organów ochrony praw podstawowych” (art. 77 AI Act), do których należy zaliczyć także organy ochrony danych (wobec brzmienia art. 51 ust. 1 RODO). Organy zakwalifikowane do tej kategorii (art. 77 ust. 2 AI Act) są uprawnione do wnioskowania o przedstawienie dokumentów w odniesieniu do systemów wysokiego ryzyka (w Załączniku III), a także o wnioskowanie do organów nadzoru rynku o przeprowadzenie testów systemów wysokiego ryzyka (art. 77 ust. 3 AI Act). Ponadto, organy nadzoru rynku zobowiązane są do poinformowania „organów ochrony praw podstawowych” po stwierdzeniu ryzyka dla praw podstawowych (art. 78 ust. 2 AI Act) i – w przypadku takiego unormowania na poziomie krajowym – współpracy przy wykonywaniu kompetencji naprawczych, a także informowania o poważnych incydentach związanych z ochroną praw podstawowych (art. 77 ust. 7 AI Act). Ponadto, właściwe organy krajowe przy wydawaniu *soft law*, w tym „wskazówek i porad” dla podmiotów nadzorowanych, zobowiązane są zasięgnąć opinii innych organów (w tym organów ochrony danych), w przypadku, jeżeli dotyczy to kwestii, w których to te organy są kompetentne (art. 70 ust. 8 AI Act).

3.6. PODSUMOWANIE

W tym rozdziale scharakteryzowano kompetencje 16 organów – 7 organów na poziomie unijnym i 9 organów na poziomie krajowym. Z tej analizy wynika, że organy te najczęściej działają w tandemie, w którym zasadniczą część kompetencji proceduralnych i naprawczych przyznano organom krajowym, natomiast organy na poziomie unijnym wyposażono w kompetencje współpracy i doradcze w celu zapewnienia spójności. Nie jest to jedyny model struktury organów, jaki zidentyfikowano. Zasadne jest wyróżnienie co najmniej trzech modeli według kryterium rodzaju kompetencji przyznanych organom na poziomie unijnym. Pierwszy to scentralizowany model charakterystyczny tak dla unijnego prawa konkurencji z kluczową rolą Komisji (w sprawach kwalifikowanych jako wspólnotowe), jak i dla DMA. Drugi to model pośredni, w którym organowi na poziomie unijnym, oprócz roli doradczej, przyznano także pewne kompetencje w procedurze wydawania decyzji, przyznając tym samym kompetencje naprawcze, co jest charakterystyczne dla RODO, które ustanawia mechanizm spójności z udziałem EROD, ale także dla m.in. AI Act. Trzeci model jest zdecentralizowany – organ unijny otrzymuje kompetencje (w przeważającej mierze) doradcze, co charakteryzuje z kolei Akt w sprawie Danych i Akt w sprawie Zarządzania Danymi. Wybór modelu uzależniony jest od szeregu czynników, począwszy od dylematu między efektywnością stosowania prawa wynikającą z centralizacji (zwłaszcza wobec największych podmiotów) a ustanowieniem organów blisko podmiotów danych w ich państwach członkowskich, aby ułatwić realizację praw podstawowych, aż po polityczną wolę państw członkowskich w trakcie unijnego procesu legislacyjnego.

Z uwagi na sposób formułowania przepisów normujących przetwarzanie danych osobowych, który polega na preferowaniu przez prawodawcę norm-zasad i terminów nieostrych, kompetencje organów administracji publicznej powinny być analizowane łącznie z krzyżowaniem się zakresu przedmiotowego tych aktów. Pozwala to na ustalenie, że kompetencje organów ustanowionych na podstawie RODO krzyżują się z kompetencjami innych organów. To krzyżowanie nie jest w pełni oczywiste na podstawie samego brzmienia tych aktów, lecz ujawnia się najczęściej dopiero na etapie ich stosowania. Zwiększa to znaczenie organów stosujących to prawo, ponieważ dysponują one dyskretywnością przy dokonywaniu wykładni tych norm-zasad i terminów nieostrych, jak i *soft law* jako instrumentu, który zmniejsza niepewność prawną po stronie podmiotów nadzorowanych.

Jak ustalono, każdy z analizowanych organów wyposażony jest w kompetencje, które na etapie stosowania prawa wpływają lub mogą wpłynąć na przetwarzanie danych osobowych. Na

podstawie każdego z tych aktów istnieje możliwość nałożenia wysokich, wielomilionowych kar pieniężnych przez te organy. Wszystkie te struktury pozostają ze sobą w interakcji zarówno na poziomie unijnym, jak i krajowym w związku z rozbudowanymi kompetencjami doradczymi, edukacyjnymi i informacyjnymi oraz (w ograniczonym zakresie) kompetencjami proceduralnymi i naprawczymi. Kompetencje współpracy między organami w poszczególnych strukturach, które umożliwiają tę interakcję, nie są jednak precyzyjne i zasadniczo nie są obligatoryjne, co powoduje, że niejasne jest, w jakich sytuacjach, w jakich formach i z jakimi skutkami prawnymi ta współpraca powinna następować. Analiza zjawiska krzyżowania się kompetencji i instrumentów prawnych wprowadzonych, aby zredukować negatywne konsekwencje tego zjawiska, jest przedmiotem kolejnego rozdziału.

Najważniejszą rolę wśród organów stosujących prawo w tym obszarze należy przypisać organom nadzorczym ustanowionym na podstawie RODO (w Polsce – PUODO). Nie wynika to tylko z brzmienia RODO i UODO, ale także z wagi przypisanej tym organom w KPP i TFUE. W konsekwencji, są to organy kompetentne we wszelkich sprawach dotyczących ochrony danych osobowych. Tak szeroko ujęta kompetencja prowadzi do krzyżowania się z kompetencjami innych organów. Dotyczy to zarówno organów ustanowionych w odrębnych kompleksowych gałęziach prawa z kilkudziesięcioletnią historią, jak na przykład Komisji i Prezesa UOKiK jako organów prawa konkurencji, jak i organów właściwych ustanowionych na podstawie DGA i Data Act, które należałoby (przynajmniej roboczo) zaliczyć do dopiero powstającej odrębnej kompleksowej gałęzi prawa – „prawa danych osobowych” lub „prawa ochrony danych osobowych”⁷¹⁶. Niezależność tych organów (albo przynajmniej postulat niezależnego wykonywania przez nie kompetencji) jest w mniejszym lub w większym stopniu ustanowiona jako postulat w tych aktach. W żadnym jednak wypadku, nawet w odniesieniu do Prezesa UOKiK, nie wprowadzono równie rozbudowanych gwarancji tej niezależności jak w wypadku organów ustanowionych na podstawie RODO. W konsekwencji, to, że innym organom administracji publicznej, w tym organom stanowiącym element struktury organizacyjnej administracji rządowej (na przykład, GIIF) przyznano kompetencje w obszarze przetwarzania danych osobowych stanowi zagrożenie dla tej niezależności, co z kolei jest zagrożeniem dla prawidłowego wykonywania praw podmiotowych – prawa do prywatności i prawa do ochrony danych osobowych.

⁷¹⁶ Analiza tej kwestii jest przedmiotem badania w podrozdziale 5.5. tej rozprawy.

4. ROZDZIAŁ 4 – KRZYŻOWANIE SIĘ KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ STOSUJĄCYCH AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

4.1. WSTĘP

W tym rozdziale dokonano analizy zjawiska krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych. W pierwszej kolejności zbadano, czym jest pojęcie krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych, a następnie dokonano wyróżnienia typów tego zjawiska. Weryfikacji podlegała hipoteza, że przez krzyżowanie się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych należy rozumieć sytuację prawną, w której co najmniej dwóm organom przyznane zostały kompetencje w tej samej sprawie albo w odniesieniu do tego samego zagadnienia w taki sposób, że może prowadzić to do rozstrzygnięcia tej samej sprawy lub tego samego zagadnienia odmiennie. Do spełnienia tej definicji nie jest jednak konieczne, aby doszło do takiego odmiennego rozstrzygnięcia.

Zasadne jest wyróżnienie następujących typów tego zjawiska: właściwe i niewłaściwe; zamierzone (kiedy było to intencją prawodawcy) i niezamierzone (kiedy nie było to intencją prawodawcy); w wymiarze horyzontalnym (kiedy krzyżowanie się kompetencji ujawnia się z perspektywy organów administracji) i wertykalnym (kiedy krzyżowanie się kompetencji ujawnia się z perspektywy podmiotów nadzorowanych). W dalszej części rozdziału zweryfikowane zostało czy wprowadzone zostały skuteczne instrumenty prawne, aby zredukować negatywne konsekwencje zjawiska krzyżowania się kompetencji tych organów, przyjmując, że za niewystarczające należy uznać dotychczas wprowadzone instrumenty zarówno w wymiarze prawa procesowego (np. rozstrzyganie sporów o właściwość i instrumenty współpracy), jak i prawa materialnego (np. klauzule „bez uszczerbku”). Następnie zbadano skutki tego zjawiska dla administracji publicznej, podmiotów nadzorowanych i podmiotów danych oraz dla gospodarki.

W ostatniej części celem ustalenia czy zjawisko to występuje tylko w polskiej jurysdykcji, czy tylko w jurysdykcjach unijnych, dokonano ograniczonej analizy prawnoporównawczej jurysdykcji Królestwa Niderlandów i Wielkiej Brytanii w odniesieniu do rozwiązań przyjętych w tych jurysdykcjach w celu zredukowania negatywnych skutków analizowanego w tym rozdziale zjawiska.

4.2. DEFINICJA KRZYŻOWANIA SIĘ KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ STOSUJĄCYCH AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

W niniejszym podrozdziale zaproponowano definicję zjawiska krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych. Zanim propozycja tej definicji zostanie przedstawiona, wpierw należy wskazać, że poprawne sformułowanie jakiegokolwiek definicji w nauce prawa (administracyjnego) wymaga ścisłego przestrzegania logicznych reguł prawidłowego ich formułowania (warunków poprawności definicji)⁷¹⁷. Definicja wyrazu (*definiendum*) „polega na podaniu równoznacznika definiowanego wyrazu lub typowego kontekstu, w którym wyraz ten bywa używany” (*definiens*)⁷¹⁸; kontekst podawany jest zwłaszcza, aby wprowadzić we właściwe rozumienie *definiendum*ⁱ. Propozycja poniższej definicji projektującej jest użyteczna, ponieważ wprowadza do języka prawniczego dogmatyki prawa administracyjnego nowy termin, który dotychczas nie był używany w proponowanym znaczeniu. Tymczasem jego wprowadzenie i użycie jest potrzebne, aby adekwatnie opisać zjawisko, którego występowanie w obszarze przetwarzania danych osobowych uległo intensyfikacji w ostatnich latach, stąd też wprowadzenie tej definicji ma wartość poznawczą dla dyskusji o przyszłości modelu regulacji przetwarzania danych osobowych w UE ⁷¹⁹. Według wiedzy autora zaprezentowane w niniejszej rozprawie całościowe ujęcie zjawiska krzyżowania się kompetencji organów w obszarze przetwarzania danych osobowych, którego dokonano w niniejszej rozprawie, stanowi *novum* w polskiej i anglojęzycznej dogmatyce prawa. Niniejsza rozprawa ma tę lukę uzupełnić.

Zjawisko krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych należy zdefiniować jako sytuację prawną, w której co najmniej dwóm organom administracji publicznej przyznane zostały kompetencje w tej samej sprawie albo w odniesieniu do tego samego zagadnienia w taki sposób, że może prowadzić to do rozstrzygnięcia tej samej sprawy lub tego samego zagadnienia w sposób odmienny⁷²⁰.

⁷¹⁷ Por. przykładowo K. Ajdukiewicz, *Zarys logiki*, Warszawa 1958, s. 29-46.

⁷¹⁸ K. Ajdukiewicz, *Zarys logiki*, Warszawa 1958, s. 30.

⁷¹⁹ Por. analizę w przedmiocie rozłączenia regulacyjnego w podrozdziale 5.2. rozprawy.

⁷²⁰ Por. też P. Hajduk, *A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research* (November 23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 – Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.), s. 4-5.

Poniżej scharakteryzowane zostaną elementy tej definicji. Pojęcia kompetencji organów administracji publicznej i organów administracji publicznej zbadano już w rozdziale I rozprawy. Celem zastosowania terminu „zjawisko” w *definiendum* jest podkreślenie, że chodzi o element rzeczywisty, który występuje w czasie i przestrzeni (w ten sposób ukazuje się świadomości⁷²¹), a oprócz jego normatywnego wymiaru powinien być także ujmowany z perspektywy prakseologicznej i nauki o administracji. Termin „zjawisko” używany jest w języku prawnym i prawniczym. Zgodnie z analizą ilościową w SIP LEX, termin ten użyty był w języku prawnym w obowiązujących aktach prawnych 12.103 razy⁷²², a w języku prawniczym w dziedzinie „Administracyjne prawo i postępowanie” – 3.941 razy⁷²³. Jest to zatem termin, którego użycie jest powszechne.

Zbliżony cel służy użyciu terminu „sytuacja prawna” w *definiensie*⁷²⁴. „Sytuacja prawna” pojmowana jest jako sytuacja („ogół warunków, w których coś się odbywa”⁷²⁵) podmiotu, której elementy ukształtowane są bezpośrednio lub pośrednio prawnie⁷²⁶. Użycie terminu „sytuacja prawna” pozwala zatem zwrócić uwagę, że definiowane zjawisko ujawnia się także poza jego podstawowym wymiarem normatywnym. Tworzy bowiem ogół warunków (w tym ekonomicznych), w których działania podejmują (lub uprawnione są albo zobowiązane są podjąć, ale nie wypełniają tego obowiązku) organy administracji publicznej, jak i podmioty nadzorowane oraz podmioty danych.

Zasadne jest także użycie frazy „krzyżowania się”⁷²⁷ w *definiendum*. Fraza „krzyżowanie się” w odniesieniu do stosunku między zakresami pojęć używana jest w logice; „pojęcie S krzyżuje się (...) z zakresem pojęcia P, gdy: a) każdy z obu zakresów ma elementy tylko jemu

⁷²¹ Por. Podsiad A., *Słownik terminów i pojęć filozoficznych*, Warszawa 2001, s. 961-962.

⁷²² Odczyt na dzień 11 września 2024 r.

⁷²³ Odczyt na dzień 11 września 2024 r. Przykładowe użycie tego terminu przez Z. Kmiecika (Z. Kmeciak, *Idea badań prawnoporównawczych Franciszka Longchamps de Bérier*, PiP 2019, nr 5, s. 22-36): „Idealistyczna wizja uniwersalnego porządku prawnego, którą jeszcze na początku XX w. roztaczało wielu autorów, została zastąpiona przyziemniejszymi hasłami. Współcześnie wyraża je dążenie do poszukiwania najlepszych sposobów rozwiązywania określonych problemów czy choćby tylko zrozumienia istoty pewnych zjawisk, ich przyczyn i następstw [podkreślenie własne autora rozprawy]”.

⁷²⁴ Por. M. Krawczyk, 5. *Teoretyczna konstrukcja władztwa administracyjnego* [w:] *Podstawy władztwa administracyjnego*, Warszawa 2016, SIP LEX. Definicja zaproponowana w tej rozprawie różni się od definicji w przywołanej pozycji, w tym przez usunięcie wyrazu „społeczna” po wyrazie „sytuacja”. Zdaniem autora tej rozprawy, nie ma powodu, aby ograniczać zakres znaczeniowy „sytuacji prawnej” tylko do „sytuacji społecznej”.

⁷²⁵ *Sytuacja*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/slowniki/sytuacja.html>

⁷²⁶ J. Lemańska, Część pierwsza. Wygłoszone referaty. I. Pewność sytuacji prawnej jednostki w materialnym prawie administracyjnym [w:] *Pewność sytuacji prawnej jednostki w prawie administracyjnym*, red. A. Błaś, Warszawa 2012, SIP LEX.

⁷²⁷ „Krzyżowanie się”, zgodnie ze *Słownikiem języka polskiego PWN*, to, m.in. „być ułożonym na krzyż”. Por. *Krzyżować się*, [hasło w:] *Słownik języka polskiego PWN* [online:], <https://sjp.pwn.pl/szukaj/krzyzowac%20sie.html>. W odniesieniu do definicji w tym podrozdziale bardziej adekwatne jest rozumienie terminu „krzyżowanie” w logice.

właściwe i nie należące do zakresu drugiego z tych pojęć, ale gdy b) oprócz tego istnieją też elementy wspólne obu zakresom”⁷²⁸. Analogiczna sytuacja ma miejsce w odniesieniu do definiowanego zjawiska, ponieważ część spraw lub zagadnień w obszarze przetwarzania danych osobowych, które objęte są kompetencjami jednego organu administracji publicznej (np. organu ochrony danych), objęte są także kompetencjami innego organu (np. organu prawa konkurencji), przy czym oba te organy wyposażone są w kompetencje obejmujące sprawy lub zagadnienia, które nie są dla nich wspólne. Nadto, fraza „krzyżowanie się kompetencji” używana jest już w języku prawniczym⁷²⁹ w tym w orzecznictwie sądów administracyjnych⁷³⁰. Alternatywą dla frazy „krzyżowanie się kompetencji” mogłaby być fraza „nakładanie się kompetencji”. Ta fraza jest używana w języku prawniczym⁷³¹ i w ograniczonym zakresie także w języku prawnym⁷³² w tym kontekście. Pomimo tego, że ta druga fraza („nakładanie się⁷³³ kompetencji”) również bywa używana, to, zdaniem autora tej rozprawy, użycie frazy „krzyżowanie się kompetencji” z uwagi na wskazaną wyżej konotację z logiką formalną jest bardziej adekwatne, ponieważ zwiększa precyzję języka prawniczego i prawnego.

Zjawisko krzyżowania się kompetencji może zachodzić w przypadku krzyżowania się większej liczby organów niż dwa. Istotne jest, że zjawisko to może występować w dwóch typach wyróżnione według kryterium typów kompetencji jako właściwe i niewłaściwe (por. podrozdział 4.3 rozprawy). W przypadku kompetencji określanych jako władcze będzie to krzyżowanie się kompetencji „w tej samej sprawie” (właściwe), ponieważ ujawniało się w będzie w postępowaniach dotyczących konkretnej sytuacji faktycznej i konkretnego adresata. Natomiast w przypadku kompetencji określanych jako niewładcze (doradczych, informacyjnych i edukacyjnych) będzie to krzyżowanie się kompetencji „w odniesieniu do tego

⁷²⁸ K. Ajdukiewicz, *Zarys logiki*, Warszawa 1958, s. 22.

⁷²⁹ Por. M. Cilak, Problem krzyżowania się kompetencji nadzorczych wojewody i regionalnych izb obrachunkowych w sferze działalności gospodarczej samorządu terytorialnego, FK 2013, nr 1-2, s. 40-47. Por. także F. M. Elżanowski, 1.3. Instytucja współdziałania w toku postępowania administracyjnego z organami administracji Unii Europejskiej [w:] *Prawnoprocesowa sytuacja przedsiębiorstwa energetycznego w sprawach z zakresu regulacji energetyki*, Warszawa 2015. SIP LEX. Analiza ilościowa występowania tej frazy w komentarzach i publikacjach dotyczących „Administracyjnego prawa i postępowania” w SIP LEX dała 22 rekordy (odczyt na 17.02.2024 r.).

⁷³⁰ Przykładowo: Wyrok NSA z 5.12.2017 r., II OSK 346/17, SIP LEX nr 2449251. Wyrok NSA z 6.05.2015 r., I OSK 2287/13, SIP LEX nr 1773636. Nadto, 5 wyroków WSA (odczyt na 17.02.2024 r.).

⁷³¹ Analiza ilościowa występowania tej frazy w komentarzach i publikacjach dotyczących „Administracyjnego prawa i postępowania” w SIP LEX dała 41 rekordy (odczyt na 17.02.2024 r.).

⁷³² Analiza ilościowa występowania tej frazy w obowiązujących aktach dotyczących „Administracyjnego prawa i postępowania” w SIP LEX dała 2 rekordy (odczyt na 17.02.2024 r.).

⁷³³ „Nakładanie się”, zgodnie ze *Słownikiem języka polskiego PWN*, to, m.in. „zachodzenie na siebie” lub „zostanie umieszczonym na czymś”. Por. *Nakładać się*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/slowniki/nakladac%20sie.html>

samego zagadnienia” rozumianego jako „sprawa wymagająca zastanowienia”⁷³⁴, której interpretacja została przedstawiona przez dany organ najczęściej w instrumencie typu *soft law*. Przyznane organom kompetencje prowadzą do ich krzyżowania tylko, jeżeli mogą prowadzić do odmiennego rozstrzygnięcia, lecz nie jest niezbędne, aby do tego odmiennego rozstrzygnięcia doszło, ponieważ już sama możliwość odmiennego rozstrzygnięcia wywołuje skutki, zwiększając niepewność prawną po stronie organów i podmiotów nadzorowanych.

Zastrzec należy, że powyższa definicja nie dotyczy relacji między kompetencjami organów administracji publicznej ustanowionymi w poszczególnych państwach członkowskich, czyli, przykładowo, relacji między organami ochrony danych osobowych w Niemczech i w Polsce. Zjawisko krzyżowania się kompetencji organów administracji publicznej nie jest zresztą właściwe tylko do obszaru przetwarzania danych osobowych. Z uwagi na złożoność prawa administracyjnego materialnego do tego krzyżowania się dochodzi właściwie dość często. W anglojęzycznej literaturze zjawisko to („*regulatory overlap*”) zidentyfikowano w różnych jurysdykcjach, m.in. w prawie ochrony środowiska, regulacji sektora finansowego, prawie nieruchomości i prawie handlowym⁷³⁵. W administracyjnym prawie unijnym charakterystyczne jest krzyżowanie się kompetencji między sektorowymi organami regulacyjnymi (jak Prezes Urzędu Komunikacji Elektronicznej czy Prezes Urzędu Regulacji Energetyki) a organami prawa konkurencji i ochrony konsumenta (w Polsce Prezesem Urzędu Ochrony Konkurencji i Konsumenta), który jest kompetentny wobec wszystkich sektorów⁷³⁶. W literaturze wskazuje się, że kompetencje sektorowych organów regulacyjnych i organów prawa konkurencji i ochrony konsumenta winny być traktowane komplementarnie⁷³⁷. Krzyżowanie się kompetencji organów administracji publicznej nie jest także zjawiskiem zupełnie nowym dla obszaru przetwarzania danych osobowych. W dokumentach urzędowych EIOD jego istnienie sygnalizowane było już co najmniej do 2014 r.⁷³⁸ To, co uległo zmianie od 2014 r. to intensyfikacja procesu transformacji

⁷³⁴ Zagadnienie, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/sjp/zagadnienie;2542263.html>

⁷³⁵ L. Robb, T. Candy, F. Deane, *Regulatory overlap: A systematic quantitative literature review*, „Regulation & Governance” 2023, Vol. 17, No. 4, <https://doi.org/10.1111/rego.12504> (dostęp: 20.09.2024 r.), s. 1131, 1140.

⁷³⁶ K. Jaroszyński, M. Wierzbowski, §23. *Funkcja regulacji gospodarczej*, [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 326.

⁷³⁷ Por. K. Jaroszyński, M. Wierzbowski, §23. *Funkcja regulacji gospodarczej* [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 326. Por. także wyrok TS z 22.03.2022 r., C-117/20, Bpost SA przeciwko Autorité Belge De La Concurrence, SIP LEX nr 3324166, który scharakteryzowano w podrozdziale 4.5. rozprawy.

⁷³⁸ Por. Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital

cyfrowej⁷³⁹ i zwiększenie liczby aktów prawnych normujących przetwarzanie danych osobowych, w tym przede wszystkim aktów prawnych przyjętych po 2020 r. w formie rozporządzeń unijnych, które stosowane są bezpośrednio.

Tak rozumiane krzyżowanie się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych oddzielić należy od „współstosowania aktów prawnych”, które, jak wskazuje M. Sakowska-Baryła, „wprawdzie posiadają pewien wspólny obszar wpływów, ale zasadniczo służą realizacji innych celów i gwarancji konstytucyjnych”⁷⁴⁰. Przykładowo, w obszarze przetwarzania danych osobowych chodziłoby zatem o sytuacje, w których przetwarzanie danych osobowych przy jednoczesnym przestrzeganiu aktów prawnych sektorowych musi być zgodne z RODO. Podmiot nadzorowany (i organ administracji publicznej) zobowiązany jest wówczas do jednoczesnego przestrzegania RODO i sektorowego aktu prawnego⁷⁴¹. W założeniu prawa i obowiązki wynikające ze wszystkich współstosowanych aktów prawnych w systemie prawnym winny być komplementarne. Pojęcie krzyżowania się kompetencji organów jest powiązane z pojęciem współstosowania aktów prawnych, ponieważ oba dotyczą „wspólnego obszaru wpływu” prawa. Krzyżowanie się kompetencji jest jednak terminem o szerszym zakresie znaczeniowym, ponieważ obejmuje nie tylko przypadki „współstosowania prawa”, ale do stwierdzenia tego zjawiska nie jest konieczne dokonanie tego (współ-)stosowania, wystarczający jest sam fakt krzyżowania się kompetencji, który może zmaterializować się w akcie (współ-)stosowania aktów prawnych. Pojęcia krzyżowania się kompetencji organów i współstosowania organów dotyczą zatem powiązanych, ale odmiennych zjawisk. Istotne jest, że zjawisko krzyżowania się kompetencji winno być ujmowane w perspektywie prawa ustrojowego jako efekt systemowego skomplikowania pozycji ustrojowej i relacji między organami administracji publicznej (zob. poniżej pojęcie „układu kompetencyjnego”), co powoduje zwiększenie niepewności prawnej po stronie podmiotów administrujących i nadzorowanych.

Jednakże należy zgodzić się ze stanowiskiem w literaturze, że zjawiska krzyżowania się kompetencji organów administracji publicznej nie należy oceniać z góry jako pozytywnego, ani

Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 15.09.2024 r.).

⁷³⁹ Por. podrozdział 5.2. rozprawy.

⁷⁴⁰ M. Sakowska-Baryła, 3. Problem współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych [w:] P. Fajgielski, A. Mednis, K. Gałęzowska et al., Prywatność a jawność: bilans 25-lecia i perspektywy na przyszłość, Warszawa 2016.

⁷⁴¹ Por. M. Sakowska-Baryła, 6.2. Współstosowanie – znaczenie pojęcia i zakres [w:] Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego, Warszawa 2022, SIP LEX.

negatywnego. Nie ulega wątpliwości, że zjawisko to wywołuje przede wszystkim negatywne konotacje. W literaturze wskazywano na jego liczne negatywne skutki⁷⁴², np. niepewność prawną, niespójność stosowania prawa, duplikowanie działań podejmowanych przez różne organy, spory o właściwość, zwiększone koszty zarządzania administracyjnego, zmniejszenie skuteczności prawa⁷⁴³. Zjawisko to z różnych przyczyn może być jednak pożądane przez prawodawcę i mieć pozytywne skutki⁷⁴⁴, na przykład przez skonstruowanie sytuacji, w której administracja publiczna zajmuje się jednym obszarem z perspektywy różnych wartości przez różne podmioty administrujące⁷⁴⁵, co prowadzić ma ostatecznie do realizacji wspólnego interesu publicznego. Konieczne do tego jest jednak należy „współdziałanie władz”, o którym mowa w Preambule do Konstytucji RP. Negatywne i pozytywne skutki zjawiska krzyżowania się kompetencji powinny być badane w perspektywie przyczyn jego występowania, ponieważ tylko identyfikacja tych przyczyn pozwala ustalić, czy ustanowienie prawa powodującego powstanie tego zjawiska jest uzasadnione względem charakteru i wagi jego skutków⁷⁴⁶.

Dla kontekstu analizowanego zjawiska istotna jest charakterystyka zakazu domniemania kompetencji przez podmioty administrujące w odniesieniu do konstytucyjnej zasady legalizmu i osobno pojęcia układu kompetencyjnego. Zakaz domniemania kompetencji obejmuje zarówno władzę prawodawczą, sądowniczą i wykonawczą, a źródło ma w konstytucyjnych zasadach: legalizmu (art. 7 Konstytucji RP) potwierdzonej w art. 6 KPA i demokratycznego państwa prawa (art. 2 Konstytucji RP)⁷⁴⁷. Zgodnie z art. 7 Konstytucji RP, organy władzy publicznej działają na podstawie i w granicach prawa, przy czym podstawowe źródło prawa stanowi ustawa z uzupełnieniem o inne źródła powszechnie obowiązującego prawa, a w odniesieniu do prawa unijnego – ratyfikowane umowy międzynarodowe (art. 87

⁷⁴² Negatywne skutki tego zjawiska w obszarze przetwarzania danych osobowych zbadane zostały w podrozdziale 4.5. rozprawy.

⁷⁴³ L. Robb, T. Candy, F. Deane, *Regulatory overlap: A systematic quantitative literature review*, „Regulation & Governance” 2023, Vol. 17, No. 4, <https://doi.org/10.1111/rego.12504> (dostęp: 7.09.2024 r.), s. 1138. Por. także T. S. Aagaard, *Regulatory Overlap, Overlapping Legal Fields, and Statutory Discontinuities*, „Virginia Environmental Law Journal” 2011, Vol. 29, No. 3, <https://ssrn.com/abstract=1886573> (dostęp: 7.09.2024 r.), s. 286-289.

⁷⁴⁴ Ich charakterystyka nie jest przedmiotem niniejszej rozprawy z uwagi na ograniczenie długości i to, że, zdaniem autora, dyskusja w literaturze na temat tego zjawiska jest na wczesnym etapie i powinna rozpocząć się od analizy negatywnych jego skutków, aby pojąć jego pilność i wagę. Pozytywne skutki tego zjawiska stanowią interesujący problem badawczy.

⁷⁴⁵ T. S. Aagaard, *Regulatory Overlap, Overlapping Legal Fields, and Statutory Discontinuities*, „Virginia Environmental Law Journal” 2011, Vol. 29, No. 3, <https://ssrn.com/abstract=1886573> (dostęp: 7.09.2024 r.), s. 88.

⁷⁴⁶ Przyczyny zjawiska krzyżowania się kompetencji organów administracji publicznej w analizowanym obszarze zbadano w rozdziale 5 rozprawy.

⁷⁴⁷ J. Roszkiewicz, Rozdział V. Domniemanie kompetencji władzy wykonawczej, § 5. Dopuszczalne przypadki domniemania kompetencji organów administracji publicznej [w:] idem, *Zakaz domniemywania kompetencji i wyjątki od tego zakazu*. Studium publicznoprawne, Warszawa 2022, SIP Legalis.

ust. 1 Konstytucji RP)⁷⁴⁸. W orzecznictwie TK sprecyzowano, że organy władczy publicznej „nie mogą podejmować działań bez podstawy prawnej czy unikać wykonania kompetencji, jeżeli wiążące normy prawne nakładają na te organy określone obowiązki⁷⁴⁹”.

Zakaz domniemywania kompetencji pojmowany jest w nauce prawa administracyjnego jako „obowiązek ścisłej i literalnej wykładni norm kompetencyjnych”, który nie ma jednak charakteru absolutnego (wbrew stanowisku części doktryny), ponieważ należałoby go wówczas rozumieć jako absolutny zakaz stosowania przez podmioty administrujące innych językowa metod wykładni przepisów kompetencyjnych, co jednak nie ma podstawy prawnej⁷⁵⁰. Konstytucyjna zasada legalizmu nakłada natomiast na prawodawcę obowiązek prawidłowego skonstruowania przepisów kompetencyjnych tak, aby wywiedzione z nich normy kompetencyjne były odpowiednie względem zadań publicznych, które organy administracji publicznej mają wykonać⁷⁵¹. W praktyce jednak często sposób konstrukcji przepisów kompetencyjnych jest mało klarowny, a wywiedzenie z nich normy kompetencyjnej wymaga zastosowania wielu jednostek redakcyjnych z różnych aktów prawnych, w których użyto licznych terminów nieostrych i klauzul generalnych⁷⁵². Stąd też nie jest wyjątkiem, że organy administracji publicznej, wywodząc treść normy kompetencyjnej, stosują metody wykładni pozajęzykowej (tym samym domniemając kompetencji), czego dopuszczalność różni się jednak w zależności od działu prawa administracyjnego⁷⁵³. W literaturze przyjmuje się, że w prawie ustrojowym, w tym w odniesieniu do współpracy między podmiotami administrującymi, jest to dopuszczalne względnie szeroko, wężiej w prawie proceduralnym (kryterium stanowi wpływ na prawa i obowiązki jednostki), a najwężej w prawie materialnym z uwagi na konstytucyjną konieczność wyraźnej podstawy prawnej do ukształtowania praw

⁷⁴⁸ Por. P. Tuleja, *Komentarz do art. 7 Konstytucji RP*, [w:] *Konstytucja RP*, t. 1: *Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, nb 11, SIP Legalis.

⁷⁴⁹ Wyrok TK z 21.02.2001 r., P 12/00, OTK 2001, nr 3, poz. 47. Przywołanie za: Por. P. Tuleja, *Komentarz do art. 7 Konstytucji RP*, [w:] *Konstytucja RP*, t. 1: *Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, nb 11, SIP Legalis.

⁷⁵⁰ J. Roszkiewicz, Rozdział V. Domniemanie kompetencji władzy wykonawczej, § 5. Dopuszczalne przypadki domniemanie kompetencji organów administracji publicznej [w:] idem, *Zakaz domniemywania kompetencji i wyjątki od tego zakazu. Studium publicznoprawne*, Warszawa 2022, SIP Legalis.

⁷⁵¹ T. Długosz, Rozdział III. Kompetencja w świetle zasady legalizmu § 1. Zasada legalizmu [w:] idem, *Kompetencja w publicznym prawie gospodarczym*, Warszawa 2021.

⁷⁵² T. Długosz, Rozdział III. Kompetencja w świetle zasady legalizmu, § 2. Określoność przepisów kompetencyjnych, § 5. Dyskrecjonalne stosowanie prawa [w:] idem, *Kompetencja w publicznym prawie gospodarczym*, Warszawa 2021.

⁷⁵³ J. Roszkiewicz, Rozdział V. Domniemanie kompetencji władzy wykonawczej, § 7. Podsumowanie [w:] idem, *Zakaz domniemywania kompetencji i wyjątki od tego zakazu. Studium publicznoprawne*, Warszawa 2022, SIP Legalis.

i obowiązków jednostki, przy czym organy nie są ograniczone w domniemaniu niewładczych kompetencji doradczych, edukacyjnych.

Dokonanie wykładni przepisów kompetencyjnych w aktach prawnych normujących przetwarzanie danych osobowych nie jest łatwe. Po pierwsze, rekonstrukcja normy kompetencyjnej wymaga użycia przepisów z różnych aktów prawnych, w tym najczęściej jednocześnie prawa krajowego i prawa unijnego. Po drugie, przepisy te, zwłaszcza w treści zrębowych przepisach kompetentnych, posługują się terminami nieostryimi i klauzulami generalnymi odnoszącymi się do zakresu przedmiotowego tych aktów prawnych. Prawodawca chce w ten sposób zapewnić skuteczną realizację tych aktów. Stąd też można spodziewać się, że podmioty administrujące w tym obszarze, poszukując sposobów realizacji zadań publicznych, aby osiągnąć postawione przed nimi cele, będą skłonne sięgać do pozajęzykowych metod wykładni w celu rekonstrukcji ich norm kompetencyjnych. Znaczy to, że literalna (zwłaszcza dokonana pobieżnie) wykładnia przepisów w tym obszarze nie doprowadzi do ujawnienia wszystkich przypadków zjawiska krzyżowania się kompetencji. W praktyce zarządzania administrującego podmioty administrujące będą bowiem skłonne konstruować normy kompetencyjne przez rozszerzające interpretowanie przepisów kompetencji w granicach zakazu domniemania kompetencji, przede wszystkim przez wykładnię terminów nieostrych i klauzul generalnych. Wzmaga to zjawisko krzyżowania się kompetencji organów w tym obszarze, co stanowi wyraz napięcia między zasadą legalizmu (ograniczenia władczy publicznej prawem) a postulatem sprawnego (elastycznego) działania administracji publicznej.

Zjawisko krzyżowania się kompetencji organów w obszarze przetwarzania danych osobowych należy pojmować systemowo. Ani te organy (o różnym stopniu i źródle ustrojowej niezależności), ani ich kompetencje nie istnieją w izolacji, lecz stanowią elementy systemu administracji publicznej (wielopoziomowej administracji unijnej), które wzajemnie na siebie oddziałują⁷⁵⁴. Organy administracji publicznej realizują zatem swoje kompetencje w układach kompetencyjnych rozumianych jako zespół kompetencji poszczególnych organów powiązanych między sobą przez zależności prawne, które określają ich wzajemne relacje⁷⁵⁵. W ujęciu nauki administracji tworzy to układ administracyjny rozumiany jako określony

⁷⁵⁴ Por. R. Stankiewicz, § 1. *Specyfika relacji koordynacyjnej*, II. *Układ administracyjny jako pojęcie systemowe* [w:] idem, *Koordinacja w prawie administracyjnym*, Warszawa 2019, SIP Legalis. Por. scharakteryzowane tam pojęcie systemu i analizy systemowej administracji publicznej.

⁷⁵⁵ M. Kisała, *Układy kompetencyjne w samorządzie terytorialnym*, autoreferat, Lublin 2019, https://www.kul.pl/files/1418/public/habilitacje/dr_magdalena_kisaa/dr_M._Kisala_-_autoreferat.pdf (dostęp: 1.09.2024 r.), s. 4.

podział pracy między podmiotami administrującymi ⁷⁵⁶. Podobnie też z perspektywy podmiotów nadzorowanych poszczególne podmioty administrujące nie istnieją w separacji. Podmioty nadzorowane zobowiązane są (w zakresie podmiotowym) do przestrzegania każdego z aktów prawnych z osobna, a sankcje mogą zostać nałożone na nie przez te podmioty za naruszenie każdego z tych aktów z osobna. Stąd, aby zjawisko krzyżowania się kompetencji w obszarze przetwarzania danych osobowych ująć systemowo, w tej rozprawie dokonano w założeniu możliwie szerokiej analizy aktów prawnych i podmiotów administrujących w tym obszarze.

4.3. TYPOLOGIA KRZYŻOWANIA SIĘ KOMPETENCJI ORGANÓW

Definicja omawianego zjawiska i jego kontekstu uzupełniona jest w tym podrozdziale o jego typologię ⁷⁵⁷. Celem sformułowania typologii tego zjawiska jest dokonanie jego wewnętrznego zróżnicowania, co pozwolić ma na jego głębsze rozumienie. Dokonana analiza doprowadzała do wyróżnienia sześć typów tego zjawiska według trzech kryteriów: typu kompetencji (właściwe i niewłaściwe krzyżowanie się kompetencji), intencji prawodawcy (zamierzone i niezamierzone krzyżowanie się kompetencji) i perspektywy, w jakiej zjawisko to się ujawnia (horyzontalne i wertykalne krzyżowanie się kompetencji). W praktyce wyróżnione typy zjawiska krzyżują się w tym sensie, że konkretny przykład krzyżowania się kompetencji może przykładowo zostać zakwalifikowany jako jednocześnie niewłaściwy, zamierzony i ujawniający się w perspektywie horyzontalnej. W tym podrozdziale dokonano charakterystyki wszystkich typów, z uwzględnieniem analizy przykładów występowania tego zjawiska. Niektóre przykłady pochodzą spoza obszaru referencyjnego, który jednak jest obszarem przetwarzania danych osobowych, ponieważ w obszarze referencyjnym zawierającym w większości nowe akty prawne nie zidentyfikowano jeszcze takiej liczby różnorodnych spraw, aby przywołać je jako przykłady dla każdego z typów.

4.3.1. KRYTERIUM TYPU KOMPETENCJI (WŁAŚCIWE I NIEWŁAŚCIWE)

⁷⁵⁶ Pojęcie układu administracyjnego to będąc właściwym dla nauki administracji wykorzystywane jest z powodzeniem w nauce prawa administracyjnego, por. D. Cendrowicz, *I. Wstęp* [w:] *Układ administracji publicznej*, red. J. Korczak, Warszawa 2020, SIP LEX. Por. także Por. R. Stankiewicz, § 1. *Specyfika relacji koordynacyjnej*, *II. Układ administracyjny jako pojęcie systemowe*, [w:] idem, *Koordinacja w prawie administracyjnym*, Warszawa 2019, SIP Legalis.

⁷⁵⁷ Por. uwagi o formułowaniu typologii w podrozdziale 3.3. tej rozprawy.

Pierwsze z wyróżnionych kryteriów dotyczy typu kompetencji według ich typologii przedstawionego w podrozdziale 3.3. tej rozprawy. Zjawisko krzyżowania się kompetencji podmiotów administrujących stosujących akty prawne w obszarze przetwarzania danych osobowych może przybrać postać **właściwą**, kiedy dotyczy kompetencji władczych w rozumieniu kompetencji związanych z bezpośrednią możliwością zastosowania przymusu państwowego⁷⁵⁸ (proceduralnych; naprawczych, w tym do nakładania administracyjnych kar pieniężnych; do wydawania zezwoleń) albo **niewłaściwą**, kiedy dotyczy kompetencji niewładczych (doradczych, informacyjnych i edukacyjnych, w tym do wydawania rekomendacji). Wyróżnienie tych typów zjawiska jest zasadne, ponieważ jego skutki różnią się w zależności od typu. W przypadku właściwego krzyżowania się kompetencji uaktualnia się ryzyko prowadzenia równoległych postępowań w przedmiocie tych samych czynów przez różne podmioty administrujące i ryzyko nałożenia więcej niż jednej sankcji administracyjnej za ten sam czyn. Natomiast w przypadku niewłaściwego krzyżowania się kompetencji zasadniczym ryzykiem jest wydanie przez różne podmioty administrujące instrumentów prawnych typu *soft law*⁷⁵⁹, zgodnie z którymi w odniesieniu do tych samych kwestii (tego samego sposobu zachowania podmiotów nadzorowanych) zajęte zostaną sprzeczne lub niemożliwe do jednoczesnej realizacji w praktyce stanowiska, co prowadziło będzie do pogłębienia niepewności prawnej stronie podmiotów nadzorowanych⁷⁶⁰.

Przykładem właściwego krzyżowania się kompetencji jest scharakteryzowana już w rozdziale 2 rozprawy sprawa *Meta* rozpoznawana przez TSUE pod sygn. akt C-252/21 dotycząca relacji zachowania stanowiącego nadużycie pozycji dominującej (prawa konkurencji), które jednocześnie stanowiło naruszenie RODO. Jak wskazano w rozdziale 2, TSUE rozstrzygnął, że organy ochrony konkurencji mogą, dokonując badania nadużycia pozycji dominującej, ustalić, że zarówno warunki korzystania z usług, jak i ich wdrażanie w zakresie dotyczącym przetwarzania danych osobowych są niezgodne z RODO, o ile „to jest konieczne” do wykazania tego nadużycia. Są przy tym zobowiązane do uprzedniej konsultacji z organami ochrony danych osobowych. Z wyroku tego wynika nadto, że o ile dane zachowanie stanowi jednocześnie naruszenie RODO i nadużycie pozycji dominującej, to może być przedmiotem równoległych postępowań prowadzonych przez organy prawa konkurencji

⁷⁵⁸ J. Radwanowicz-Wanczewska, N. Fortunato, Niewładcze formy działania administracji publicznej w postępowaniu egzekucyjnym w administracji, BSP 2021, t. 26, nr 5, s. 232-233.

⁷⁵⁹ Analizy tych instrumentów dokonano w podrozdziale 5.3. rozprawy.

⁷⁶⁰ Charakterystyka skutków analizowanego zjawiska w podrozdziale 4.5.1. rozprawy.

i organy ochrony danych, a także to zachowanie może być podwójnie sankcjonowane na podstawie RODO i na podstawie prawa konkurencji⁷⁶¹.

Innym przykładem właściwego krzyżowania się kompetencji organów w tym obszarze jest sprawa dotycząca modelu tzw. „Pay or Consent” („wyraź zgodę albo zapłać”) stosowanych przez największe spółki technologiczne prowadzące media społecznościowe dla celów przetwarzania danych osobowych dla reklamy behawioralnej⁷⁶². Praktyka ta stała się przedmiotem czynności podejmowanych przez różne organy, w tym organy ochrony danych osobowych i EROD (głównie z perspektywy wymogu uzyskania ważnej i dobrowolnej zgody, co było przedmiotem analizy w opinii EROD)⁷⁶³; organy ochrony konsumentów z perspektywy nieuczciwych praktyk rynkowych, które mogą naruszać prawa konsumentów⁷⁶⁴; a także przez Komisję jako orga stosujący DMA i DSA z uwagi na to, że podmioty stosujące te praktyki spełniają kryteria podmiotowe tych aktów prawnych, a badaniu podlega czy praktyki te stanowią naruszenie art. 5 ust. 2 DMA (dotyczącego uzyskania zgody przez strażnika dostępu na przetwarzanie danych od użytkowników końcowych)⁷⁶⁵ oraz przepisów DSA dotyczących przejrzystości systemu rekomendacji (art. 27 DSA) i oceny ryzyka (art. 34 DSA)⁷⁶⁶. Na dzień złożenia tej rozprawy nie rozstrzygnięto czy stosowanie modelu „Pay or Consent” jest zgodne z prawem, a jeżeli tak nie jest – to jakie akty prawne i w jakim zakresie zostały naruszone. Z tego wzmożonego zainteresowania różnych organów tą samą praktyką wyprowadzić można natomiast przypuszczenie, że prawodawca celowo przewidywał, aby wybrane zachowania wybranych podmiotów były objęte kompetencjami więcej niż jednego organu, kierując się przy tym różnymi celami, które pozostają z sobą w powiązaniu (o czym niżej).

Z kolei przykładem niewłaściwego typu krzyżowania się kompetencji jest wymiana stanowisk w 2019 r. pomiędzy Ministrem Cyfryzacji a PUODO. Minister Cyfryzacji w dniu 23

⁷⁶¹ Por. analiza zastosowania zakazu *ne bis in idem* w prawie administracyjnym w podrozdziale 4.5.1. rozprawy.

⁷⁶² EROD, Opinia 08/2024 w sprawie ważnej zgody w kontekście modeli „wyraź zgodę albo zapłać” stosowanych przez duże platformy internetowe (Przyjęta 17 kwietnia 2024 r.), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_pl.pdf (dostęp: 15.09.2024 r.), p. 7-8.

⁷⁶³ EROD, Opinia 08/2024 w sprawie ważnej zgody w kontekście modeli „wyraź zgodę albo zapłać” stosowanych przez duże platformy internetowe (Przyjęta 17 kwietnia 2024 r.), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_pl.pdf (dostęp: 15.09.2024 r.), p. 7-8.

⁷⁶⁴ Bureau Européen des Unions de Consommateurs, *Consumer groups file complaint against Meta's unfair pay-or-consent model*, <https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model> (dostęp: 15.09.2024 r.).

⁷⁶⁵ Komisja, *Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_1689/IP_24_1689_EN.pdf (dostęp: 15.09.2024 r.).

⁷⁶⁶ Komisja, *Komisja wysłała do Meta wnioski o udzielenie informacji na podstawie aktu o usługach cyfrowych*, <https://digital-strategy.ec.europa.eu/pl/news/commission-sends-request-information-meta-under-digital-services-act-1> (dostęp: 15.09.2024 r.).

stycznia 2019 r. opublikował objaśnienia prawne w trybie art. 33 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców⁷⁶⁷ dotyczące m.in. gromadzenia przez pracodawców danych osobowych kandydatów do pracy po zakończeniu rekrutacji⁷⁶⁸. Minister Cyfryzacji wskazał w nich m.in., że pracodawcy mogą przetwarzać dane kandydatów także po zakończonej rekrutacji, aby mieć możliwość obrony przed roszczeniami tych kandydatów (np. o dyskryminację w rekrutacji). Objaśnienia te to, zgodnie z art. 33 ust. 1 przywołanej wyżej ustawy, „wyjaśnienia przepisów regulujących podejmowanie, wykonywanie lub zakończenie działalności gospodarczej, dotyczące praktycznego ich stosowania”. Objaśnienia te nie mają charakteru wiążącego dla podmiotów nadzorowanych i innych podmiotów administrujących, jednak przedsiębiorcy „nie może być obciążony sankcjami administracyjnymi, finansowymi lub karami w zakresie, w jakim zastosował się do” objaśnień prawnych (art. 35 ust. 1 i w zw. z art. 35 ust. 3 przywołanej wyżej ustawy)⁷⁶⁹. Objaśnienia te pozostawały jednak sprzeczne ze stanowiskiem PUODO, zgodnie z którym przetwarzanie danych kandydatów w celu ochrony przed roszczeniami jest niedopuszczalne⁷⁷⁰. PUODO w reakcji na te objaśnienia w swoim oświadczeniu wskazał, że nie jest nimi „formalnie związany”, i że jest jedynym organem uprawnionym do „dokonywania oficjalnej interpretacji prawa” w „sprawach dotyczących ochrony danych osobowych” i zaapelował o „niepodejmowanie działań, które mogą narazić polskich przedsiębiorców na negatywne konsekwencje i w dłuższej perspektywie utrudnić im działalność, a w konsekwencji rodzić pytanie o możliwą odpowiedzialność Skarbu Państwa za takie szkody”⁷⁷¹, czym zasugerował, że może stosować RODO, w tym nakładać administracyjne kary pieniężne, w sposób odmienny niż objaśnienia Ministra Cyfryzacji. Dyskusja ta została merytorycznie rozstrzygnięta ostatecznie dopiero w 2024 r. przez wyrok Naczelnego Sądu Administracyjnego (sygn. akt III OSK 2700/22), w którym orzeczono, że na podstawie przesłanki uzasadnionego interesu dopuszczalne jest przetwarzania danych kandydatów do pracy po zakończeniu rekrutacji w celu obrony pracodawców przed

⁷⁶⁷ T.j. Dz. U. z 2023 r. poz. 221 z późn. zm.

⁷⁶⁸ Ministerstwo Cyfryzacji, *Objaśnienia prawne z dnia 23 stycznia 2019 r. wydane przez Ministra Cyfryzacji na podstawie art. 33 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców na wniosek Rzecznika Małych i Średnich Przedsiębiorców*, dostęp: <https://mc.bip.gov.pl/objasnienia-prawne/objasnienia-prawne.html> (dostęp: 15.09.2024 r.).

⁷⁶⁹ P. Tracz [w:] *Prawo przedsiębiorców. Komentarz*, red. A. Pietrzak, Warszawa 2019, art. 33, pkt. 2.2., SIP LEX.

⁷⁷⁰ Pogląd ten przedstawiono w dokumencie Poradnik RODO Ochrona danych osobowych w miejscu pracy zreferowany został w A. M. Kaczyńska-Kral, *Spór kompetencyjny Ministra Cyfryzacji oraz Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 33 Prawa przedsiębiorców*, „Studia Iuridica” 2018, t. 77, <https://studiaiuridica.pl/article/131866/pl> (dostęp 8.09.2024 r.), s. 64-65.

⁷⁷¹ UODO, *Oświadczenie Prezes UODO w związku z planowaną konferencją Ministerstwa Cyfryzacji*, dostęp w archiwum internetowym: <http://web.archive.org/web/20210228125035/http://https://uodo.gov.pl/pl/138/672> (dostęp: 15.09.2024 r.) (ten komunikat usunięto ze strony internetowej PUODO).

potencjalnymi roszczeniami⁷⁷². Zasadnym jest przyjęcie, że aż pięcioletni okres oczekiwania na merytoryczne rozstrzygnięcie tej kwestii wywołał nieuzasadnioną niepewność prawną po stronie wszystkich administratorów danych będących pracodawcami w Polsce.

4.3.2. KRYTERIUM INTENCJI PRAWODAWCY (ZAMIERZONE I NIEZAMIERZONE)

Drugim z kryteriów istotnych dla wyróżnienia typów analizowanego zjawiska jest intencja prawodawcy, aby do zjawiska krzyżowania się kompetencji doszło. Dokonanie interpretacji intencji prawodawcy może być metodologicznie trudne, ale wydaje się możliwe, na przykład przez badanie historii i dokumentów procesu prawodawczego. Z uwagi na złożoność administracyjnego prawa materialnego, zjawisko krzyżowania się kompetencji podmiotów administrujących nie jest unikalne dla obszaru przetwarzania danych osobowych. Tak jak i w tym, tak również i w innych przypadkach bywa ono nieuniknione, ponieważ różne akty prawne ustanawiające podmioty administrujące mogą realizować odmienne, ale zbliżone wartości, co przekłada się na zakres kompetencji tych podmiotów i ich krzyżowanie⁷⁷³.

Zjawisko krzyżowania się kompetencji może być **zamierzone** przez prawodawcę. Wówczas można przyjąć, że jest to konsekwencja przemyślanej decyzji prawodawcy umotywowanej aksjologicznie i oczekiwać od prawodawcy, że ustanowił instrumenty prawne, aby przeciwdziałać negatywnym skutkom tego zjawiska i wzmocnić jego pozytywne skutki. Zjawisko to może być także **niezamierzone** przez prawodawcę, co znaczy, że prawodawca błędnie nie zidentyfikował ryzyka jego wystąpienia, zatem nie można oczekiwać ustanowienia odpowiednich mitygujących instrumentów prawnych.

Oczekiwanie ustanowienia takich instrumentów nie zawsze jest uzasadnione. Z każdym rozwiązaniem związane są bowiem określone konsekwencje; zwykle ustanowienie instrumentów współpracy prowadzi do wydłużenia czasu potrzebnego na załatwienie sprawy oraz do zwiększenia kosztów obsługi sprawy, ponieważ wymaga ona wówczas większego zaangażowania zasobów ludzkich. Zasadne jest zatem postulowanie wykorzystania tych instrumentów tam, gdzie ich korzyści (czyli zwiększenie skuteczności prawa i zmniejszenie niepewności prawnej) przewyższają negatywne konsekwencje. Przykładowo, w związku z niezwykle dużą liczbą aktów prawnych normujących przetwarzanie danych osobowych⁷⁷⁴

⁷⁷² Wyrok NSA z 20.02.2024 r., III OSK 2700/22, SIP LEX nr 3775351.

⁷⁷³ Por. analizę sprawy *bpost* dotyczącą regulacji sektorowych i prawa konkurencji w podrozdziale 4.5.1. rozprawy.

⁷⁷⁴ Por. podrozdział 2.5. tej rozprawy.

ustanowienie rozbudowanych instrumentów współpracy między wszystkimi podmiotami administrującymi ustanowionymi na podstawie tych aktów byłoby niezasadne, ponieważ większość z nich normuje przetwarzanie danych incydentalnie. Należałoby z tej grupy wydzielić te podmioty administrujące, które ustanowione zostały na podstawie aktów prawnych normujących przetwarzanie danych osobowych w stopniu większym niż incydentalny. Wyzwaniem jest, w jaki sposób wybrać precyzyjne kryterium dla takiej operacji⁷⁷⁵.

Przykłady zamierzonego krzyżowania się kompetencji zidentyfikować można w większości nowych aktów prawnych w analizowanym obszarze referencyjnym, w tym DSA, DMA, AI Act, Dyrektywa NIS 2, DGA i Data Act⁷⁷⁶. W tych aktach prawodawca unijny w ten czy inny sposób przyznał, że istnieje ryzyko krzyżowania się kompetencji podmiotów administrujących ustanowionych na podstawie tych aktów z organami ochrony danych osobowych. Formą tego przyznania są nie tylko te przepisy i motywy, które rozstrzygają o tym, że kompetencje organów ochrony danych osobowych powinny pozostać „bez uszczerbku” („*without prejudice*”), ale także o tym, że te nowe akty prawne pozostają bez uszczerbku dla RODO, lub że pierwszeństwo należy w przypadku różnic przyznać przepisom „prawa ochrony danych”⁷⁷⁷. Znaczy to, że prawodawca unijny dopuszcza, że w procesie stosowania tych aktów może dojść do sytuacji, które będą wymagały współstosowania RODO w ten czy inny sposób (przy ustaleniu zakresu przedmiotowego, czy przy ustaleniu treści praw i obowiązków podmiotów nadzorowanych). Gdyby prawodawca nie przewidywał takiego ryzyka (nie zamierzał, że nie do niego dojdzie), nie byłoby potrzeby formułowania tego typu przepisów.

Za przykład niezamierzonego krzyżowania się kompetencji przywołać można sprawę rozpoznaną przez WSA w Warszawie w wyroku z 23 lutego 2022 r. pod sygn. akt II SA/Wa 1128/21⁷⁷⁸. Sprawa ta dotyczyła obowiązku usunięcia danych osobowych niezbędnych do oceny zdolności kredytowej osoby fizycznej i analizy ryzyka kredytowego przez instytucję finansową (Spółdzielczą Kasę Oszczędnościowo-Kredytową). Osoba fizyczna, która wystąpiła do tej instytucji finansowej z wnioskiem o usunięcie jej danych osobowych, nie zawarła ostatecznie umowy kredytu z tą instytucją. PUODO w decyzji nakazał usunięcie danych, a decyzja ta została zaskarżona do WSA w Warszawie. Sąd ten oddalił skargę. Sąd argumentował, że instytucja ta nie miała podstawy prawnej do przetwarzania danych osobowych, ponieważ umowa kredytu nie została zawarta i nie można tej podstawy odnaleźć

⁷⁷⁵ Por. postulaty *de lege ferenda* w podrozdziale 5.7. rozprawy.

⁷⁷⁶ Por. analizy w rozdziale 2 i 3 niniejszej rozprawy.

⁷⁷⁷ Charakterystyki klauzuli „bez uszczerbku” („*without prejudice*”) dokonano w podrozdziale 4.4.1. rozprawy.

⁷⁷⁸ Wyrok WSA w Warszawie z 23.02.2022 r., II SA/Wa 1128/21, SIP LEX nr 3349591.

w unormowaniach sektorowych. Sąd wskazał, że w szczególności tej postawy nie stanowi art. 70a ust. 1 i 2 ustawy Prawo bankowe⁷⁷⁹, ani przepisy rozporządzenia w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji⁷⁸⁰, ani obowiązki wynikające z Ustawy o AML. Zdaniem WSA w Warszawie, PUODO nie był zobowiązany do współdziałania z KNF przy rozstrzyganiu tej sprawy. W odniesieniu do tego uzasadnienia orzeczenia M. Nowakowski podnosi, że jest ono dyskusyjne w zakresie, w jakim utrudnia realizację przez instytucje finansowe możliwości budowania modeli scoringu kredytowego i powoduje techniczne trudności związane z usuwaniem danych osobowych, które nie były zanonimizowane, ale posłużyły do budowania tych modeli⁷⁸¹.

Tę sprawę można zakwalifikować jako przykład niewłaściwego krzyżowania się kompetencji. Scharakteryzowane wyżej zagadnienia, wbrew stanowisku WSA wyrażonemu w tej sprawie, należą do zagadnień, które objęte są kompetencjami KNF co najmniej w odniesieniu do kompetencji doradczych, informacyjnych i edukacyjnych oraz wymagają uwzględnienia wymogów regulacyjnych sektora finansowego, co wymagało współdziałania z KNF na podstawie art. 7b KPA (zgodnie z odmienną linią orzecniczą sądów administracyjnych analizowaną niżej). Nie ma podstaw, aby uznać, że prawodawca przewidywał i zamierzał doprowadzić do krzyżowania się kompetencji organów ochrony danych osobowych i organów nadzoru finansowego w odniesieniu do tego zagadnienia.

⁷⁷⁹ T.j. Dz. U. z 2023 r. poz. 2488 z późn. Zm.

⁷⁸⁰ Dz. Urz. z 2012 r. nr 201, s. 1 z późn. zm.

⁷⁸¹ M. Nowakowski, *Jeśli nie ma umowy kredytowej to dane klienta pozyskane w toku procesu oceny zdolności kredytowej powinny zostać usunięte?*, Bank.pl 12.07.2022, <https://bank.pl/jesli-nie-ma-umowy-kredytowej-to-dane-klienta-pozyskane-w-toku-procesu-oceny-zdolnosci-kredytowej-powinny-zostac-usuniete/> (dostęp: 15.09.2024 r.); Por. też D. Lesner, *Prawo.pl 05.07.2022, https://www.prawo.pl/biznes/czy-bank-moze-przetwarzac-dane-osobowe-niedoszlego-kredytobiorcy,515830.html* (dostęp: 15.09.2024 r.). Wskazać należy, że to zagadnienie jest przedmiotem szeregu orzeczeń sądów administracyjnych.

4.3.3. KRYTERIUM PERSPEKTYWY, W JAKIEJ KRZYŻOWANIE SIĘ UJAWNIA (HORYZONTALNE I WERTYKALNE)

Ostatnim wyróżnionym kryterium jest perspektywa, w jakiej ujawniają się negatywne skutki analizowanego zjawiska. Mowa o perspektywie **horyzontalnej**, kiedy krzyżowanie się kompetencji ujawnia się z perspektywy struktury administracji publicznej (pomiędzy podmiotami administrującymi) i **wertykalnej**, kiedy krzyżowanie się kompetencji ujawnia się z perspektywy podmiotów nadzorowanych. Oba te typy występują zazwyczaj jednocześnie, ponieważ, jeżeli zjawisko to ma wymiar wertykalny, to ma również wymiar horyzontalny. Nie jest tak jednak w każdym przypadku, ponieważ zjawisko to może ujawnić się tylko w wymiarze horyzontalnym, jeżeli organy ochrony danych osobowych zastosują sankcję wobec innych organów administracji publicznej jako administratorów danych osobowych, jeżeli naruszenie przez nie ochrony danych osobowych spowodowane jest niezgodną z prawem, zdaniem organów ochrony danych osobowych, wykładnią prawa⁷⁸². Bardziej precyzyjne byłoby określenie, że wyróżniono typy skutków tego zjawiska (wertykalne i horyzontalne). Wyróżnienie to jest jednak także wartościowe poznawczo dla analizy kontekstu samego zjawiska. Z horyzontalnej perspektywy zjawisko to sprowadza się bowiem do ustalenia, który z podmiotów administrujących jest kompetentny do załatwienia określonej sprawy lub zajęcia stanowiska wobec określonego zagadnienia, lub w jaki sposób procedować w przypadku wystąpienia tego zjawiska w określonym układzie kompetencyjnym. Natomiast z perspektywy wertykalnej zjawisko to sprowadza się do powstania po stronie podmiotów nadzorowanych niepewności prawnej co do kompetentnego podmiotu administrującego, prawidłowej interpretacji prawa materialnego i ryzyka podwójnego ukarania za to samo zachowanie, jak również ryzyka, że to samo zachowanie będzie stanowiło delikt administracyjny zgodnie ze stanowiskiem jednego podmiotu administrującego wbrew przeciwnemu stanowisku innego podmiotu. Wyróżnienie tych dwóch perspektyw prowadzi do odmiennego ujmowania skutków tego zjawiska, jak i odmiennego zapatrywania na wagę poszczególnych instrumentów prawnych ustanowionych, aby przeciwdziałać skutkom prawnym tego zjawiska.

⁷⁸² Przykładem jest spór między Głównym Geodetą Kraju a PUODO dotyczący publikacji numerów ksiąg wieczystych w publicznie dostępnym systemie teleinformatycznym Geoportal, w którym PUODO nałożył na Głównego Geodetę Kraju administracyjne kary pieniężne. Główny Geodeta Kraju bronił się argumentując, że numery wieczystych to nie są dane osobowe, oraz że miał podstawę prawną do udostępniania tych numerów w Ustawie z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne w związku z ustawą z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej. Por. w tej sprawie wyrok WSA w Warszawie, 5 maja 2022 r., sygn. akt II SA/Wa 2222/20 i artykuł autora niniejszej rozprawy doktorskiej: P. Hajduk, *Divergence between authorities on publicly available spatial data in Poland*, „GIS Odyssey Journal” 2022, Vol. 2, No. 2.

Przykładem sytuacji, w której zjawisko to ujawnia się w wymiarze horyzontalnym, jest sprawa rozstrzygnięta przez WSA w Warszawie w wyroku z 28 września 2021 r. pod sygn. akt II SA/Wa 474/21. Klient banku będący osobą fizyczną złożył skargę do PUODO, żądając nakazania usunięcia jego danych przetwarzanych przez bank w związku ze złożonymi przez tego klienta zapytaniami kredytowymi. PUODO wydał decyzję nakazującą usunięcie danych, argumentując, że brak jest podstaw prawnych do przetwarzania jego danych. Merytorycznie sprawa dotyczyła tego samego zagadnienia, co sprawa rozpoznawana pod sygn. akt II SA/Wa 1128/21 scharakteryzowana wyżej. Inaczej niż w tej sprawie, WSA w Warszawie uchylił decyzję PUODO. WSA w Warszawie orzekł, że doszło do naruszenia art. 7b KPA, ponieważ PUODO zaniechało współdziałania z Komisją Nadzoru Finansowego jako organem kompetentnym w sprawach związanych m.in. z badaniem zdolności kredytowej i analizą ryzyka kredytowego, a także budową modeli oceny wiarygodności kredytowej. Zgodnie z zasadą wyrażoną art. 7b KPA, „w toku postępowania organy administracji publicznej współdziałają ze sobą w zakresie niezbędnym do dokładnego wyjaśnienia stanu faktycznego i prawnego sprawy, mając na względzie interes społeczny i słuszny interes obywateli oraz sprawność postępowania, przy pomocy środków adekwatnych do charakteru, okoliczności i stopnia złożoności sprawy”. WSA w Warszawie argumentował, że rozstrzygnięcie tej sprawy wymaga specjalistycznej wiedzy regulacyjnej związanej z interpretacją przepisów ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe⁷⁸³, innych regulacji sektorowych, w tym rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji⁷⁸⁴ (zwanego rozporządzeniem CRR) oraz wymogów organu nadzoru finansowego (np. w rekomendacjach KNF). PUODO złożył skargę kasacyjną od tego wyroku, argumentując, że orzeczenie to stanowi zagrożenie jego niezależności. Według wiedzy autora pracy (na dzień 15 lutego 2024 r.) sprawa ta nie została jeszcze prawomocnie rozstrzygnięta przez NSA. Zestawienie tych dwóch wyroków i analiza pozostałego orzecznictwa sądów administracyjnych prowadzi do wniosku, że nie ukształtowała się jednolita linia orzecznicza w odniesieniu do tego zagadnienia⁷⁸⁵. Sprawa ta stanowi typ krzyżowania się kompetencji, który ujawnia

⁷⁸³ T.j. Dz. U. z 2023 r. poz. 2488 z późn. zm.

⁷⁸⁴ Dz. U. UE L z 2012 r. nr 201, s. 1 z późn. zm. W tym przywołanych w uzasadnieniu tego wyroku: art. 144 ust. 1 lit. d, art. 145 ust. 1, art. 170 ust. 3 lit. a, art. 171 ust. 2 i art. 179 ust. 1 lit. a tego rozporządzenia.

⁷⁸⁵ Por. *Sądy raz każą usuwać, raz zachowywać dane. Niejasne przepisy ws. przetwarzania informacji o klientach*, Dziennik Gazeta Prawna 13 września 2022 r., <https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8535477,rodo-uodo-dane-przetrzywanie-danych.html> (dostęp: 15.09.2024 r.).

się w wymiarze horyzontalnym, ponieważ dla organów administracji publicznej (tak PUODO, jak i KNF) niejasne jest czy w tego typu sprawach PUODO zobowiązany jest współdziałać z KNF czy też nie. Sprawa ta ma również wymiar wertykalny, ponieważ niepewność prawną co do tej kwestii dzielą także podmioty nadzorowane i podmioty danych.

Z kolei przykłady spraw, w których do ujawnienia się skutków tego zjawiska dochodzi w wymiarze wertykalnym, zostały już scharakteryzowane w tym podrozdziale. To m.in. sprawa *Meta*, z której wynika, że organy ochrony konkurencji mogą incydentalnie wyklądać przepisy RODO (i w konsekwencji stosować niezależne sankcje administracyjne), czy też sprawa wymiany stanowisk między Ministrem Cyfryzacji a PUODO, która ukazała ryzyko odmiennej wykładni prawa dokonywanej przez różne organy administracji publicznej w instrumentach prawnych typu *soft law*. Podobną sytuacją do tej ostatniej jest także wymiana stanowisk między PUODO, GIIF i KNF na przełomie 2019 r. i 2020 r. dotyczących weryfikacji tożsamości klientów (możliwości kopiowania dokumentów tożsamości) przez instytucje obowiązane (przede wszystkim banki) w rozumieniu Ustawy AML, która była analizowana w podrozdziale 2.6.1. tej rozprawy.

4.4. INSTRUMENTY PRAWNE DO ZREDUKOWANIA NEGATYWNYCH SKUTKÓW

Sformułowanie definicji zjawiska krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych i typologii tego zjawiska z omówieniem przykładów pozwoliła na zrozumienie tego zjawiska i jego relacji względem zasady legalizmu oraz zakazu domniemania kompetencji. Prawodawca unijny i krajowy (co było przedmiotem analizy w poprzednich rozdziałach) w niektórych aktach prawnych zidentyfikował ryzyko krzyżowania się zakresu aktów prawnych w obszarze przetwarzania danych osobowych, a w konsekwencji ryzyko krzyżowania się kompetencji podmiotów administrujących. W konsekwencji, prawodawca ustanowił instrumenty prawne w wymiarze prawa materialnego (np. klauzule „bez uszczerbku”), ustrojowego (np. wyznaczenie organów ochrony danych osobowych jako kompetentnych „w sprawach dotyczących przetwarzania danych osobowych” w niektórych aktach prawnych), jak i procesowego (np. obowiązek współpracy z organami ochrony danych osobowych), które w założeniu mają zmniejszyć negatywne skutki występowania tego zjawiska. Oprócz specjalnie ustawionego instrumentarium ten cel mogą spełniać także przepisy KPA, np. art. 7b

KPA normujący współdziałanie organów administracji publicznej w zakresie niezbędnym do dokładnego wyjaśnienia stanu faktycznego i prawnego sprawy.

W tym podrozdziale zweryfikowano, czy instrumenty prawne ustanowione lub możliwe do zastosowania do zredukowania negatywnych skutków⁷⁸⁶ analizowanego zjawiska są wystarczające, aby skutki te zmitygować⁷⁸⁷. Dokonano charakterystyki instrumentów w wymiarze prawa materialnego, ustrojowego i procesowego. W nauce prawa administracyjnego podkreśla się związek między tymi trzema działami prawa administracyjnego, ponieważ nawet optymalnie skonstruowane prawo materialne nie może osiągnąć swoich celów bez odpowiednich unormowań ustrojowych i proceduralnych⁷⁸⁸. Chociaż zjawisko krzyżowania się kompetencji pozostaje zjawiskiem właściwym przede wszystkim dla administracyjnego prawa ustrojowego, to jego przyczyny sięgają prawa materialnego, zwłaszcza sposobu ukształtowania zakresu przedmiotowego aktów prawnych⁷⁸⁹.

Analizowanych w niniejszym podrozdziale instrumentów nie można uznać za w pełni skuteczne w tym sensie, że nie prowadzą one do zasadniczego zmniejszenia niepewności prawnej (zmniejszą ją co najwyżej częściowo). Konieczne jest zastrzeżenie, że dokonanie pełnej weryfikacji tak sformułowanej hipotezy badawczej wymagałoby badań empirycznych, które obejmowałyby zakresem zarówno urzędników podmiotów administrujących, pracowników podmiotów nadzorowanych, jak i podmioty danych. Takie badania, chociaż miałyby dużą wartość poznawczą, wykraczają poza założenia i metody tej rozprawy. Dodatkowo, przeprowadzenie takich badań na tym etapie stosowania tych aktów prawnych mogłoby być przedwczesne, ponieważ stosowanie części z nich albo jeszcze się nie rozpoczęło, albo jest na wczesnym etapie.

4.4.1. WYMIAR PRAWA MATERIALNEGO

W części dotyczącej analizy instrumentów prawnych ustanowionych w wymiarze prawa materialnego scharakteryzowano tzw. klauzule „bez uszczerbku” i normy ustanawiające relacje między aktami prawnymi w tym obszarze, które można scharakteryzować jako emanację reguły *lex specialis derogat legi generali*⁷⁹⁰.

⁷⁸⁶ Por. J. Kunysz, *Skuteczność prawa: (zagadnienia wybrane)*, „Administracja: Teoria, Dydaktyka, Praktyka” 2014, nr 2, s. 72, 74. Analizy skutków tego zjawiska dokonano w podrozdziale 4.5. poniżej.

⁷⁸⁷ O pojęciu skuteczności prawa administracyjnego por. podrozdział 4.5. poniżej.

⁷⁸⁸ M. Rudnicki, K. Sobieraj, Skuteczność prawa administracyjnego na przykładzie regulacji z zakresu międzynarodowego przemieszczania odpadów, RPEiS 2013, t. 75, z. 2, s. 15-16.

⁷⁸⁹ Por. także przyczyny analizowanego zjawiska zbadane w rozdziale 5 niniejszej rozprawy.

⁷⁹⁰ Por. Wyrok TK z 13.03.2007 r., K 8/07, OTK-A 2007, nr 3, poz. 26.

Analizowane akty prawne na poziomie unijnym wprowadzają przepisy, zgodnie z którymi ich przestrzeganie i stosowanie winno pozostawać „bez uszczerbku dla” („*without prejudice*”) „unijnego prawa danych osobowych”⁷⁹¹, w tym przede wszystkim RODO, jak i kompetencji organów ochrony danych⁷⁹². Istota problemu sprowadza się do udzielenia odpowiedzi na pytanie, czym właściwie są klauzule „bez uszczerbku” i „kolizyjną”. W literaturze (w odniesieniu do DMA), klauzula „bez uszczerbku” rozumiana jest w ten sposób, że stosowanie danego aktu prawnego powinno pozostawać bez (negatywnego) wpływu na stosowanie RODO⁷⁹³, a kompetencje organów ochrony danych osobowych nie powinny zostać ani prawnie ani faktycznie zmodyfikowane przez jego stosowanie⁷⁹⁴. Nakłada zatem na podmioty administrujące obowiązek dokonywania przestrzegania prawa w taki sposób, aby nie oddziaływało to negatywnie (sprzecznie z treścią i niezgodnie z celem) na przestrzeganie RODO. Znajduje to potwierdzenie w orzecznictwie TSUE, zgodnie z którym w przypadku braku jednoznacznego rozstrzygnięcia o pierwszeństwie jednego z rozporządzeń unijnych nad drugim, konieczne jest takie ich stosowanie, aby zapewnić ich spójność i zgodność między nimi⁷⁹⁵.

W tym kontekście wskazać należy, że w DGA i Data Act wprowadzono przepisy, zgodnie z którymi w przypadku „kolizji z prawem (...) w dziedzinie ochrony danych osobowych pierwszeństwo ma odpowiednie prawo [...] w dziedzinie ochrony danych osobowych” (por. np. brzmienie art. 1 ust. 3 DGA). Znaczy to, że jeżeli w trakcie wykładni ustalone zostanie, że ta sama sprawa objęta jest hipotezą zarówno RODO, jak i DGA, a zastosowanie DGA doprowadziłoby do innego rozstrzygnięcia, niż gdy zastosowano RODO, to należy zastosować RODO. W praktyce to organy właściwe na podstawie DGA będą podczas dokonywania wykładni operatywnej dokonywać weryfikacji tego, przy czym powinny skonsultować rozstrzygnięcie z organami ochrony danych osobowych (zgodnie z cytowanym niżej motywem 44 DGA). Funkcjonalnie ta klauzula jest regułą kolizyjną zbliżoną do reguły porządku treściowego *lex specialis derogat legi generali*, której zastosowanie poprzedzone powinno być

⁷⁹¹ M.in. DGA, Data Act, DSA, DMA, Dyrektywa NIS 2, Dyrektywa AML 5. Por. analizy poszczególnych aktów w rozdziale 2 i 3.

⁷⁹² M.in. NIS 2, DMA, DGA, Data Act. Por. analizy poszczególnych aktów w rozdziale 2 i 3.

⁷⁹³ G. Materna, A. Szmigielski, Komentarz do art. 1, nb. 42 [w:] Akt o rynkach cyfrowych – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828. Komentarz, red. M. Grochowski [w:] Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz, red. M. Grochowski, Warszawa 2024, SIP Legalis.

⁷⁹⁴ Por. też P. Hajduk, *AI Act And GDPR: On The Path Towards Overlap Of The Enforcement Structures*, 1.10.2023, <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/?cn-reloaded=1&cn-reloaded=1> (dostęp: 15.09.2024 r.).

⁷⁹⁵ Wyrok TSUE T-653/16, Republika Malty przeciwko Komisji Europejskiej, pkt. 137-140.

wykładnią językową i funkcjonalną⁷⁹⁶. Jeżeli nie doprowadzi ona do usunięcia kolizji, należy zastosować właśnie regułę *lex specialis derogat legi generali*, co prowadzić powinno do zastosowania normy szczególnej i pominięcia normy ogólnej⁷⁹⁷. W tym przypadku rolę przepisów korzystających z pierwszeństwa miałyby RODO⁷⁹⁸.

W literaturze słusznie wskazuje się, że w zestawieniu z wykorzystaną techniką legislacyjną (tj. normy-zasady, terminy nieostre i metoda oparta na ryzyku⁷⁹⁹) znaczenie i rola klauzul „bez uszczerbku” i „kolizyjnej” są niejasne (nazywane są „sztuczką retoryczną”), ponieważ nie dostarczają wskazówek, w jaki sposób ustalić relację między poszczególnymi aktami prawnymi⁸⁰⁰. Do ustalenia tej relacji dochodzi bowiem zasadniczo na etapie stosowania prawa przy jego konkretyzowaniu przez podmioty administrujące. Nawet jeżeli bowiem brzmienie tych aktów wydaje się komplementarne, to faktycznej oceny krzyżowania się ich zakresów przedmiotowych i treści wynikających z nich praw i obowiązków dokonać można dopiero na etapie ich stosowania przy uwzględnieniu znacznej władzy dyskrecyjnej podmiotów administrujących. Stąd też klauzule „bez uszczerbku” i „kolizyjną” badać można jako instrument, który wpływa na analizowane zjawisko krzyżowania się kompetencji organów.

Klauzula „bez uszczerbku” określana jest w literaturze w odniesieniu do DMA wprost jako „mit”⁸⁰¹. K. Bania argumentuje, że w przy realizacji DMA (także w zestawieniu z RODO) „może dojść do sytuacji, w których realizacji DMA uczyni niektóre przepisy bezcelowymi (choć nie było to intencją prawodawcy)”, co powoduje, że DMA „pomimo klauzuli „bez uszczerbku”, (...) nie uzupełni (lecz zagrozi) skuteczności przepisów”⁸⁰². Przykłady krzyżowania się zakresu przedmiotowego RODO z DMA scharakteryzowane zostały

⁷⁹⁶ Por. B. Wojciechowski, § 25 Zastosowanie reguł kolizyjnych w dyskursie walidacyjno-interpretacyjnym, [w:] Wykładnia w prawie administracyjnym, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 385.

⁷⁹⁷ Por. B. Wojciechowski, § 25 Zastosowanie reguł kolizyjnych w dyskursie walidacyjno-interpretacyjnym, [w:] Wykładnia w prawie administracyjnym, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 385.

⁷⁹⁸ Por. B. Wojciechowski, § 25 Zastosowanie reguł kolizyjnych w dyskursie walidacyjno-interpretacyjnym, [w:] Wykładnia w prawie administracyjnym, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 385.

⁷⁹⁹ Por. podrozdział 5.2. rozprawy.

⁸⁰⁰ P. de Hert, Post-GDPR Lawmaking in the Digital Data Society: Mimesis without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law [in:] Data at the Boundaries of European Law, ed. by D. Curtin, M. Catanzariti, Oxford 2023, <https://doi.org/10.1093/oso/9780198874195.003.0004> (dostęp: 30.01.2024 r.), s. 31.

⁸⁰¹ K. Bania, Fitting the Digital Markets Act in the existing legal framework: the myth of the “without prejudice” clause, „European Competition Journal” 2023, Vol.19, No. 1, s. 116-149.

⁸⁰² K. Bania, Fitting the Digital Markets Act in the existing legal framework: the myth of the “without prejudice” clause, „European Competition Journal” 2023, Vol.19, No. 1, s. 116-118: There may also be occasions where the DMA may render certain rules devoid of purpose (when this was clearly not the intention of the legislator). In such cases, despite a “without prejudice” clause, the DMA would not necessarily complement (but could possibly endanger) the effectiveness of existing rules, thereby undermining the overall regulatory framework that seeks to protect businesses and consumers against problematic platform conduct.

w rozdziale 2. Tutaj należy podkreślić, że przy tak znacznej bliskości zakresów przedmiotowych tych aktów prawnych i szczególnie szerokim zakresie przedmiotowym RODO nie sposób jest przy realizacji tych aktów prawnych nie „oddziaływać” (być „bez uszczerbku”) na przestrzeganie RODO i szerokie kompetencje organów ochrony danych. Te same podmioty nadzorowane są bowiem przez różne organy i zobowiązane są do przestrzegania różnych aktów prawnych, ale sposób ich działalności (i zapewnienie zgodności z prawem) może być tylko jeden. Jeżeli więc, przykładowo, podmiot nadzorowany musi dostosować działalność zgodnie z decyzją koordynatora ds. usług cyfrowych na podstawie DSA i nawet pośrednio wpływa to na przetwarzanie przez niego danych osobowych, to decyzja ta z natury rzeczy wpływa na stosowanie RODO i kompetencji organów ochrony danych i może spowodować „uszczerbek” dla RODO, ponieważ oddziałuje na sposób przetwarzania danych osobowych. Oczekiwanie, że wprowadzenie klauzuli „bez uszczerbku” doprowadzi do braku krzyżowania się zakresów przedmiotowych i krzyżowania się kompetencji organów ochrony danych powodującego ryzyko „uszczerbku” dla realizacji RODO jest bezpodstawne. Aby przeciwdziałać negatywnym skutkom tego zjawiska, konieczne byłoby ustanowienie adekwatnych instrumentów prawnych, przede wszystkim ścisłej współpracy z organami ochrony danych, co mogłoby zapewnić spójność na etapie stosowania poszczególnych aktów prawnych nie tylko na poziomie krajowym, ale także między państwami członkowskimi i w relacji wertykalnej przy stosowaniu prawa przez organy na poziomie unijnym, w tym Komisję.

Konkludując, chociaż zatem prawodawca prawidłowo zidentyfikował ryzyko krzyżowania się zakresów przedmiotowych analizowanych aktów prawnych i ryzyko krzyżowania się kompetencji podmiotów administrujących, to wprowadzone w prawie materialnym rozwiązania nie prowadzą do zmniejszenia niepewności przy ustaleniu zakresu kompetencji organów ochrony danych. Z uwagi na analizowany w rozdziale 5. rozprawy wybór techniki prawodawczej, klauzule „bez uszczerbku” i klauzule „kolizyjne” nie mogą usunąć wątpliwości przy ustalaniu tej relacji w konkretnych sytuacjach. Stanowią one jednak pomocną dyrektywę interpretacyjną, która może być wykorzystywana zwłaszcza na etapie sądowej kontroli administracji. Zasadne byłoby, aby w możliwie niedługim czasie ukształtowane zostało orzecznictwo w przedmiocie interpretacji obu klauzul, ponieważ dopiero skonkretyzowanie ich znaczenia w odniesieniu do stwierdzania czy zakres jednej normy

zawiera się w drugiej ⁸⁰³, mogłoby zasadniczo pomóc podmiotom administrującym i podmiotom nadzorowanym.

4.4.2. WYMIAR PRAWA USTROJOWEGO

W niektórych aktach prawnych w obszarze referencyjnym organy ochrony danych osobowych wskazane zostały wprost jako organy właściwe w odniesieniu do niektórych spraw. Sposób sformułowania tych przepisów ustanawiających kompetencje organów ochrony danych osobowych budzi jednak istotne wątpliwości. Przykładowo, organy nadzorcze ustanowione na podstawie RODO zostały wprost wskazane na mocy art. 37 ust. 3 Data Act jako „odpowiedzialne za monitorowanie stosowania [Data Act] w zakresie ochrony danych osobowych” (*„insofar as the protection of personal data is concerned”*). Celem przyjęcia tego rozwiązania jest zapewnienie spójności stosowania RODO i Data Act. Pojawia się jednak pytanie, jakie kwestie w Data Act objęte są „zakresem ochrony danych osobowych” z uwagi na niejasne pojęcie ochrony danych osobowych. Nie tylko niejasne jest, jakie informacje stanowią dane osobowe,⁸⁰⁴ ale także jakie konkretnie kwestie dotyczą ich ochrony, a jakie nie, w szczególności czy kryterium winien stanowić główny cel, dla którego konkretna kwestia została uregulowana. Z analizy angielskiej wersji językowej Data Act, którą zasadniej byłoby przetłumaczyć jako „w zakresie, w jakim [Data Act] dotyczy ochrony danych osobowych”, należałoby wywieść szeroką interpretację, zgodnie z którą organy nadzorcze ustanowione na podstawie RODO są odpowiedzialne za stosowanie Data Act we wszelkich kwestiach, pozostających w związku z ochroną danych osobowych (na taką interpretację wskazywałoby również brzmienie motywu 107 Data Act *in fine*⁸⁰⁵).

Chociaż przyjęcie takiej interpretacji ułatwia zdekodowanie zakresu odpowiedzialności organów w ten sposób, że wątpliwości należy rozstrzygać tak, aby to organy ochrony danych były odpowiedzialne za monitorowanie Data Act w możliwie szerokim zakresie, to wyzwanie stanowiła będzie interpretacja kwestii „z pogranicza”, na przykład w odniesieniu do danych pierwotnie nie-osobowych, które na skutek nieodpowiednio przeprowadzonej anonimizacji lub

⁸⁰³ Por. B. Wojciechowski, § 25 Zastosowanie reguł kolizyjnych w dyskursie walidacyjno-interpretacyjnym, [w:] Wykładnia w prawie administracyjnym, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 385.

⁸⁰⁴ Pojęcie danych osobowych zostało scharakteryzowane w podrozdziale 2.3. tej rozprawy.

⁸⁰⁵ Wersja polska: „Organy odpowiedzialne za nadzór nad przestrzeganiem prawa ochrony danych oraz właściwe organy wyznaczone na podstawie prawa Unii lub prawa krajowego powinny być odpowiedzialne za stosowanie niniejszego rozporządzenia w obszarach swoich kompetencji”. Wersja angielska: *„The authorities responsible for the supervision of compliance with data protection law and competent authorities designated under Union or national law should be responsible for the application of this Regulation in their areas of competence”*.

rozwoju technicznego, np. kryptografii kwantowej⁸⁰⁶, staną się danymi osobowymi, ponieważ okaże się, że można przypisać je do osoby fizycznej. Przyjęcie interpretacji, że także te kwestie objęte są zakresem odpowiedzialności organów ochrony danych osobowych, będzie oznaczało, że organy te mogą być odpowiedzialne za monitorowanie przestrzegania Data Act także w odniesieniu do przetwarzania danych nie-osobowych, o ile istnieje ryzyko, że mogą stać się danymi osobowymi. Te kwestie bowiem „dotyczą ochrony danych osobowych”. Istotne jest, że organy ochrony danych osobowych nie są odpowiedzialne za „stosowanie i egzekwowanie” Data Act tak jak właściwe organy (art. 37 ust. 1 Data Act), lecz są odpowiedzialne wyłącznie za „monitorowanie stosowania” Data Act. W praktyce pojawiają się wątpliwości, czy oznacza to, że obowiązki użytkowników, posiadaczy i odbiorców danych względem właściwych organów przewidziane w Data Act, np. obowiązki notyfikacyjne posiadaczy danych na podstawie art. 4 ust. 8 Data Act, powinny być realizowane wobec organów właściwych ustanowionych na podstawie art. 37 ust. 1 Data Act (odpowiedzialnych za „stosowanie i egzekwowanie”), czy też względem organów ochrony danych osobowych, które odpowiedzialne są tylko za „monitorowanie stosowania” Data Act. Fakt rozróżnienia brzmienia przepisów sugerowałby bowiem, że uprawnienia i obowiązki obu podmiotów administrujących w jakiś sposób się różnią.

Skoro scharakteryzowane wyżej rozwiązania powodują fundamentalną niepewność co do zakresu kompetencji organów ochrony danych osobowych względem innych organów, to nie można twierdzić, że jest to optymalne. W takich przypadkach prostym rozwiązaniem byłoby ustanowienie przez prawodawcę krajowego organów ochrony danych jako wyłącznie kompetentnych do stosowania tych aktów prawnych na poziomie krajowym, na co, przykładowo, Data Act, Digital Services i DGA pozwalają.

4.4.3. WYMIAR PRAWA PROCESOWEGO

W wymiarze prawa procesowego zbadano instrumenty współpracy podmiotów administrujących za pośrednictwem organów unijnych na poziomie unijnym i na poziomie krajowym; rozstrzyganie sporów o właściwość między organami administracji publicznej i sporów kompetencyjnych między centralnymi konstytucyjnymi organami państwa. Charakterystyczne jest, że pomiędzy analizowanymi organami trudno jest zidentyfikować

⁸⁰⁶ Por. *Kryptografia kwantowa*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 255-256.

klasyczne prawnoadministracyjne relacje kierownictwa i nadzoru⁸⁰⁷. Wynika to z czynników ustrojowych, w tym przyznania większości z tych organów przymiotu niezależności (o różnym stopniu nasilenia organizacyjnego i finansowego, który ewoluuje w kierunku jej wzmocnienia), jak również – w przypadku organów na poziomie krajowym – z unikalnego umiejscowienia tych organów w systemie unijnej administracji publicznej między poziomem krajowym a poziomem unijnym, w tym jako członków ponadnarodowych sieci administracyjnych i kolegialnych organów na poziomie unijnym.

Przed przystąpieniem do dalszej analizy, najpierw scharakteryzowane zostanie pojęcie współpracy administracyjnej. W odniesieniu do tego pojęcia zidentyfikowany został nieporządek pojęciowy tak w prawie polskim, jak i unijnym, ponieważ prawodawca posługuje się różnymi określeniami niekonsekwentnie, m.in. „wzajemna pomoc”, „pomoc międzynarodowa”, „pomoc prawna”, „pomoc administracyjna” czy „administracyjne zarządzanie informacjami”⁸⁰⁸. Od pojęcia współpracy należy odróżnić pojęcie koordynacji, które rozumiane jest jako „uprawnienie organu w stosunku do innych organów lub podmiotów, które nie są mu bezpośrednio podporządkowane (...) w celu zharmonizowania [ich] działań (...)”, a zatem zawiera element relacji podrzędności⁸⁰⁹, przy czym wskazuje się, że koordynacja powiązana pozostaje z pojęciem współdziałania organów, któremu przypisuje się najbardziej ogólny charakter, obejmujący zarówno współpracę administracyjną, jak i koordynację⁸¹⁰.

W literaturze zaproponowano funkcjonalną definicję europejskiej współpracy administracyjnej, zgodnie z którą jest to „zorganizowany ciąg czynności urzędowych (oficjalnych) organu administrującego, podejmowanych z urzędu lub na wniosek organu innego państwa członkowskiego albo organu UE, nieodzownych dla zabezpieczenia efektywności prawa UE”⁸¹¹. Definicję tę analogicznie zastosować można do analizowanego

⁸⁰⁷ Można argumentować, że odmienności w tym zakresie dotyczą organów właściwych do spraw cyberbezpieczeństwa i GIIF, które obecnie jednoznacznie stanowią element administracji rządowej, a także UOKiK, nad którego działalnością nadzór sprawuje Prezes Rady Ministrów, zgodnie z art. 33a ust. 1 pkt 6) ustawy z dnia 4 września 1997 r. o działach administracji rządowej (t.j. Dz. U. z 2024 r. poz. 1370 z późn. zm.). Skoro wszystkie te organy są organami administracji rządowej istnieje przynajmniej pośredni tryb ich współdziałania w ramach tej administracji.

⁸⁰⁸ A. Cebera, J. G. Firlus [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. H. Knysiak-Sudyka, Warszawa 2023, art. 260(a), pkt 9, SIP LEX.

⁸⁰⁹ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 101.

⁸¹⁰ E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 141.

⁸¹¹ A. Cebera, J. G. Firlus [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. H. Knysiak-Sudyka, Warszawa 2023, art. 260(a), pkt 9, SIP LEX. Por. także M. Niedźwiedz, Zakres sądowej kontroli decyzji administracyjnych wydanych w związku z wykonaniem wniosku o przekazanie informacji w ramach współpracy administracyjnej w sprawach podatkowych – wprowadzenie i wyrok Trybunału Sprawiedliwości z 16.05.2017 r., C-682/15, Berlioz Investment Fund S.A. przeciwko Directeur de l’administration des Contributions directes, EPS 2020, nr 10, s. 52-64.

obszaru przetwarzania danych osobowych. Wówczas przez współpracę administracyjną w tym obszarze należałoby rozumieć „zorganizowany ciąg czynności urzędowych (oficjalnych) podmiotu administrującego stosującego akty prawne w obszarze przetwarzania danych osobowych, podejmowanych z urzędu lub na wniosek innego podmiotu administrującego (w Polsce lub w innym państwie członkowskim) lub organu UE stosującego akty prawne w tym obszarze, nieodzownych dla zabezpieczenia efektywności tych aktów prawnych”. Przyjęcie tej szerokiej, funkcjonalnej definicji współpracy administracyjnej pozwala na objęcie nią wszystkich analizowanych instrumentów współpracy.

Tak rozumiana współpraca administracyjna może przybrać różną postać normatywną. Można wyróżnić ogólny obowiązek współpracy, nałożony na poszczególne organy bez jej konkretyzowania, jak i szczególne obowiązki współpracy, w których sprecyzowano okoliczności, tryb albo konsekwencje nawiązania (i nienawiązania) tej współpracy. Przykładem szczególnego obowiązku współpracy jest art. 35 ust. 1 Dyrektywy NIS 2, który nakłada na organy właściwe do spraw cyberbezpieczeństwa obowiązek poinformowania organów ochrony danych bez zbędnej zwłoki o naruszeniu przez podmiot kluczowy lub ważny obowiązków określonych w art. 21 i 23 Dyrektywy NIS 2, które może pociągać za sobą naruszenie ochrony danych osobowych.

W prawie unijnym obowiązek współpracy między podmiotami administrującymi stosującymi prawo unijne wynika z zasad ogólnych prawa unijnego, w tym obowiązku lojalnej współpracy i zapewnienia skuteczności prawa unijnego⁸¹², a w prawie polskim nakaz współdziałania organów władzy publicznej (w tym organów administracji publicznej) wywodzony jest z preambuły Konstytucji RP w połączeniu z zasadą podziału i równowagi władzy (art. 10 Konstytucji RP)⁸¹³, a także art. 28 ustawy – Prawo Przedsiębiorców. Wskazać przy tym należy, że opieranie podstaw współpracy między podmiotami administrującymi na normach-zasadach nie rozwiązuje problemu braku jednoznacznych podstaw do wymiany informacji i dokumentów między tymi podmiotami na potrzeby tej współpracy. Ustanowienie kompletnych reguł współpracy wymaga doprecyzowania tej kwestii, co jest przedmiotem wywodu w rozdziale omawiającym postulaty *de lege ferenda*.

4.4.3.1. WSPÓŁPRACA PODMIOTÓW ADMINISTRUJĄCYCH ZA POŚREDNICTWEM ORGANÓW UNIJNYCH NA POZIOMIE UNIJNYM

⁸¹² K. Flisek, *Europejska współpraca administracyjna*, PPP 2020, nr 6, s. 83-97, s. 85-87.

⁸¹³ Por. W. Brzozowski, *Współdziałanie władz publicznych*, PiP 2010, nr 2, s. 3-16. s. 4 i 6.

Zasadnicza większość aktów prawa unijnego⁸¹⁴ w obszarze referencyjnym ustanawia odrębne organy na poziomie unijnym, które w założeniu pełnią funkcję koordynacyjną w odniesieniu do krajowych organów ustanowionych na podstawie tych aktów, a także zapewniać mają spójność stosowania prawa unijnego na terytorium UE, w tym także z innymi aktami prawa unijnego. Te organy mają niejednorodną pozycję ustrojową, kompetencje, strukturę, chociaż zasadniczo są organami kolegialnymi, w skład których wchodzi przedstawiciele organów krajowych ustanowionych w poszczególnych państwach członkowskich (chyba że takich organów nie ma jak w przypadku DMA)⁸¹⁵. Tym organom na poziomie unijnym przyznano kompetencję w postaci ogólnego obowiązku współpracy z innymi organami. Kompetencje te nie precyzują jasno, kiedy należy nawiązywać współpracę ani w jakiej formie tego dokonać, wreszcie zaś nie mają charakteru obligatoryjnego. W skład większości z tych organów jako stały członek wchodzi EROD lub EIOD, natomiast nie jest tak w każdym przypadku, np. nie jest tak w przypadku Europejskiej Rady ds. Usług Cyfrowych (DSA) oraz w projektowanej Radzie ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia na podstawie art. 64 ust. 1 Wniosku Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia⁸¹⁶, który jest jednym z aktów prawnych projektowanych w celu ustanowienia europejskich przestrzeni danych⁸¹⁷. Takie rozwiązanie należy ocenić negatywnie, ponieważ stanowiska zajmowane przez przedstawicieli EROD i EIOD jako członków tych organów (lub przynajmniej stałych uczestników prac tych organów) stanowiłyby szansę na zwiększenie spójności stosowania innych aktów prawnych względem RODO.

W konsekwencji, nie tylko zatem na poziomie krajowym ustanowione zostały (zostaną) podmioty administrujące, których kompetencje w tym obszarze krzyżują się. Refleksem krzyżowania się zakresu podmiotowego i przedmiotowego aktów prawnych w tym obszarze jest także krzyżowanie się kompetencji organów na poziomie unijnym. Rodzi to wątpliwości przy ustaleniu, które z organów na poziomie unijnym kompetentne będą do wydawania rekomendacji i opinii w sprawach, które (w mniejszym lub większym stopniu) dotyczą przetwarzania danych osobowych, oraz w jakich przypadkach konieczna jest współpraca

⁸¹⁴ W odniesieniu do regulacji AML w UE obecnie procedowane są zmiany w prawie, których częścią jest ustanowienie agencji unijnej do sprawy AML.

⁸¹⁵ Por. podrozdziały 3.2. i 5.3. rozprawy.

⁸¹⁶ COM/2022/197 final.

⁸¹⁷ Por. P. Hajduk, A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research (November 23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 - Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.), s. 14.

z EROD i EIOD. Chociaż obowiązek tej współpracy można wyprowadzić z ogólnych zasad prawa unijnego, to nie można wykluczyć, że z czasem stosowania poszczególnych aktów prawnych poszczególne organy na poziomie unijnym będą wydawały instrumenty typu *soft law*, które nie będzie w pełni koherentne. Nie ulega przy tym wątpliwości, że racjonalna współpraca między tymi organami stwarza jednocześnie szansę zmniejszenia ryzyka niepewności prawnych wynikających ze stosowania tych różnych, ale zakresowo zbliżonych aktów prawnych, na przykład przez publikowanie wspólnych (lub przynajmniej uzgodnionych) instrumentów typu *soft law*.

Na marginesie wskazać należy, że same organy na poziomie unijnym w ostatnich latach podejmowały inicjatywy w celu sformalizowania współpracy w obszarze przetwarzania danych osobowych między nimi. Przykładem tego jest porozumienie (*Memorandum of Understanding*) zawarte między EIOD a ENISA z 30.11.2022 r. „w celu ściślejszej współpracy [przez] ustanowienie, zdefiniowanie i promowanie zorganizowanej współpracy zgodnie z (...) odpowiednimi zadaniami statutowymi i uprawnieniami wynikającymi z prawa Unii”⁸¹⁸. Świadczy to o tym, że organy na poziomie unijnym identyfikują potrzebę zapewnienia większej spójności w stosowaniu aktów prawnych w tym obszarze.

4.4.3.2. WSPÓŁPRACA PODMIOTÓW ADMINISTRUJĄCYCH NA POZIOMIE KRAJOWYM

Każdy z analizowanych aktów prawnych na poziomie unijnym zawiera przepisy nakładające na podmioty administrujące, ustanowione w celu stosowania tych aktów na poziomie krajowym, obowiązek współpracowania z innymi krajowymi podmiotami administrującymi, w tym organami ochrony danych osobowych. Zarówno jednak tryb tej współpracy, jak i obowiązek jej prowadzenia w poszczególnych sprawach ani konsekwencje jej braku nie zostały w zasadzie unormowane⁸¹⁹. Pewne wskazówki odnaleźć można w motywach do niektórych aktów prawnych. Przykładowo, w motywie 44 do DGA wskazano, że: „w przypadku wszelkich kwestii wymagających oceny przestrzegania rozporządzenia (UE) 2016/679 [RODO] organ właściwy do spraw usług pośrednictwa danych powinien zwrócić się,

⁸¹⁸ EIOD, *Memorandum of Understanding on increasing cooperation between the European Data Protection Supervisor and the European Union Agency for Cybersecurity*, https://www.edps.europa.eu/system/files/2022-11/22-11-30_edps_enisa_mou_en.pdf (dostęp: 15.09.2024 r.).

⁸¹⁹ Por. P. Hajduk, *A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research* (November 23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 - Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.), s. 13.

w stosownych przypadkach, o opinię lub decyzję do właściwego organu nadzorczego ustanowionego na podstawie tego rozporządzenia”. Motyw ten odwołuje się jednak do „opinii lub decyzji”, zatem wciąż pozostawia doprecyzowanie tej kwestii prawodawcy krajowemu zgodnie z zasadą autonomii proceduralnej⁸²⁰.

Ta wstrzeźliwość prawodawcy unijnego w bardziej szczegółowym regulowaniu współpracy administracyjnej nie jest unikalna dla regulacji przetwarzania danych osobowych. Chociaż współpraca podmiotów administrujących ustanowionych na podstawie poszczególnych aktów prawa unijnego administracyjnego jest istotna dla zapewnienia jego spójności, to jej tryb jest często pomijany (albo traktowany zdawkowo) w prawie UE z uwagi na umieszczenie współpracy administracyjnych wśród kompetencji UE o charakterze działań mających na celu wspieranie, koordynowanie lub uzupełnianie działań (art. 6 TUE)⁸²¹. Prawodawca unijny tworzy zwykle jedynie ramy dla tej współpracy.

Instrumenty tej współpracy konkretyzowane są na podstawie prawa krajowego, a na organach krajowych spoczywa obowiązek efektywnego stosowania prawa unijnego w połączeniu z wywiedzionym z preambuły Konstytucji RP obowiązkiem „współdziałania władczy publicznej”, który konkretyzowany jest np. w przywołanym wyżej art. 7b KPA⁸²² normującym obowiązek współdziałania organów administracji publicznej „w zakresie niezbędnym do dokładnego wyjaśnienia stanu faktycznego i prawnego sprawy”. Instrumenty współpracy należy pojmować z uwzględnieniem zakazu domniemania kompetencji i wyróżnionych typów kompetencji, co odpowiada typowi właściwemu i niewłaściwemu badanego zjawiska krzyżowania się kompetencji. Należy uznać, że w odniesieniu do kompetencji o charakterze niewładczym (kompetencji doradczych, edukacyjnych i informacyjnych) nie istnieje konieczność istnienia osobnej podstawy prawnej do nawiązania współpracy między podmiotami administrującymi (np. organem ochrony danych osobowych a organem prawa konkurencji). Daje to, np. sposobność do wspólnego wydawania opinii w ramach instrumentów typu *soft law*. Szerokie korzystanie z tej możliwości mogłoby znacznie zwiększyć pewność prawną po stronie podmiotów nadzorowanych bez konieczności jakichkolwiek zmian w prawie. Konieczna jest jednak inicjatywa samych podmiotów administrujących i wola współpracy.

⁸²⁰ Analiza zasady autonomii proceduralnej i instytucjonalnej w podrozdziale 5.4.

⁸²¹ J. G. Firlus, A. Cebera, 5.5.2. Europejska współpraca administracyjna w prawie polskim i unijnym [w:] System Prawa Administracyjnego Procesowego, t. 4: Postępowania autonomiczne i szczególne. Postępowania niejurysdykcyjne, red. A. Matan, Warszawa 2021, SIP LEX.

⁸²² A. Wróbel [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, SIP LEX/el. 2023, art. 7(b), pkt 2, SIP LEX.

Inaczej rzecz się ma w odniesieniu do stosowania instrumentów współpracy w odniesieniu do pozostałych kompetencji, które mają charakter „władczy” (np. prowadzenie postępowań zakończonych wydaniem decyzji nakładającej administracyjną karę pieniężną). W zasadniczej większości wykonywane są one przez podmioty administrujące w trybie postępowania administracyjnego unormowanego w KPA z modyfikacjami tego postępowania w poszczególnych aktach prawnych i odpowiednim stosowaniem przepisów KPA, które nie zostały zmodyfikowane. Stąd też należy zbadać, czy KPA zawiera przepisy, mogące stanowić odpowiednią podstawę do realizacji współpracy, której ogólny obowiązek ustanowiony został w aktach prawnych prawa unijnego. Scharakteryzowana zostanie możliwość zastosowania przywołanego już art. 7b KPA, art. 106 § 1 KPA i przepisy działu VIIIA KPA normujące europejską współpracę administracyjną jak instrument współpracy między podmiotami administrującymi w obszarze referencyjnym⁸²³.

Art. 7b KPA był już przywołany wyżej przy dokonywaniu analizy sprawy rozpoznawanej przez WSA w Warszawie pod sygn. akt II SA/Wa 474/21, w której sąd ten orzekł, że doszło do jego naruszenia, ponieważ PUODO zaniechało współdziałania z KNF jako organem kompetentnym w sprawach związanych m.in. z badaniem zdolności kredytowej i analizą ryzyka kredytowego przy rozstrzyganiu sprawy dotyczącej usunięcia danych klienta instytucji finansowej. Jak wskazano wyżej, ten wyrok nie stanowi ugruntowanej linii orzeczniczej i wydano wyroki rozstrzygające odmiennie. Ta sytuacja obrazuje, że jednoznaczne ustalenie obowiązku zastosowanie art. 7b KPA stanowiącego zasadę ogólną postępowania administracyjnego jest trudne, ponieważ przesłanki obowiązku współdziałania są ocenne. W obszarze referencyjnym taki „wzmocniony” obowiązek można byłoby wywodzić z ogólnych obowiązków współpracy między organami administracji publicznej, które nałożone zostały w zasadniczej większości analizowanych aktów prawnych. Zasada ta nie określa jednak form współdziałania podmiotów administrujących, a jedynie kryteria ich doboru⁸²⁴. Nadto, w wyroku NSA z 17 października 2022 r. wyraźnie ograniczono możliwość zastosowania art. 7b KPA, rozstrzygając, że artykuł ten nie może stanowić podstawy prawnej do występowania przez jeden organ z zapytaniem do innego w przedmiocie wykładni przepisów,

⁸²³ Por. także Pkt 2. Środki współdziałania w postępowaniu administracyjnym [w:] Z. Kmieciak [w:] J. Wegner, M. Wojtuń, Z. Kmieciak, Kodeks postępowania administracyjnego. Komentarz, Warszawa 2023, art. 7(b), SIP LEX.

⁸²⁴ A. Wróbel [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, SIP LEX/el. 2023, art. 7(b), pkt 5, SIP LEX.

o ile nie jest to rzeczywiście „niezbędne”⁸²⁵, nawet jeżeli chodzi o organ „o częściowo zbieżnej kompetencji”.⁸²⁶

W praktyce z perspektywy podmiotów administrujących wykładnia tego przepisu może budzić wątpliwości co do zakresu ich obowiązku współdziałania, jak również sposobu jego wykonania. Wydaje się, że tę wątpliwość podziela także PUODO, ponieważ od wskazanego wyżej wyroku wniósł on skargę kasacyjną do NSA, podnosząc w komunikacie prasowym, że „zaprezentowany przez WSA pogląd przeczy zatem idei RODO w zakresie powołanej fundamentalnej zasady niezależności organu nadzorczego”⁸²⁷.

Z kolei, zgodnie z art. 106 § 1 KPA, jeżeli przepis prawa uzależnia wydanie decyzji od zajęcia stanowiska przez inny organ (wyrażenia opinii lub zgody albo wyrażenia stanowiska w innej formie), decyzję wydaje się po zajęciu stanowiska przez ten organ, wyrażonego w drodze postanowienia, na które służy zażalenie (art. 106 § 5 KPA). Istotą tego przepisu będącego normą-regułą⁸²⁸ jest, że do jego zastosowania niezbędne jest istnienie innego przepisu prawa, który jednoznacznie będzie uzależniał wydanie decyzji od stanowiska innego organu, co jest mało elastycznym rozwiązaniem z perspektywy prawnoporównawczej, które może być łagodzone przez art. 7b KPA⁸²⁹. Skutki zajęcia stanowiska mogą być różne – zasadniczo opinie mają charakter niewiążący, natomiast pozostałe formy zajęcia stanowiska przez inny organ zbliżają wydaną decyzję do ich „współdecyzji”⁸³⁰. W obszarze referencyjnym nie wprowadzono w sposób systematyczny i jednoznacznych przepisów, które mogłyby stanowić podstawę prawną do zastosowania art. 106 § 1 KPA. Taki obowiązek można wyprowadzić, np. z analizowanego w rozdziale 3 rozprawy art. 35 ust. 1-2 Dyrektywy NIS 2 nakładającego obowiązek organów odpowiedzialnych za cyberbezpieczeństwo z organami ochrony danych osobowych. Pośrednio taki obowiązek można byłoby próbować wywieść również z motywów 44 i 51 DGA (zwrócić jednak należy uwagę na specyficzny zasadniczo

⁸²⁵ M. Błachucki, Współdziałanie organów administracji publicznej a obowiązek dokonywania urzędowej interpretacji przepisów. Glosa do wyroku Naczelnego Sądu Administracyjnego z 17.10.2022 r. (II GSK 1971/21), PPP 2024, nr 4, s. 100-110.

⁸²⁶ Wyrok NSA z 17.10.2022 r., II GSK 1971/21, SIP LEX nr 3442475.

⁸²⁷ UODO, *Skarga kasacyjna od wyroku WSA ws. przetwarzania danych osobowych klienta banku*, 13.01.2022, <https://uodo.gov.pl/pl/138/2379> (dostęp: 15.09.2024 r.). Na dole strony internetowej znaleźć można link do skargi kasacyjnej wniesionej przez PUODO.

⁸²⁸ A. Wróbel [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, SIP LEX/el. 2023, art. 7(b), pkt 1, SIP LEX.

⁸²⁹ Z. Kmiecik [w:] J. Wegner, M. Wojtuń, Z. Kmiecik, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2023, art. 106, pkt 1, SIP LEX.

⁸³⁰ Z. Kmiecik [w:] J. Wegner, M. Wojtuń, Z. Kmiecik, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2023, art. 106, pkt 1, SIP LEX.

niewiążący charakter prawny motywów w prawie unijnym⁸³¹) wskazujących na powinność organów właściwych ustanowionych na podstawie DGA do „zwrócenia się, w stosownych przypadkach, o opinię lub decyzję do” organu ochrony danych, które należałoby interpretować wówczas w połączeniu z ogólnymi obowiązkami współpracy między organami unormowanymi w DGA. Co więcej, niektóre akty prawne, jak np. Data Act zdają się ograniczać prawodawcę krajowego w wyborze form wykonywania współpracy między organami właściwymi i innymi organami, przez uregulowanie, że organy właściwe ustanowione na podstawie Data Act nie mogą „o instrukcje w indywidualnych sprawach do [...] innego organu publicznego [...] ani nie przyjmują takich instrukcji” (art. 37 ust. 8 Data Act). Jak wskazano w rozdziale 3, literalnie interpretując, ogranicza to prawodawcę krajowego w wyborze form wykonywania współpracy między organami właściwymi i innymi organami.

Dział VIIIA KPA (wszedł w życie w 2017 r.) normuje ramy europejskiej współpracy administracyjnej (art. 260a-260g KPA). Otwierający dział VIIIA art. 260a § 1 KPA reguluje obowiązek organów administracji publicznej do udzielania pomocy organom innych państw członkowskich UE oraz organom administracji UE, jeżeli przepisy prawa UE tak stanowią na zasadach w nich określonych. Jest to rozwiązanie potrzebne, ponieważ ustanawia jednolite podstawy prawne do współpracy i udzielania tej pomocy w celu zapewnienia skuteczności prawa unijnego, natomiast ma w tym kształcie charakter subsydiarny, to znaczy pozwala na realizację pomocy innym organom administracji publicznej jedynie w zakresie, w jakim dopuszcza to odpowiednie przepisy tego prawa⁸³². Zastosowanie tych przepisów wymaga zatem uprzedniej aktywności prawodawcy europejskiego. Dla analizowanego obszaru referencyjnego kluczowe jest jednak, że przepis ten dotyczy wyłącznie współpracy między organami różnych państw członkowskich stosującymi akty administracyjnego prawa unijnego, a nie organami krajowymi stosującymi te akty.

Powyższa analiza pokazuje, że chociaż niektóre przepisy KPA, zwłaszcza art. 7b KPA, mogłyby, będąc odpowiednio wykładane, stanowić podstawę do współpracy w odniesieniu do wykonywania kompetencji o charakterze „władczym”, to jednak niejednoznaczny sposób ich sformułowania i brak ugruntowanej interpretacji w orzecznictwie sądów administracyjnych odbiera im *de lege lata* przymiot skutecznych instrumentów prawnych do zredukowania

⁸³¹ Por. T. Klimas, J. Vaiciukaite, *The Law of Recitals in European Community Legislation*, „ILSA Journal of International & Comparative Law” 2008, Vol. 15, No. 1, <https://ssrn.com/abstract=1159604> (dostęp 12.09.2024 r.), s.61-94.

⁸³² Por. A. Cebera, J. G. Firlus [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. H. Knysiak-Sudyka, Warszawa 2023, art. 260(a), pkt 8, SIP LEX.

negatywnych skutków zjawiska krzyżowania się kompetencji. Istotne jest natomiast, aby organy administracji publicznej bardziej zdecydowanie współpracowały przy wykorzystaniu kompetencji doradczych, edukacyjnych i informacyjnych przy wydawaniu dokumentów stanowiących niewiążące instrumenty typu *soft law*. Nie wymaga to bowiem zmiany przepisów prawa.

4.4.3.3. ROZSTRZYGANIE SPORÓW O WŁAŚCIWOŚĆ MIĘDZY ORGANAMI ADMINISTRACJI PUBLICZNEJ

Jednym ze skutków zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych jest ryzyko powstania sporów o właściwość między tymi organami. Stąd też niezbędne jest zbadanie instrumentów prawnych ustanowionych do rozstrzygania tych sporów. Różnica w prawie administracyjnym procesowym między „sporami o właściwość” i „sporami kompetencyjnymi” dotyczy ich zakresu podmiotowego. Termin „spory kompetencyjne” używany jest w odniesieniu do sporów między organami samorządu terytorialnego a organami administracji rządowej, natomiast terminu „spory o właściwość” używa się na określenie sporów między organami w „tym samym pionie ustrojowym administracji (rządowej lub samorządowej)”⁸³³ (ujęcie normatywne). Wprowadzenie tego rozróżnienia do języka prawnego jest krytykowane w literaturze jako wprowadzające nieporządek⁸³⁴. Termin „spór kompetencyjny” w ujęciu doktrynalnym jest używany także w szerszym znaczeniu jako „każdy przypadek rozbieżności poglądów co do zakresu działania organów państwa, który podlega ocenie powołanego przez prawo organu rozstrzygającego”⁸³⁵. Tak rozumiany termin „spór kompetencyjny” obejmuje zakresem znaczeniowym nie tylko spory o właściwość i spory kompetencyjne w ujęciu normatywnym, ale także rozbieżności „poglądów co do zakresu działania”, które nie dotyczą załatwiania konkretnych spraw administracyjnych, ale wykonywania kompetencji informacyjnych, doradczych i edukacyjnych, w tym wydawanie instrumentów typu *soft law*

⁸³³ M. Krawczyk, Zakres kognicji Naczelnego Sądu Administracyjnego w rozstrzyganiu sporów kompetencyjnych i o właściwość, ST 2023, nr 6, s. 20-31, s. 20-21.

⁸³⁴ M. Krawczyk, Zakres kognicji Naczelnego Sądu Administracyjnego w rozstrzyganiu sporów kompetencyjnych i o właściwość, ST 2023, nr 6, s. 20-31, s. 20-21. Por. także J. Człowiekowska, Mnożenie pojęć w prawie administracyjnym w kontekście aktualności pojęć tego prawa [w:] Aktualność pojęć prawa administracyjnego, red. W. Jakimowicz, Warszawa 2021, SIP LEX.

⁸³⁵ A. P. Skoczylas, Rozdział I Zagadnienia ogólne [w:] Rozstrzyganie sporów kompetencyjnych i o właściwość przez NSA, Warszawa 2008; M. Pyziak, Rozstrzyganie sporów kompetencyjnych na ziemiach polskich. Od Rady Stanu Księstwa Warszawskiego do współczesności, „Studia z Dziejów Państwa i Prawa Polskiego” 2010, t. 13, s. 237 (za przywołanym tam J. Zimmermannem).

(przykładem byłby charakteryzowany wyżej spór między Ministrem Cyfryzacji i PUODO dotyczący wydania objaśnień prawnych przez Ministra Cyfryzacji). Z uwagi na to, że organy w obszarze referencyjnym nie są organami samorządu terytorialnego, rozważania w tym podrozdziale dotyczą tylko sporów o właściwość. Należy także wskazać, że zastosowania w tym obszarze nie znajduje art. 189 Konstytucji RP, zgodnie z którym to TK rozstrzyga spory kompetencyjne pomiędzy centralnymi konstytucyjnymi organami państwa. Analizowane organy nie stanowią bowiem centralnych konstytucyjnych organów państwa⁸³⁶.

Zgodnie z art. 1 pkt 3 KPA, kodeks ten normuje postępowanie w sprawach rozstrzygania sporów o właściwość między organami jednostek samorządu terytorialnego i organami administracji rządowej oraz między organami i innymi podmiotami, gdy są one powołane z mocy prawa lub na podstawie porozumień do załatwiania spraw (por. także art. 4 Ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi⁸³⁷). Spory o właściwość mogą być pozytywne, gdy oba organy twierdzą, że są właściwie do załatwienia sprawy, albo negatywne, kiedy żaden z organów nie uznaje się za właściwy⁸³⁸. Art. 22 § 1 KPA wskazuje podmioty, które dokonują rozstrzygnięcia sporów o właściwość m.in. między organami administracji publicznej innymi niż wymienione w pkt 1-4, 6 i 7 tego paragrafu spory te rozstrzyga wspólny dla nich organ wyższego stopnia, a w razie jego braku takiego organu – minister właściwy do spraw administracji publicznej, natomiast spory między organami administracji publicznej, gdy jeden z nich jest ministrem, rozstrzyga Prezes Rady Ministrów.

Chociaż cel prowadzenia sporów o właściwość to „wiążące wskazanie organu administracji publicznej właściwego do załatwienia konkretnej sprawy administracyjnej”, które ma istotny wpływ na uprawnienia procesowe stron postępowania administracyjnego, to tryb i forma rozstrzygania tych sporów nie zostały dostatecznie precyzyjnie unormowane⁸³⁹. Spór o właściwość nie może być abstrakcyjny, a więc ustalać właściwy organ w sprawie przed jej wszczęciem i dotyczyć musi tej samej (tożsamość) sprawy, co znaczy, że zachodzić powinna „identyczność przedmiotu, podmiotu oraz podstawy prawnej i faktycznej”⁸⁴⁰. Stwierdzenie tożsamości sprawy, chociaż fundamentalne dla zaistnienia sporu o właściwość, może sprawić

⁸³⁶ Por. B. Naleziński [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, SIP LEX/el. 2021, art. 189, pkt 2, SIP LEX.

⁸³⁷ T.j. Dz. U. z 2023 r. poz. 1634 z późn. zm.

⁸³⁸ J. Wegner [w:] Z. Kmiecik, M. Wojtuń, J. Wegner, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2023, art. 22, pkt 2, SIP LEX.

⁸³⁹ S. Gajewski, Tryb i forma rozstrzygania sporów o właściwość na gruncie kodeksu postępowania administracyjnego oraz jego sądowoadministracyjna kontrola, PPP 2016, nr 11, s. 69-81, s. 80.

⁸⁴⁰ A. P. Skoczyła, Rozdział I Zagadnienia ogólne [w:] *Rozstrzyganie sporów kompetencyjnych i o właściwość przez NSA*, Warszawa 2008, SIP LEX.

problemy, a ustalenie, że tej tożsamości nie ma, powoduje, że spór o właściwość należy uznać za pozorny⁸⁴¹.

Przyjąć można, że w przypadku sporów o właściwość w obszarze referencyjnym co najmniej jednemu z organów przysługiwał będzie status niezależności (np. PUODO czy Prezes UOKiK), który wynika z prawa unijnego, a jednocześnie wszystkie te organy są centralnymi organami administracji publicznej. Najczęściej do sporów o właściwość w tym obszarze może dochodzić w sytuacji, w której jednym z organów będzie PUODO. Dyskusyjna jest kwalifikacja PUODO jako ministra w rozumieniu art. 5 § 2 pkt 4 KPA⁸⁴², albo też jako organu administracji publicznej w rozumieniu art. 5 § 2 pkt 3 KPA⁸⁴³. Ma to znaczenie dla ustalenia organu, który rozstrzygałby ewentualny spór o właściwość między PUODO a innym organem (byłby to wówczas albo minister właściwy do spraw administracji publicznej, albo Prezes Rady Ministrów). Nie jest jasne czy z uwagi na przymiot niezależności PUODO art. 22 KPA w obecnym brzmieniu powinien mieć w ogóle zastosowanie do spraw, które rozpatrywałby PUODO. *De lege lata* wydaje się, że art. 22 KPA mógłby znaleźć zastosowanie, ponieważ kwalifikacja PUODO jako „organu administracji publicznej” albo „ministra” prowadziłaby do zastosowania art. 22 KPA, co nie zostało wyłączone⁸⁴⁴. W praktyce oznaczałoby to jednak, że spory o właściwość z udziałem PUODO rozstrzygałby minister właściwy do spraw administracji publicznej, albo Prezes Rady Ministrów. Stanowiłoby to zagrożenie dla traktatowej niezależności organów ochrony danych, ponieważ mogłoby stanowić to narzędzie do faktycznego zmniejszenia zakresu kompetencji organów ochrony danych. Należy zatem *de lege ferenda* postulować, aby spory o właściwość, gdzie jedną ze stron jest organ administracji publicznej, któremu zapewniono prawnie niezależność, rozstrzygane były przez sąd administracyjny.

Powyższa analizuje, że instrumenty rozwiązywania sporów o właściwość w administracyjnym prawie procesowym nie są skuteczne do zredukowania negatywnych skutków zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze

⁸⁴¹ A. P. Skoczylas, Rozdział I Zagadnienia ogólne [w:] Rozstrzyganie sporów kompetencyjnych i o właściwość przez NSA, Warszawa 2008, SIP LEX.

⁸⁴² Tak orzeczono bezpośrednio w odniesieniu do GIODO w wyroku WSA w Warszawie z 18.11.2022 r., II SA/Wa 193/22, SIP LEX nr 3457484.

⁸⁴³ Tak twierdzi P. Fajgielski [w:] Komentarz do ustawy o ochronie danych osobowych [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2022, art. 34, pkt 14, SIP LEX. Por. także K. Klonowski [w:] Kodeks postępowania administracyjnego. Komentarz, red. H. Knysiak-Sudyka, Warszawa 2023, art. 5, pkt 4, SIP LEX.

⁸⁴⁴ Możliwość taką dopuszczono w literaturze względem Prezesa UKE; por. P. Kledzik, 3. Konsekwencje procesowe związane z posiadaniem przez Prezesa UKE statusu centralnego organu administracji rządowej [w:] Rynek usług telekomunikacyjnych, red. H. Babis, K. Flaga-Gieruszyńska, Warszawa 2011, SIP LEX.

przetwarzania danych osobowych. Przede wszystkim tryb ten może być wykorzystany wyłącznie w odniesieniu do konkretnych spraw, a zatem nie można stosować go prospektywnie i abstrakcyjnie, co nie pozwala usunąć niepewności prawnej dotyczącej, np. wydawania instrumentów prawnych typu *soft law* (jak w przypadku przywoływanego już sporu PUODO i Ministra Cyfryzacji). Nadto, nie jest jasne, jaki status podmiotowy na gruncie KPA ma PUODO, co przekłada się na niepewność w ustaleniu organu rozstrzygającego spory o właściwość. Nie jest również klarowne czy art. 22 KPA może znaleźć w ogóle zastosowanie do sporów z udziałem PUODO jako organu o szczególnej pozycji ustrojowej, chociaż *de lege lata* nie ma takich jednoznacznych przeszkód. Wreszcie, ustalenie tożsamości spraw stanowiące przesłankę zaistnienia sporu o właściwość w obszarze przetwarzania danych osobowych stanowi trudność, a tożsamość ta może okazać się pozorna, na przykład, kiedy każdy z analizowanych unijnych aktów prawnych ustanawia osobne przepisy sankcjonujące (lub zobowiązanie do ich ustanowienia przez państwa członkowskie), zatem prowadzenie równoległych postępowań prowadzących do nałożenia administracyjnych kar pieniężnych za to samo zachowanie, które stanowi naruszenie różnych aktów prawnych, wydaje się teoretycznie możliwe. Sprawy te nie będą mogły jednak zostać za tożsame z uwagi na odmienne podstawy prawne (por. analizę możliwości zastosowania zasady *ne bis in idem* poniżej).

W takim układzie organom stosującym akty prawne w obszarze przetwarzania danych osobowych pozostaje możliwość skorzystania z art. 7b KPA analizowanego wyżej lub nawiązywanie uprzedniej, nieformalnej (nieunormowanej) współpracy z innymi organami, która w praktyce prowadzona jest przez kontakty między urzędnikami załatwiającyymi poszczególne sprawy w celu skoordynowania działań. Przykładem takich (częściowo formalizowanych) działań jest podpisanie 7.12.2023 r. porozumienia pomiędzy PUODO i Głównym Inspektorem Farmaceutycznym w przedmiocie „współpracy w związku z naruszeniami prawa związanymi z przetwarzaniem danych osobowych pacjentów i pracowników aptek ogólnodostępnych” (§ 1 tego porozumienia), która polegała będzie m.in. na „wzajemnym przekazywaniu informacji istotnych dla skutecznego przeciwdziałania i eliminowania naruszeń prawa związanych z przetwarzaniem danych osobowych pacjentów i pracowników aptek ogólnodostępnych” (§ 2 ust. 1 tego porozumienia)⁸⁴⁵.

⁸⁴⁵ UODO, Główny Inspektor Farmaceutyczny, 7.12.2023, <https://uodo.gov.pl/pl/file/4537> (dostęp: 11.09.2024 r.).

4.5. SKUTKI KRZYŻOWANIA SIĘ KOMPETENCJI ORGANÓW

Konstatacja, że brak jest efektywnych instrumentów do zredukowania negatywnych skutków analizowanego zjawiska krzyżowania się kompetencji podmiotów administrujących w obszarze przetwarzania danych osobowych, prowadzi do analizy skutków krzyżowania się kompetencji organów. W niniejszym podrozdziale zbadane zostaną te skutki dla administracji publicznej (podmiotów administrujących), podmiotów nadzorowanych i podmiotów danych, w tym dla ochrony praw podstawowych, oraz pozaprawne, gospodarcze skutki tego zjawiska dla gospodarki. Brak efektywnych instrumentów prawnych powoduje, że zjawisko to prowadzi do zmniejszenia skuteczności aktów prawnych w tym obszarze i niepewności prawnej po stronie podmiotów administrujących, podmiotów nadzorowanych i podmiotów danych zarówno w odniesieniu do podziału kompetencji między tymi podmiotami, jak i właściwej wykładni aktów prawnych w tym obszarze. Stanowi to także zagrożenie dla realizacji zasady *ne bis in idem* w prawie administracyjnym i prowadzi do zmniejszenia efektywności ochrony praw podstawowych. To zjawisko może mieć także negatywny wpływ na rozwój gospodarki unijnej, ponieważ niepewność prawna prowadzi do zwiększenia kosztów zapewnienia przestrzegania prawa przez podmioty nadzorowane, co, jak bywa argumentowane, utrudnia rozwój unijnej gospodarki opartej na przetwarzaniu danych osobowych.

4.5.1. SKUTKI DLA ADMINISTRACJI PUBLICZNEJ, PODMIOTÓW NADZOROWANYCH I PODMIOTÓW DANYCH

Zjawisko krzyżowania się kompetencji organów administracji publicznej („*regulatory overlap*”) nie jest charakterystyczne tylko dla regulacji przetwarzania danych osobowych. Skutki występowania tego zjawiska w różnych obszarach unormowania są zasadniczo podobne. Zasadnie wskazuje się, że zjawisko to powoduje zmniejszenie skuteczności aktów prawnych, zwiększenie niepewności prawnej po stronie podmiotów administrujących, podmiotów danych i podmiotów nadzorowanych oraz ryzyko stosowania wielokrotnych sankcji administracyjnych za to samo zachowanie (zagrożenie dla realizacji zasady *ne bis in idem*)⁸⁴⁶. Stąd też w tym podrozdziale w kontekście analizowanego zjawiska zbadano pojęcie skuteczności prawa administracyjnego, pojęcie niepewności prawnej i ryzyko dla realizacji zasady *ne bis in idem* w prawie administracyjnym w obszarze referencyjnym.

⁸⁴⁶ L. Robb, T. Candy, F. Deane, *Regulatory overlap: A systematic quantitative literature review*, „Regulation & Governance” 2023, Vol. 17, No. 4, <https://doi.org/10.1111/rego.12504> (dostęp: 20.09.2024 r.), s. 1131, 1140.

Pojęcie skuteczności prawa administracyjnego jest wieloznaczne, a w naukach prawnych winno być badane z wykorzystaniem dorobku prakseologii⁸⁴⁷. Badanie skuteczności prawa administracyjnego jest przedmiotem zainteresowania polskiej nauki prawa administracyjnego od kilku dziesięcioleci⁸⁴⁸. Skuteczność („*effectiveness*”) należy odróżnić od efektywności („*efficiency*”), chociaż pojęcia te bywają nieprawidłowo utożsamiane⁸⁴⁹. Efektywność („*efficiency*”) rozumiana jest jako „zdolność osiągania najwyższego możliwego poziomu użytecznej pracy przy najmniejszym możliwym wysiłku”⁸⁵⁰, a jej badanie jest charakterystyczne dla ekonomicznej analizy prawa⁸⁵¹. W literaturze w ujęciu funkcjonalnym skuteczność rozumiana jest dwojako – jako uzyskanie zachowania zgodnego z normami prawnymi⁸⁵², i jako osiągnięcie celu ustanowienia tych norm⁸⁵³, czyli zazwyczaj realizacji lub ochrony określonych wartości⁸⁵⁴. Działania można uznać za skuteczne, kiedy prowadzą do realizacji celu⁸⁵⁵. Odminną perspektywę badawczą należy przyjąć przy badaniu skuteczności pojedynczej normy prawnej niż przy badaniu skuteczności gałęzi prawa⁸⁵⁶. W tym podrozdziale przedmiotem badania jest skuteczność aktów prawnych w odniesieniu do zjawiska krzyżowania się kompetencji w obszarze przetwarzania danych osobowych rozumianego jako pewna całość (porównywalna do kompleksowej gałęzi prawa)⁸⁵⁷.

⁸⁴⁷ Pogląd H. Izdebskiego przywołany za L. J. Żukowski, *Spoleczna skuteczność prawa administracyjnego (zarys koncepcji)*, PiP 2017, nr 5, s. 95-108, s. 98.

⁸⁴⁸ Por. przegląd poglądów w literaturze dokonany w: M. Szczypczyk, *Skuteczność prawa administracyjnego na przykładzie nowelizacji ustaw podatkowych w latach 2016–2019* [w:] *Skuteczność w prawie administracyjnym*, red. C. Martysz, Warszawa 2022, SIP LEX.

⁸⁴⁹ J. Wegner-Kowalska, Rozdział IV Dylematy badania skuteczności unijnego prawa administracyjnego (w kontekście ochrony weterynaryjnej) [w:] *Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej*, Warszawa 2017, SIP LEX.

⁸⁵⁰ *Efficiency*, [hasło w:] Cambridge Dictionary [Online], <https://dictionary.cambridge.org/dictionary/english/efficiency#> (dostęp: 12.09.2024 r.).

⁸⁵¹ J. Wegner-Kowalska, Rozdział IV Dylematy badania skuteczności unijnego prawa administracyjnego (w kontekście ochrony weterynaryjnej) [w:] *Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej*, Warszawa 2017, SIP LEX.

⁸⁵² M. Szczypczyk, *Skuteczność prawa administracyjnego na przykładzie nowelizacji ustaw podatkowych w latach 2016–2019* [w:] *Skuteczność w prawie administracyjnym*, red. C. Martysz, Warszawa 2022, SIP LEX.

⁸⁵³ J. Wegner-Kowalska, Rozdział IV Dylematy badania skuteczności unijnego prawa administracyjnego (w kontekście ochrony weterynaryjnej) [w:] *Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej*, Warszawa 2017.

⁸⁵⁴ M. Szczypczyk, *Skuteczność prawa administracyjnego na przykładzie nowelizacji ustaw podatkowych w latach 2016–2019* [w:] *Skuteczność w prawie administracyjnym*, red. C. Martysz, Warszawa 2022, SIP LEX.

⁸⁵⁵ M. Maciejewski, Normy celowościowe i normy zadaniowe w prawie administracyjnym. Dobra chronione jako ustawowe cele organów administracji [w:] *Dobra chronione w prawie administracyjnym*, red. Z. Duniewska, Łódź 2014, s. 32.

⁸⁵⁶ Pogląd H. Izdebskiego przywołany za L. J. Żukowski, *Spoleczna skuteczność prawa administracyjnego (zarys koncepcji)*, PiP 2017, nr 5, s. 95-108, s. 98-99.

⁸⁵⁷ Analiza balansowania celów przez podmioty administrujące w obszarze referencyjnym w podrozdziale 5.6. rozprawy.

Za J. Wróblewskim wyróżnia się trzy typy skuteczności prawa, które osiągnąć mogą być razem lub osobno: 1) behawioralna, kiedy norma prawna jest przestrzegana; 2) psychologiczna, kiedy norma wpływa na jej adresata, modyfikując jego motywacje i przeżycia; 3) finistyczna, czyli osiągnięcie pożądanego stanu rzeczy, przy czym skuteczność behawioralna nie zawsze prowadzi do skuteczności finistycznej, jeżeli normy (środki) zostały przez prawodawcę niewłaściwie dobrane do celów⁸⁵⁸. W tej rozprawie termin „skuteczność prawa” używany jest przede wszystkim w finistycznym rozumieniu. Z. Kmiecik wyróżnia trzy ujęcia skuteczności prawa administracyjnego: 1) szerokie rozumiane jako „relacja skutków funkcjonowania norm prawnych do celów, które założył prawodawca”; 2) węższe, czyli „skuteczność decyzji stosowania prawa”; i najwęższe odnoszące się do „skuteczności sposobu wykonania decyzji stosowania prawa”⁸⁵⁹. W odniesieniu do analizowanego zjawiska wszystkie trzy ujęcia mieszają się, ponieważ wykonywanie decyzji stosowania prawa i same te decyzje w obszarze referencyjnym z uwagi na zastosowane techniki prawodawcze i potrzebę użycia metod celowościowej oraz funkcjonalnej w operatywnej wykładni prawa⁸⁶⁰ pozostają jednocześnie ściśle powiązane z szerokim rozumieniem skuteczności prawa⁸⁶¹.

W odniesieniu do oceny skuteczności unijnego prawa administracyjnego⁸⁶² wskazuje się, że z uwagi na wielopoziomowy charakter tego prawa relacje między poszczególnymi typami skuteczności komplikują się z uwagi na zwiększenie liczby adresatów norm celowościowych i sposobów ich realizacji⁸⁶³. Cele poszczególnych aktów prawa unijnego (których hierarchia nie jest zresztą jasna) wyznaczone są bowiem na poziomie unijnym, ale ich realizacji dokonywana jest na poziomie krajowym, wymagając uprzedniej transpozycji do krajowego porządku prawnego, zatem prawodawca krajowy staje się (dodatkowym) adresatem norm

⁸⁵⁸ Pogląd J. Wróblewskiego przywołany za: M. E. Stefaniuk, *Skuteczność prawa i jej granice*, Studia Iuridica Lublinensia 2011, No. 16, s. 62 i przywołana tam literatura.

⁸⁵⁹ Pogląd Z. Kmiecika przywołany za: L. J. Żukowski, *Spoleczna skuteczność prawa administracyjnego (zarys koncepcji)*, PiP 2017, nr 5, s. 95-108, s. 95; por. Z. Kmiecik, *Skuteczność regulacji administracyjnoprawnej*, Łódź 1994.

⁸⁶⁰ Por. podrozdział 5.3. poniżej.

⁸⁶¹ Poglębiona analiza pojęcia skuteczności prawa była dokonywana w literaturze także w odniesieniu do prawa ochrony danych osobowych w powiązaniu z analizą celu i zakresu tego prawa, por. A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wrocław, 2019, Rozdział 3 „Cel, zakres i skuteczność prawa ochrony danych osobowych”, s. 111-154.

⁸⁶² Wskazać należy, że zasada efektywności (skuteczności) prawa unijnego jest kluczowa dla relacji prawa unijnego i krajowego jako element procesu tworzenia rynku wspólnego, por. M. Accetto, *The Principle of Effectiveness: Rethinking Its Role in Community Law*, „European Public Law” 2005, Vol. 11, Iss. 3, <https://doi.org/10.54648/euro2005030> (dostęp: 20.09.2024 r.), s. 379-383.

⁸⁶³ J. Wegner-Kowalska, *Rozdział IV Dylematy badania skuteczności unijnego prawa administracyjnego (w kontekście ochrony weterynaryjnej)* [w:] *Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej*, Warszawa 2017.

celowościowych⁸⁶⁴. Tak jest też w przypadku obszaru przetwarzania danych osobowych, gdzie prawodawca unijny określił cele na poziomie aktów prawa unijnego, ale pozostawił prawodawcy krajowemu ustanowienie struktury podmiotów administrujących i procedur do ich osiągnięcia, przy czym ustanowione podmioty administrujące powinny, stosując akty prawne, poszukiwać punktu odniesienia (np. w wykładni prawa) w celach ustanowionych na poziomie unijnym. Powoduje to „autonomizację celów regulacji prawnej”, ale może także w praktyce prowadzić do rozbieżności celów „prawodawcy i decydenta”⁸⁶⁵.

W literaturze sformułowano trafny pogląd o metodologicznej trudności w ocenie finistycznej skuteczności (progowej⁸⁶⁶) prawa administracyjnego nie tylko dlatego, że zdekodowanie celów aktów prawa administracyjnego (zatem kryterium weryfikacji skuteczności) nie zawsze jest łatwe, ale także dlatego, że materiał badawczy do badań ilościowych jest ograniczony⁸⁶⁷, zatem pozostaje prowadzenie badań jakościowych przez analizę konkretnych spraw i wnioskowanie o skuteczności na ich podstawie⁸⁶⁸. W konsekwencji prowadzi to do wyników analizy na poziomie dość abstrakcyjnym, co nie jest satysfakcjonujący z perspektywy praktyki, która oczekiwałaby konkretnych rekomendacji⁸⁶⁹. Nie budzi wątpliwości, że jednym z warunków skuteczności prawa administracyjnego jest odpowiednie ukształtowanie struktury podmiotów administrujących, podziału kompetencji i układów kompetencyjnych między nimi oraz sposobu ich działania („aparatu publicznego”)⁸⁷⁰. Pożądane byłoby, aby ukształtowanie to było optymalne, czyli najlepsze z możliwych w danych warunkach⁸⁷¹.

W tej perspektywie ocenić należy zjawisko krzyżowania się kompetencji organów administracji publicznej w obszarze referencyjnym. Chociaż z uwagi na systemowe przyczyny jego wystąpienia⁸⁷², należy uznać je za nieuchronne samo w sobie, to brak optymalnych

⁸⁶⁴ J. Wegner-Kowalska, Rozdział IV Dylematy badania skuteczności unijnego prawa administracyjnego (w kontekście ochrony weterynaryjnej) [w:] Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej, Warszawa 2017.

⁸⁶⁵ G. Szpor, *Jawność i jej ograniczenia*, t. 1: *Idee i pojęcia*, Warszawa 2016, s. 188-189.

⁸⁶⁶ Termin „skuteczności progowej” wprowadzony został przez Z. Kmiecika na określenie „minimalnego poziomu zgodności skutków działania administracji z realizowanym celem”. Przywołanie za: M. Maciejewski, *Rozdział 6. Skuteczność a jawność administracji* [w:] *Jawność i jej ograniczenia*, t. 3: *Skuteczność regulacji*, red. G. Szpor, Z. Kmiecik, Warszawa 2013, SIP Legalis.

⁸⁶⁷ O badaniu ilościowym skuteczności stosowania RODO w podrozdziale 5.2. rozprawy.

⁸⁶⁸ J. Wegner-Kowalska, 3. Problem oceny skutków interwencji prawnej [w:] Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej, Warszawa 2017.

⁸⁶⁹ M. Maciejewski, Rozdział 6. Skuteczność a jawność administracji [w:] *Jawność i jej ograniczenia*, t. 3: Skuteczność regulacji, red. G. Szpor, Z. Kmiecik, Warszawa 2013, SIP Legalis.

⁸⁷⁰ G. Szpor, *Jawność i jej ograniczenia*, t. 1: *Idee i pojęcia*, Warszawa 2016, s. 188 i cytowana tam literatura.

⁸⁷¹ *Optymalny*, [hasło w:] *Słownik języka polskiego PWN* [Online], <https://sjp.pwn.pl/slowniki/optymalny.html> (dostęp: 15.09.2024 r.).

⁸⁷² Por. rozdział 5 tej rozprawy.

instrumentów do zredukowania negatywnych skutków doprowadza do zwiększonej niepewności prawnej w porównaniu do optymalnej sytuacji (por. postulaty *de lege ferenda* drugiej części rozdziału 5 tej rozprawy). Niepewność prawna jest istotnym czynnikiem wpływającym na skuteczność aktów prawnych w obszarze przetwarzania danych osobowych w perspektywie analizowanego zjawiska krzyżowania się kompetencji podmiotów administrujących. Wpływa negatywnie na skuteczność psychologiczną, prowadząc do frustracji po stronie podmiotów nadzorowanych, dla których niejasny jest wybór zachowania zgodnego z prawem, co prowadzi do obniżenia przekonania o możliwości przestrzegania prawa⁸⁷³. Nadto, jeżeli znaczenie przepisów prawnych jest niejasne, zmniejsza to szansę na behawioralnej skuteczności prawa, ponieważ podmioty nadzorowane mają mniejszą szansę przestrzegania przepisów, z którymi związana jest trudność odczytania oczekiwanego sposobu zachowania. Ostatecznie, prowadzi to do zagrożenia skuteczności finistycznej, ponieważ zagrożenie skuteczności behawioralnej i psychologicznej (przy założeniu, że środki zostały prawidłowo dobra do celów) stanowi także zagrożenie dla osiągnięcia pożądanego stanu rzeczy, przy czym zagrożenie to jest stopniowalne.

Niepewność prawna jest terminem języka prawnego (użyty został w 16 obowiązujących aktach prawnych⁸⁷⁴) i prawniczego. Zgodnie ze *Słownikiem języka polskiego PWN*, niepewny to „taki, na którym nie można polegać” lub „zawierający ryzyko lub trudny do przewidzenia”⁸⁷⁵. Niepewność prawna związana jest zatem z przekonaniem o trudności przewidzenia prawidłowego (zgodniej z wykładnią przyjętą przez podmioty administrujące lub sądy) znaczenia przepisów prawa lub trudności przewidzenia wyniku stosowania prawa (przez podmioty administrujące lub sądy, co może, ale nie musi być związane z pierwszą trudnością). Pojęcie niepewności prawnej definiowane jest w literaturze w pokrewny sposób jako „sytuacja, która ma miejsce w systemie prawnym, gdy system ten zawiera co najmniej jedną sprawę, która co do zasady nie może zostać rozstrzygnięta w sposób możliwy do zidentyfikowania i jednoznacznie poprawny” („the situation that obtains in a legal system when that system contains at least one case that in principle cannot be decided in an identifiably and uniquely correct way”) albo „sytuacja, w której istnieje więcej niż jedno optymalne rozwiązanie

⁸⁷³ Stanowiąc także naruszenie co najmniej dwóch z ośmiu zasad wewnętrznej moralności prawa zgodnie z myślą filozofa prawa L. Fullera, czyli jasności prawa, także na poziomie jego stosowania (czwartej zasady) i niesprzeczności prawa (piątej zasady), które stanowią warunek praworządności (*rule of law*). Por. C. Murphy, *Lon Fuller and the Moral Value of the Rule of Law*, „Law and Philosophy” 2005, t. 24, nr 3, s. 239-262; E. W. Tucker, *The morality of law*, by Lon L. Fuller, „Indiana Law Journal” 1965, Vol. 40, no. 2, s. 5.

⁸⁷⁴ Odczyt w SIP LEX na dzień 14.02.2024 r.

⁸⁷⁵ *Niepewny*, [hasło w:] *Słownik języka polskiego PWN* [Online], <https://sjp.pwn.pl/slowniki/niepewność.html> (dostęp: 15.09.2024 r.).

problemu prawnego, sąd ma pełną swobodę wyboru optymalnego rozwiązania, które uważa za najbardziej odpowiednie, co oznacza, że strony nie mogą mieć żadnych oczekiwań w takich sytuacjach” („[the situation] where there is more than one optimal solution to a legal problem, judge has absolute discretion to pick the optimal solution he likes best, implying parties can have no expectations in such situations”)⁸⁷⁶. Kontekstem dla pojęcia niepewności prawnej jest zasada pewności prawa. W orzecznictwie TSUE ukształtowano tę zasadę jako ogólną zasadę prawa UE komplementarną dla zasady demokratycznego państwa prawa.⁸⁷⁷ Wymaga ona, aby „przepisy prawne były jasne, precyzyjne i przewidywalne co do ich skutków, w szczególności, gdy mogą mieć skutki niekorzystne dla jednostek i przedsiębiorstw”⁸⁷⁸. Celem jest, aby jednostka mogła jednoznacznie ustalić swoje prawa i obowiązki⁸⁷⁹. Niepewność prawna wynikać może jednak nie tylko z niejasnego sformułowania przepisów, ale także z takiego ukształtowania układu kompetencyjnego, który powoduje, że jednostka nie może przewidzieć oceny prawnej skutków zachowania w sytuacji, gdy to samo zachowanie może zostać uznane za prawidłowe przez jeden organ, podczas gdy inny organ może uznać je za niezgodne z prawem.

Analiza tych definicji prowadzi do wniosku, że niepewność prawna związana jest z niemożnością (trudnością) przewidzenia wyniku stosowania prawa. Definicje te odwołują się do „sytuacji w systemie prawnym”, jednak niepewność prawna ma także wymiar subiektywny, to znaczy związany z uzasadnionym przekonaniem danego podmiotu o trudności w przewidzeniu wykładni prawa lub wyniku jego stosowania. W tym wymiarze niepewność prawna ma charakter stopniowalny, to znaczy może być większa lub mniejsza (większa trudność w przewidzeniu lub mniejsza) i powinna zasadniczo ulegać zmniejszeniu z upływem czasu na skutek aktów stosowania prawa dokonywanych przez podmioty administrujące i sądy. W literaturze pozytywnie zweryfikowano hipotezę przy wykorzystaniu metody empirycznej, że niepewność prawna może negatywnie wpływać na rozwój gospodarczy⁸⁸⁰. Tak rozumiana niepewność wynikająca z analizowanego zjawiska krzyżowania się kompetencji dotyka

⁸⁷⁶ A. D'Amato, *Legal Uncertainty*, „California Law Review” 1983, Vol. 71, No. 1, s. 2, przypis nr 4.

⁸⁷⁷ A. Szmigielski, Nowe formy nadużycia pozycji dominującej w świetle zasady pewności prawa - rozważania na kanwie sprawy Google Search, EPS 2019, nr 10, s. 27-33.

⁸⁷⁸ Wyrok TS z 18.11.2008 r., C-158/07, JACQUELINE FÖRSTER v. Hoofddirectie Van De Informatie Beheer Groep, ZOTSiS 2008, nr 11, poz. I-8507. Przywołanie za: A. Szmigielski, *Nowe formy nadużycia pozycji dominującej w świetle zasady pewności prawa – rozważania na kanwie sprawy Google Search*, EPS 2019, nr 10, s. 27-33.

⁸⁷⁹ Wyrok TS z 10.03.2009 r., C-345/06, Gottfried Heinrich, ZOTSiS 2009, nr 3A, poz. I-1659, p. 78.

⁸⁸⁰ J. Lee, D. Schoenherr, J. Starmans, *The Economics of Legal Uncertainty*, “European Corporate Governance Institute – Law Working Paper” 2023, No. 669/2022, <http://dx.doi.org/10.2139/ssrn.4276837> (dostęp: 15.09.2024 r.), s. 16.

zarówno podmiotów administracji publicznej, podmiotów nadzorowanych i podmiotów danych. Niepewność ta dotyczy zarówno wykładni przepisów prawa (np. w instrumentach typu *soft law*⁸⁸¹), jak i podziału kompetencji oraz sposobu ich wykonywania, przy czym oba te wymiary niepewności prawnej są z sobą powiązane. Powoduje to ryzyko niespójnej wykładni prawa, a w konsekwencji także stosowania prawa, prowadzenia równoległych postępowań w tych samych sprawach przez różne podmioty, co z kolei stanowi zagrożenie dla zasady *ne bis in idem*, jak i sporów kompetencyjnych (tutaj rozumianych szeroko jako wszystkie przypadki rozbieżności poglądów podmiotów administrujących co do zakresu ich działania w odniesieniu do załatwiania danej sprawy⁸⁸²).

Jak wskazano w podrozdziale 2.2. rozprawy, celem podstawowego aktu prawnego w obszarze przetwarzania danych osobowych, RODO, jest zarówno swobodny przepływ danych osobowych, jak i ochrona osób fizycznych w związku z przetwarzaniem tych danych. Drugi z tych celów stanowi emanację podstawowego prawa do ochrony danych osobowych i prawa do prywatności. Niepewność prawna wywołana zjawiskiem krzyżowania się kompetencji prowadzi do obniżenia finistycznej skuteczności prawnej RODO, której kryterium (celem) jest zapewnienie ochrony praw podstawowych. Ponieważ zjawisko to prowadzi do niepewności po stronie podmiotów administrujących, w tym organów ochrony danych, których istnienie i niezależność przewiduje art. 8 ust. 3 KPP, ustanowienie nowych podmiotów administrujących jako kompetentnych w obszarze przetwarzania danych osobowych stanowi zagrożenie dla traktatowo chronionej niezależności organów ochrony danych osobowych. Dochodzi objawem do faktycznego przyznania (przekazania) kompetencji w obszarze ochrony danych osobowych innym organom w strukturze administracji publicznej, co prowadzi do osłabienia roli organów ochrony danych osobowych.

Ponadto, rozbudowana struktura podmiotów administrujących w obszarze przetwarzania danych osobowych w poszczególnych państwach członkowskich, której ustanowienie dopuszczają nowe akty prawne UE (w tym DSA, DGA, Data Act), zwiększa ryzyko zróżnicowanego poziomu ochrony prawnej w każdym z tych państw. Im większa jest liczba podmiotów administrujących w tym obszarze, tym trudniejsze jest zapewnienie ekwiwalentnego poziomu ochrony prawnej. Może prowadzić to do ryzyka wystąpienia

⁸⁸¹ Por. analizę instrumentów *soft law* w podrozdziale 5.3. tej rozprawy.

⁸⁸² A. P. Skoczylas, Rozdział I Zagadnienia ogólne [w:] Rozstrzyganie sporów kompetencyjnych i o właściwość przez NSA, Warszawa 2008; M. Pyziak, Rozstrzyganie sporów kompetencyjnych na ziemiach polskich. Od Rady Stanu Księstwa Warszawskiego do współczesności, „Studia z Dziejów Państwa i Prawa Polskiego” 2010, t. 13, s. 237 (za przywołanym tam J. Zimmermannem).

zjawiska, tzw. forum *shoppingu* przez podmioty nadzorowane rozumianego jako prowadzenie działalności w jurysdykcji o najbardziej korzystnym (zazwyczaj najmniej surowym lub najbardziej przewidywalnym) prawie⁸⁸³. Gdyby do tego doszło, prowadziłoby to do pogłębienia braku skuteczności prawnej w sensie oddalenia od osiągnięcia celu wspólnego unijnego rynku.

Ryzyko, że wobec podmiotu nadzorowanego zostanie zastosowana więcej niż jedna sankcja administracyjna⁸⁸⁴ za to samo zachowanie, dodatkowo pogłębia niepewność prawną po stronie podmiotów nadzorowanych. Takie ryzyko w analizowanym obszarze referencyjnym istnieje. Przykładowo, organ ochrony danych osobowych może nałożyć administracyjną karę pieniężną na administratora danych za zachowania stanowiące naruszenie RODO, które organ ochrony konkurencji uzna jednocześnie za nadużycie pozycji dominującej, nakładając na administratora (przedsiębiorstwa) administracyjną karę pieniężną na podstawie unijnego albo krajowego prawa konkurencji. Zasadność i kształt zastosowania zasady *ne bis in idem* (zakaz podwójnego karania za to samo zachowanie) w unijnym prawie administracyjnym jest przedmiotem dyskusji w literaturze anglojęzycznej⁸⁸⁵ i polskiej (scharakteryzowanej niżej). Poniższe rozważania będą ograniczone do stosowania sankcji w postaci administracyjnych kar pieniężnych, które podmioty administracyjne mogą nakładać na w związku ze stosowaniem każdego z analizowanych aktów prawnych.

Nakładanie administracyjnych kar pieniężnych unormowane zostało w Dziale IVA KPA. Zgodnie z art. 189b § 1 KPA, administracyjna kara pieniężna to „określona w ustawie sankcja o charakterze pieniężnym, nakładana przez organ administracji publicznej, w drodze decyzji, w następstwie naruszenia prawa polegającego na niedopełnieniu obowiązku albo naruszeniu zakazu ciążącego na osobie fizycznej, osobie prawnej albo jednostce organizacyjnej nieposiadającej osobowości prawnej”. Art. 189f § 1 pkt 2 KPA przewiduje, że organ administracji publicznej zobligowany jest do odstąpienia od nałożenia administracyjnej kary pieniężnej, jeżeli spełnione zostały dwie przesłanki: 1) za to samo zachowanie prawomocną

⁸⁸³ Por. M. Szydło, Zapobieganie forum shopping w europejskim prawie upadłościowym, PiP 2008, nr 9, s. 82-93. F. Zopf, Two Worlds Colliding - The GDPR in between Public and Private Law, EDPL 2022, Vol. 8, No. 2, s. 217.

⁸⁸⁴ O pojęciu sankcji administracyjnej zob. Marta Zwierz, *Zakaz ne bis in idem w prawie administracyjnym*, rozprawa doktorska, Warszawa 2019, s. 96-103, <https://depotuw.ceon.pl/bitstream/handle/item/3660/2200-DR-PR-310905.pdf?sequence=1> (dostęp: 15.09.2024 r.).

⁸⁸⁵ Por. przykładowo w odniesieniu zwłaszcza do prawa konkurencji: P. Van Cleynenbreugel, BPost and Nordzucker: Searching for the Essence of Ne Bis in Idem in European Union Law, ECJ 22 March 2022, Case C-117/20, BPost v Autorité belge de la concurrence Case C-151/20, Bundeswettbewerbsbehörde v Nordzucker AG e.a., „European Constitutional Law Review” 2022, Vol. 18, Iss. 2, <https://doi.org/10.1017/S1574019622000190> (dostęp: 20.09.2024 r.). M. Cappai, G. Colangelo, Applying ne bis in idem in the Aftermath of bpost and Nordzucker: The Case of EU Competition Policy in Digital Markets, „Market Law Review” 2023, <http://dx.doi.org/10.2139/ssrn.434407> (dostęp: 20.09.2024 r.).

decyzją na stronę została uprzednio nałożona administracyjna kara pieniężna przez inny uprawniony organ administracji publicznej; 2) uprzednia kara spełnia cele, dla których miałyby być nałożona administracyjna kara pieniężna. To unormowanie wprowadza zasadę *ne bis in idem* w wersji umiarkowanej, przyjmując jednocześnie szerokie jej rozumienie zgodnie z orzecznictwem EPTC i TK, ponieważ nie zakazuje w pełni nakładania administracyjnych kar pieniężnych, a jedynie odstępianie od ich nakładania po spełnieniu obu przesłanek⁸⁸⁶. Ustawodawca wskazał na priorytetową rolę prewencyjnego (ogólnego i szczególnego) oraz represyjnego celu kary, a celowi kompensacyjnemu kary przyznał rolę uzupełniającą⁸⁸⁷. Druga z przesłanek, tj. spełnienie celów kary, jest ocenna *ad casum*⁸⁸⁸. W literaturze, za cytowanym tam orzecznictwem TK⁸⁸⁹, wskazuje się, że przy tej ocenie należy brać pod uwagę, czy ta inna sankcja służy „ochronie tożsamyh dóbr prawnie doniosłych”⁸⁹⁰.

Te przepisy KPA (przepisy ogólne) mogą być modyfikowane przez ustawy (przepisy szczególne) (art. 189a § 2 KPA). Tak też się stało w UODO, zgodnie z którym (art. 106 UODO) art. 189f KPA nie stosuje się do administracyjnych kar pieniężnych nakładanych na podstawie RODO. Oznacza to, że polski ustawodawca wyraził wolę niestosowania tak rozumianej zasady *ne bis in idem* w odniesieniu do tych kar. To wyłączenie w połączeniu z podstawą rolę RODO w unormowaniu przetwarzania danych osobowych powoduje, że podmioty nadzorowane w obszarze przetwarzania danych osobowych narażone są na ryzyko bycia podwójnie karanym za to samo zachowanie. Podkreślić należy, że dyskusyjne wydaje się czy art. 189f § 1 pkt 2 KPA mógłby mieć zastosowanie przez podmiot administrujący inny niż PUODO w sytuacji, w której administracyjna kara pieniężna nakładana byłaby przez ten podmiot już po nałożeniu administracyjnej kary pieniężnej przez PUODO. Ponieważ UODO art. 106 UODO ma zastosowanie do kar administracyjnych nakładanych na podstawie RODO, nie powinien mieć zastosowania do innych aktów prawnych. *Lege non distinguente nec nostrum est distinguere*.

Stąd też analizie poddać należy czy zakaz *ne bis in idem* (przy założeniu, że zastosowanie art. 189f § 1 pkt 2 KPA wyłączono w UODO) wpływa na niepewność prawną w odniesieniu

⁸⁸⁶ A. Wróbel [w:] M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, SIP LEX/el. 2023, art. 189(f), pkt 8.

⁸⁸⁷ R. Suwaj, 5.4. Obligatoryjne odstępianie od nałożenia administracyjnej kary pieniężnej [w:] *Zasady nakładania administracyjnych kar pieniężnych*, Warszawa 2021, SIP LEX.

⁸⁸⁸ A. Cebera, J. G. Firlus [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. H. Knysiak-Sudyka, Warszawa 2023, art. 189(f), pkt 5.

⁸⁸⁹ Wyrok TK z 20.06.2017 r., P 124/15, OTK-A 2017, nr 50.

⁸⁹⁰ M. Jabłoński, *Komentarz do art. 189f KPA* [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. M. Wierzbowski, A. Wiktorowska, Warszawa 2023.

do podwójnego sankcjonowania za to samo zachowanie w obszarze przetwarzania danych osobowych. Obowiązywanie zakazu *ne bis in idem* w prawie administracyjnym uznawane jest za poważny problem „ustrojowy i systemowy na styku prawa administracyjnego i karnego”⁸⁹¹. Formalnie, zakaz ten stanowi zasadę prawa karnego chroniącą przed „nadmierną reakcją ze strony państwa za zachowanie sprzeczne z prawem”, co w aspekcie proceduralnym znaczy niemożność wszczęcia i obowiązek umorzenia prowadzenia postępowania o czyn, który został już osądzony, a w aspekcie materialnym –zakaz podwójnego karania za to samo zachowanie (czyn)⁸⁹². Chodzi o to samo zachowanie w rozumieniu ontologicznym, to znaczy „ten sam czym stanowiący konkretny wycinek rzeczywistości”⁸⁹³. W orzecznictwie ETPC, TSUE i TK ukształtowany został pogląd o rozszerzeniu tego zakazu z formalnie rozumianej odpowiedzialności prawnokarnej na odpowiedzialność określaną jako „represyjna”, którą kwalifikować należy autonomicznie przez ocenę funkcji, jaką pełni sankcja⁸⁹⁴, co może obejmować także sankcje administracyjne, w tym administracyjne kary pieniężne⁸⁹⁵. W orzecznictwie TSUE możliwość zastosowania zakazu *ne bis in idem* w prawie administracyjnym wywodzone jest także z brzmienia art. 50 KPP⁸⁹⁶, odnoszącego się wprost tylko do sankcji prawnokarnych, zgodnie z którym „[n]ikt nie może być ponownie sądzony lub ukarany w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary, w odniesieniu, do którego zgodnie z ustawą został już uprzednio uniewinniony lub za który został już uprzednio skazany prawomocnym wyrokiem na terytorium Unii”.

W prawie administracyjnym zastosowanie tego zakazu może być rozważane zarówno w odniesieniu do zbiegu sankcji administracyjnoprawnych z sankcjami karnoprawnymi⁸⁹⁷, jak i zbiegu sankcji administracyjnoprawnych z sankcjami administracyjnoprawnymi.

⁸⁹¹ R. Suwaj, 5.3. Dopuszczalność wielokrotności karania innymi karami i środkami penalnymi (dualizm wewnętrzny i zewnętrzny) [w:] Zasady nakładania administracyjnych kar pieniężnych, Warszawa 2021, SIP LEX.

⁸⁹² M. Zwierz, *Zakaz ne bis in idem w prawie administracyjnym*, rozprawa doktorska, Warszawa 2019, <https://depotuw.ceon.pl/bitstream/handle/item/3660/2200-DR-PR-310905.pdf?sequence=1> (dostęp: 15.09.2024 r.), s. 49-50.

⁸⁹³ A. Cebera, J. G. Firlus [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. H. Knysiak-Sudyka, Warszawa 2023, art. 189(f), pkt 5, SIP LEX.

⁸⁹⁴ A. Błachnio-Parzych, *Zasada ne bis in idem a odpowiedzialność w sprawach ochrony konkurencji i konsumentów* [w:] *Standardy rzetelności postępowania w sprawach z zakresu ochrony konkurencji i konsumentów*, red. W. Jasiński, Warszawa 2016.

⁸⁹⁵ Por. M. Zwierz, *Zakaz ne bis in idem w prawie administracyjnym*, rozprawa doktorska, Warszawa 2019, <https://depotuw.ceon.pl/bitstream/handle/item/3660/2200-DR-PR-310905.pdf?sequence=1> (dostęp: 15.09.2024 r.), s. 8-10.

⁸⁹⁶ Por. M. Jaśkowski, 3.2. *Ne bis in idem* [w:] *Sądowa kontrola legalności aktów administracyjnych Unii Europejskiej*, Warszawa 2016, SIP LEX. Por. także A. Wróbel, P. Wróbel, Wyrok TS z dnia 14 września 2023 r. w sprawie C-55/22 NK przeciwko Bezirkshauptmannschaft Feldkirch, ZNSA 2023, nr 5, s. 75-80.

⁸⁹⁷ Por. A. Błachnio-Parzych, *Zbieg odpowiedzialności karnej i administracyjno-karnej jako zbieg reżimów odpowiedzialności represyjnej*, Warszawa 2016, SIP LEX.

Przedmiotem badania w tej rozprawie jest wyłącznie ta druga sytuacja. Z uwagi na heterogeniczność prawa administracyjnego materialnego nie istnieje jednolita konstrukcja zakazu *ne bis in idem* w prawie administracyjnym⁸⁹⁸. Zasada ta została uznana w orzecznictwie TK za element zasady demokratycznego państwa prawa (art. 2 Konstytucji RP) powiązany z proporcjonalną reakcją państwa na naruszenie prawa⁸⁹⁹, przy czym można wnioskować, że nie może być naruszona, jeżeli administracyjne kary pieniężne (sankcje administracyjne) służyłyby ochronie różnych dóbr prawnych⁹⁰⁰. TK w ugruntowanej linii orzeczniczej przyjął, że: „jeżeli dwa lub więcej środk[i] mają (...) charakter [represyjny], konieczna jest weryfikacja, czy realizują one te same, czy odmienne cele. Realizacja identycznych celów przez różne środki o charakterze represyjnym winna co do zasady prowadzić do wniosku o naruszeniu zasady *ne bis in idem*”⁹⁰¹. Podobne kryterium, „tożsamości interesu prawnego” jako elementu tożsamości przedmiotu odpowiedzialności (w kontekście spraw z zakresu prawa konkurencji), przyjmowane jest także przez TSUE, chociaż orzecznictwo w tej kwestii nie jest jednolite⁹⁰².

Nawet jeżeli przyjąć, że – pomimo wyłączenia art. 189f KPA w UODO – zakaz *ne bis in idem* w powyższym rozumieniu znajduje zastosowanie przy nakładaniu administracyjnych kar pieniężnych w obszarze przetwarzania danych osobowych, ponieważ stanowi element konstytucyjnej zasady demokratycznego państwa prawa⁹⁰³, to do jego zastosowania w konkretnych sprawach wymagana byłaby realizacja tożsamych celów przez nakładane kary, czyli ochrona tych samych dóbr prawnych. Z analizy aktów prawnych w rozdziale 2 w obszarze referencyjnym nie wynika, aby te akty chroniły one te same dobra prawne. Można argumentować, że jest tak w odniesieniu do niektórych z nich, na przykład RODO, DGA i Data

⁸⁹⁸ M. Zwierz, *Zakaz ne bis in idem w prawie administracyjnym*, rozprawa doktorska, Warszawa 2019, s. 49-50, <https://depotuw.ceon.pl/bitstream/handle/item/3660/2200-DR-PR-310905.pdf?sequence=1> (dostęp: 15.09.2024 r.), s. 108,

⁸⁹⁹ Wyrok TK z 20.06.2017 r., P 124/15, OTK-A 2017, nr 50 przywołany za: I. Wereśniak-Masri, 9.2. *Problem ze stosowaniem zasady ne bis in idem* [w:] *Prawo o odpadach. Wybrane problemy*, red. B. Rakoczy, Warszawa 2019, SIP LEX.

⁹⁰⁰ I. Wereśniak-Masri, 9.2. *Problem ze stosowaniem zasady ne bis in idem* [w:] *Prawo o odpadach. Wybrane problemy*, red. B. Rakoczy, Warszawa 2019, SIP LEX.

⁹⁰¹ Wyrok TK z 20.06.2017 r., P 124/15, OTK-A 2017, nr 50; por. także przywołane tam inne wyroki TK: Wyrok TK z 21.04.2015 r., P 40/13, OTK-A 2015, nr 4, poz. 48. Wyrok TK z 21.10.2014 r., P 50/13, OTK-A 2014, nr 9, poz. 103. Wyrok TK z 1.12.2016 r., K 45/14, OTK-A 2016, nr 99. Wyrok TK z 1.12.2016 r., K 45/14, OTK-A 2016, nr 99.

⁹⁰² Por. A. Błachnio-Parzych, 2.2.2. Tożsamość przedmiotu odpowiedzialności w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej [w:] *Standardy rzetelności postępowania w sprawach z zakresu ochrony konkurencji i konsumentów*, red. W. Jasiński, Warszawa 2016, SIP LEX i analizowane tam orzecznictwo.

⁹⁰³ Por. M. Zwierz, *Zakaz ne bis in idem w prawie administracyjnym*, rozprawa doktorska, Warszawa 2019, s. 49-50, <https://depotuw.ceon.pl/bitstream/handle/item/3660/2200-DR-PR-310905.pdf?sequence=1> (dostęp: 15.09.2024 r.), s. 201-202.

Act, ponieważ za jeden z nich podstawowych celów⁹⁰⁴ można uznać ochronę danych osobowych. Jednak odmienne dobra prawne niewątpliwie chronione są przez, przykładowo, DSA, DMA, akty prawne regulujące AML i prawo konkurencji. Ochrona danych osobowych stanowi co najwyżej komplementarny, nie zaś główny ich cel. W konsekwencji, sankcje nakładane na ich podstawie służą do ochrony innych dóbr prawnie chronionych. Stąd też, jeżeli to samo zachowanie podmiotu nadzorowanego naruszało będzie jednocześnie RODO (ochrona danych osobowych) i przykładowo, DMA oraz art. 102 TFUE (jako nadużycie pozycji dominującej sankcjonowane w celu zapewnienia prawidłowego funkcjonowania rynku), to istniało będzie ryzyko nałożenia niezależnych administracyjnych kar pieniężnych za to samo zachowanie przez organy ochrony danych i krajowe organy ochrony konkurencji (lub Komisję⁹⁰⁵), co nie będzie stanowiło naruszenia zakazu *ne bis in idem*.

Istnienie tak rozumianego ryzyka potwierdza najnowsze orzecznictwo TSUE dotyczące jednoczesnego naruszenia prawa konkurencji i regulacji sektorowych. W wyroku z 22 marca 2022 r. w sprawie *bpost*⁹⁰⁶ TSUE, dokonując interpretacji art. 50 KPP w zw. z art. 52 ust. 1 KPP, orzekł, że „nie stoi on na przeszkodzie ukaraniu osoby prawnej grzywną za popełnienie naruszenia prawa konkurencji Unii, gdy w odniesieniu do tych samych czynów wobec osoby tej wydano już, po przeprowadzeniu postępowania dotyczącego naruszenia przepisów sektorowych mających za przedmiot liberalizację danego rynku, prawomocne orzeczenie”. TSUE wprowadził rozbudowane warunki umożliwiające przyjęcie tej interpretacji, to jest istnieją (1) „jasne i precyzyjne zasady pozwalające przewidzieć, jakie czyny i zaniechania mogą stanowić przedmiot kumulacji postępowań i sankcji, oraz 2) zapewniające koordynację pomiędzy dwoma właściwymi organami, że dwa postępowania były prowadzone w sposób wystarczająco skoordynowany i w krótkim czasie oraz 3) wszystkie sankcje odpowiadają wadze popełnionych naruszeń”. Z tego orzeczenia wynika, że TSUE dopuszcza możliwość wszczęcia i prowadzenia odrębnych postępowań administracyjnych oraz nałożenia niezależnych sankcji administracyjnych (administracyjnych kar pieniężnych), o ile postępowania te i sankcje dotyczą odrębnych celów, chroniąc odrębne dobra prawne, co w tej sprawie obejmowało z jednej strony liberalizację rynku usług pocztowych, a z drugiej ochronę

⁹⁰⁴ Por. analizę balansowania celów przez poszczególne podmioty administrujące w podrozdziale 5.6. rozprawy i postulaty *de lege ferenda* w podrozdziale 5.7. rozprawy.

⁹⁰⁵ Por. M. Cappai, G. Colangelo, *Applying ne bis in idem in the Aftermath of bpost and Nordzucker: The Case of EU Competition Policy in Digital Markets*, „Market Law Review” 2023, <http://dx.doi.org/10.2139/ssrn.434407> (dostęp: 20.09.2024 r.), s. 10-11.

⁹⁰⁶ Wyrok TS z 22.03.2022 r., C-117/20, BPOST SA przeciwko Autorité Belge De La Concurrence, SIP LEX nr 3324166.

konkurencyjnego rynku⁹⁰⁷. Wymagane jest jednak ukształtowanie procedur w taki sposób, aby zapewnić spójność między postępowaniami dotyczącymi tego samego zachowania prowadzonymi przez różne podmioty administrujące, co zwiększać ma pewność prawną po stronie podmiotów nadzorowanych.

Prawodawca unijny identyfikuje ryzyko niejasności zastosowania zakazu *ne bis in idem* w obszarze przetwarzania danych osobowych w sposób wybiórczy. Ta wybiórczość nie usuwa niepewności prawnej po stronie podmiotów nadzorowanych, ale warta jest odnotowania jako (możliwy) kierunek zmiany. Jak scharakteryzowano już w podrozdziale 2.6.2. rozprawy, unikalnym rozwiązaniem jest art. 35 ust. 2 Dyrektywy NIS 2, który przewiduje, że jeżeli organy ochrony danych nałożą na podmiot nadzorowany administracyjną karę pieniężną na podstawie RODO za naruszenie ochrony danych, to organy właściwe do spraw cyberbezpieczeństwa nie mogą nałożyć administracyjnej kary pieniężnej na podstawie Dyrektywy NIS 2 w celu sankcjonowania tego samego zachowania stanowiącego naruszenie obowiązków w art. 21 i 23 Dyrektywy NIS 2. Mogą one zastosować inne „środki egzekwowania przepisów”. Chociaż, jak wskazano, rozwiązanie to należy ocenić pozytywnie (jako zmniejszające niepewność prawną), to jego wykorzystanie powodowało będzie w praktyce wątpliwości. Przykładowo, nie jest jasne, czy to ograniczenie w nakładaniu administracyjnej kary pieniężnej przez organy właściwe do spraw cyberbezpieczeństwa dotyczy wszystkich naruszeń art. 21 i 23 Dyrektywy NIS 2, które objęte zostały taką karą przez organy ochrony danych, czy też tylko takich, o których organy właściwe do spraw cyberbezpieczeństwa przekazały uprzednio informację do organów ochrony danych w trybie art. 35 ust. 1 Dyrektywy NIS 2. Niezależnie jednak od tych wątpliwości, zasadne byłoby, aby podobne rozwiązania zostały wprowadzone w większej liczbie aktów prawnych normujących przetwarzanie danych osobowych (przykładowo, w DGA i Data Act) w zakresie, w jakim stosowanie różnych administracyjnych kar pieniężnych przez różne podmioty administrujące chroniłoby w istocie to samo dobro prawne⁹⁰⁸.

4.5.2. SKUTKI DLA GOSPODARKI

Jak wskazano we Wprowadzeniu i w podrozdziale 2.3. tej rozprawy dotyczącym pojęcia danych osobowych, stanowią one kluczowe aktywo niematerialne w gospodarce doby

⁹⁰⁷ A. Zientara, 3. Zasada *ne bis in idem* w orzecznictwie Trybunału Sprawiedliwości [w:] *Prawnokarna ochrona przed nieuczciwą konkurencją w ustawie o zwalczaniu nieuczciwej konkurencji*, Warszawa 2023, SIP LEX.

⁹⁰⁸ Por. postulaty *de lege ferenda* w podrozdziale 5.7. rozprawy.

transformacji cyfrowej. Jednocześnie idea ochrony danych osobowych stanowiąca węzłowy cel unijnych aktów prawnych normujących przetwarzanie danych osobowych wywodzi się z tradycji praw człowieka. Ten podwójny charakter danych osobowych doprowadził do sformułowania dwóch odmiennych poglądów w publicznej debacie co do skutków aktów prawnych w obszarze przetwarzania danych osobowych dla rozwoju gospodarki. Jedni uważają, że akty te hamują innowacyjność i wzrost gospodarczy w UE, zwłaszcza w sektorze małych i średnich przedsiębiorstwach, ponieważ są zbyt skomplikowane i nakładają liczne obowiązki⁹⁰⁹. Drudzy, wychodząc z perspektywy ochrony praw podstawowych, stoją na stanowisku, że akty te, zwłaszcza na etapie ich stosowania, są niewystarczająco restrykcyjne w stosunku do administratorów danych osobowych, zwłaszcza tzw. gigantów cyfrowych⁹¹⁰. Źródła tych różnic należy doszukiwać się w odmiennych podejściach do innowacyjności⁹¹¹ i odmiennych poglądach etycznych na regulację zmian spowodowanych transformacją cyfrową⁹¹².

Skutki aktów prawnych dla gospodarki są skutkami pozaprawnymi, to znaczy wykraczają poza system prawny, a w konsekwencji poza dogmatykę prawa. Stąd też zajęcie stanowiska wobec powyższych poglądów, jak również dokonanie szacunków skutków (kosztów) ekonomicznych związanych z realizacją analizowanych aktów prawnych wymagałoby wyjścia poza przedmiot tej rozprawy i obrania metod badawczych wykraczających poza nauki prawne, głównie z nauk ekonomicznych⁹¹³. W odniesieniu do większości aktów nie byłoby nadto możliwe, ponieważ akty te albo jeszcze nie są stosowane, albo też zaczęły być stosowane

⁹⁰⁹ Przykładowo por. G. Johnson, *Economic Research on Privacy Regulation: Lessons From the GDPR and Beyond* [in:] *The Economics of Privacy*, ed. by A. Goldfarb, C. Tucker, Chicago 2024, <http://dx.doi.org/10.2139/ssrn.4290849> (dostęp: 7.09.2024 r.), s. 3-4, 21; N. Yaraghi, *A case against the General Data Protection Regulation*, <https://www.brookings.edu/articles/a-case-against-the-general-data-protection-regulation/> (dostęp: 7.09.2024 r.). Por. także Ch. Peukert, S. Bechtold, M. Batikas et al., *Regulatory spillovers and data governance: Evidence from the GDPR*, „Marketing Science” 2022, Vol. 41, No. 4, s. 746-768. Jeszcze inni uważają przeciwnie, że RODO jest czynnikiem stymulującym innowację, por. C. Niebel, *The impact of the general data protection regulation on innovation and the global political economy*, CLSR 2021, Vol. 40.

⁹¹⁰ Przykładowo: M. Burgess, *How GDPR is failing*, 23.05.2022, <https://www.wired.co.uk/article/gdpr-2022> (dostęp: 15.09.2024 r.).

⁹¹¹ Por. A. Butenko, P. Larouche, *Regulation for Innovativeness or Regulation of Innovation?*, „TILEC Discussion Paper” 2015, No. 2015-007, <https://ssrn.com/abstract=2584863> (dostęp: 5.09.2024 r.); T. A. Hemphill, *The Innovation Governance Dilemma: Alternatives to the Precautionary Principle*, „Technology in Society” 2020, Vol. 63, <https://doi.org/10.1016/j.techsoc.2020.101381> (dostęp: 20.09.2024 r.).

⁹¹² Por. *Oxford Handbook of Digital Ethics*, ed. By C. Véliz, Oxford 2023, <https://doi.org/10.1093/oxfordhb/9780198857815.001.0001> (dostęp: 1.02.2024 r.).

⁹⁰⁰ Z zastrzeżeniem, że wartościowe poznawczo mogłoby mieć zastosowanie ekonomicznej analizy prawa; por. np. L. Kornhauser, *The Economic Analysis of Law*, [in:] *The Stanford Encyclopedia of Philosophy*, ed. by E. N. Zalta, (Spring 2022 Edition), <https://plato.stanford.edu/archives/spr2022/entries/legal-econanalysis/> (dostęp: 20.09.2024 r.).

relatywnie niedawno. Analiza literatury dotyczącej ekonomicznych skutków RODO⁹¹⁴ prowadzi do wniosku, że regulacja w obszarze ochrony danych osobowych wywiera skutki ekonomiczne, chociaż nie można jednoznacznie stwierdzić czy skutki te są pozytywne, negatywne czy też mieszane albo też czy ich ocena możliwa jest wyłącznie kontekstowo⁹¹⁵. W literaturze dyskutowane jest jakie kryterium należy obrać dla oceny ekonomicznej efektywności prawa. Wyróżniane są m.in. następujące kryteria: maksymalizacji dobrobytu społecznego (Posner); poprawy sytuacji ekonomicznej co najmniej jednego podmiotu, przy braku zmian sytuacji pozostałych (Pareto); czy też zmniejszenie kosztów krańcowych (koszt wyprodukowania jednej dodatkowej jednostki)⁹¹⁶.

Najbardziej przekonujący wydaje się pogląd, że RODO wywiera skutki mieszane, które można oceniać wyłącznie kontekstowo, w odniesieniu do poszczególnych sektorów⁹¹⁷, przy czym dynamikę innowacji w UE na skutek stosowania RODO określić można raczej jako inkrementalną niż skokową (rewolucyjną)⁹¹⁸. Negatywnymi skutkami mogą być w szczególności: porzucenie rozwoju produktów lub usług z uwagi na ryzyka związane z przestrzeganiem RODO, zniechęcenie do podejmowania nowej działalności gospodarczej z uwagi na te ryzyka, ograniczanie zbierania danych osobowych ponad poziom wynikający z zasady minimalizacji danych, podczas gdy dane te mogą w przyszłości okazać się przydatne dla nieznanych w momencie ich zbierania celów (np. trenowania modeli sztucznej inteligencji); natomiast do pozytywnych skutków zaliczyć można zwłaszcza inspirowanie modyfikacji produktów i usług w taki sposób, aby RODO było przestrzegane oraz tworzenie nowych produktów i usług, które

⁹¹⁴ Por. np. D. W. E. Allen, A. Berg, Ch. Berg et al. *Some Economic Consequences of the GDPR*, „Economics Bulletin” 2019, Vol. 39, No. 2, <https://ssrn.com/abstract=3160404> (dostęp: 20.09.2024 r.), s. 785-797; S. Goldberg, G. Johnson, S. Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR*, „Law & Economics Center at George Mason University Scalia Law School Research Paper Series” 2022, No. 22-025, <http://dx.doi.org/10.2139/ssrn.3421731> (dostęp: 7.09.2024 r.); N. Martin, Ch. Matt, C. Niebel et al., *How data protection regulation affects startup innovation*, „Information systems frontiers” 2019, Vol. 21, s. 1307-1324.

⁹¹⁵ K. Blind, C. Niebel, Ch. Rammer, *The Impact of the EU General Data Protection Regulation on Innovation in Firms*, „ZEW - Centre for European Economic Research Discussion” 2022, No. 22-047, <http://dx.doi.org/10.2139/ssrn.4257740> (dostęp: 20.09.2024 r.), s. 2-6.

⁹¹⁶ A. Nadolska, Komisja Nadzoru Finansowego w nowej instytucjonalnej architekturze europejskiego nadzoru finansowego, Warszawa 2014, s. 297-298.

⁹¹⁷ Por. K. Blind, C. Niebel, Ch. Rammer, *The Impact of the EU General Data Protection Regulation on Innovation in Firms*, „ZEW - Centre for European Economic Research Discussion” 2022, No. 22-047, <http://dx.doi.org/10.2139/ssrn.4257740> (dostęp: 20.09.2024 r.); N. Martin, Ch. Matt, C. Niebel et al., *How data protection regulation affects startup innovation*, „Information systems frontiers” 2019, Vol. 21, s. 1307-1324.

⁹¹⁸ K. Blind, C. Niebel, Ch. Rammer, *The Impact of the EU General Data Protection Regulation on Innovation in Firms*, „ZEW - Centre for European Economic Research Discussion” 2022, No. 22-047, <http://dx.doi.org/10.2139/ssrn.4257740> (dostęp: 20.09.2024 r.), s. 3. Por. także K. Blind, C. Niebel, Ch. Rammer, *The Impact of the EU General data protection regulation on product innovation, Industry and Innovation*, „Industry and Innovation”, Vol. 31, Iss. 3.

pomogą przestrzegać RODO (np. narzędzi informatycznych do anonimizacji danych osobowych)⁹¹⁹.

Niezależnie od prezentowanych poglądów na temat skutków aktów prawnych w obszarze przetwarzania danych osobowych w UE dla gospodarki wskazać należy, że obrany w UE model regulacji tego obszaru wynika z prawa podstawowego UE, w tym KPP, który stanowi element systemu ochrony praw człowieka. Zarówno przystąpienie państw członkowskich do UE (jako organizacji międzynarodowej), jak i przyjęcie prawa pierwotnego UE, a następnie prawa wtórnego UE znajduje legitymację demokratyczną. Ostatecznie zatem za obranym modelem regulacji stoi wola obywateli UE, która jest jednocześnie wyrazem określonego wyboru aksjologicznego.

W odniesieniu natomiast do skutków analizowanego zjawiska dla gospodarki istotne jest, że zwiększa ono niepewność prawną po stronie podmiotów nadzorowanych⁹²⁰. Uprawnione jest poczynienie założenia, że zwiększona niepewność powoduje większe koszty zapewnienia zgodności z prawem po stronie podmiotów nadzorowanych (w tym droższą obsługę prawną), ale także zwiększa ryzyko prowadzenia działalności w UE z wykorzystaniem (znacznych ilości) danych osobowych, ponieważ różne podmioty administrujące mogą w odmienny sposób interpretować te same stany faktyczne i wykonywać kompetencje naprawcze niezależnie od siebie⁹²¹. Wobec tych okoliczności, w określonych sytuacjach, np. przy wyborze jurysdykcji do trenowania modelu sztucznej inteligencji przy użyciu danych (w tym danych osobowych), przedsiębiorstwo motywowane dążeniem do zmniejszenia ryzyka prawnego i kosztów obsługi prawnej skłonne będzie wybrać inną (mniej restrykcyjną) jurysdykcję, ponieważ jurysdykcje unijne związane będą z wyższym kosztem regulacyjnym⁹²².

Jeżeli inne jurysdykcje globalnie przyjmą model regulacji przetwarzania danych osobowych, w którym koszty prawne i ryzyko związane ze zjawiskiem krzyżowania się kompetencji w tym obszarze będą niższe, uczyni to jurysdykcje unijne mniej atrakcyjnymi dla zewnętrznych inwestycji związanych z przetwarzaniem (znacznych ilości) danych osobowych, ale również z zasady uczyni trudniejszym konkurowanie przedsiębiorstwom unijnym poza UE,

⁹¹⁹ N. Martin, Ch. Matt, C. Niebel et al., *How data protection regulation affects startup innovation*, „Information systems frontiers” 2019, Vol. 21, s. 1307-1324, 7 Conclusion and Limitations.

⁹²⁰ Por. L. Robb, T. Candy, F. Deane, *Regulatory overlap: A systematic quantitative literature review*, „Regulation & Governance” 2023, Vol. 17, No. 4, <https://doi.org/10.1111/rego.12504> (dostęp: 20.09.2024 r.), s. 1131, 1139.

⁹²¹ Por. L. Robb, T. Candy, F. Deane, *Regulatory overlap: A systematic quantitative literature review*, „Regulation & Governance” 2023, Vol. 17, No. 4, <https://doi.org/10.1111/rego.12504> (dostęp: 20.09.2024 r.), s. 1131, 1140.

⁹²² O pojęciu kosztu alternatywnego w naukach ekonomicznych por. J. M. Buchanan, *Opportunity cost* [in:] *The world of economics*, ed. by J. Eatwell, London 1991.

ponieważ koszty regulacyjne będą dla nich wyższe niż dla przedsiębiorstw, które tym regulacjom nie podlegają.

Zjawisko to prowadzi także do zwiększonego zaangażowania urzędników obsługujących podmioty administrujące w tym obszarze, których wysiłki nakierowane będą na zmniejszenie negatywnych skutków jego występowania. Tymczasem wysiłki te, zamiast być skierowane do wewnątrz administracji publicznej, mogłyby być skierowane na zewnątrz wobec podmiotów nadzorowanych i podmiotów danych i nakierowane na rozwiązanie problemów regulacyjnych tych podmiotów oraz zredukowania ryzyk w obszarze. Stąd też, aby zoptymalizować administrowanie w tym obszarze, konieczne jest wprowadzenie skutecznych instrumentów prawnych, aby przeciwdziałać negatywnym skutkom tego zjawiska. Chociaż można przeciwdziałać negatywnym skutkom tego zjawiska, to samo to zjawisko należy jednak uznać za nieuniknione i nieusuwalne co do istoty w tym modelu regulacji tego obszaru. Zanim sformułowane zostaną zatem postulaty *de lege ferenda*, konieczne jest wpięrow identyfikacja i analiza jego przyczyn (por. rozdział 5 rozprawy).

4.6. KRZYŻOWANIE SIĘ KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH W UJĘCIU PRAWNOPORÓWNAWCZYM

Zjawisko krzyżowania się kompetencji organów administracji publicznej nie jest właściwe tylko polskiej jurysdykcji. Zjawisko to, stanowiąc emanację procesu europeizacji prawa administracyjnego państw członkowskich⁹²³, występuje także w pozostałych jurysdykcji unijnych. Z uwagi na charakter zjawiska wywoływany transformacją cyfrową i związanym z tym „rozłączeniem regulacyjnym”⁹²⁴, występuje także w jurysdykcjach nie-unijnych, w których unormowano obszar przetwarzania danych osobowych. Spowodowane jest to także wpływem modelu przyjętego w prawie unijnym na kształtowanie prawodawstwa globalnie znane w literaturze jako „*Brussels effect*” („efekt Brukseli”) ⁹²⁵, czego konsekwencją jest transplantacja zalet i wad unijnej regulacji.

⁹²³ Por. podrozdział 5.2. rozprawy.

⁹²⁴ Por. podrozdział 5.4. rozprawy.

⁹²⁵ Por. np. S. Gunst, F. De Ville, *The Brussels effect: how the GDPR conquered Silicon Valley*, „European Foreign Affairs Review” 2021, Vol. 26, Iss. 3, <https://doi.org/10.54648/eerr2021036> (dostęp 07.09.2024 r.), s. 437-458. O zjawisku „Brussels effect” por. A. Bradford, *The Brussels effect: How the European Union rules the world*. Oxford 2020.

W tym podrozdziale dokonano ograniczonej analizy prawno porównawczej rozwiązań prawnych w Królestwie Niderlandów jako dojrzałej unijnej jurysdykcji prawa kontynentalnego i w Wielkiej Brytanii jako przykład nie-unijnego systemu prawa *common law*. Te dwa państwa wybrane zostały jako przykłady do prawno porównawczej analizy, ponieważ w obu wprowadzono nowatorskie rozwiązania, to jest podmioty koordynujące działania podmiotów administrujących w obszarze przetwarzania danych osobowych. Punktem odniesienia dla tej analizy będą właśnie te rozwiązania. Wskazać należy, że także w innych jurysdykcjach unijnych również wprowadzone zostały podobne rozwiązania, na przykład w Irlandii⁹²⁶ i w Niemczech⁹²⁷. Sam fakt, że takie inicjatywy są wdrażane świadczy o oddolnej potrzebie koordynacji działań pomiędzy tymi organami.

Zasadne jest poczynienie wstępnych uwag o charakterze metodologicznym. Z każdą analizą prawno porównawczą obszaru unormowania lub instytucji prawnej związane jest ryzyko jej powierzchowności lub nawet przeinaczenia, spowodowane brakiem (ograniczeniem) całościowego rozumienia systemu prawnego porównawczo badanej jurysdykcji⁹²⁸, jak i barierami językowymi⁹²⁹, które występować mogą nawet przy zaawansowanej znajomości języka obcego. To ryzyko jest tym większe w prawie administracyjnym, które, będąc prawem publicznym, wpisane jest w normy i tradycję konstytucyjną poszczególnych jurysdykcji i z zasady związane z wykonywaniem władztwa publicznego (także sposobem jego wykonywania, co jest przedmiotem badania nauki administracji i nauki o zarządzaniu)⁹³⁰. Formuła i objętość tej rozprawy nie pozwalają na przeprowadzenie kompleksowej analizy prawno porównawczej obu jurysdykcji. Stąd też ograniczona analiza w niniejszym rozdziale dokonana została w ujęciu funkcjonalnym⁹³¹ z ograniczeniem do zbadania rozwiązań (podmiotów) o funkcji

⁹²⁶ Sieć pod nazwą „Digital Regulators Group”, w której skład wchodzi także irlandzki organ ochrony danych, por. *Data Protection Commission, Data Protection Commission publishes 2022 Annual Report*, <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commissionpublishes-2022-annual-report> (dostęp: 12.02.2024 r.).

⁹²⁷ Sieć pod nazwą „Digital Cluster Bonn”, w której skład wchodzi także niemiecki organ ochrony danych, por. *Digital Cluster Bonn*, <https://www.digitalclusterbonn.de/DCB/start.html> (dostęp: 12.02.2024 r.).

⁹²⁸ J. S. Bell, *Comparative Administrative Law*, [in:] *The Oxford Handbook of Comparative Law*, 2nd edn, ed. by M. Reimann, R. Zimmermann, Oxford 2019, <https://doi.org/10.1093/oxfordhb/9780199296064.001.0001> (dostęp: 12.02.2024 r.), s. 1251.

⁹²⁹ J. C. Reitz, *How to Do Comparative Law*, „American Journal of Comparative Law” 1998, Vol. 46, No. 4., s. 620-621.

⁹³⁰ Por. J. Boughey, *Administrative Law: The Next Frontier For Comparative Law*, „International and Comparative Law Quarterly” 2013, No. 62(1), <https://doi.org/10.1017/S0020589312000553> (dostęp: 5.09.2024 r.).

⁹³¹ R. Michaels, *The Functional Method of Comparative Law* [in:] *The Oxford Handbook of Comparative Law*, 2nd edn, edited by M. Reimann, R. Zimmermann, Oxford 2019, <https://doi.org/10.1093/oxfordhb/9780199296064.013.0011> (dostęp: 12.02.2024 r.), s. 386-388.

koordynującej ustanowionych w obu tych państwach, co uzupełnione jest o ogólne uwagi o prawie administracyjnym obu tych państw.

4.6.1. KRÓLESTWO NIDERLANDÓW

Królestwo Niderlandów (Holandia), to parlamentarna monarchia konstytucyjna, będąca jednym z państw założycielskich Unii Europejskiej, w której władzę wykonawczą sprawuje rada ministrów⁹³². Tak jak w Polsce, rozporządzenia unijne są w Holandii bezpośrednio stosowane, natomiast dyrektywy podlegają implementacji w krajowym porządku prawnym. Zasadniczo zatem zastosowanie mają analizy o krzyżowaniu się zakresów przedmiotowych aktów prawnych prawa unijnego i kompetencji podmiotów administrujących ustanowionych na poziomie prawa unijnego.

W Holandii dokonano kodyfikacji postępowania administracyjnego w akcie prawnym z 1994 r. – Ustawie o ogólnym prawie administracyjnym (*Algemene wet bestuursrecht*), który uzupełniany był o kolejne części, m.in. w 1998 r. i w 2009 r.⁹³³ Akt ten reguluje m.in. wykonywanie decyzji organów UE (tytuł 1.2), reguły prowadzenia postępowania administracyjnego (rozdział 2), wydawania aktów administracyjnych (ogólne reguły w rozdziale 3 i szczególne w rozdziale 4), elementy przeprowadzania kontroli (art. 5:17 i następne), a także procedurę odwołania od aktów administracyjnych i elementy sądowej kontroli administracji (rozdziały 6 i 7). Przykładowo, Ustawa o ogólnym prawie administracyjnym definiuje pojęcie „organu administracji publicznej” szeroko: jest nim każdy organ ustanowiony na podstawie prawa publicznego lub inny podmiot, którym powierzono jakąkolwiek władzę publiczną (Artykuł 1:1 Ustawy o ogólnym prawie administracyjnym⁹³⁴). Termin odpowiadający terminowi „kompetencja” lub „kompetentny” użyty został 20 razy w Ustawie o ogólnym prawie administracyjnym, ale nie został w niej zdefiniowany.

⁹³² UE, *Kraje UE, Holandia*, https://european-union.europa.eu/principles-countries-history/country-profiles/netherlands_pl#:~:text=W%20UE%3A%20od%201%20stycznia,Waluta%3A%20euro (dostęp: 15.09.2024 r.).

⁹³³ T. Barkhuysen, W. Ouden, Y. E. Schuurmans, *The law on administrative procedures in the Netherlands*, „Netherlands Administrative Law Library” 2012, dostęp: <https://www.nall.nl/tijdschrift/nall/2012/06/NALL-D-12-00004.pdf> (dostęp: 02.09.2024 r.), s. 1, 7.

⁹³⁴ Tłumaczenie ustawy z języka holenderskiego na język angielski dostępne na stronie internetowej holenderskiego organu prawa konkurencji De Autoriteit Consument & Markt (ACM) https://www.acm.nl/sites/default/files/old_publication/publicaties/15446_dutch-general-administrative-law-act.pdf (dostęp: 05.09.2024 r.). Tłumaczenie to nie zawiera wszystkich zmian (por. Y. E. Schuurmans, T. Barkhuysen, W. den Willemien, *Codification of Administrative Law in the Netherlands* [in:] *Codification of Administrative Law: A Comparative Study on the Sources of Administrative Law*, ed by F. Uhlmann, London 2023, s. 193), a wersja w języku holenderskim dostępna jest na stronie internetowej: <https://wetten.overheid.nl/BWBR0005537/2024-01-01> (dostęp: 05.09.2024 r.).

W jurysdykcji holenderskiej ustanowionych jest wiele szczególnych postępowań administracyjnych, które modyfikują tę Ustawę o ogólnym prawie administracyjnym (z wyłączeniem przepisów bezwzględnie obowiązujących)⁹³⁵. W literaturze kodyfikacja holenderska (zawierająca ponad 500 przepisów) uznawana jest za jedną z najbardziej kompleksowych⁹³⁶. W Królestwie Niderlandów, podobnie jak w Polsce, nie ma osobnego aktu prawnego kodyfikującego ogólne przepisy administracyjnego prawa materialnego. W państwie tym, będącym członkiem UE, w obszarze przetwarzania danych osobowych bezpośrednio zastosowanie znajduje RODO jako rozporządzenie unijne, przy czym, analogicznie jak w Polsce, prawodawca krajowy przyjął akt prawny nakierowany na wdrożenie wybranych przepisów RODO pod tytułem „*Uitvoeringswet Algemene verordening gegevensbescherming*” („Ustawa wdrażająca ogólne rozporządzenie o ochronie danych”)⁹³⁷. Ten akt prawny nie jest przedmiotem badania w niniejszym podrozdziale. W niniejszym podrozdziale analizie poddano jedynie rozwiązania przyjęte w Królestwie Niderlandów w celu zredukowania negatywnych skutków zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych.

Zgodnie z informacjami na stronie internetowej holenderskiego organu prawa konkurencji *Autoriteit Consument & Markt* (ACM; Urząd ds. Konsumentów i Rynków), Platforma Współpracy w Zakresie Regulacji Cyfrowych (*Samenwerkingsplatform Digitale Toezichthouders*; SDT) została utworzona w 2021 r. przez Urząd ds. Konsumentów i Rynków (ACM), czyli organ ochrony konkurencji i konsumentów, Urząd ds. Rynków Finansowych (*Autoriteit Financiële Markten*; AFM), czyli organ nadzoru rynku finansowego, Urząd Ochrony Danych (*Autoriteit Persoonsgegevens*; AP), czyli organ ochrony danych osobowych i Urząd ds. Mediów (*Commissariaat voor de Media*; CvdM)⁹³⁸, który nadzoruje m.in. rynek

⁹³⁵ T. Barkhuysen, W. Ouden, Y. E. Schuurmans, *The law on administrative procedures in the Netherlands*, „Netherlands Administrative Law Library” 2012, dostęp: <https://www.nall.nl/tijdschrift/nall/2012/06/NALL-D-12-00004.pdf> (dostęp: 020.09.2024 r.), s. 11.

⁹³⁶ Y. E. Schuurmans, T. Barkhuysen, W. den Willemien, *Codification of Administrative Law in the Netherlands* [in:] *Codification of Administrative Law: A Comparative Study on the Sources of Administrative Law*, ed by F. Uhlmann, London 2023, s. 193.

⁹³⁷ „Uitvoeringswet Algemene verordening gegevensbescherming.” *Wetten.nl*, 1 lipca 2021. <https://wetten.overheid.nl/BWBR0040940/2021-07-01> (dostęp: 15.09.2024 r.). Dutch General Data Protection Regulation Implementation Act (Holenderska ustawa wdrażająca ogólne rozporządzenie o ochronie danych, nieoficjalne tłumaczenie na język angielski), https://www.dataguidance.com/sites/default/files/dutch_general_data_protection_regulation_implementation_act.pdf (dostęp: 15.09.2024 r.).

⁹³⁸ *Autoriteit Consument & Markt* (ACM), SDT members to expand their collaboration regarding digital regulation, <https://www.acm.nl/en/publications/sdt-members-expand-their-collaboration-regarding-digital-regulation> (dostęp: 15.09.2024 r.); *Samenwerkingsplatform Digitale Toezichthouders* (SDT); <https://www.acm.nl/nl/organisatie/samenwerking/nationale-samenwerking/samenwerkingsplatform-digitale-toezichthouders-sdt> (dostęp: 15.09.2024 r.).

mediów publicznych i dostawców usług medialnych oraz usług medialnych na żądanie (jak *Video on Demand*)⁹³⁹. Celem było powołanie specyficznego podmiotu o funkcji koordynującej efektywne stosowanie aktów prawnych w obszarze „regulacji cyfrowej” (w tym „sztuczna inteligencja, algorytmy, przetwarzanie danych, projektowanie online, personalizacja, manipulacja i wprowadzające w błąd praktyki”⁹⁴⁰) i wymiana wiedzy i doświadczeń między wskazanymi wyżej podmiotami administrującymi⁹⁴¹. Podmiot ten składa się m.in. z izby (*chamber*) generalnej i z izby dedykowanej stosowaniu DSA i nadzorowi nad sztuczną inteligencją⁹⁴². Inicjując to przedsięwzięcie, przedstawiciele tych podmiotów administrujących wskazywali na ryzyko krzyżowania się kompetencji między nimi i szansę zwiększenia skuteczności przez współpracę w tym obszarze⁹⁴³. Ponieważ jest to inicjatywa samych podmiotów administrujących, powołanie SDT nie wywołuje zmian w kompetencjach tych podmiotów. Dotychczasowa działalność SDT obejmowała m.in. opublikowanie podstawowych reguł skutecznego dostarczania informacji w Internecie, a także podstawowych reguł marketingu internetowego skierowanego do dzieci⁹⁴⁴.

Królestwo Niderlandów jest zatem przykładem jurysdykcji unijnej, w której to same podmioty administrujące w obszarze przetwarzania danych zidentyfikowały ryzyko krzyżowania się ich kompetencji. Aby zmniejszyć negatywne skutki tego zjawiska, podjęły inicjatywę powołania specyficznego podmiotu – Platforma Współpracy w Zakresie Regulacji Cyfrowych, która od 2021 r. zrealizowała szereg inicjatyw, przede wszystkim w zakresie kompetencji doradczych, informacyjnych i edukacyjnych tych podmiotów. Inicjatywę tę należy ocenić pozytywnie jako przejaw pragmatycznego i „oddolnego” działania administracji publicznej w interesie publicznym. Wskazać należy, że zastrzeżenia do legalności powołania

⁹³⁹ Commissariaat voor de Media, English summary Dutch Media Authority, <https://www.cvdm.nl/english-summary-dutch-media-authority/> (dostęp: 15.09.2024 r.).

⁹⁴⁰ Autoriteit Consument & Markt (ACM), Dutch regulators strengthen oversight of digital activities by intensifying cooperation, <https://www.acm.nl/en/publications/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation> (dostęp: 15.09.2024 r.).

⁹⁴¹ Autoriteit Consument & Markt (ACM), SDT members to expand their collaboration regarding digital regulation, <https://www.acm.nl/en/publications/sdt-members-expand-their-collaboration-regarding-digital-regulation> (dostęp: 15.09.2024 r.).

⁹⁴² Autoriteit Consument & Markt (ACM), SDT members to expand their collaboration regarding digital regulation, <https://www.acm.nl/en/publications/sdt-members-expand-their-collaboration-regarding-digital-regulation> (dostęp: 15.09.2024 r.).

⁹⁴³ Autoriteit Consument & Markt (ACM), Dutch regulators strengthen oversight of digital activities by intensifying cooperation, <https://www.acm.nl/en/publications/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation> (dostęp: 15.09.2024 r.).

⁹⁴⁴ Autoriteit Consument & Markt (ACM), SDT members to expand their collaboration regarding digital regulation, <https://www.acm.nl/en/publications/sdt-members-expand-their-collaboration-regarding-digital-regulation> (dostęp: 15.09.2024 r.).

tego typu podmiotów można byłoby formułować z perspektywy zasady legalizmu⁹⁴⁵. W przypadku polskiej jurysdykcji uznać jednak należałoby, że skoro inicjatywa taka realizowana w wewnętrznej strukturze administracji publicznie nie zmienia podziału kompetencji tych podmiotów administrujących, to nie można uczynić wobec niej zarzutu przekroczenia zasady legalizmu.

4.6.2. WIELKA BRYTANIA

W Wielkiej Brytanii⁹⁴⁶, będącej monarchią parlamentarną, która nie posiada spisanej konstytucji, występują trzy odrębne systemy prawne: Anglii i Walii, Szkocji i Irlandii Północnej⁹⁴⁷. Każdy z tych systemów zaliczany jest do systemu prawa zwyczajowego *common law*⁹⁴⁸. Historycznie w Wielkiej Brytanii prawo administracyjne jako odrębna gałąź prawa wykształciło się późno, ale obecnie uważane jest za w pełni rozwinięte, stanowiąc część prawa konstytucyjnego w zakresie działania i kontroli egzekutywy⁹⁴⁹. Wbrew szeroko podzielanemu przekonaniu, to prawo stanowione stanowi kluczowy element brytyjskiego prawa administracyjnego, chociaż orzecznictwo (zwłaszcza wydawane w trybie tzw. *judicial review*) odgrywa w nim istotną rolę⁹⁵⁰. Pomimo podejmowania wielu inicjatyw porządkujących brytyjskie prawo administracyjne (określanych jako „mini-kodyfikacje”), w tym racjonalizacji systemu kontroli sądowej administracji publicznej, nie dokonano kodyfikacji ani administracyjnego prawa procesowego, jak i ogólnego prawa administracyjnego materialnego⁹⁵¹.

⁹⁴⁵ Por. analiza zasady legalizmu w kontekście badanego zjawiska w podrozdziale 4.2. niniejszej rozprawy.

⁹⁴⁶ Pełna oficjalna nazwa to Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej.

⁹⁴⁷ Judiciary, *The justice system and the constitution*, <https://www.judiciary.uk/about-the-judiciary/our-justice-system/jud-acc-ind/justice-sys-and-constitution/#:~:text=The%20United%20Kingdom%20has%20three,of%20Union%201707%20and%201800> (dostęp: 15.09.2024 r.).

⁹⁴⁸ M. Kasiński, 2.6.7. Samorząd w Anglii [w:] System prawa samorządu terytorialnego, t. 1: Podstawowe pojęcia i podstawy prawne funkcjonowania, red. I. Lipowicz, Warszawa 2022, SIP LEX.

⁹⁴⁹ P. Przybysz, 1.4.2. Administracja i prawo administracyjne w Anglii w XIX w. [w:] Instytucje prawa administracyjnego, Warszawa 2020, SIP LEX.

⁹⁵⁰ S. Nason, *Codification of Administrative Law in the United Kingdom* [in:] *Codification of Administrative Law: A Comparative Study on the Sources of Administrative Law*, ed by F. Uhlmann, London 2023, s. 297.

⁹⁵¹ Por. S. Nason, *Codification of Administrative Law in the United Kingdom* [in:] *Codification of Administrative Law: A Comparative Study on the Sources of Administrative Law*, ed by F. Uhlmann, London 2023, s. 305-322. Por. także M. Sikora, *Relacje Między Prawem Administracyjnym a Konstytucyjnym – Perspektywa angielska* [in:] *Comparative perspectives for public administration and administrative law*, red. D. Cendrowicz, A. Chrisidu-Budnik, Wrocław 2018,

http://www.repozytorium.uni.wroc.pl/Content/92950/PDF/03_01_M_Sikora_Administrative_Law_and_Constitutional_Matrix-English_Perspective.pdf (dostęp: 7.09.2024 r.).

Wielka Brytania nie jest państwem członkowskim UE od 2020 r.⁹⁵² Komisja wydała jednak decyzję stwierdzającą odpowiedni poziom ochrony danych osobowych w Wielkiej Brytanii („decyzję o adekwatności”) w 2021 r., co umożliwia transfer danych z UE bezpośrednio na podstawie art. 45 ust. 1 RODO⁹⁵³. Brytyjskie akty prawne w obszarze przetwarzania danych osobowych w swoich założeniach i modelu wciąż pozostają zbliżone do regulacji unijnych⁹⁵⁴, chociaż podlegają stopniowej ewolucji⁹⁵⁵. Cechą charakterystyczną tej ewolucji jest regulacja w kierunku zmniejszenia (liberalizacji) ochrony przetwarzania danych osobowych względem modelu unijnego⁹⁵⁶. Wielka Brytania pozostaje sygnatariuszem Konwencji 108 i Konwencji 108+⁹⁵⁷. W związku z wystąpieniem z UE w porządku prawnym Wielkiej Brytanii zasadniczo pozostawiono – m.in. przez przyjęcie aktu prawnego *„The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019”*⁹⁵⁸ – tak w zakresie materialnym, jak i procesowym przepisy RODO jako obowiązujące. To unormowanie w języku prawniczym określane jest jako „UK GDPR” (czyli „RODO w wersji brytyjskiej”)⁹⁵⁹. Oddaje to aktualny stan zasadniczego podobieństwa unormowania przetwarzania danych osobowych w Wielkiej Brytanii do unijnego RODO. Brytyjską regulację

⁹⁵² Government of the Netherlands, *What is Brexit?*, <https://www.government.nl/topics/european-union/question-and-answer/what-is-brexit> (dostęp: 15.09.2024 r.).

⁹⁵³ UODO, Brexit, <https://uodo.gov.pl/pl/535/2509#:~:text=Możliwość%20swobodnego%20przekazywania%20danych%20do,prze pisami%20o%20ochronie%20danych%20osobowych.&text=Obie%20decyzje%20weszły%20w%20życie,czas%20określony%20wynoszący%20cztery%20lata> (dostęp: 15.09.2024 r.).

⁹⁵⁴ K. McCullagh, *Post-Brexit UK Data Protection: Maintaining Alignment with or Diverging from the GDPR?* [in:] *Data Protection and Digital Sovereignty Post-Brexit*, ed. by E. Celeste, R. Costello, E. Harbinja et al., Oxford 2023, <http://dx.doi.org/10.5040/9781509966516.ch-002> (dostęp: 13.02.2024 r.), s. 33.

⁹⁵⁵ A. Harcourt, *Data Protection and Privacy Post-Brexit* [in:] eadem, *Brexit and the Digital Single Market*, Oxford 2023; <https://doi.org/10.1093/oso/9780192899378.003.0010>, (dostęp: 12.02.2024 r.), s. 190-196. Por. także E. Harbinja, *Regulatory Divergence: The Effects of UK Technology Law Reforms on Data Protection and International Data Transfers* [in:] *Data Protection and Digital Sovereignty Post-Brexit*, ed. by E. Celeste, R. Costello, E. Harbinja et al., Oxford 2023, <http://dx.doi.org/10.5040/9781509966516.ch-008> (dostęp: 13.02.2024 r.).

⁹⁵⁶ A. Harcourt, *Data Protection and Privacy Post-Brexit* [in:] eadem, *Brexit and the Digital Single Market*, Oxford 2023; <https://doi.org/10.1093/oso/9780192899378.003.0010>, (dostęp: 12.02.2024 r.), s. 190-196. Por. także K. McCullagh, *Post-Brexit UK Data Protection: Maintaining Alignment with or Diverging from the GDPR?* [in:] *Data Protection and Digital Sovereignty Post-Brexit*, ed. by E. Celeste, R. Costello, E. Harbinja et al., Oxford 2023, <http://dx.doi.org/10.5040/9781509966516.ch-002> (dostęp: 13.02.2024 r.), s. 14-16.

⁹⁵⁷ Council of Europe, *United Kingdom*, <https://www.coe.int/en/web/data-protection/united-kingdom> (dostęp: 15.09.2024 r.).

⁹⁵⁸ *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.* UK Statutory Instruments 2019 No. 419. Ustanowione 28 lutego 2019. <https://www.legislation.gov.uk/uksi/2019/419/contents> (dostęp: 15.09.2024 r.).

⁹⁵⁹ Termin ten używany jest w dokumentach urzędowych, np. „Wielka Brytania. Explanatory Memorandum to The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. UK Statutory Instruments 2019 No. 419.”, https://www.legislation.gov.uk/uksi/2019/419/pdfs/uksiem_20190419_en.pdf (dostęp: 15.09.2024 r.).

ochrony danych osobowych dopełnia akt prawny „*Data Protection Act*”.⁹⁶⁰ Niezależnym organem ochrony danych osobowych jest Information Commissioner⁹⁶¹, który działa przy pomocy urzędu Information Commissioner’s Office (ICO)⁹⁶². Jak wskazano, w zasadniczych rozwiązaniach regulacja ochrony danych osobowych w Wielkiej Brytanii jest zatem zbliżona do RODO⁹⁶³. Brytyjskie akty prawne normujące przetwarzanie danych osobowych nie są jednak przedmiotem szczegółowego badania w niniejszym podrozdziale. Analizie poddano jedynie rozwiązania przyjęte w Wielkiej Brytanii w celu zredukowania negatywnych skutków badanego w tej pracy zjawiska krzyżowania się kompetencji.

Digital Regulation Cooperation Forum (Forum Współpracy Regulacji Cyfrowych; DRCF), podobnie jak holenderska SDT, jest specyficznym podmiotem, który został utworzony w 2020 r., a udział w jego pracach ma charakter dobrowolny. W jego skład wchodzi Urząd Komisarza ds. Informacji (*Information Commissioner’s Office*), Urząd ds. Konkurencji i Rynków (*Competition and Markets Authority*; CMA), Urząd do spraw Komunikacji (*the Office of Communications*; Ofcom), który jest organem regulacyjnym i organem ds. konkurencji dla sektora łączności (w tym telewizja i radio, telefonia komórkowej i usługi pocztowe⁹⁶⁴) oraz Urząd Nadzoru Finansowego (*Financial Conduct Authority*; FCA)⁹⁶⁵. Zgodnie z dokumentem normującym działalność DCRF „*DRCF Terms of Reference*”⁹⁶⁶, członkostwo w tym podmiocie ma charakter otwarty i członkami mogą zostać także inne „niezależne organy administracji publicznej wyposażone w ustawowe uprawnienia do regulowania usług cyfrowych (*regulating digital services*), o ile mają one znaczący związek (*significant intersection*) z organami będącymi członkami DRCF”. Działalność DCRF nakierowana jest na realizację sześciu celów, m.in. współpracę w opracowaniu spójnej polityki regulacyjnej; wymianę wiedzy i informacji o podejmowanych działaniach w tym obszarze regulacji; wspólne przewidywanie zmian i ryzyk z nimi związanych; promowanie innowacji;

⁹⁶⁰ UK legislation, *Data Protection Act 2018*, <https://www.legislation.gov.uk/ukpga/2018/12/contents> (dostęp: 15.09.2024 r.).

⁹⁶¹ Part 5 of the *Data Protection Act 2018*, <https://www.legislation.gov.uk/ukpga/2018/12/contents> (dostęp: 15.09.2024 r.).

⁹⁶² ICO, *Who we are*, <https://ico.org.uk/about-the-ico/who-we-are/> (dostęp: 15.09.2024 r.).

⁹⁶³ A. Harcourt, *Data Protection and Privacy Post-Brexit* [in:] eadem, *Brexit and the Digital Single Market*, Oxford 2023; <https://doi.org/10.1093/oso/9780192899378.003.0010>, (dostęp: 12.02.2024 r.), s. 190.

⁹⁶⁴ DCRF, *About the DCRF*, <https://www.drcf.org.uk/about-us> (dostęp: 15.09.2024 r.).

⁹⁶⁵ ICO, *Digital Regulation Cooperation Forum*, <https://ico.org.uk/about-the-ico/what-we-do/digital-regulation-cooperation-forum/> (dostęp: 15.09.2024 r.).

⁹⁶⁶ DCRF, *DRCF Terms of Reference*, https://www.drcf.org.uk/_data/assets/pdf_file/0030/258573/DRCF-Terms-of-Reference.pdf (dostęp: 15.09.2024 r.).

pogłębiona międzynarodowa współpraca ⁹⁶⁷ . DCFR jest zatem podmiotem o funkcji koordynacyjnej. Organy będące członkami DCFR realizują w ramach tego podmiotu szereg inicjatyw, m.in. pilotażową usługę informacyjnego punktu wsparcia dla podmiotów chcących zapewnić zgodność wdrażanych i projektowanych rozwiązań sztucznej inteligencji z prawem⁹⁶⁸.

W literaturze wskazuje się na problemy związane z efektywnym funkcjonowaniem DRCF, m.in. na fakt, że jest to podmiot niepowołany ustawą o dobrowolnym członkowstwie bez formalnych instrumentów współpracy; ograniczoną liczbę organów wchodzących w skład tego podmiotu; brak niezależności i kompetencji władczych, który wynika z nieformalnego charakteru DRCF⁹⁶⁹. Te same zastrzeżenia znajdują zastosowanie do holenderskiej SDT. W tym kontekście brytyjska Izba Lordów w raporcie z 2021 r. wskazywała na problem braku wystarczającej współpracy między organami administracji publicznej w obszarze „regulacji cyfrowej” i ryzyko fragmentacji oraz rozdrobienia polityki regulacyjnej w tym obszarze, postulując sformalizowanie i rozszerzenie działalności DRCF, co jednak nie spotkało się z przychylnością brytyjskiego rządu i nie zostało zrealizowane⁹⁷⁰.

Zarówno holenderski SDT, jak i brytyjski DRCF wykazują liczne podobieństwa. Oba zostały ustanowione jako pochodna „oddolnej inicjatywy” organów administracji publicznej i nie mają podstawy w prawie stanowionej. Jest to wyrazem przekonania organów w obu tych jurysdykcjach o krzyżowaniu się ich kompetencji w obszarze przetwarzania danych osobowych i potrzebie wprowadzenia rozwiązań dla zwiększenia efektywności podejmowanych przez nie działań. Stąd też oba te podmioty pełnią funkcję koordynacyjną, która polega zasadniczo na synchronizacji polityki regulacyjnej, działań podejmowanych przez te organy i wymianie informacji bez modyfikacji kompetencji tych organów. Podmioty te mają ograniczenia, które wynikają przede wszystkim z ich nieformalnej struktury. Obie te inicjatywy należy ocenić pozytywnie, ponieważ celem ich jest zmniejszenie niepewności i zwiększenie skuteczności stosowania aktów prawnych. Należy spodziewać się, że w najbliższych latach

⁹⁶⁷ DCFR, *DCRF Terms of Reference*, https://www.drcf.org.uk/_data/assets/pdf_file/0030/258573/DCRF-Terms-of-Reference.pdf (dostęp: 15.09.2024 r.).

⁹⁶⁸ DCFR, *DCRF to pilot new advisory service as part of Government's plans for AI*, <https://www.drcf.org.uk/news-and-events/news/drcf-to-pilot-new-advisory-service-as-part-of-governments-plans-for-ai> (dostęp: 15.09.2024 r.).

⁹⁶⁹ A. D. Vanberg, *Coordinating digital regulation in the UK: is the digital regulation cooperation forum (DRCF) up to the task?*, *Int. Rev. Law Comput. Technol.* 2023, Vol. 37, Iss. 2, <https://doi.org/10.1080/13600869.2023.2192566> (dostęp: 20.09.2024 r.), s. 134-137.

⁹⁷⁰ House of Lords Library, N. Newson, *Digital regulation*, <https://lordslibrary.parliament.uk/digital-regulation/#heading-4> (dostęp: 15.09.2024 r.).

w innych jurysdykcjach powstaną podobne podmioty, których działalność z czasem zostanie sformalizowana i ustrukturyzowana⁹⁷¹.

4.7. PODSUMOWANIE

W niniejszym rozdziale sformułowano definicję zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych i zaproponowano typologię tego zjawiska. Zgodnie z tą definicją, krzyżowanie się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych to sytuacja prawna, w której co najmniej dwóm organom przyznane zostały kompetencje w tej samej sprawie albo w odniesieniu do tego samego zagadnienia w taki sposób, że może prowadzić to do rozstrzygnięcia tej samej sprawy lub tego samego zagadnienia odmiennie. Zjawisko to jest wielowymiarowe i wpisane w podstawowe zasady prawa publicznego, co zbadano w kontekście pojęcia zasady legalizmu, zakazu domniemywania kompetencji i pojęcia układów kompetencyjnych. Następnie, charakteryzując przykłady tego zjawiska, wyróżniono sześć typów tego zjawiska według trzech kryteriów: typu kompetencji (właściwe i niewłaściwe), intencji prawodawcy (zamierzone i niezamierzone) i ujęcia, w jakim zjawisko to ujawnia się (horyzontalne i wertykalne).

W kolejnym podrozdziale wykazano, że brak jest skutecznych instrumentów prawnych do rozwiązania negatywnych skutków, które wynikają z tego zjawiska. Chociaż prawodawca unijny (a następnie krajowy) dostrzegł ryzyko występowania tego zjawiska, to instrumenty, które zostały ustanowione, aby przeciwdziałać jego negatywnym konsekwencjom, okazały się niewystarczające. W aktualnym stanie prawnym zjawisko to wywołuje zatem negatywne skutki dla administracji publicznej, podmiotów nadzorowanych i podmiotów danych oraz dla gospodarki, które nie mogą zostać skutecznie zmitygowane. Skutki te to przede wszystkim zwiększenie nieskuteczności aktów prawnych prawa administracyjnego w tym obszarze, pogłębiona niepewność prawna po stronie podmiotów administrujących, podmiotów nadzorowanych i podmiotów danych oraz zagrożenie dla zasady *ne bis in idem* w prawie administracyjnym, a nadto zwiększone koszty ekonomiczne i organizacyjne przestrzegania prawa przez podmioty nadzorowane, co stanowi z kolei utrudnienie dla wejścia nowych podmiotów gospodarczych na rynek unijny i krajowy oraz rozwoju działających już podmiotów.

⁹⁷¹ Por. A. De Streel, G. Monti, *Improving Institutional Design to Better Supervise Digital Platforms*, CERRE, Bruxelles 2022, <https://pure.unamur.be/ws/portalfiles/portal/62618173/8834.pdf> (dostęp: 15.09.2024 r.), s. 41.

Chociaż pozytywne skutki analizowanego zjawiska nie są przedmiotem tej rozprawy, to wskazać należy, że zwiększenie liczby podmiotów administrujących w tym obszarze, które stosują prawo w odmiennych celach⁹⁷², prowadzi do zwiększonej aktywności administracji publicznej w tym obszarze, co zasadniczo winno prowadzić do realizacji odmiennych, ale komplementarnych wartości, służąc interesowi publicznemu⁹⁷³. Dla osiągnięcia tego efektu niezbędne jest jednak wprowadzenie efektywnych instrumentów do zredukowania negatywnych skutków tego zjawiska, w tym instrumentów współpracy między podmiotami administrującym. W przeciwnym wypadku, zjawisko to, wywołując ten pozytywny skutek, doprowadzi także do pogłębionej niepewności prawnej, co obniży skuteczność stosowania aktów prawnych w tym obszarze i zwiększy negatywne skutki pozaprawne (gospodarcze). Stąd też przed prawodawcą stoi wyzwanie, aby – zachowując podstawy modelu regulacji w obszarze przetwarzania danych osobowych – zmniejszyć ryzyka, uwalniając pozytywne efekty związane z tym zjawiskiem (w kolejnym rozdziale rozprawy sformułowano postulaty *de lege ferenda*).

Zjawisko krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych występuje także w innych jurysdykcjach unijnych prawa kontynentalnego (w Królestwie Niderlandów) i jurysdykcjach nie-unijnych prawa *common law* (w Wielkiej Brytanii). Te dwa państwa wybrane zostały jako przykłady do prawnoporównawczej analizy, ponieważ w obu tych państwach wprowadzono nowatorskie rozwiązania koordynujące działania podmiotów administrujących w obszarze przetwarzania danych osobowych. Ich analiza ma wartość poznawczą przede wszystkim z perspektywy rozwiązań, które mogłyby zostać zastosowane w innych państwach (członkowskich) w celu zmitygowania negatywnych skutków tego zjawiska.

⁹⁷² Por. podrozdział 5.6. rozprawy.

⁹⁷³ T. S. Aagaard, *Regulatory Overlap, Overlapping Legal Fields, and Statutory Discontinuities*, „Virginia Environmental Law Journal” 2011, Vol. 29, No. 3, <https://ssrn.com/abstract=1886573> (dostęp: 20.09.2024 r.).

5. ROZDZIAŁ 5 – PRZYCZYNY KRZYŻOWANIA SIĘ KOMPETENCJI ORGANÓW ADMINISTRACJI PUBLICZNEJ W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH I POSTULATY *DE LEGE FERENDA*

5.1. WSTĘP

Przedmiotem tego rozdziału jest zbadanie przyczyn występowania zjawiska krzyżowania się kompetencji organów administracji publicznej stosujących akty prawne w obszarze przetwarzania danych osobowych. Analiza doprowadziła do wyodrębnienia pięciu przyczyn. Przyczyny te są złożone i pozostają ze sobą powiązane w tym sensie, że wzajemnie się umacniają. Wynikają zarówno z trudności sformułowania przez prawodawcę adekwatnej odpowiedzi na socjo-techniczne zmiany spowodowane transformacją cyfrową, procesem europeizacji prawa administracyjnego i ograniczeń konstytucyjnych prawodawcy unijnego, jak i z rozbieżnych celów, jakie mają zostać zrealizowane organy ustanowione przez akty prawne w obszarze przetwarzania danych osobowych. Każda z przyczyn zostanie przeanalizowana w kolejnych podrozdziałach.

Pierwszą przyczyną jest nieadekwatność odpowiedzi prawodawcy unijnego i krajowego na socjo-techniczne zmiany spowodowane transformacją cyfrową skutkująca rozłączeniem regulacyjnym (*regulatory disconnect*). Kolejną przyczyną to wybór techniki legislacyjnej przez prawodawcę, aby obszar ten uregulować za pomocą zasad (*principles*), terminów nieostrych i metody opartej na ryzyku w celu zapewnienia neutralności technologicznej oraz możliwości ich horyzontalnego stosowania. Doprowadziło to do zwiększenia roli celowościowej i funkcjonalnej metody wykładni operatywnej przez organy administracji publicznej. Inną przyczyną tego zjawiska jest niejasność taksonomiczna w odniesieniu do prawa ochrony danych osobowych. Ta niejasność taksonomiczna powiązana jest z tym, że kluczowe akty prawne w obszarze przetwarzania danych osobowych przyjęte zostały przez prawodawcę unijnego, podczas gdy stosowane są (w większości) na poziomie krajowym przez organy administracji publicznej ustanowione przez krajowego prawodawcę na podstawie kompetencji bezpośrednio w aktach prawa unijnego. Stąd też zjawisko krzyżowania się kompetencji wpisane jest w proces europeizacji prawa administracyjnego. Prawodawca unijny, pomimo kształtowania prawa materialnego w tym obszarze, ograniczony jest w kształtowaniu prawa proceduralnego z powodu autonomii instytucjonalnej i proceduralnej państw członkowskich. W konsekwencji, ogranicza to prawodawcę unijnego w możliwości wprowadzenia efektywnych instrumentów, które mogłyby negatywne skutki tego zjawiska zredukować.

Jako ostatnią z przyczyn tego zjawiska zidentyfikowano zjawisko balansowania realizacji celów wyznaczonych poszczególnym organom w obszarze przetwarzania danych osobowych. Nie wszystkie bowiem akty prawne w tym obszarze przyjęte zostały w przeważającym celu ochrony danych osobowych, lecz także w innych przeważających celach (ochrona danych osobowych jest wówczas komplementarnym, dodatkowym celem), np. poprawy konkurencyjności na rynkach cyfrowych (np. DMA), czy zapewnienie cyberbezpieczeństwa (np. Dyrektywa NIS 2). Cele wyznaczone organom ochrony administracji wpływają na sposób wykonywania ich kompetencji. Pełna realizacja poszczególnych celów może prowadzić do napięć między tymi organami w określonych układach kompetencyjnych.

W perspektywie tak scharakteryzowanych przyczyn zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych, w odniesieniu do przedstawionego problemu badawczego sformułowano cztery postulaty *de lege ferenda*, które omówione zostały w drugiej części piątego rozdziału. Są to: 1) Wyodrębnienie prawa danych jako odrębnej kompleksowej gałęzi prawa; 2) Centralizacja struktury stosowania RODO wobec największych podmiotów nadzorowanych i ustanowienie organów ochrony danych jako organów właściwych dla stosowania aktów prawnych w obszarze przetwarzania danych osobowych; 3) Wprowadzenie efektywnych instrumentów współpracy między podmiotami administrującymi stosującymi akty prawne w obszarze przetwarzania danych osobowych; 4) Wprowadzenie rozwiązania typu klauzula „safe harbour” dla podmiotów nadzorowanych.

5.2. PRZYCZYNA NR 1: ROZŁĄCZENIE REGULACYJNE SPOWODOWANE TRANSFORMACJĄ CYFROWĄ

Ostatnią rewolucyjną zmianą spowodowaną rozwojem technicznym, jakiej doświadczyła ludzkość, jest trwająca co najmniej od początku lat 90. ubiegłego wieku transformacja cyfrowa⁹⁷⁴ rozumiana jako proces zmian technicznych, ekonomicznych i społecznych o charakterze globalnym spowodowanych przejściem od zapisu i przetwarzania danych w postaci analogowej do postaci cyfrowej, ich automatycznym przetwarzaniem⁹⁷⁵ oraz

⁹⁷⁴ Proces ten rozumiany jest niejednoznacznie. Por. *Transformacja cyfrowa*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021.

⁹⁷⁵ *Transformacja cyfrowa*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 444.

upowszechnieniem systemu informatycznego World Wide Web (WWW)⁹⁷⁶. Szybkość tych przemian jest unikalna. Te przemiany, redukujące „bariery czasowe i przestrzenne komunikacji oraz powodujące rozwój struktur sieciowych”⁹⁷⁷, mają charakter powszechny, to znaczy dotyczą wszystkich obszarów życia. Prowadzi to do przekształcenia dotychczasowych modeli gospodarczych, systemów społecznych i politycznych, wartości i rynku pracy, w tym sposobu jej wykonywania⁹⁷⁸. Konsekwencją jest przebudowa funkcjonowania społeczeństw, prowadząca do integracji tego funkcjonowania z systemami teleinformatycznymi⁹⁷⁹. W doktrynie wyróżnia się skutki transformacji cyfrowej szczególnie istotne dla prawa, m.in.: konieczność balansowania prawa do informacji z ochroną danych osobowych, w tym z uwagi na użycie „big data”; osłabienie skuteczności egzekwowania tradycyjnych instrumentów prawnych prawa publicznego; zwiększoną dostępność do usług i włączenie społeczne spowodowane ograniczeniem barier czasu i przestrzeni; połączenie tego, co wirtualne, z tym, co realne, przez upowszechnienie Internetu Rzeczy („Internet of Things”); rozwój i upowszechnienie sztucznej inteligencji oraz nowych form rozprzestrzeniania się dezinformacji⁹⁸⁰.

Skutki tego wszechogarniającego procesu wymagały i wymagają zatem odrębnego unormowania, ponieważ regulacje, które były skuteczne w przestrzeni analogowej, tracą tę skuteczność w przestrzeni cyfrowej z uwagi na jej dystynktywne cechy, w tym brak fizycznej obecności kilku osób w jednym miejscu), a jednocześnie identyfikowane są ryzyka, które do tej pory były nieznane lub nieznaczące; przykładowo, ochrona dzieci przed dostępem do pornografii jest w „cyberprzestrzeni” iluzoryczna z uwagi na trudność w weryfikacji wieku osoby, która chciałaby uzyskać dostęp do pornografii⁹⁸¹. Potrzeba ta wynika z konieczności

⁹⁷⁶ A. Bounfour, 2.3 *Digital Transformation* [in:] *Digital Futures, Digital Transformation: From Lean Production to Acceluction*, Cham 2016, s. 20-23. Por. także G. Vial, *Understanding digital transformation: A review and a research agenda* [in:] *Managing digital transformation*, ed. by A. Hinterhuber, T. Vescovi, F. Checchinato, Abingdon, New York 2021, s. 13-66; J. Supernat, 12.6. *Transformacja cyfrowa* [w:] *System prawa samorządu terytorialnego*, t. 3: *Samodzielność samorządu terytorialnego – granice i perspektywy*, red. I. Lipowicz, Warszawa 2023.

⁹⁷⁷ *Transformacja cyfrowa*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 444.

⁹⁷⁸ M. Minčičová, *Digital Skills in the Workplace and Training of Jobseekers and Employees*, „Technium Social Sciences Journal” 2020, Vol. 12, s. 86.

⁹⁷⁹ D. Trescakova, *Digital Transformation of Business Entities under the Current Conditions - Reality or Utopia?*, „EU and Comparative Law Issues and Challenges Series” 2020, Vol. 4, s. 798-814.

⁹⁸⁰ G. Szpor, 1.4. Explanations of a term „digital transformation” in the literature [w] *Instruments of Public Law: Digital Transformation During the Pandemic*, ed. by I. Lipowicz, G. Szpor, A. Syrt, London 2022.

⁹⁸¹ L. Lessig, *The Law of the Horse: What CyberLaw Might Teach*, „Harvard Law Review” 1999, Vol. 113, No. 2, s. 503-505.

ochrony różnych dóbr⁹⁸². Celem tej ochrony nie jest objęta tylko prywatność i dane osobowe, ale także, przykładowo, bezpieczeństwo systemów informatycznych (cyberbezpieczeństwo), stabilność i przejrzystość sektora finansowego (sektorowe regulacje sektora finansowego), własność intelektualna, prawidłowe funkcjonowanie rynków (prawo konkurencji). Kluczowe dla tej rozprawy jest jednak, że w istotę transformacji cyfrowej wpisany jest właśnie radykalny wzrost liczby automatycznie przetwarzanych danych⁹⁸³, w tym danych osobowych⁹⁸⁴. Przykładowo, w 2016 r. ustalono, że 90% danych na świecie zostało wytworzonych w ciągu dwóch poprzedzających lat⁹⁸⁵. Dane osobowe nie stanowią tylko informacji będących przedmiotem ochrony praw podstawowych, które są wolne od ekonomicznego uwikłania, ale także tworzą nową klasę aktywów niematerialnych, do których dostęp decyduje o efektywności i zyskowności podmiotów operujących w gospodarce cyfrowej⁹⁸⁶.

Pomimo tego podwójnego charakteru danych osobowych, europejska regulacja ich ochrony wywodzi się z tradycji prawno-człowieczej⁹⁸⁷, a prawo do prywatności i prawo do ochrony danych osobowych stanowią prawa podstawowe w pierwotnym prawie UE. Cele RODO, jak wskazano w podrozdziale 2.2. niniejszej rozprawy, są szersze niż ochrona osób fizycznych w związku z przetwarzaniem tych danych i obejmują także swobodny przepływ danych osobowych (por. art. 1 ust. 3 RODO), które winny zostać pogodzone tak, aby „przetwarzanie danych osobowych [zorganizowane było tak], aby służyło ludzkości” (motyw 4 RODO). Choć historia aktów prawnych w państwach europejskich nakierowanych na ochronę danych osobowych sięga lat 70. XX wieku⁹⁸⁸, a zatem wyprzedza o co najmniej dwie dekady proces transformacji cyfrowej, to można argumentować, że wzmocniona ochrona normatywna była uzasadniona z uwagi na zwiększenie ilości przetwarzanych danych osobowych w sposób automatyczny (czyli zasadniczo najczęściej z wykorzystaniem systemów

⁹⁸² Por. D. Gruszecka, *Pojęcie dobra prawnego w prawie karnym*, „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie” 2008, s. 135-155.

⁹⁸³ W tym kontekście rozumianych jako „odwzorowanie stanu właściwości obiektów ze względu na potrzeby zapamiętywania określonych faktów, zdarzeń, miar, ocen itp.”; za: Dane, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 97.

⁹⁸⁴ Pojęcie danych osobowych zbadano w podrozdziale 2.3. rozprawy.

⁹⁸⁵ European Parliamentary Research Service, M. Szczepański, *Is Data the New Oil? Competition Issues in the Digital Economy*, European Parliamentary Research Service 2020, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf) (dostęp: 7.09.2024 r.), s. 4.

⁹⁸⁶ Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 15.09.2024 r.), s. 9.

⁹⁸⁷ Por. podrozdział 2.2. niniejszej rozprawy.

⁹⁸⁸ Por. podrozdział 3.5.1. tej rozprawy.

informatycznych)⁹⁸⁹. Świadczy o tym Konwencja 108 (1981 r.) „o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych” i motyw 4 do Dyrektywy ODO (1995 r.), zgodnie z którym: „[c]oraz częściej we Wspólnocie korzysta się z przetwarzania danych osobowych w różnych sferach życia gospodarczego i społecznego; postęp w dziedzinie technologii informatycznych sprawia, że przetwarzanie i wymiana takich danych stają się coraz łatwiejsze”. Ryzyka dla ochrony danych osobowych (praw i wolności osób fizycznych w związku z przetwarzaniem) związane są zatem zasadniczo z automatycznym przetwarzaniem znacznych ilości danych osobowych (w postaci cyfrowej), co jest z kolei konsekwencją zwiększenia znaczenia danych osobowych na skutek transformacji cyfrowej.

W literaturze dyskutowane jest, czy model unijnej regulacji ochrony danych osobowych ukształtowany w swojej podstawie co najmniej pół wieku temu jest optymalny dla skutecznego zredukowania ryzyk dla praw i wolności osób fizycznych w związku ze zmianami stanowiącymi transformację cyfrową, czy też wymaga rewizji⁹⁹⁰. Kontekstem dla tej dyskusji jest szerokie pojmowanie danych osobowych, które czyni z aktów prawnych nakierowanych na ochronę danych osobowych (przede wszystkim RODO) „prawo wszystkiego”, tracące efektywność z uwagi na swoją ten szeroki zakres przedmiotowy, podmiotowy i terytorialny⁹⁹¹. To zjawisko może być pojmowane jako badane w literaturze anglojęzycznej „rozłączenie regulacyjne” (*regulatory disconnection*). Rozumiane jest ono jako sytuacja, w której istnieje luka (rozbieżność) między regulacją a jej celem spowodowana rozwojem techniki, który jest bardziej dynamiczny lub też inny niż pierwotnie zakładano⁹⁹²; stawiana jest teza, że normowanie zmian wywołanych rozwojem techniki z natury zagrożone jest ryzykiem rozłączenia regulacyjnego z uwagi na odmienny ich charakter – dynamiczny charakter rozwoju

⁹⁸⁹ D. Erdos, The Development of European Data Protection Law and Regulation [in:] idem, *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?*, Oxford 2019, s. 36.

⁹⁹⁰ Por. przykładowo, N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, Law Innov. Technol. 2018, Vol. 10, No. 1 <https://doi.org/10.1080/17579961.2018.1452176> (dostęp: 20.09.2024 r.), s. 40-81. O. Lynskey, *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.). D. J. Solove *Data is what data does: Regulating based on harm, and risk instead of sensitive data*, GWU Legal Studies Research Paper 2023, No. 2023-22. R. Mühlhoff, *Predictive privacy: Collective data protection in the context of AI and Big Data*, „Big Data & Society” 2023, Vol. 10, No. 1, s. 1-14.

⁹⁹¹ Por. podrozdział 5.5. tej rozprawy i analizowana tam literatura.

⁹⁹² A. Butenko, *Sharing Energy: Dealing with Regulatory Disconnect in Dutch Energy Law*, 2016, <https://ssrn.com/abstract=2847590> (dostęp: 20.09.2024 r.), s. 9 i przywołana tam literatura. Por. także R. Brownsword, *The Challenge of Regulatory Connection, Rights, Regulation, and the Technological Revolution*, Oxford 2008, <https://doi.org/10.1093/acprof:oso/9780199276806.003.0006>, (dostęp: 7.02.2024 r.), s. 162-170, gdzie wyróżnione różne typy *regulatory disconnection*: *descriptive and normative disconnection*; *productive and unproductive disconnection*; *intelligent and unintelligent purposive re-connection* (opisowe i normatywne rozłączenie; produktywne i nieproduktywne rozłączenie; inteligentne i nieinteligentne celowe ponowne połączenie).

technicznego i statyczny charakter prawa, co powoduje, że prawo jest z natury reaktywne względem tego rozwoju⁹⁹³. Może to prowadzić do „porażki regulacyjnej” (*regulatory failure*) pojmowanej jako nieosiągnięcie celów regulacji, jakie przed nią postawiono lub też osiągnięcie tych celów w taki sposób, że wywołuje to niepożądane i nieprzewidziane skutki⁹⁹⁴. To, czy unijne akty prawne nakierowane na ochronę danych osobowych (przede wszystkim RODO) dotknięte są „rozłączeniem regulacyjnym”, jest dyskusyjne⁹⁹⁵. Z perspektywy ponad pięciu lat obowiązywania RODO (maj 2018 r.) refleksję budzić winno, że zgodnie z raportem noyb. European Center for Digital Rights (z 2024 r.) aż 74.4% z ankietowanych specjalistów ochrony danych osobowych zatrudnionych w podmiotach na terytorium UE (w tym jako inspektorzy ochrony danych w tych podmiotach) uważa, że organy ochrony danych osobowych zidentyfikowałyby istotne naruszenia RODO w przypadku kontroli w tych podmiotach, a 46% jest zdania, że opinie wydawane przez EROD nie mają wpływu („*are not influential*”) na ochronę danych osobowych w tych podmiotach⁹⁹⁶. Autorzy raportu jako *remedium* postulują zwiększenie intensywności stosowania RODO przez organy ochrony danych osobowych, w tym nakładanie wysokich administracyjnych kar pieniężnych, które będą publicznie dostępne⁹⁹⁷. Nie rozstrzygając tej kwestii w tej rozprawie, rozważyć należy poddać czy faktyczną przyczyną (jedną z przyczyn) nieskuteczności RODO rozumianej jako wysoki współczynnik braku zgodności praktyk podmiotów nadzorowanych z RODO jest brak efektywnego stosowania RODO, czy też przyczyny należy doszukiwać się w nieadekwatności modelu regulacji, na jakiej oparte jest RODO do rzeczywistości transformacji cyfrowej.

Istotną przyczyną zjawiska krzyżowania się kompetencji organów jest oparcie unijnego modelu ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych o pojęcie danych osobowych i ich ochrony, co znajduje aksjologiczne uzasadnienie w europejskim systemie ochrony praw człowieka. W zestawieniu z krytyką tego modelu w przywołanej literaturze można tę sytuację określić jako „rozłączenie regulacyjne” w ujęciu

⁹⁹³ R. Brownsword, *The Challenge of Regulatory Connection*, *Rights, Regulation, and the Technological Revolution*, Oxford 2008, <https://doi.org/10.1093/acprof:oso/9780199276806.003.0006>, (dostęp: 7.02.2024 r.), s. 160-161.

⁹⁹⁴ A. Butenko, *Sharing Energy: Dealing with Regulatory Disconnect in Dutch Energy Law*, 2016, <https://ssrn.com/abstract=2847590> (dostęp: 5.09.2024 r.), s. 8-9 i przywołana tam literatura.

⁹⁹⁵ Por. W. Li, Z. Li, W. Li et al., *Mapping the Empirical Evidence of the GDPR (In-) Effectiveness: A Systematic Review*, arXiv:2310.16735, 2023, <https://doi.org/10.48550/arXiv.2310.16735> (dostęp: 20.09.2024 r.).

⁹⁹⁶ noyb. European Center for Digital Rights, *GDPR: a culture of non-compliance? Numbers of evidence-based enforcement efforts*, https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance_2.pdf (dostęp: 15.09.2024 r.).

⁹⁹⁷ noyb. European Center for Digital Rights, *GDPR: a culture of non-compliance? Numbers of evidence-based enforcement efforts*, https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance_2.pdf (dostęp: 15.09.2024 r.), s. 21

scharakteryzowanym powyżej⁹⁹⁸. Wniosek ten nie oznacza, że podstawy aktualnego modelu należy ocenić negatywnie. Jak zostało wskazane, są one głęboko wpisane w europejską tradycję prawnocząłowieczą i mają aksjologiczne uzasadnienie. Powinno to być jednak przedmiotem pogłębionej dyskusji. Konsekwencją zastosowania tego modelu w transformacji cyfrowej jest to, że RODO ma zastosowanie do wszystkich aspektów rzeczywistości transformacji cyfrowej, zatem nieuniknione jest krzyżowanie się zakresu przedmiotowego i podmiotowego RODO z innymi aktami prawnymi, które częściowo (sektorowo) lub incydentalnie normują przetwarzanie danych osobowych. Konsekwentnie dochodzi do krzyżowania się kompetencji organów ochrony danych osobowych i innych podmiotów administrujących ustanowionych na podstawie wspomnianych innych aktów prawnych. To, że zjawisko krzyżowania się kompetencji przy przyjętym modelu jest nieuniknione, nie oznacza, że jego negatywne skutki nie mogą zostać zmniejszone przez dokonanie zmian bez zmiany podstaw aktualnego modelu regulacji (postulaty *de lege ferenda* sformułowano w dalszej części tego rozdziału).

W literaturze proponowano różne, w założeniu autorów, bardziej adekwatne alternatywy dla centralnego pojęcia „danych osobowych”. Przykładowo, N. Purtova proponowała, aby w miejsce „danych osobowych” centralnym pojęciem uczynić „szkody wyrządzone przez informacje” rozumiane szeroko jako „wszelkie indywidualne lub zbiorowe negatywne konsekwencje przetwarzania informacji”, co pozwoliłoby odejść od dychotomii dane osobowe/nie-osobowe i przeniosłoby uwagę z „przetwarzania danych osobowych” na unormowanie negatywnych jego skutków⁹⁹⁹. Z kolei D. Solove w podobny sposób postulował, aby centralnego pojęcia nie stanowiły dane osobowe jako takie (czy też ich przetwarzanie), lecz ryzyko i szkody związane z tym przetwarzaniem, podnosząc, że RODO w niewystarczającym stopniu uwzględnia oba te pojęcia w przyjętym modelu regulacji¹⁰⁰⁰. W jeszcze innym kierunku argumentuje Blessing Mutiro, który proponował, aby rozszerzyć przedmiot ochrony o ochronę danych zbiorowych (kolektywnych; „*collective rights to data protection*”) i wprowadzić pojęcie kolektywnych podmiotów danych rozumianych jako społeczności i grupy etniczne, którym przyznać należy ochronę prawną¹⁰⁰¹.

⁹⁹⁸ Por. podrozdział 5.5. tej rozprawy i analizowana tam literatura.

⁹⁹⁹ N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, Law Innov. Technol. 2018, Vol. 10, No. 1 <https://doi.org/10.1080/17579961.2018.1452176> (dostęp: 20.09.2024 r.), s. 79-80.

¹⁰⁰⁰ D. J. Solove *Data is what data does: Regulating based on harm, and risk instead of sensitive data*, GWU Legal Studies Research Paper 2023, No. 2023-22, s. 1128-1136.

¹⁰⁰¹ B. Mutiro, *The Future of EU Data Protection Law for Collectives: A Reverse Brussels Effect*, EDPL 2023, Vol. 9, Iss. 4, <https://doi.org/10.21552/edpl/2023/4/7> (dostęp: 20.09.2024 r.).

Powyższa dyskusja dotycząca w istocie adekwatności odpowiedzi prawodawcy na zmiany spowodowane rozwojem technicznym (w tym przypadku transformacją cyfrową) powinna być rozpatrywana w powiązaniu z obszarem badań naukowych nazywanych w literaturze anglojęzycznej *Science and Technology Studies* (STS)¹⁰⁰², rozumianym jako interdyscyplinarne badania obejmujące m.in., nauki prawne, socjologię, ekonomię, antropologię, historię, filozofię, których przedmiotem jest zintegrowana analiza przebiegu i skutków relacji pomiędzy rozwojem techniki i nauki a społeczeństwem¹⁰⁰³. W odniesieniu do zagadnień prawnych tak ujęty obszar badań określany bywa jako *Law, Technology and Science*¹⁰⁰⁴. Przykładowo, jest to nazwa jednego z instytutów wydziału prawa Uniwersytetu w Tilburgu w Holandii, tj. *Tilburg Institute for Law, Technology and Science* (Instytut Prawa, Technologii i Nauki w Tilburgu). Zgodnie z informacją na jego stronie internetowej, akademicy w tym instytucie prowadzą interdyscyplinarne badania w przedmiocie wpływu zmian socjo-technicznych na regulację aktywności ekonomicznej w rzeczywistości transformacji cyfrowej, aby zaproponować możliwie optymalną regulację¹⁰⁰⁵. Generalne pytania badawcze, będące przedmiotem zainteresowania badaczy-prawników w tym obszarze to m.in.: 1) Co powinno być przedmiotem regulacji? 2) Dlaczego należy regulować? 3) Kiedy należy regulować? 3) W jaki sposób należy regulować?¹⁰⁰⁶

Tak sformułowany przedmiot badań pozwala ująć unormowania stanowiące odpowiedź na transformację cyfrową w szerszej perspektywie. Nie jako unikalne i bezprecedensowe

¹⁰⁰² B. Turner, M. G. Wiber, *Legal Pluralism and Science and Technology Studies: Exploring Sources of the Legal Pluriverse*, „Science, Technology, & Human Values” 2023, Vol. 48, Iss. 3, <https://doi.org/10.1177/01622439211069659> (dostęp: 20.09.2024 r.).

¹⁰⁰³ Por. *The handbook of science and technology studies*, ed. by E. J. Hackett et al., Cambridge, MA 2008, <https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-wyatt-2007b.pdf> (dostęp: 20.09.2024 r.), s. 1-2, 13, 33. Por. także S. Sismondo, *Preface, A Preview of Science and Technology Studies* [in:] *An Introduction to Science and Technology Studies*, Malden 2011, <https://books.google.pl/books?id=TsEfNbMtSmoC&lpg=PA1&hl=pl&pg=PP1#v=onepage&q&f=false> (dostęp: 20.09.2024 r.).

¹⁰⁰⁴ Por. czasopismo naukowe „Law, Innovation and Technology” wydawane przez wydawnictwo Taylor & Francis, który bada następujące, m.in.: „technologie informacyjno-komunikacyjne, biotechnologie, nanotechnologie, neurotechnologie, robotykę i sztuczną inteligencję”, szukając odpowiedzi na pytania badawcze: „Jak prawo wpływa na nowe technologie? Jaki wpływ mają nowe technologie na prawo? Czy możliwe jest poleganie na technologii jako narzędziu regulacyjnym?” <https://www.tandfonline.com/action/journalInformation?show=aimsScope&journalCode=rlit20> (dostęp: 15.09.2024 r.).

¹⁰⁰⁵ *About TILT*, <https://www.tilburguniversity.edu/about/schools/law/departments/tilt/about> (dostęp: 15.09.2024 r.).

¹⁰⁰⁶ Lista pytań badawczych sformułowana została w oparciu o wykłady wygłoszone przez prof. Ronalda Leenesa na Uniwersytecie w Tilburgu w ramach kursu „Regulation: Ethics, Acceptance, Legitim” (i materiały z tego kursu). Idee przedstawione w tym podrozdziale i w podrozdziale 5.5. (i cytowana literatura) także zainspirowana została tymi wykładami. Z informacji uzyskanych od Prof. Ronalda Leenes’a wynika, że pracuje on nad podręcznikiem, który kompleksowo opisywał będzie te zagadnienia.

wydarzenie w historii (prawa), ale jako przykład prawodawstwa stanowiącego odpowiedź na zmiany socjo-techniczne spowodowane przez rozwój techniczny. Wartość poznawcza tego ujęcia polega na możliwości zastosowania wniosków z badań do innych zmian socjo-technicznych spowodowanych postępowaniem technicznym w przeszłości i w przyszłości, jak i ubogacenia perspektywy nauk prawnych o dorobek innych dyscyplin, co pozwala holistycznie identyfikować negatywne skutki wynikające z rozwoju techniki (które wymagają unormowania)¹⁰⁰⁷. Autor tej rozprawy stoi na stanowisku, że przyjęcie opisanej wyżej interdyscyplinarnej perspektywy badawczej jest niezbędne dla sformułowania optymalnych postulatów regulacji zmian spowodowanych transformacją cyfrową, co samo w sobie wykracza poza zakres tej rozprawy¹⁰⁰⁸. Istotne jest jednak, aby kompetencje podmiotów administrujących w obszarze przetwarzania danych osobowych, jak i zjawisko krzyżowania się kompetencji ujmować systemowo jako jeden z elementów modelu unijnej regulacji przetwarzania danych osobowych zbudowanego tak, aby realizować określone cele. Dyskusja o postulatach *de lege ferenda* w odniesieniu do kompetencji podmiotów administrujących w tym obszarze nie jest zatem możliwa bez uprzedniego pojęcia tej kwestii.

5.3. PRZYCZYNA NR 2: WYBÓR TECHNIKI PRAWODAWCZEJ SPOWODOWANY POTRZEBĄ ZAPEWNIENIA NEUTRALNOŚCI TECHNOLOGICZNEJ REGULACJI

Analizowany obszar referencyjny dotyczy, jak wskazano wyżej, unormowania przetwarzania danych osobowych, które stanowi kluczowy element ewoluującego procesu transformacji cyfrowej. Ewolują nie tylko formy życia społecznego i politycznego, ale także zmianie ulega technika, na przykład przez proliferację rozwiązań opartych na uczeniu maszynowym¹⁰⁰⁹. W konsekwencji tych ciągłych zmian wszystkie akty prawne w tym obszarze narażone są na ryzyko anachroniczności (forma „rozłączenia regulacyjnego”) rozumianej jako ich nieprzystawanie do aktualnych rozwiązań technicznych. Jakikolwiek prawodawca odpowiadający na jakąkolwiek zmianę socjo-techniczną narażony jest także z zasady na zarzut zbyt wczesnej regulacji, która ogranicza rozwój innowacji albo zbyt późnej regulacji, kiedy

¹⁰⁰⁷ Por. wnioski sformułowane w Zakończeniu tej rozprawy.

¹⁰⁰⁸ Istotną pozycją jest w szczególności: *The Oxford Handbook of Regulation*, ed. by R. Baldwin, M. Cave, M. Lodge, Oxford 2010. *Understanding Regulation: Theory, Strategy, and Practice*, ed. by R. Baldwin, M. Cave, M. Lodge, Oxford 2012, <https://doi.org/10.1093/acprof:osobl/9780199576081.003.0007> (dostęp: 10.02.2024 r.). Por. Przykładowo także artykuły w przywołanym wyżej czasopiśmie naukowym „Law, Innovation and Technology”, na przykład: L. B. Moses, *How to Think about Law, Regulation and Technology: Problems with ‘Technology’ as a Regulatory Target*, „Law, Innovation and Technology” 2013, Vol. 5, No.1, s. 1-20.

¹⁰⁰⁹ Por. podrozdział 2.6.4. rozprawy.

ryzyka zdążyły się już zmaterializować (jest to jeden z aspektów znanego w literaturze dylematu Collingridge'a¹⁰¹⁰). Odpowiednie dobranie momentu i instrumentów regulacji jest zatem w założeniu trudne¹⁰¹¹.

Prawodawca unijny zdecydował się uregulować akty prawne w analizowanym obszarze referencyjny w sposób zapewniający neutralność technologiczną, co ma zwiększyć stabilność prawa stanowionego w tym obszarze. Zgodnie z motywem 15 RODO, „aby zapobiec poważnemu ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik”. Neutralność technologiczna nakłada się na to, że akty prawne w analizowanym obszarze referencyjnym mają horyzontalne zastosowanie, zasadniczo do wszystkich sektorów gospodarki. W konsekwencji, nie tylko „nie powinny zależeć od stosowanych technik” w danym momencie rozwoju technicznego, ale także powinny być stosowalne we wszystkich sektorach gospodarki, w których zarówno sposoby, jak i ryzyka przetwarzania danych osobowych mogą znacznie różnić się od siebie.

To podejście ma zastosowanie nie tylko do RODO, ale także do pozostałych aktów prawnych w tym obszarze¹⁰¹². Zapewnienie neutralności określić należy jako jeden z ich celów. Aby ten cel osiągnąć, konieczne jest dobranie adekwatnych metod techniki prawodawczej. Technika prawodawcza definiowana jest jako „celowy, racjonalny, oparty na wiedzy sposób wykonywania czynności związanych z tworzeniem prawa”¹⁰¹³. Prawodawca unijny wybrał użycie metody regulacji opartej na ryzyku (*risk-based approach*), norm-zasad (bardziej niż norm-reguł) i terminów nieostrych. Konsekwencją tego wyboru jest zwiększenie roli celowościowej i funkcjonalnej metody wykładni operatywnej przez organy administracji publicznej. W tak ukształtowanej regulacji to na podmiotach administrujących (i sądach administracyjnych w toku sądowej kontroli administracji publicznej) spoczywa zasadniczy ciężar dekodowania znaczenia przepisów z uwagi na luz decyzyjny, jaki otrzymały na etapie stosowania prawa. Konkretyzowanie prawa przez podmioty administrującego określone jest w literaturze jako dekodowanie uprawnień osób fizycznych i obowiązków podmiotów

¹⁰¹⁰ Por. A. Genus, A. Stirling Collingridge and the dilemma of control: Towards responsible and accountable innovation, „Research policy” 2018, Vol. 47, No. 1, s. 61-69.

¹⁰¹¹ Sposoby regulacji (nazywa „strategiami regulacyjnymi”) są przedmiotem analizy w literaturze, m.in. *Regulatory Strategies* [in:] *Understanding Regulation: Theory, Strategy, and Practice*, ed. by R. Baldwin, M. Cave, M. Lodge, Oxford 2012, <https://doi.org/10.1093/acprof:osobl/9780199576081.003.0007> (dostęp: 10.02.2024 r.).

¹⁰¹² Por. B. A. Greenberg, *Rethinking Technology Neutrality*, „Minnesota Law Review” 2016, Vol. 100, No. 4, s. 1495-1562.

¹⁰¹³ G. Wierczyński [w:] Komentarz do rozporządzenia w sprawie „Zasad techniki prawodawczej” [w:] Redagowanie i ogłaszanie aktów normatywnych. Komentarz, Warszawa 2016, SIP LEX.

nadzorowanych, które ustanowione zostały w abstrakcyjnych i generalnych normach, co powoduje dopiero „wyzwolenie skutków prawnych” tych norm¹⁰¹⁴. Zestawienie tego sposobu regulacji z szerokim (i zbliżonym co do rodzaju spraw) zakresem przedmiotowym i podmiotowym aktów prawnych oraz sposobem unormowania kompetencji tych podmiotów prowadzi do konkluzji, że nie jest możliwe uprzednie przewidzenie i precyzyjne rozgraniczenie przez prawodawcę zakresu spraw objętych tymi kompetencjami. W konsekwencji nie może być zaskakujące, że kompetencje te krzyżują się w tym rozumieniu, że w procesie wykładni operatywnej dokonywanej przez podmioty administrujące dochodzą one do wniosku, że skuteczne (z perspektywy celu aktu prawnego) wykonywanie ich kompetencji obejmuje sprawy, które objęte są także kompetencją innego organu.

Do konkretyzowania prawa przez podmioty administrujące dochodzi nie tylko w sprawach prowadzących do konkretnego rozstrzygnięcia (decyzją), ale także w *soft law* (np. opinie EROD i krajowych organów ochrony danych osobowych, czy stanowiska prezentowane przez GIIF). Wpływają one na sposób ukształtowania praktyki zapewnienia zgodności działalności z prawem przez podmioty nadzorowane, które uwzględniają je w swojej działalności z uwagi na obawę nałożenia na nie administracyjnych kar pieniężnych (wpływ *soft law* można zatem scharakteryzować jako pośredni). W tym podrozdziale dokonano syntetycznej analizy zastosowania metody regulacji opartej na ryzyku (*risk-based approach*), norm-zasad, terminów nieostrych i *soft law* w kontekście wykładni prawa administracyjnego w analizowanym obszarze referencyjnym (ze szczególnym uwzględnieniem rozwiązań w RODO jako najgłębiej zbadanego aktu prawnego w tym obszarze).

Podejście oparte na ryzyku (*risk-based approach*) zastosowano w większości aktów prawnych w obszarze referencyjnym, w tym RODO (terminu „risk” [„ryzyko”] użyto 75 razy w tekście), AI Act, DSA, akty prawne regulujące cyberbezpieczeństwo i AML¹⁰¹⁵. Podejście oparte na ryzyku nie jest natomiast charakterystyczne dla unijnego i krajowego prawa konkurencji oraz DMA. W podejściu tym „ryzyko” stanowi z jednej strony „kryterium wyboru interwencji regulacyjnych”¹⁰¹⁶, co oznacza, że to podmiot administrujący decyduje – przy uwzględnieniu tego kryterium – jakimi sprawami będzie się zajmował (przyznawał priorytet), a z drugiej strony kryterium, według którego to podmioty nadzorowane zobowiązane są

¹⁰¹⁴ T. Woś, *Wstęp* [w:] *Postępowanie administracyjne*, red. T. Woś, Warszawa 2017, s. 23.

¹⁰¹⁵ Por. analizy dokonane w rozdziale 2 rozprawy.

¹⁰¹⁶ M. Pichlak, K. Gaczoł, *Refleksyjna regulacja ryzyka w ochronie danych osobowych. Podstawy teoretyczne i praktyka działalności Prezesa UODO*, Łódź 2022, s. 64.

„dookreślać” (konkretyzować) swoje obowiązki w danych stanach faktycznych¹⁰¹⁷. Określane jest w to w literaturze jako „meta-regulacja”, gdyż „przenosi” na podmiot nadzorowany obowiązki w zakresie określania standardów zachowania, które w typowym modelu spoczywają na podmiotach administrujących¹⁰¹⁸. Tak jest właśnie w przypadku RODO, w którym, przykładowo, administrator zgodnie z podstawowymi obowiązkami (art. 24 RODO) „wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać”, jednocześnie uwzględniając „charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze”¹⁰¹⁹. Termin „ryzyko” rozumiany jest niejednoznacznie¹⁰²⁰, przy czym często przyjmuje się, że ryzyko stanowi iloczyn prawdopodobieństwa wystąpienia szkody i wagi tej szkody¹⁰²¹. Jego interpretacji należy dokonywać kontekstowo z uwzględnieniem przedmiotu ryzyka. W RODO termin „ryzyka” odnosi się do „naruszenia praw i wolności osób fizycznych” (np. motywy 74-76 RODO; art. 33 ust. 1 RODO, art. 34 ust. 1 RODO, art. 35 ust. 1 RODO), którego „prawdopodobieństwo i wagę (...) należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych” na podstawie „obiektywnej oceny” (motyw 76 RODO)¹⁰²². Oznacza to zatem, że analiza ryzyka naruszenia praw lub wolności osób fizycznych przez podmioty administrujące i podmioty nadzorowane wymaga przyjęcia standardów mierzenia tego ryzyka¹⁰²³, a następnie dokonywania kontekstowego testu balansującego przy wyborze środków organizacyjnych i technicznych, które winny być lub zostały wdrożone¹⁰²⁴. W odniesieniu do RODO jako aktu prawnego nakierowanego na ochronę danych osobowych w praktyce jego przestrzegania widoczne jest napięcie między tak rozumianym podejściem na

¹⁰¹⁷ M. Pichlak, K. Gaczoł, Refleksyjna regulacja ryzyka w ochronie danych osobowych. Podstawy teoretyczne i praktyka działalności Prezesa UODO, Łódź 2022, s. 64 i przywołana tam literatura.

¹⁰¹⁸ R. Gellert, Conclusions: Back to the rights/risk-based approaches, and the future of data protection [in:] idem, The risk-based approach to data protection, Oxford 2020, s. 239.

¹⁰¹⁹ Por. M. Mostowik, Rozdział V. Instrumenty ochrony danych osobowych w Internecie rzeczy związane z podejściem opartym na ryzyku i zasadą rozliczalności [w:] idem, Ochrona danych osobowych w Internecie rzeczy w prawie UE, Warszawa 2022.

¹⁰²⁰ R. Gellert, Fundamental notions: Risk and regulation [in:] idem, The risk-based approach to data protection, Oxford 2020, s. 26-31. Por. także M. Macenaite, The “Riskification” of European Data Protection Law through a two-fold Shift, Eur. J. Risk Regul. 2017, Vol. 8, Iss. 3, <https://doi.org/10.1017/err.2017.40> (dostęp: 20.09.2024 r.).

¹⁰²¹ A. Molfetas, L. Grava, *Risk-Based Approaches to Business Regulation*, Washington, DC 2020, <https://documents1.worldbank.org/curated/en/880271603464018549/pdf/A-Note-for-Reformers.pdf> (dostęp: 20.09.2024 r.), s. 3.

¹⁰²² Por. analiza RODO w podrozdziale 2.2.1. rozprawy.

¹⁰²³ Por. Grupa Robocza, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP 248 rev.01, 4 April 2017, <https://ec.europa.eu/newsroom/article29/items/611236> (dostęp: 15.09.2024 r.), s. 5.

¹⁰²⁴ R. Gellert, Conclusions: Back to the rights/risk-based approaches, and the future of data protection [in:] idem, The risk-based approach to data protection, Oxford 2020, s. 240-241.

ryzyku a ochroną praw podstawowych (której minimalnej poziom powinien być w założeniu jednoznacznie ustalony i niemodyfikowalny przez kwantyfikator ryzyka)¹⁰²⁵.

Zasady prawa są pojęciem niejednoznacznym.¹⁰²⁶ A jednocześnie są one szczególnymi normami w systemie (w gałęziach) prawa administracyjnego, które stanowią nakazy optymalizacyjne¹⁰²⁷. Ze swej natury pozostają niedookreślone, będąc wyrazem „aksjologii wewnętrzprawnej”¹⁰²⁸. Zasady te winny być uwzględniane przy wykorzystaniu reguł systemowo-aksjologicznej w wykładni operatywnej dokonywanej przez podmioty administrujące¹⁰²⁹. RODO, będące aktem prawnym o fundamentalnym znaczeniu dla przetwarzania danych osobowych w UE, unormowane zostało właśnie w oparciu o model zasad (kompleksowej gałęzi prawa) ustanowionych w art. 5 RODO¹⁰³⁰. Obranie zasad jako techniki prawodawczej istotne jest także dla regulacji sztucznej inteligencji w UE¹⁰³¹. Dalsza analiza dotycząca zasad zastosowanych w obszarze referencyjnym prowadzona będzie na przykładzie RODO. R. Dworkin, przedstawiciel teorii prawa (prawa *common law*), wyróżnił w systemie prawnym normy-reguły (*norms-rules*) i normy-zasady (*norms-principles*) (teoria Dworkina została rozwinięta przez R. Alexy’ego w kontekście prawa kontynentalnego)¹⁰³². Istotą tych pierwszych jest jednoznaczne („zero-jedynkowe”) określenie należytego sposobu zachowania w danym stanie faktycznym (w sposób aprioryczny), podczas gdy normy-zasady winny być realizowane „stopniowalnie i sytuacyjnie” w granicach „prawnych i rzeczywistych możliwości działania”, co limitowane jest przez inne normy-zasady i normy-reguły, co oznacza, że możliwe jest jedynie aposterioryczne określenie należytego sposobu zachowania¹⁰³³. Normy-zasady w prawie administracyjnym podlegają konkretyzacji w różnych

¹⁰²⁵ R. Gellert, Conclusions: Back to the rights/risk-based approaches, and the future of data protection [in:] idem, *The risk-based approach to data protection*, Oxford 2020, s. 241.

¹⁰²⁶ T. Grzybowski, M. Sarnowiec-Cisłak, *Ważenie zasad prawa w orzecznictwie sądów administracyjnych*, ZNSA 2018, nr 6, s. 47-71, s. 48-49.

¹⁰²⁷ T. Grzybowski, M. Sarnowiec-Cisłak, *Ważenie zasad prawa w orzecznictwie sądów administracyjnych*, ZNSA 2018, nr 6, s. 47-71, s. 53.

¹⁰²⁸ L. Leszczyński, § 25 *Wykładnia systemowo-aksjologiczna*, [w:] *Wykładnia w prawie administracyjnym*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 261.

¹⁰²⁹ L. Leszczyński, § 25 *Wykładnia systemowo-aksjologiczna*, [w:] *Wykładnia w prawie administracyjnym*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 265.

¹⁰³⁰ Charakterystyki tych zasad w RODO dokonano w podrozdziale 2.2.1. rozprawy.

¹⁰³¹ Por. podrozdział 2.6.4. tej rozprawy.

¹⁰³² M. Kamiński, Normy-zasady prawa administracyjnego i ich konkretyzacja [w:] *Zasady w prawie administracyjnym. Teoria, praktyka, orzecznictwo*, red. Z. Duniewska, A. Krakala, M. Stahl, Warszawa 2018, SIP LEX.

¹⁰³³ M. Kamiński, Normy-zasady prawa administracyjnego i ich konkretyzacja [w:] *Zasady w prawie administracyjnym. Teoria, praktyka, orzecznictwo*, red. Z. Duniewska, A. Krakala, M. Stahl, Warszawa 2018, SIP LEX. Rozbudowana analiza zasad w prawie administracyjnym w przywołanej monografii; por. także Korzeniowski, Piotr. Zasady prawne ochrony środowiska. Wydawnictwo Uniwersytetu Łódzkiego, 2010., a z literatura anglojęzycznej, przykładowo J. Black, *The Rise, Fall and Fate of Principles Based Regulation*, „LSE Legal Studies Working Paper” 2010, No. 17, <http://dx.doi.org/10.2139/ssrn.1712862> (dostęp: 20.09.2024 r.); G. Laurie,

konfiguracjach z normami-regułami, przy czym najczęściej konkretyzowane są pośrednio (przez interpretację treści aktów prawnych) wraz z bezpośrednią konkretyzacją (określeniem skutków prawnych) norm-reguł z uwagi na zbieg podstaw prawnych w procesie stosowania prawa¹⁰³⁴.

Zastosowanie tych rozważań do obszaru referencyjnego prowadzi do konkluzji, że zasady ustanowione w RODO stanowią zasady prawa właściwe dla kompleksowej gałęzi prawa. Pełnią one podwójną funkcję – z jednej strony mogą stanowić samodzielną podstawę odpowiedzialności administratora (art. 5 ust. 2 RODO), z drugiej zaś strony stanowią dyrektywę interpretacyjną (odzwierciedlającą wewnętrzną aksjologię¹⁰³⁵) przy dekodowaniu (określaniu „prawnych i rzeczywistych możliwości działania”) obowiązków administratora i podmiotu przetwarzającego zarówno przez te podmioty, jak i podmioty nadzorowane. W literaturze wskazuje się także na dwie inne funkcje: wytycznych legislacyjnych (zasady mają zapewniać jednolity kierunek rozwoju prawodawstwa w tym obszarze) i systematyzującą (porządkującą normy-reguły przetwarzania danych osobowych, co uzupełnia funkcję dyrektyw interpretacyjnych)¹⁰³⁶. Z perspektywy analizowanego zjawiska krzyżowania się kompetencji wybór zastosowania zasad jako techniki prawodawczej należy interpretować razem z pozostałymi technikami, które intencjonalnie pozostawiają luz decyzyjny podmiotom administrującym i sądom administracyjnym, co z natury rzeczy uniemożliwia aprioryczne określenie zakresu kompetencji przez podmioty administrujące, czyniąc ujawnienie się zjawiska krzyżowania się kompetencji nieuniknionym.

Terminy (określenia) nieostre są intensywnie wykorzystywane przez prawodawcę w każdym z aktów prawnych w obszarze referencyjnym¹⁰³⁷. Przykładowo, scharakteryzowany wyżej termin „ryzyko” i termin „dane osobowe” analizowany w rozdziale 2. tej rozprawy

N. Sethi, *Towards Principles-Based Approaches to Governance of Health-Related Research Using Personal Data*, Eur. J. Risk Regul. 2013, Vol. 4, No. 1, s. 43-57.

¹⁰³⁴ M. Kamiński, 3. Zagadnienie konkretyzacji norm-zasad prawa administracyjnego [w:] *Zasady w prawie administracyjnym. Teoria, praktyka, orzecznictwo*, red. Z. Duniewska, A. Krakala, M. Stahl, Warszawa 2018.

¹⁰³⁵ Por. także M. Sakowska-Baryła, 5.4. Zasady prawa a wartości zabezpieczane przez prawo do ochrony danych osobowych i prawa dostępowe [w:] *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

¹⁰³⁶ P. Litwiński, P. Barta, M. Kawecki, Komentarz do art. 5 RODO, nb 1 [w:] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, red. P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, SIP Legalis.

¹⁰³⁷ Por. analizy przeprowadzone w rozdziale 2 rozprawy.

są terminami nieostrymi¹⁰³⁸. Charakterystyczne jest, że nawet wprowadzenie definicji legalnej terminów nieostrych (jak w przypadku „danych osobowych”) w tych aktach prawnych najczęściej nie usuwa niepewności prawnej, ponieważ ich *definiens* zbudowany jest z kolejnych terminów nieostrych. Stąd też wykorzystanie terminów nieostrych w unormowaniu przetwarzania danych osobowych to celowe działanie prawodawcy. Jego celem jest uelastycznienie znaczenia aktów prawnych¹⁰³⁹. K. Ajdukiewicz „nazwami nieostrymi” określa „nazwy, których znaczenie uzbraja [...] w metodę pozwalającą w zastosowaniu do pewnych tylko przedmiotów rozstrzygnąć czy można o nich tę nazwę orzec, czy też nie, ale w stosunku do innych przedmiotów nie wyznacza żadnej metody, która by na to pozwalała”¹⁰⁴⁰. Tak dokładnie jest w odniesieniu, na przykład do terminu „dane osobowe”. Uznanie pewnych informacji, jak imię i nazwisko czy numer PESEL, za dane osobowe nie budzi wątpliwości. Wątpliwości budzą natomiast te informacje, które kontekstowo powodują „identyfikowalność” osoby fizycznej, a rozstrzygnięcie, czy można o nich orzec nazwę „dane osobowe”, z konieczności dokonywane jest kazuistycznie. Terminy nieostre odróżnić należy od innych rozwiązań zwiększających elastyczność aktów prawnych prawa administracyjnego, jak na przykład klauzule generalne i wprowadzenie uznania administracyjnego¹⁰⁴¹. Elastyczność aktu prawnego przez użycie terminów nieostrych wynika z wykorzystania wieloznaczności (semantycznej nieostrości¹⁰⁴²) języka prawnego. Interpretacja terminów nieostrych nie stanowi tym samym uznania administracyjnego, ponieważ podmioty administracyjne mają obowiązek wywiedzenia (odczytania) prawidłowego znaczenia terminów nieostrych w danym stanie faktycznym. W ten właśnie sposób znaczenie terminów nieostrych konkretyzowane jest dopiero na etapie stosowania prawa przez podmioty administrujące i sądy, co daje im dyskrecjonalność, umożliwiającą interpretację adekwatną do różnorodnych stanów faktycznych w granicach metod wykładni prawa administracyjnego. Tak jak w odniesieniu do pozostałych technik, ceną za elastyczność jest zwiększenie niepewności prawnej.

Każdy z podmiotów administrujących w obszarze referencyjnym wyposażony został w kompetencje do korzystania z instrumentów prawnych, które zakwalifikować można jako

¹⁰³⁸ O pojęciu terminu nieostrego por. M. Przełęcki, *W sprawie terminów nieostrych*, „Studia Logica: An International Journal for Symbolic Logic” 1958, No. 8, s. 313-317.

¹⁰³⁹ A. Błaś, J. Boć, R. Hauser et al., § 7. *Indywidualny akt administracyjny – jego istota* [w:] *Prawne formy działania administracji*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2013, s. 182, SIP Legalis.

¹⁰⁴⁰ K. Ajdukiewicz, *Zarys logiki*, Warszawa 1958, s. 58.

¹⁰⁴¹ M. Jędrzejczak, K. Ziemiński, *Władza dyskrecjonalna czy arbitralna?* [w:] *Władza w przestrzeni administracji publicznej*, red. Z. Duniewska, r. Lewicka, M. Lewicki, Warszawa 2020.

¹⁰⁴² L. Leszczyński, §30. Zwroty ocenne w wykładni przepisów prawa administracyjnego, [w:] *Wykładnia w prawie administracyjnym*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 360-361.

soft law o funkcji informacyjnej w postaci opinii, rekomendacji, wytycznych, stanowisk zajmowanych przez te podmioty administrujące lub nawet informacji zawartych na stronach internetowych podmiotów administrujących w zakładkach z najczęściej zadawanymi pytaniami¹⁰⁴³. Przykładowo, są to wielokrotnie przywoływane w tej rozprawie opinie (nazywane wytycznymi) Grupy Roboczej, a następnie EROD, czy też wytyczne wydawane przez Komisję w unijnym prawie konkurencji. Instrumenty te, charakterystyczne dla unijnego prawa administracyjnego i regulacji sektorowych (np. sektor telekomunikacyjny i energetyczny) w założeniu powinny zmniejszać niepewność prawną przez zajęcie przez podmioty administrujące stanowiska stanowiącego konkretyzację rozumienia aktów prawnych i wyraz polityki administracyjnej tych podmiotów¹⁰⁴⁴. Instrumenty *soft law* stanowią niejednorodną kategorię dokumentów, które nie mają mocy wiążącej¹⁰⁴⁵ i których treść nie podlega kontroli abstrakcyjnej, ale podmioty nadzorowane w praktyce identyfikują je jako obowiązujące, ponieważ fakt ich przyjęcia zwiększa prawdopodobieństwo, że podmioty administrujące będą stosować akty prawne zgodnie z wydanym przez siebie *soft law*¹⁰⁴⁶. Ten *quasi*-normatywny charakter instrumentów *soft law* powoduje, że ich umiejscowienie w systemie źródeł prawa, koncepcji wynikającej z pozytywizmu prawniczego, sprawia poważne trudności¹⁰⁴⁷, a w konsekwencji ich wykorzystywanie bywa krytykowane jako zagrożenie dla zasady państwa prawa z perspektywy ryzyka potencjalnych nadużyć tych instrumentów¹⁰⁴⁸. Z drugiej jednak strony, *soft law* identyfikowany jest jako użyteczny instrument regulacyjny pozwalający elastycznie reagować na zmiany rzeczywistości bez konieczności zmiany prawa stanowionego¹⁰⁴⁹. W analizowanym obszarze referencyjnym instrumenty *soft law* uzupełniają prawo stanowione, stanowią „samoograniczenie władzy dyskrecyjnej” przez podmioty administrujące¹⁰⁵⁰. Ich skutkiem jest zatem zmniejszenie

¹⁰⁴³ K. Jaroszyński, M. Wierzbowski, §23. *Funkcja regulacji gospodarczej*, [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 322-323.

¹⁰⁴⁴ K. Jaroszyński, M. Wierzbowski, §23. *Funkcja regulacji gospodarczej*, [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 322-323.

¹⁰⁴⁵ B. Fischer, *Prawne aspekty norm technicznych. Normalizacja jako wsparcie legislacji administracyjnej*, Warszawa 2017, s. 188-189.

¹⁰⁴⁶ K. Jaroszyński, M. Wierzbowski, §23. *Funkcja regulacji gospodarczej*, [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 322-323.

¹⁰⁴⁷ M. Grochowski, J. Helios, B. Liżewski et al., § 18. *Soft law w wykładni i stosowaniu prawa UE*, [w:] *Wykładnia prawa Unii Europejskiej*, red. L. Leszczyński, Warszawa 2019, s. 339, SIP Legalis.

¹⁰⁴⁸ *Research Handbook on Soft Law*, ed. by M. Eliantonio, E. Korkea-aho E., U. Mörrth, Cheltenham 2023, s. 44.

¹⁰⁴⁹ M. Pietrzyk, *Soft law i hard law w europejskim prawie administracyjnym: relacja alternatywy, uzupełnienia, wykluczenia oraz przejścia* [w:] *Administracja publiczna wobec wyzwań i oczekiwań społecznych*, red. M. Gięda, R. Raszevska-Skałeczka, Wrocław 2015, <http://www.bibliotekacyfrowa.pl/publication/73349> (dostęp: 20.09.2024 r.), s. 133-134.

¹⁰⁵⁰ M. Pietrzyk, *Soft law i hard law w europejskim prawie administracyjnym: relacja alternatywy, uzupełnienia, wykluczenia oraz przejścia* [w:] *Administracja publiczna wobec wyzwań i oczekiwań społecznych*, red. M. Gięda,

niepewności prawnej po stronie podmiotów nadzorowanych. Z uwagi na szeroko i nieostro sformułowany zakres przedmiotowy aktów prawnych w obszarze przetwarzania danych osobowych, którego konsekwencją są szerokie i nieostro rozgraniczone kompetencje podmiotów administrujących, w praktyce to właśnie na poziomie instrumentów *soft law* (formalnie niewiążącej konkretyzacji prawa stanowionego) dochodzić może do materializacji zjawiska krzyżowania się kompetencji podmiotów administrujących w tym obszarze. Przykładem takiego krzyżowania się kompetencji, do którego doszło w instrumentach typu *soft law*, był spór między PUODO a Ministrem Cyfryzacji dotyczący wydania przez Ministra objaśnień prawnych na podstawie art. 33 Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców¹⁰⁵¹ scharakteryzowany w rozdziale 4. niniejszej rozprawy¹⁰⁵².

Konsekwencją realizacji obranego przez prawodawcę celu w postaci neutralności technologicznej i horyzontalnego zastosowania aktów prawnych w obszarze przetwarzania danych osobowych jest przeniesienie konkretyzacji przepisów z etapu stosowania prawa na etap stanowienia prawa (przez podmioty administrujące i sądy administracyjne oraz TSUE), co osiągnięte jest przez wybór scharakteryzowanych wyżej technik prawodawczych: metody opartej na ryzyku, zastosowania norm-zasad i terminów nieostrych. Techniki te nakładają się na zjawisko otwartej tekstowości języka rozumiane w ten sposób, że z uwagi na naturę języka jako takiego (który stanowi budulec prawa) zawsze ujawnić się może stan faktyczny, w odniesieniu, do którego zakres lub znaczenie normy pozostaje niejasne¹⁰⁵³. Wszystkie te elementy ujmowane łącznie powodują zwiększenie niepewności prawnej co do zakresu przedmiotowego i podmiotowego aktów prawnych, treści uprawnień i obowiązków oraz kompetencji podmiotów administrujących po stronie samej administracji publicznej, jak i podmiotów nadzorowanych oraz podmiotów danych. Prowadzi to do zwiększenia roli metody systemowo-aksjologicznej, celowościowej i funkcjonalnej wykładni prawa administracyjnego¹⁰⁵⁴, powodując prymat wykładni dynamicznej nad statyczną, aby podmioty administracyjne mogły zapewnić nie tylko poszanowanie wartości, na których strażą stoją, ale

R. Raszevska-Skałeczka, Wrocław 2015, <http://www.bibliotekacyfrowa.pl/publication/73349> (dostęp: 20.09.2024 r.), s. 136.

¹⁰⁵¹ T.j. Dz. U. z 2023 r. poz. 221 z późn. zm.

¹⁰⁵² W podrozdziale, w którym zaproponowano typologię zjawiska krzyżowania się kompetencji organów.

¹⁰⁵³ I. Bogucka, 9.5. Rola wartości w porządku prawnym [w:] System prawa administracyjnego procesowego, t. 1: Zagadnienia ogólne, red. G. Łaszczyca, A. Matan, Warszawa 2017, SIP LEX.

¹⁰⁵⁴ Zagadnienia związane z wykładnią prawa administracyjnego są obszerne i wielowątkowe, a przedmiotem niniejszego podrozdziału nie jest ich charakterystyka. Wyczerpująca analiza tego zagadnienia w *Wykładnia w prawie administracyjnym*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015.

także ochronę wartości, które mają chronić¹⁰⁵⁵. Powoduje to bowiem, że w wykładni operatywnej prawa przez podmioty administrujące bezpośrednie rozumienie prawa ustalane przy wykorzystaniu metody językowej każdorazowo musi być uzupełnione o wszystkie pozostałe metody od początku procesu wykładni, gdyż tylko w ten sposób można osiągnąć jasność znaczenia zgodnie z paremią *interpretatio cessat in claris*¹⁰⁵⁶. Przedmiotem szerokiej i pogłębionej debaty należałoby uczynić to, czy z uwagi na aksjologicznie umotywowaną konieczność odpowiedzi na transformację cyfrową i naturę przebiegu transformacji cyfrowej opartej o ewoluujące rozwiązania technicznie istnieje realna alternatywa dla tego modelu¹⁰⁵⁷, czy też konieczne jest jego zaakceptowanie i przyjęcie rozwiązań mitygujących negatywne skutki z niego wynikające (patrz: postulaty *de lege ferenda*).

5.4. PRZYCZYNA NR 3: PROCES EUROPEIZACJI PRAWA ADMINISTRACYJNEGO

Wszystkie analizowane akty prawne w obszarze referencyjnym albo są aktami prawa unijnego, albo stanowią ich implementację w krajowym porządku prawnym. Jak wykazano w rozdziale 3, poza sytuacją, w której to Komisja jest właściwym organem unijnym ustanowionym na podstawie aktów prawnych regulujących unijne prawo konkurencji, DSA i DMA, zasadniczy ciężar stosowanie tych aktów przekazano organom krajowym, podczas gdy organy na poziomie unijnym wyposażone zostały w kompetencje doradcze, informacyjne i edukacyjne. Stanowienie, stosowanie i wykładnia aktów prawnych w analizowanym obszarze referencyjnym stanowi zatem egzemplifikację procesu europeizacji krajowego prawa administracyjnego (dotyczy to wszystkich jurysdykcji unijnych, nie tylko polskiej).

Charakterystyczną cechą tego procesu w obszarze przetwarzania danych osobowych jest, że prawodawca unijny przechodzi od wyboru rodzaju aktów prawnych, które nie są bezpośrednio stosowane i wymagają transpozycji przez państwa członkowskie (dyrektyw jak Dyrektywa ODO) do rozporządzeń bezpośrednio stosowanych (art. 288 TFUE)¹⁰⁵⁸, przy czym prawodawcy krajowemu zasadniczo pozostawione jest ustanowienie instytucji i procedur do stosowania tych aktów prawnych na poziomie państw członkowskich (zasada autonomii instytucjonalnej i proceduralnej scharakteryzowana poniżej). Konsekwencją tego jest

¹⁰⁵⁵ W. Jakimowicz, 4. Wykładnia celowościowa w prawie administracyjnym [w:] W. Jakimowicz, Wykładnia w prawie administracyjnym, Kraków 2006, SIP LEX.

¹⁰⁵⁶ L. Leszczyński, §30. Kryteria otwarte w wykładni przepisów prawa administracyjnego, [w:] Wykładnia w prawie administracyjnym, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 346-348.

¹⁰⁵⁷ Por. wnioski w Zakończeniu.

¹⁰⁵⁸ D. Curtin, T. Manucharyan *Legal acts and hierarchy of norms in EU law* [in:] *The Oxford Handbook of European Union Law*, ed. by A. Arnall, D. Chalmers, Oxford 2015, s. 103-125 (107-108).

bezpośrednie stosowanie tych samych przepisów prawa materialnego przez różne organy (z odmienną pozycją ustrojową w strukturze administracji publicznej poszczególnych państw członkowskich) według krajowych, różniących się od siebie (i wynikających z odmiennych kultur prawnych) procedur administracyjnych. Ograniczenie prawodawcy unijnego w kształtowaniu instytucji i procedur krajowych prowadzi do mozaikowego charakteru zarówno struktury organów na poziomie krajowym stosujących akty prawne w obszarze referencyjnym, jak i procedur, według których akty te są stosowane. Taka sytuacja – chociaż uzasadniona ograniczeniami ustrojowymi prawodawcy unijnego – wpływa negatywnie na skuteczność stosowania tych aktów prawnych zwłaszcza w sprawach transgranicznych, co jest przedmiotem dyskusji w odniesieniu do postępowania kompozytowego (pojęcie analizowane niżej) w sprawach transgranicznych w RODO, czyli procedury *one-stop shop*¹⁰⁵⁹.

Należy podkreślić, że zarządzanie administracyjne w obszarze przetwarzania danych osobowych ma szczególny charakter z uwagi na niematerialną naturę przedmiotu unormowania, czyli przetwarzania danych osobowych, co stanowi wyzwanie dla tradycyjnie pojmowanego terytorializmu działania administracyjnego¹⁰⁶⁰, indukując działania o charakterze transgranicznym przez podmioty administrujące, aby zapewnić skuteczność prawa. Dane osobowe są bowiem z niezwykłą łatwością przetwarzane transgranicznie lub przekazywane do państw trzech (brak komponentu fizycznego i wykorzystywanie infrastruktury teleinformatycznej), co oznacza, że te same operacje przetwarzania mogą podlegać jednocześnie różnym jurysdykcjom (także poza UE) w tym sensie, że wywierają wpływ na prawa i wolności podmiotów danych w różnych jurysdykcjach. Zarządzanie administracyjne wobec takiego przedmiotu unormowania jest zatem fundamentalnie inne niż w tradycyjnych obszarach regulacji, na przykład na rynku farmaceutycznym (np. w zakresie obrotu produktami leczniczymi w UE), czy w sprawach wprowadzenia na rynek unijny produktów spożywczych. Powoduje to, że ryzyka dotyczące skuteczności¹⁰⁶¹ zarządzania administracyjnego wynikające z europeizacji prawa administracyjnego nasilają się, a znaczenia dla zapewnienia tej skuteczności nabiera spójność i szybkość działań podejmowanych przez podmioty administrujące. W obranym modelu europeizacji prawa administracyjnego osiągnięcie tego jest jednak trudne z przyczyn strukturalnych.

¹⁰⁵⁹ Por. krytykę *one-stop shop* scharakteryzowaną w podrozdziale 3.4.1. rozprawy (końcowa część).

¹⁰⁶⁰ Por. B. Kowalczyk, Zasada terytorializmu działania administracji a transgraniczność spraw administracyjnych, [w:] Współpraca transgraniczna w administracji publicznej, red. R. Kusiak-Winter, Wrocław 2015, http://repozytorium.uni.wroc.pl/Content/79066/PDF/10_Barbara_Kowalczyk.pdf (dostęp: 20.09.2024 r.).

¹⁰⁶¹ Por. podrozdział 4.5. rozprawy o pojęciu skuteczności prawa administracyjnego.

Europeizacja prawa administracyjnego rozumiana jest w dwóch ujęciach – *top-down*, czyli wpływ ustrojowego, materialnego i proceduralnego prawa administracyjnego UE na ustrojowe, materialne i proceduralne prawo administracyjne państw członkowskich i *bottom-up*, czyli wpływ prawa administracyjnego państw członkowskich na prawo administracyjne UE¹⁰⁶² w kierunku ich konwergencji¹⁰⁶³. Ta wertykalna relacja nie oznacza jednak istnienia klarownej hierarchii czy podporządkowania prawa krajowego prawu unijnemu¹⁰⁶⁴. Najsilniejsza europeizacja typu *top-down* dotyczy prawa materialnego, ponieważ prawodawca unijny ustanawia normy tego prawa bezpośrednio w aktach prawnych, włączając te normy bezpośrednio do krajowego porządku prawnego lub też zobowiązując państwa członkowskie do ich implementacji i stosowania; w odniesieniu do prawa proceduralnego wpływ osiągany jest przede wszystkim przez wiążący charakter zasad ogólnych prawa unijnego i elementy unormowań proceduralnych w poszczególnych aktach (z ograniczeniem wynikającym z zasady autonomii proceduralnej analizowanej niżej); z kolei wpływ prawodawcy unijnego na prawo administracyjne ustrojowe państw członkowskich ograniczony jest do kształtowania krajowej administracji publicznej przez zobowiązanie do ustanowienia europejskich organów administracji publicznej jako elementu transpozycji aktów prawa unijnego¹⁰⁶⁵.

Podkreślić należy, że europeizacja prawa administracyjnego bywa identyfikowana (także krytycznie) jako proces „erozji części suwerenności” państw członkowskich z uwagi na ograniczenie władztwa państwa nad krajową władzą wykonawczą, która punkt odniesienia znajduje na poziomie unijnym¹⁰⁶⁶. Europeizacja prawa administracyjnego prowadzi do powstania europejskiego prawa administracyjnego, które w doktrynie rozumiane jest dwojako – w sposób wąski albo szeroki¹⁰⁶⁷. Wąskie pojmowanie dotyczy wyłącznie prawa administracyjnego przyjęte przez prawodawcę unijnego, natomiast europejskie prawo

¹⁰⁶² A. Wróbel, *Rozdział I. Europeizacja prawa administracyjnego – pojęcie i konteksty*, § 2. *Europeizacja prawa administracyjnego, I. Pojęcie i rodzaje* [w:] R. Hauser (red.), *System Prawa Administracyjnego Tom 3, Europeizacja prawa administracyjnego*, Warszawa 2014, Legalis.

¹⁰⁶³ K. Ziółkowska, *Nowe inicjatywy Unii Europejskiej w ramach jednolitego rynku cyfrowego na tle procesu europeizacji prawa administracyjnego* [w:] Kryzys, stagnacja, renesans? *Prawo administracyjne przyszłości. Księga jubileuszowa profesora dr hab. Jacka Jagielskiego*, red. M. Cherka, P. Gołaszewski, J. Piecha et al., Warszawa 2021. Por. także omówione tam pojęcie europeizacji prawa administracyjnego.

¹⁰⁶⁴ A. Wróbel, *Rozdział I. Europeizacja prawa administracyjnego – pojęcie i konteksty*, § 2. *Europeizacja prawa administracyjnego, I. Pojęcie i rodzaje* [w:] *Europeizacja prawa administracyjnego*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2014, Legalis.

¹⁰⁶⁵ A. Wróbel, *Rozdział I. Europeizacja prawa administracyjnego – pojęcie i konteksty*, § 2. *Europeizacja prawa administracyjnego, I. Pojęcie i rodzaje* [w:] *Europeizacja prawa administracyjnego*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2014, Legalis.

¹⁰⁶⁶ I. Lipowicz, *Europeizacja administracji publicznej*, RPEiS 2008, R. LXX, z. 1, s. 6.

¹⁰⁶⁷ M. Niedźwiedź, *Doktryna Meroni i jej znaczenie dla europejskiego prawa administracyjnego - wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.06.1958 r., 9/56, Meroni & Co., Industrie Metallurgiche, SpA przeciwko Wysokiej Władzy EWWiS*, EPS 2020, nr 1, s. 51-57, s. 51.

administracyjnym rozumiane szeroko to wskazane wyżej prawo administracyjne i prawo administracyjne państw członkowskich oraz „konwencyjne prawo administracyjne (np. regulacje przyjmowane w ramach Rady Europy”¹⁰⁶⁸. W tej rozprawie termin „europejskie prawo administracyjne” używany jest w obu znaczeniach, w zależności od kontekstu. Powstająca w ten sposób europejska przestrzeń administracyjna¹⁰⁶⁹ jest zasadniczo dwupoziomowa¹⁰⁷⁰. Zbudowana jest z administracji na szczeblu Unii, czyli unijnej (administracji bezpośredniej) i z administracji pośredniej – na poziomie państw członkowskich¹⁰⁷¹, chociaż w ostatnich latach odchodzi się od tej dychotomii z uwagi na nowe rozbudowane instrumenty współpracy wertykalnej i horyzontalnej¹⁰⁷². Cechy dystynktywne europejskiej przestrzeni administracyjnej są trudne do identyfikacji z uwagi na jej niejednorodną naturę¹⁰⁷³, nieuporządkowanie procedur administracyjnych¹⁰⁷⁴ i brak kodyfikacji ogólnego prawa administracyjnego materialnego¹⁰⁷⁵. Cechą dystynktywną tej przestrzeni można uznać zatem właśnie tę systemową niejednorodność. W literaturze wskazuje się na mozaikowość struktury podmiotów administrujących na poziomie unijnym i krajowym¹⁰⁷⁶ oraz brak jasnych stosunków hierarchicznych między nimi¹⁰⁷⁷ ze wzrastającą rolą różnorodnych rozwiązań o funkcji koordynacyjnej, na przykład rozrost zdecentralizowanych agencji unijnych i sieci organów (scharakteryzowane niżej)¹⁰⁷⁸.

¹⁰⁶⁸ M. Niedźwiedz, Doktryna Meroni i jej znaczenie dla europejskiego prawa administracyjnego - wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.06.1958 r., 9/56, Meroni & Co., Industrie Metallurgiche, SpA przeciwko Wysokiej Władzy EWWiS, EPS 2020, nr 1, s. 51-57, s. 51.

¹⁰⁶⁹ Wnioski i cytowana literatura w tym akapicie pochodzi z: P. Hajduk, A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research (November 23, 2023). Forthcoming, 18th IFIP Privacy and Identity Management 2023 - Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 15.09.2024 r.), s. 11.

¹⁰⁷⁰ M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et. al, *Rozdział IX. Zarys systemu podmiotów administrujących w Unii Europejskiej* [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 558.

¹⁰⁷¹ J. Olsen, Towards a European administrative space? J. Eur. Public Policy 2003, Vol. 10, Iss. 4.

¹⁰⁷² M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et. al, *Rozdział IX. Zarys systemu podmiotów administrujących w Unii Europejskiej* [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 558.

¹⁰⁷³ J. Trondal, B. G. Peters, A Conceptual Account of the European Administrative Space, [in:] M.W. Bauer, J. Trondal, The Palgrave Handbook of the European Administrative System. European Administrative Governance, New York 2015.

¹⁰⁷⁴ M. Wilbrandt-Gotowicz, Europeanisation of Administrative Proceedings Law – Opportunities and Risks. BSP 2018, nr 2, s. 25-37.

¹⁰⁷⁵ C. Patrascu, G. Schin, Challenges of the EU administrative space: convergence of national administrations to the European administrative law, „Union of Jurists of Romania. Law Review” 2017, Vol. 7, Iss. 2, s. 24-34.

¹⁰⁷⁶ C. Patrascu, G. Schin, Challenges of the EU administrative space: convergence of national administrations to the European administrative law, „Union of Jurists of Romania. Law Review” 2017, Vol. 7, Iss. 2, s. 24-34.

¹⁰⁷⁷ N.M. Vestlund, *Pooling administrative resources through EU regulatory networks*, J. Eur. Public Policy 2017, Vol. 24, No. 1, s. 61-80.

¹⁰⁷⁸ Por. także M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et. al, *Rozdział IX. Zarys systemu podmiotów administrujących w Unii Europejskiej* [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 556-559.

Jak scharakteryzowano w podrozdziale 3.2. tej rozprawy, to na państwach członkowskich spoczywa przede wszystkim obowiązek stosowania administracyjnego prawa unijnego (pośrednie wykonywanie prawa UE) z ograniczoną rolą organów i instytucji unijnych w określonych przypadkach (bezpośrednie wykonywanie prawa UE), co określane jest jako model federalizmu wykonawczego¹⁰⁷⁹. Państwa te mogą zasadniczo wybrać instytucje i procedury tego stosowania (zasada autonomii instytucjonalnej i proceduralnej), będąc ograniczonymi obowiązkiem zapewnienia efektywności i ekwiwalentności¹⁰⁸⁰ (art. 291 ust. 1 TFEU i art. 298 TFUE) oraz lojalnej współpracy (art. 4 ust. 3 TUE).

Zasada autonomii instytucjonalnej państw członkowskich rozumiana jest jako swoboda państw członkowskich (limitowana ograniczeniami wskazanymi wyżej¹⁰⁸¹) w ukształtowaniu struktur instytucjonalnych stosowania prawa unijnego zgodnie z krajowym prawem konstytucyjnym i prawem administracyjnym ustrojowym¹⁰⁸². Przykładowo, w państwach federalnych (jak Niemcy) ustanowione zostały organy ochrony danych osobowych w każdym z landów i organ na poziomie federalnym, podczas gdy w Polsce jest tylko jeden organ ochrony danych osobowych. W analizowanych aktach prawnych w obszarze referencyjnym (poza DMA i krajowym prawem konkurencji) prawodawca unijny pozostawił znaczną swobodę prawodawcy krajowemu w ukształtowaniu struktury instytucjonalnej podmiotów administrujących ustanowionych do stosowania tych aktów prawnych. Chociaż rola UE w kształtowaniu administracji publicznej państw członkowskich jest, zgodnie z traktatami unijnymi, pomocnicza (por. art. 198 TFUE), to zasada ta nie ma charakteru bezwzględnej, ponieważ mogłoby to uniemożliwiać wykonywanie pozostałych kompetencji UE¹⁰⁸³.

¹⁰⁷⁹ M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et. al, *Rozdział IX. Zarys systemu podmiotów administrujących w Unii Europejskiej* [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 558.

¹⁰⁸⁰ *Law of Administrative Procedure of the European Union: European Added Value Assessment (+ Annexes I-III)*, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/dv/eav_lawofadminprocedure_/EAV_LawofAdminprocedure_EN.pdf (dostęp: 20.09.2024 r.), s. II-49

¹⁰⁸¹ Patrz jednak: J. Bois, P. Van Cleynenbreugel, *National Institutional Autonomy and EU law: time to reframe the stakes of interdisciplinary scholarship?*, „EUDAMONIA Working Paper” 2021, No. 1, s. 11, gdzie argumentowano, że sądy unijne jednoznacznie ograniczają zasadę autonomii proceduralnej niż instytucjonalnej.

¹⁰⁸² D.G. Dimitrakopoulos, *The Transposition of EU Law: ‘Post-Decisional Politics’ and Institutional Autonomy*, „European Law Journal” 2001, Vol. 7, No. 4, <https://doi.org/10.1111/1468-0386.00137> (dostęp: 20.09.2024 r.), s. 444-445.

¹⁰⁸³ K. Ziółkowska, *Nowe inicjatywy Unii Europejskiej w ramach jednolitego rynku cyfrowego na tle procesu europeizacji prawa administracyjnego* [w:] *Kryzys, stagnacja, renesans? Prawo administracyjne przyszłości. Księga jubileuszowa profesora dr hab. Jacka Jagielskiego*, red. M. Cherka, P. Gołaszewski, J. Piecha et al., Warszawa 2021.

W zakresie, w jakim jest to zatem niezbędne do wykonywania tych pozostałych kompetencji, UE może wpływać na krajową administrację publiczną w wymiarze instytucjonalnym¹⁰⁸⁴.

Z kolei zasada autonomii proceduralnej państw członkowskich ukształtowana (podobnie jak zasada autonomii instytucjonalnej) w orzecznictwie TSUE pojmowana jest jako możliwość państw członkowskich do unormowania procedur (w tym postępowania administracyjnego i sądowno-administracyjnego) służących stosowaniu prawa unijnego w wybrany przez siebie sposób, o ile nie uregulowano tego uprzednio w prawie unijnym, przy czym na państwach członkowskich spoczywa obowiązek efektywności i ekwiwalentności (niedyskryminacji)¹⁰⁸⁵. Oznacza to, że jeżeli w prawie unijnym nie unormowano kwestii proceduralnych, to, z zastrzeżeniem powyższych ograniczeń i zasad ogólnych prawa UE, mogą być one unormowane swobodnie przez państwa członkowskie, co oznaczać będzie ustanowienie różnorodnych rozwiązań proceduralnych w poszczególnych kwestiach dla tych samych instytucji w akcie unijnym (np. trybu rozpatrywania skarg zgłaszanych przez osoby fizyczne w związku z przetwarzaniem danych osobowych).

W literaturze wskazuje się na tendencję prawodawcy unijnego do rozszerzenia normowania zarówno kwestii instytucjonalnych i proceduralnych (bezpośrednio lub pośrednio) w prawie unijnym ograniczając obie autonomie¹⁰⁸⁶, co jednak nie stanowi procesu linearnego¹⁰⁸⁷. Stąd też prawodawca unijny wykorzystuje także inne instrumenty zapewnienia spójności administracyjnego prawa unijnego jak rozszerzenie roli agencji unijnych i sieci organów. Konieczność pogłębionej harmonizacji proceduralnej w kierunku ograniczenia autonomii proceduralnej państw członkowskich została zidentyfikowana w obszarze unormowania przetwarzania danych osobowych przez EROD w oświadczeniu z 28 kwietnia 2022 r. (znanym jako „wiedeńskie oświadczenie”), gdzie zawarto zobowiązanie do w identyfikacji listy kwestii proceduralnych wymagających dalszej harmonizacji odniesieniu

¹⁰⁸⁴ K. Ziółkowska, Nowe inicjatywy Unii Europejskiej w ramach jednolitego rynku cyfrowego na tle procesu europeizacji prawa administracyjnego [w:] Kryzys, stagnacja, renesans? Prawo administracyjne przyszłości. Księga jubileuszowa profesora dr hab. Jacka Jagielskiego, red. M. Cherka, P. Gołaszewski, J. Piecha et al., Warszawa 2021.

¹⁰⁸⁵ A. Wróbel, Autonomia proceduralna państw członkowskich. Zasada efektywności i zasada efektywnej ochrony sądowej w prawie Unii Europejskiej, RPEiS 2005, t. 67, z. 1, s. 35-58, s. 40-41. Por. także D. U. Galetta, Procedural autonomy of EU Member States: paradise lost?: a study on the „functionalized procedural competence” of EU Member States, Cham 2010, s. 7-32.

¹⁰⁸⁶ Por. K. Ziółkowska, Nowe inicjatywy Unii Europejskiej w ramach jednolitego rynku cyfrowego na tle procesu europeizacji prawa administracyjnego [w:] Kryzys, stagnacja, renesans? Prawo administracyjne przyszłości. Księga jubileuszowa profesora dr hab. Jacka Jagielskiego, red. M. Cherka, P. Gołaszewski, J. Piecha et al., Warszawa 2021.

¹⁰⁸⁷ J. Chlebny, 6.10. Zasada autonomii proceduralnej państw członkowskich. Prawo unii jako źródło norm administracyjnego prawa procesowego [w:] System prawa administracyjnego procesowego, t. 1: Zagadnienia ogólne, red. G. Łaszczyca, A. Matan, Warszawa 2017, SIP LEX; i przywołana tam literatura.

do stosowania RODO w sprawach transgranicznych¹⁰⁸⁸. Następnie, w piśmie do Komisji z dnia 10 października 2022 r. EROD wykonał to zobowiązanie, identyfikując m.in. kwestię statusu stron postępowań administracyjnych, dostęp stron do akt sprawy, prawo do bycia wysłuchanym i sposób współpracy między organami ochrony danych osobowych w różnych jurysdykcjach¹⁰⁸⁹. Wobec tej inicjatywy Komisja przedstawiła projekt rozporządzenia ustanawiającego dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679¹⁰⁹⁰, który obecnie jest procedowany.

Pozycja i kompetencje organów na poziomie unijnym, czyli zasadniczo tak zwanych agencji unijnych (regulacyjnych) ustanowionych w obszarze przetwarzania danych osobowych i Komisji scharakteryzowane zostały w podrozdziale 3.2. tej rozprawy. Poniżej przedstawione zostaną uwagi do zjawiska określanego w literaturze jako „*agencification*” administracji unijnej i tak zwanej doktryny Meroni, które mają wpływ na kształt struktury agencji unijnych w analizowanym obszarze referencyjnym. Wyróżnia się dwa typy agencji unijnych (agencji administracji własnej UE): agencje wykonawcze (kontrolowane przez Komisję; ich zadaniem jest zarządzanie programami unijnymi wsparcia finansowego) i agencje zdecentralizowane o heterogenicznym charakterze, którym wyznaczono realizację niejednorodnych zadań w różnorodnych obszarach, pozostające w stosunku (większej lub mniejszej; czasami bardzo ograniczonej) niezależności wobec Komisji¹⁰⁹¹. Definiowane są w literaturze (nazywane także jako „agencje regulacyjne”) jako „wyodrębnione strukturalnie ciała, niebędące formalnie częścią instytucji lub organów traktatowych, tworzone na podstawie aktu prawa pochodnego”¹⁰⁹². Organy na poziomie unijnym w analizowanym obszarze referencyjnym (poza samą Komisją) zaliczyć należy do drugiego typu agencji zdecentralizowanych. Właśnie do tego drugiego typu agencji w literaturze podnoszone są wątpliwości co do ich demokratycznej legitymacji¹⁰⁹³. Zjawisko *agencification* rozumiane jest w literaturze jako sposób kształtowania

¹⁰⁸⁸ EROD, *Statement on enforcement cooperation* Adopted on 28 April 2022, [edpb_statement_20220428_on_enforcement_cooperation_en.pdf](https://edpb.europa.eu/system/files/2022-10/edpb_statement_20220428_on_enforcement_cooperation_en.pdf) (europa.eu)

¹⁰⁸⁹ EROD, *EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level*, https://www.edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf (europa.eu)

¹⁰⁹⁰ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679 COM/2023/348 final

¹⁰⁹¹ E. Schmidt-Aßmann, *Dogmatyka prawa administracyjnego. Bilans rozwoju, reformy i przyszłych zadań*, Warszawa 2022, s. 227-229.

¹⁰⁹² Definicja J. Barcza i M. Górki przywołana za M. Dyl, A. Paczkowska-Tomaszewska, R. Stankiewicz et al., *Rozdział IX. Zarys systemu podmiotów administrujących w Unii Europejskiej* [w:] *Podmioty administrujące*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2011, s. 572.

¹⁰⁹³ E. Schmidt-Aßmann, *Dogmatyka prawa administracyjnego. Bilans rozwoju, reformy i przyszłych zadań*, Warszawa 2022, s. 229.

ustroju unijnej administracji przez powoływanie licznych odrębnych podmiotów administrujących (w większości nazywanych agencjami, przy czym nie wszystkie mają tę nazwę) i przyznawanie im wyspecjalizowanych zadań oraz kompetencji do ich wykonywania¹⁰⁹⁴. Przyjęcie tego sposobu motywowane jest osiągnięciem kompromisu między funkcjonalną potrzebą centralizacji wykonywania władzy wykonawczej na poziomie UE a niechęcią państw członkowskich do dokonywania tego¹⁰⁹⁵. Obecnie w UE ustanowionych jest aż ponad 30 agencji zdecentralizowanych (regulacyjnych)¹⁰⁹⁶.

Dla zakresu (delegacji) kompetencji (do) agencji unijnych istotna jest sformułowana podstawie orzeczenia TSUE z 1958 r. doktryna *Meroni*¹⁰⁹⁷. Doktryna ta przewiduje, że nie można delegować agencjom innych lub szerszych kompetencji niż te, które zostały przyznane podmiotowi delegującemu, delegowanie nie może być dorozumiane i musi być niezbędne dla realizacji określonych zadań, a przedmiotem delegacji mogą być tylko ściśle określone kompetencje, których wykonywanie podlega kontroli podmiotu delegującego i kontroli sądowej¹⁰⁹⁸. W literaturze podnosi się, że doktryna ta znajduje zastosowanie w odniesieniu do agencji wykonawczych, natomiast przełamywana jest (a jej obowiązywanie kwestionowane jest) wobec agencji zdecentralizowanych (regulacyjnych) ustanawianych bezpośrednio przez prawodawcę unijnego, są (mniej lub bardziej) niezależne od Komisji i pozostałych organów oraz instytucji unijnych, a nadto posiadają własne kompetencje, w tym dyskrecyjne¹⁰⁹⁹. Postulowane jest, aby w odniesieniu do delegacji uprawnień do agencji regulacyjnych sformułowana została dedykowana doktryna¹¹⁰⁰. Nieuporządkowany charakter agencji

¹⁰⁹⁴ D. Levi-Faur, *Regulatory networks and regulatory agencification: towards a Single European Regulatory Space*, J. Eur. Public Policy 2011, Vol. 18, Iss. 6, <https://doi.org/10.1080/13501763.2011.593309> (dostęp: 20.09.2024 r.), s. 814.

¹⁰⁹⁵ M. Egeberg, J. Trondal, *Agencification of the European Union Administration: Connecting the Dots*, „TARN Working Paper” 2016, No. 1, <https://ssrn.com/abstract=2754716> (dostęp: 20.09.2024 r.), s. 1.

¹⁰⁹⁶ EU, *Decentralised agencies*, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/types-institutions-and-bodies_en

¹⁰⁹⁷ Wyrok TSUE z dnia 13 czerwca 1958 r. *Meroni & Co., Industrie Metallurgiche, SpA przeciwko Wysokiej Władzy EWWiS*. Sprawa 9-56. ECLI:EU:C:1958:7.

¹⁰⁹⁸ J.-P. Schneider, *A Common Framework for Decentralized EU Agencies and the Meroni Doctrine*, Special Issue of „Administrative Law Review” 2009, Vol. 61., s. 35-35; M. Niedźwiedź, *Doktryna Meroni i jej znaczenie dla europejskiego prawa administracyjnego - wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.06.1958 r., 9/56, Meroni & Co., Industrie Metallurgiche, SpA przeciwko Wysokiej Władzy EWWiS*, EPS 2020, nr 1, s. 51-57, s. 53.

¹⁰⁹⁹ M. Niedźwiedź, *Doktryna Meroni i jej znaczenie dla europejskiego prawa administracyjnego - wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.06.1958 r., 9/56, Meroni & Co., Industrie Metallurgiche, SpA przeciwko Wysokiej Władzy EWWiS*, EPS 2020, nr 1, s. 51-57, s. 54. Por. także H. C. H. Hofmann, *Seven challenges for EU administrative law*, „Review of European Administrative Law” 2009, Vol. 2, No. 2, s. 45-48; oraz M. Chamon, *EU Agencies: Does the Meroni Doctrine Make Sense?* Maastricht Journal of European and Comparative Law, 17(3), 281-305. <https://doi.org/10.1177/1023263X1001700304>

¹¹⁰⁰ M. Niedźwiedź, *Doktryna Meroni i jej znaczenie dla europejskiego prawa administracyjnego - wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.06.1958 r., 9/56, Meroni & Co., Industrie Metallurgiche, SpA przeciwko*

unijnych i proces delegacji kompetencji oraz relacji między nimi, który bardziej przypomina improwizowane działania niż przemyślany proces, jest rozpoznawany w doktrynie jako największe wyzwanie „europeizacji strukturalnej”, ponieważ samo istnienie tych agencji (nawet bez kompetencji władczych) wpływa na sposobów stosowania aktów prawnych przez organy krajowe¹¹⁰¹.

W wielopoziomowym modelu unijnego zarządzania administracyjnego zasadniczą rolę wciąż odgrywają jednak organy krajowe, które mają dwojaki charakter – stanowią element struktury administracji państw członkowskich (są organami administracji krajowej) i stosują prawo unijne, współpracując z agencjami unijnymi, i w ramach sieci organów (są organami administracji unijnej)¹¹⁰². Charakteryzuje je niejednorodność, spowodowana odmiennymi wyborami prawodawców krajowych, co umożliwia zasady autonomii instytucjonalnej i proceduralnej (scharakteryzowane wyżej). Stąd też prawodawca unijny w prawie unijnym ustanawia tak zwane „sieci organów”. Wszystkie analizowane organy (z wyłączeniem Komisji jako organu stosującego DMA; ustanowiono jednak Grupę Wysokiego Szczebla, która może być klasyfikowana jako specyficzna agencja unijna) w obszarze przetwarzania danych osobowych można zakwalifikować do jednej z szeroko pojmowanych sieci organów¹¹⁰³. Ich celem jest zinstytucjonalizowanie zarówno współpracy horyzontalnej między organami w poszczególnych państwach członkowskich (w ramach tych sieci), jak i współpracy wertykalnej między organami państw członkowskich a agencjami unijnymi. Oprócz współpracy w sprawach transgranicznych w postępowaniach kompozytowych (scharakteryzowane niżej), istotna jest także wymiana informacji i koordynacja działań między tymi organami, które wpływają na kierunek władczych rozstrzygnięć poszczególnych organów w sieci, co w konsekwencji ma wzmacniać spójność stosowania prawa unijnego między poszczególnymi państwami członkowskimi¹¹⁰⁴.

Sieci te współistnieją z agencjami unijnymi, tworząc unikalne struktury identyfikowane w literaturze jako (w zależności od indywidualnych okoliczności) „*agencified networks*”

Wysokiej Władzy EWWiS, EPS 2020, nr 1, s. 51-57, s. 54. Por. także H. C. H. Hofmann, Seven challenges for EU administrative law, „Review of European Administrative Law” 2009, Vol. 2, No. 2, s. 45-48; oraz M. Chamon, EU Agencies: Does the Meroni Doctrine Make Sense? Maastricht Journal of European and Comparative Law” 2010, nr 17(3). <https://doi.org/10.1177/1023263X1001700304> (dostęp: 20.09.2024 r.).

¹¹⁰¹ I. Lipowicz, *Europeizacja administracji publicznej*, RPEiS 2008, R. LXX, z. 1, s. 9.

¹¹⁰² Por. szerzej E. Schmidt-Aßmann, Dogmatyka prawa administracyjnego. Bilans rozwoju, reformy i przyszłych zadań, Warszawa 2022, s. 230-233.

¹¹⁰³ Por. analiza podmiotów administrujących w obszarze przetwarzania danych osobowych w rozdziale 3 rozprawy.

¹¹⁰⁴ I. Lipowicz, *Europeizacja administracji publicznej*, RPEiS 2008, R. LXX, z. 1, s. 12.

(„agencyjne sieci”) lub „*networked agency*” („usieciowione agencje”)¹¹⁰⁵. Terminy te oddają to, że relacja między podmiotami administrującymi na poziomie państw członkowskich, które współpracują z sobą horyzontalnie w ramach sieci organów, uwikłana jest w relację związaną ze współpracą wertykalną z agencjami unijnymi lub Komisją, tworząc złożone formalne i nieformalne zależności w wykonywaniu wszystkich typów kompetencji. Chociaż w założeniu umożliwia to konwergencję stosowania unijnego prawa administracyjnego w taki sposób, w jaki jest to prawnie i politycznie możliwe, to w konsekwencji stanowi wyzwanie dla zapewnienia przejrzystości procedur i demokratycznej legitymacji oraz spójności i pewności prawa.

Tworzenie unijnych sieci administracyjnych, rozumianych jako różnorodne formy „zinstytucjonalizowanej współpracy” między podmiotami administrującymi w państwach członkowskich (w ujęciu horyzontalnym) lub między tymi podmiotami a podmiotami na poziomie unijnym (w ujęciu wertykalnym)¹¹⁰⁶ jest uznawane za jedno z kluczowych zjawisk rozwoju unijnego zarządzania administracyjnego. Sieci te – podobnie jak i samą europejską przestrzeń administracyjną – cechuje niejednorodność rozumiana jako współistnienie różnych instytucjonalnych i proceduralnych rozwiązań¹¹⁰⁷. Sieci te mogą służyć tylko wymianie informacji między krajowymi organami stosującymi prawo unijne, ale mogą być także w ich ramach wykonywane istotnie kompetencje władcze (na przykład w procesie wydawania transnarodowych aktów administracyjnych)¹¹⁰⁸. Celem sieci, podobnie jak agencji unijnych, jest zapewnienie spójności i koordynacji w stosowaniu unijnego prawa administracyjnego¹¹⁰⁹ wobec istniejących ograniczeń ustrojowych i politycznych UE. Bywa, że istnienie tych sieci strukturalnie wbudowane jest w agencje unijne. Przykładowo, w skład EROD¹¹¹⁰ wchodzi organy ochrony danych osobowych państw członkowskich i EIOD. W tym sensie wszystkie te

¹¹⁰⁵ D. Levi-Faur, *Regulatory networks and regulatory agencification: towards a Single European Regulatory Space*, J. Eur. Public Policy 2011, Vol. 18, Iss. 6, <https://doi.org/10.1080/13501763.2011.593309> (dostęp: 20.09.2024 r.), s. 826-827.

¹¹⁰⁶ M. Niedźwiedź, Rozdział II. Administracyjne wykonywanie prawa Unii Europejskiej, § 6. Bezpośrednie wykonywanie prawa UE przez administrację UE [w:] *Europeizacja prawa administracyjnego*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2014, Legalis.

¹¹⁰⁷ P. P. Craig, *Shared Administration and Networks: Global and EU Perspectives*, „Oxford Legal Studies Research Paper” 2009, No. 6, <https://ssrn.com/abstract=1333557> (dostęp: 20.09.2024 r.), s. 34.

¹¹⁰⁸ F. M. Elżanowski, 1.3. Instytucja współdziałania w toku postępowania administracyjnego z organami administracji Unii Europejskiej [w:] *Prawnoprocesowa sytuacja przedsiębiorstwa energetycznego w sprawach z zakresu regulacji energetyki*, Warszawa 2015, SIP LEX.

¹¹⁰⁹ E. Mastenbroek, D. Sindbjerg Martinsen, *Filling the gap in the European administrative space: the role of administrative networks in EU implementation and enforcement*, J. Eur. Public Policy 2018, Vol. 25, Iss. 3, <https://doi.org/10.1080/13501763.2017.1298147> (dostęp: 20.09.2024 r.), s. 424.

¹¹¹⁰ Scharakteryzowane w rozdziale 3.

podmioty stanowią sieć organów, która jednak funkcjonuje strukturalnie jako niezależny podmiot z własnymi kompetencjami (zdecentralizowana agencja unijna¹¹¹¹).

W literaturze w odniesieniu do sieci organów identyfikowane jest ryzyko braku elastyczności tych sieci w tym rozumieniu, że mogą być one zbyt złożone podmiotowo, aby efektywnie odpowiadać na nowe problemy, a nadto, że zarzucić im można brak wystarczającej legitymacji w demokratycznych państwach prawa¹¹¹². W analizowanym obszarze referencyjnym zasadniczo ustanowione zostały podmioty administracji unijnej, które zakwalifikować można jako „*networked agency*” („usieciowione agencje”). Jak było to już wskazywane, w odniesieniu do EROD zgłaszany bywa zarzut nieefektywności w podejmowaniu decyzji w ramach procedury *one-stop shop*, co spowodowane ma być m.in. koniecznością uwzględnienia stanowiska wielu organów ochrony danych w ramach tej procedury kompozytowej¹¹¹³.

Procedury kompozytowe, powiązane ze zjawiskiem sieci organów, to transnarodowe (multijurysdykcyjne) postępowania administracyjne unormowane w prawie unijnym o niejednorodnej i stale ewoluującej naturze¹¹¹⁴. Charakteryzowane są jako forma wieloetapowej współpracy między podmiotami administracyjnymi poszczególnych państw członkowskich, a także podmiotami administracyjnymi na poziomie UE, której cechą charakterystyczną jest „kumulacja kompetencji organów jurysdykcji w jednej sprawie” w taki sposób, że jeden z organów odpowiada za wydanie decyzji (najczęściej transnarodowy akt administracyjny) w sprawie, a inne dokonują określonych czynności przygotowawczych¹¹¹⁵. Doktryna identyfikuje procedury kompozytowe jako przykład kwestionowania podziału administracji unijnej na pośrednią i bezpośrednią, ponieważ z założenia są one multicentryczne¹¹¹⁶. W literaturze wyróżniane są trzy typy procedur kompozytowych: wertykalne (współpraca organu państwa członkowskiego i organów UE), horyzontalne (tylko współpraca organów poszczególnych państw członkowskich) i hybrydowe (współpraca

¹¹¹¹ Taka klasyfikacja jest jednak dyskutowana w literaturze, por. L. Jančiūtė, *European data protection board: nascent EU agency or an 'intergovernmental club'?*, Int. Data Priv. Law 2020, 10(1), s. 57-75.

¹¹¹² I. Lipowicz, *Europeizacja administracji publicznej*, RPEiS 2008, R. LXX, z. 1, s. 7.

¹¹¹³ Por. krytykę scharakteryzowaną w podrozdziale 3.4.1. rozprawy (końcowa część).

¹¹¹⁴ Ł. Prus, B. Kowalczyk, Wstęp [w:] *Aktualność pojęć prawa administracyjnego*, red. W. Jakimowicz, Warszawa 2021. Ł. Prus, 2. Pojęcie procedur kompozytowych w zintegrowanej administracji Unii Europejskiej [w:] *Kierunki rozwoju jurysdykcji administracyjnej*, red. M. Kruś, L. Staniszevska, M. Szewczyk, Warszawa 2022.

¹¹¹⁵ Ł. Prus, B. Kowalczyk, Wstęp [w:] *Aktualność pojęć prawa administracyjnego*, red. W. Jakimowicz, Warszawa 2021.

¹¹¹⁶ Ł. Prus, 5. Podsumowanie [w:] *Kierunki rozwoju jurysdykcji administracyjnej*, red. M. Kruś, L. Staniszevska, M. Szewczyk, Warszawa 2022.

organów poszczególnych państw członkowskich połączona ze współpracą z organem UE)¹¹¹⁷. Ostatecznie to organ krajowy albo organ unijny wydaje decyzję w sprawie¹¹¹⁸. W tym kontekście M. Wilbrandt-Gotowicz, proponując oryginalną typologię procedur kompozytowych¹¹¹⁹, zasadnie wskazuje, że brak jest spójności w realizacji kontroli sądowych czynności organów administracji (decyzji) podejmowanych na różnych etapach procedur kompozytowych, co stanowi zagrożenie dla prawa do sądu¹¹²⁰.

W analizowanym obszarze referencyjnym różnorodne procedury kompozytowe ustanowione zostały w sprawach transgranicznych w części analizowanych aktów prawnych (w tym RODO, DSA, AI Act). Najgłębiej zbadanym przykładem takiej procedury w doktrynie jest procedura *one-stop shop* scharakteryzowana w podrozdziale 3.4.1. rozprawy z udziałem EROD i organów ochrony danych osobowych, których dotyczy dana sprawa. Takie procedury zidentyfikować można także m.in. w DSA i AI Act. W odniesieniu do zjawiska krzyżowania się kompetencji należy podkreślić, że procedury kompozytowe dodatkowo komplikują układy kompetencyjne, w jakich znajdują się krajowe podmioty administrujące. W sprawach transgranicznych podmioty administrujące poszczególnych państw członkowskich mogą bowiem w wykonywaniu swoich kompetencji być uzależnione od zajęcia stanowiska lub opinii przez organy innych unijnych jurysdykcjach lub organy unijne, albo też mogą w ogóle zobowiązane być do przekazania sprawy do organu innej unijnej jurysdykcji jako organu właściwego w danej sprawie transgranicznej (np. art. 56 RODO, właściwość wiodącego organu nadzorczego).

Konkludując, jedną z przyczyn zjawiska krzyżowania się kompetencji organów administracji publicznej jest dynamika i kształt ewoluującego procesu europeizacji prawa administracyjnego, która związana jest z ograniczeniami ustrojowymi prawodawcy unijnego i naturą relacji administracyjnego prawa unijnego do administracyjnego prawa krajowego w zestawieniu ze specyficzną charakterystyką unormowania przetwarzania danych osobowych. Jest to sytuacja zrozumiała, ale trudna, ponieważ charakterystyka ta (zasadnicza niematerialność przetwarzania, jego transgraniczny charakter, powszechna obecność danych osobowych) wymagałaby raczej bardziej scentralizowanego modelu stosowania prawa

¹¹¹⁷ Ł. Prus, 3. *Modele procedur kompozytowych* [w:] *Kierunki rozwoju jurysdykcji administracyjnej*, red. M. Kruś, L. Staniszeńska, M. Szewczyk, Warszawa 2022.

¹¹¹⁸ M. Wilbrandt-Gotowicz, *Judicial Control in Integrated Composite Administrative Proceedings—Monism or Duality of Protection of Individual Rights?*, „*Studia Iuridica Lublinensia*” 2023, Vol. 32, No. 1, s. 296.

¹¹¹⁹ M. Wilbrandt-Gotowicz, *Judicial Control in Integrated Composite Administrative Proceedings—Monism or Duality of Protection of Individual Rights?*, „*Studia Iuridica Lublinensia*” 2023, Vol. 32, No. 1, s. 297-298.

¹¹²⁰ M. Wilbrandt-Gotowicz, *Judicial Control in Integrated Composite Administrative Proceedings—Monism or Duality of Protection of Individual Rights?*, „*Studia Iuridica Lublinensia*” 2023, Vol. 32, No. 1, s. 315-317.

i ustanowienia na poziomie unijnym pogłębionego instrumentarium współpracy między podmiotami administrującymi, aby zapewnić spójność i skuteczność jego stosowania. Z perspektywy funkcjonowania europejskiej administracji publicznej jako całości nie należy postrzegać każdego ze scharakteryzowanych w tym podrozdziale elementów procesu europeizacji prawa administracyjnego z osobna, lecz należy rozpatrywać je łącznie, w ujęciu funkcjonalnym¹¹²¹ w uzupełnieniu o pozostałe przyczyny zjawiska krzyżowania się kompetencji organów, które – jak zostało wskazane – pozostają ze sobą powiązane i wzajemnie się umacniają. W perspektywie postulatów *de lege ferenda* (zwłaszcza postulatu nr 2 i 3 poniżej) rozważenia wymaga, na ile zasadne jest przełamywanie zasady autonomii proceduralnej i instytucjonalnej państw członkowskich, co miałyby być motywowane zwiększeniem skuteczności regulacji w obszarze przetwarzania danych osobowych z uwagi na jego szczególną naturę oraz do jakiego stopnia jest to możliwe prawnie (przy obecnym kształcie traktatów unijnych) i realnie politycznie.

5.5. PRZYCZYNA NR 4: PRAWO OCHRONY DANYCH OSOBOWYCH JAKO PRAWO WSZYSTKIEGO?

Organy ochrony danych osobowych to jedyne podmioty administrujące, których istnienie i niezależność przewidziano w KPP. Zgodnie z art. 8 ust. 3 KPP, „przestrzeganie tych zasad [to jest zgodnie z art. 8 ust. 2 KPP: „Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania”] podlega kontroli niezależnego organu”. Obowiązek ustanowienia organów ochrony danych osobowych w państwach członkowskich konkretyzuje RODO, jednocześnie normując kompetencje tych organów w szeroki sposób¹¹²².

Wyzwanie dla art. 8 ust. 3 KPP, jak i samego RODO stanowi szerokie pojęcie danych osobowych¹¹²³. Jest to uzasadnione potrzebą zapewnienia możliwie szerokiej ochrony praw podstawowych i z tej przyczyny postulowanie zawężenia pojęcia danych osobowych jest niezasadne. Konsekwencją tego jest jednak nie tylko to, że dane (informacje) jedynie pośrednio związane z podmiotami danych (osobami fizycznymi) stanowią dane osobowe, ale także to, że

¹¹²¹ E. Schmidt-Aßmann, *Dogmatyka prawa administracyjnego. Bilans rozwoju, reformy i przyszłych zadań*, Warszawa 2022, s. 130.

¹¹²² Por. podrozdział 3.5.1. rozprawy.

¹¹²³ Por. podrozdział 2.3. rozprawy.

te same dane (informacje) mogą nie mieć charakteru danych osobowych, gdy posiadane są przez jeden podmiot i nabyć ten charakter, gdy znajdują się w posiadaniu innego podmiotu. Oznacza to, że pojęcie danych osobowych jest nieostre. Skutkiem tego jest nie tylko nieostry zakres kompetencji organów ochrony danych osobowych na podstawie RODO, ale także trudność w ustaleniu, jakie sprawy (podlegające kontroli niezależnego organu) objęte są hipotezą art. 8 ust. 3 KPP.

Ta nieostrość ujawnia się w rzeczywistości transformacji cyfrowej, w której dane osobowe są węzłowym aktywem niematerialnym obecnym we wszystkich sektorach gospodarki. Powoduje to normowanie przetwarzania danych osobowych w niezwykle licznych aktach prawnych na poziomie unijnym i krajowym¹¹²⁴. Ta wzmożona aktywność prawodawcy wywołała potrzebę jej systematyzacji dla prowadzenia badań i stosowania oraz wykładni prawa. Próbowano tego dokonać przez wyodrębnienie nowej kompleksowej gałęzi prawa i dyscypliny nauk prawnych, obierając za kryterium przedmiot regulacji. W literaturze proponowano różne nazwy dla tej nowej gałęzi prawa, których znaczenia zakresowo zachodzą na siebie, ale nie są tożsame, na przykład „prawo nowych technologii”¹¹²⁵ (419 wyników w SIP LEX), „prawo danych osobowych” (179 wyników w SIP LEX), „prawo ochrony danych osobowych”¹¹²⁶ (464 wyników w SIP LEX), „the law of global digitality” („prawo globalnej cyfryzacji”) ¹¹²⁷ i „prawo informatyczne” ¹¹²⁸ (101 wyników w SIP LEX) ¹¹²⁹. Z kolei prawodawca unijny w tych aktach prawnych posługuje się określeniem „prawa [dotyczącego] ochrony danych osobowych”, np. art. 1 ust. 5 Data Act¹¹³⁰. Sam fakt użycia różnych nazw dla tej nowej gałęzi oznacza, że w doktrynie nie ma jednomyślności co do kryterium jej wyodrębnienia. Konsekwencją tego jest, że zakresem znaczeniowym poszczególnych nazw objęte są różne akty prawne, w tym także akty prawne normujące zagadnienia prawa prywatnego (na przykład, akty prawne normujące ochronę prawnoautorską w Internecie¹¹³¹ zaliczyć można do „prawa nowych technologii”, ale nie do „prawa ochrony danych osobowych”, niemniej elementy realizacji tej ochrony prawnoautorskiej dotyczyć będą także

¹¹²⁴ Por. podrozdział 2.5. rozprawy.

¹¹²⁵ Np. K. Flaga-Gieruszyńska, J. Gołaczyński, A. M. Arkuszewska et al., *Prawo nowych technologii*, Warszawa 2021.

¹¹²⁶ Np. P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019.

¹¹²⁷ C. M. Kettemann, A. Peukert, *The law of global digitality*, Taylor & Francis, 2022.

¹¹²⁸ G. Szpor, *Jawność i jej ograniczenia*, t. 1: *Idee i pojęcia*, Warszawa 2016, s. 266-267.

¹¹²⁹ Wszystkie wyszukiwania w SIP LEX, o którym mowa w tym zdaniu na dzień 14 stycznia 2024 r.

¹¹³⁰ Analiza relacji zakresu przedmiotowego aktów prawnych w obszarze referencyjnym do RODO została dokonana w rozdziale 2 rozprawy.

¹¹³¹ Przykładowo, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. Urz. UE L z 2019 r. nr 130, s. 92).

przetwarzania danych osobowych). Utrudnia to stanowienie oraz stosowanie i wykładnię prawa przez podmioty administrujące w tym obszarze. Przykładowo, w odniesieniu do zakresu kompetencji organów ochrony danych osobowych utrudnia to wyznaczenie zakresu spraw, które objęte są hipotezą art. 8 ust. 3 KPP. Byłoby to możliwe, gdyby dokonać konwencyonalnego wyznaczenia granic „prawa ochrony danych osobowych” albo „prawa danych” i w ten sposób delimitować obszar kompetencji organów ochrony danych osobowych. Chroniłoby to ich niezależność, która może być obecnie zagrożona na skutek nowych aktów prawnych scharakteryzowanych w niniejszej rozprawie przez faktyczne ograniczanie zakresu kompetencji organów ochrony danych osobowych na rzecz pomiotów administrujących ustanowionych na podstawie tych aktów, których niezależność nie jest jednak zagwarantowana przez prawo pierwotne UE (KPP).

Chociaż różnice między zakresami tych nazw nie są przedmiotem pogłębionej analizy w tej rozprawie, to wymaga wskazania, że różnica między „prawem ochrony danych osobowych” a „prawem danych osobowych”, chociaż jest nieznaczna, to występuje. Sprowadza się do tego, że pierwszy termin odnosi się do „ochrony” danych osobowych, wskazując na kryterium celu aktów prawnych (ochronę tych danych), podczas gdy drugi termin odnosi się tylko do „danych osobowych” jako przedmiotu regulacji, a zatem jego zakres jest szerszy, ponieważ obejmuje także te akty, których przedmiotem regulacji są dane osobowe, ale ich ochrona nie musi być podstawowym celem tych aktów (to, na przykład, DGA i Data Act). W niniejszej rozprawie konsekwentnie posługiwano się zwrotem „akty prawne w obszarze przetwarzania danych osobowych”, aby przedmiotem analizy objąć nie tylko akty prawne zaliczane do „prawa ochrony danych osobowych”, ale, szerzej, także te akty prawne, które regulują przetwarzanie danych osobowych rozumiane w sposób zdefiniowany w RODO, co pozwala w ujęciu funkcjonalnym pojąć zjawisko krzyżowania się kompetencji organów tak, jak jawi się ono z perspektywy podmiotów administrujących i nadzorowanych.

W literaturze ten taksonomiczny problem ujmowany w perspektywie szerokiego pojmowania danych osobowych jest krytykowany jako pogłębiający nieporządek w prawodawstwie, który wzmocniony jest rozszerzającą wykładnią pojęcia danych osobowych w orzecznictwie. N. Purtova zasadnie wskazała, że szerokie pojęcie danych osobowych w powiązaniu z rozwojem technicznym prowadzącym w kierunku możliwości identyfikacji niemal każdej informacji jako danych osobowych prowadzi do tego, że „prawo ochrony danych osobowych” stanie się „prawem wszystkiego” („*law of everything*”), co uczyni je niemożliwym do skutecznego stosowania (to znaczy prowadzącego do zapewnienia faktycznej ochrony praw

i wolności osób fizycznych w związku z przetwarzaniem danych osobowych)¹¹³². O tym, że ten pogląd jest podzielany w literaturze i stanowi przedmiot pogłębionej refleksji świadczy, że artykuł z 2017 r., w którym autorka sformułowała powyższy pogląd cytowany był ponad 300 razy¹¹³³. Kontynuując rozważania N. Purtovej, O. Lynskey argumentuje, że poszerzenie normatywnej ochrony danych osobowych na podstawie RODO przez przyjęcie rozszerzającej wykładni pojęć podstawowych dla zakresu przedmiotowego i podmiotowego RODO w praktyce osłabia skuteczności tej ochrony i prowadzi do wątpliwości co do przyjętego sposobu regulacji¹¹³⁴ (*Meaningless Law on the Books?*¹¹³⁵). Autorka ta analizuje rolę organów ochrony danych osobowych jako „regulatorów wszystkich”, wskazując, że szeroki (horyzontalny) zakres podmiotowy RODO powoduje, że podmioty nadzorowane wywodzą się z różnych sektorów, nie tworząc „tej samej wspólnej społeczności interpretacyjnej” („*the same cohesive interpretive community*”) tak jak jest to w przypadku regulacji sektorowych (np. energetycznej)¹¹³⁶. Utrudnia to zachowanie spójności (*cohesion*) pojmowania praw i obowiązków wynikających z RODO, co w konsekwencji zmniejsza skuteczność stosowanego tego prawa¹¹³⁷.

W literaturze zaproponowano rozmaite rozwiązania dla tego problemu¹¹³⁸. Przykładowo, w anglojęzycznej doktrynie M. Guihot, posługując się terminem „prawo technologii” (*technology law*), dokonał weryfikacji, czy brak jest jemu spójności (*field coherence*)¹¹³⁹, rozumianej jako cztery elementy: 1) redukcjonistyczne skupienie się na wewnętrznym sposobie rozumienia w ramach kompleksowej gałęzi prawa; 2) argumentowanie przez odwoływanie się do podstawowych zasad właściwych dla danej kompleksowej gałęzi prawa; 3) postulowanie potrzeby przemyślanego, linearnego rozwój instytucji motywowanego historycznie; oraz 4)

¹¹³² N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, Law Innov. Technol. 2018, Vol. 10, No. 1 <https://doi.org/10.1080/17579961.2018.1452176> (dostęp: 20.09.2024 r.), s. 40-41.

¹¹³³ Google Scholar, https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=The+law+of+everything.+Broad+concept+of+personal+data+and+future+of+EU+data+protection+law&btnG= (dostęp: 20.01.2024 r.).

¹¹³⁴ O. Lynskey, *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.), s. 297.

¹¹³⁵ O. Lynskey, *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.), s. 317.

¹¹³⁶ O. Lynskey, *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.), s. 326.

¹¹³⁷ O. Lynskey, *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.), s. 326.

¹¹³⁸ Por. G. Szpor, *Wprowadzenie [w:] Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 7-9.

¹¹³⁹ M. Guihot, *Coherence in technology law*, Law Innov. Technol. 2019, Vol. 11, No. 2, s. 311.

wysoki poziom specyfikacji instytucji¹¹⁴⁰. M. Guihot postuluje, aby ideą integrującą „prawo technologii” były ryzyka, które mogą powstać w związku z rozwojem danej technologii, co pozwoliłoby zakwalifikować do „prawa technologii” te akty prawne, które mogą ograniczyć te ryzyka spowodowane daną technologią¹¹⁴¹.

Takie próby wyróżniania gałęzi prawa w oparciu o kryterium przedmiotu regulacji były obiektem intensywnej dyskusji w literaturze anglojęzycznej w odniesieniu do „prawa cybernetycznego” (*cyberlaw*) już w latach 90. ubiegłego wieku. F.H. Easterbrook w 1996 r. użył ironicznego terminu „prawo konia” (*law of horse*) na określenie „prawa cybernetycznego” rozumianego jako kompleksowa gałąź prawa obejmująca akty prawne regulujące Internet we wczesnej fazie jego rozwoju¹¹⁴². Opowiedział się on przeciwko wyodrębnieniu takiej gałęzi, argumentując, że optymalnym sposobem „poznania prawa mającego zastosowanie do specjalistycznych obszarów jest studiowanie ogólnych zasad. Wiele spraw dotyczy sprzedaży koni; inne dotyczą osób kopniętych przez konie; jeszcze inne dotyczą licencjonowania i wyścigów koni, opieki weterynaryjnej nad końmi lub nagród na pokazach koni. Jakikolwiek próby zebrania tych wątków w ramach kursu zatytułowanego „Prawo konia” są skazane na płytkość i pominięcie unifikujących zasad”¹¹⁴³. Kluczowy w jego rozumieniu jest zatem brak „unifikujących zasad”, co oznacza, że odrzuca on przedmiot regulacji jako adekwatne kryterium wyodrębnienia kompleksowej gałęzi prawa, odmawiając wartości poznawczej takiemu zabiegowi. Z argumentami F.H. Easterbrook’a nie zgodził się harwardzki akademik L. Lessing, publikując odpowiedź *The Law of the Horse: What Cyber Law Might Teach* (*Prawo konia: czego może nauczyć prawo cybernetyczne*)¹¹⁴⁴. Artykuł ten, zgodnie z Google Scholar, cytowany był ponad 1.500 razy w literaturze, co świadczy o znaczeniu sporu między Lessingiem a Easterbrook’a w kształtowaniu taksonomii w obszarze regulacji związanym z transformacją cyfrową¹¹⁴⁵. Lessing argumentuje, że wyróżnienie „prawa cybernetycznego” jest zasadne z uwagi na unikalne cechy „cyberprzestrzeni”, które powodują, że regulacje

¹¹⁴⁰ M. Guihot, *Coherence in technology law*, Law Innov. Technol. 2019, Vol. 11, No. 2, s. 315.

¹¹⁴¹ M. Guihot, *Coherence in technology law*, Law Innov. Technol. 2019, Vol. 11, No. 2, s. 312.

¹¹⁴² F. H. Easterbrook, *Cyberspace and the Law of the Horse*, „The University of Chicago Legal Forum” 1996, Vol. 1996, No 1, s. 207-216. Artykuł ten, zgodnie z Google Scholar, cytowany był ponad 1.000 razy w literaturze; por. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Law+of+the+Horse+&btnG= (dostęp: 6.01.2024 r.).

¹¹⁴³ F. H. Easterbrook, *Cyberspace and the Law of the Horse*, „The University of Chicago Legal Forum” 1996, Vol. 1996, No 1, s. 207.

¹¹⁴⁴ L. Lessig, *The Law of the Horse: What CyberLaw Might Teach*, „Harvard Law Review” 1999, Vol. 113, No. 2, s. 501-549.

¹¹⁴⁵ Stan na dzień 6.01.2024 r. Por. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Law+of+the+Horse+&btnG=

w fizycznej przestrzeni są nieskuteczne¹¹⁴⁶. Wymaga to rozważenia sposobu regulacji spraw w cyberprzestrzeni w sposób odmienny od tego w fizycznej przestrzeni, co powoduje, że wyróżnienie „prawa cybernetycznego” ma wartość poznawczą i jest funkcjonalne, ponieważ pozwala prowadzić zunifikowaną dyskusję o sposobie regulacji w cyberprzestrzeni, w tym o podstawach aksjologicznych tej regulacji, co winno doprowadzić do przyjęcia ujednoliconej (skutecznej) kombinacji sposobów regulacji¹¹⁴⁷.

Z kolei w nowszej literaturze (2021 r.) T. Streinz sugeruje zasadność wyodrębnienia „europejskiego prawa danych”¹¹⁴⁸ jako kompleksowej gałęzi prawa, która obejmuje nie tylko akty prawne nakierowane na ochronę danych osobowych (przede wszystkim RODO i Dyrektywa LED określone jako „prawo ochrony danych osobowych”), ale także akty prawne regulujące przetwarzanie danych nakierowane na inne cele przeważające niż ich ochrona, oraz regulację przetwarzania danych nie-osobowych („europejskie prawo danych nieosobowych”; „europejskie prawo własności danych”; „europejskie prawo dostępu do danych”¹¹⁴⁹. Zdaniem tego autora, „europejskie prawo danych” *sensu largo* mogłoby obejmować także „prawo bezpieczeństwa danych, łączące elementy ochrony danych, prawa telekomunikacyjnego i prawa cyberbezpieczeństwa”, „unijne prawo usług (cyfrowych), zgodnie z którym dane mogą być usługą samą w sobie lub nośnikiem, za którego pośrednictwem świadczone są usługi”¹¹⁵⁰, a także akty prawne regulujące sprawy dotyczące własności danych (np. ochrony własności intelektualnej związanej z bazami danych) i dostępu do danych¹¹⁵¹ (np. prawo dostępu do informacji publicznej). Prowadziłoby do objęcia zakresem tak rozumianego „europejskiego prawa danych” także aktów prawnych regulujących cyberbezpieczeństwo, DMA i DSA. Kryterium wyróżnienia dla tego autora byłby zatem przedmiot regulacji, czyli dane (zarówno osobowe, jak i nieosobowe). Należy uznać tak rozumiany zakres terminu „europejskiego prawa danych” za zbyt szeroki, aby jego przyjęcie mogło pełnić funkcję konsolidującą, a to z uwagi

¹¹⁴⁶ L. Lessig, *The Law of the Horse: What CyberLaw Might Teach*, „Harvard Law Review” 1999, Vol. 113, No. 2, s. 503-505.

¹¹⁴⁷ L. Lessig, *The Law of the Horse: What CyberLaw Might Teach*, „Harvard Law Review” 1999, Vol. 113, No. 2, s. 501-502, 548-549.

¹¹⁴⁸ T. Streinz, *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, edited by P. Craig, G. de Búrca, Oxford 2021, <https://ssrn.com/abstract=3762971> (dostęp: 20.09.2024 r.). Por. także N. Riis, *Shaping the Field of EU Data Law*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law” 2023, Vol. 14, No. 1, s. 54-65.

¹¹⁴⁹ T. Streinz, *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, edited by P. Craig, G. de Búrca, Oxford 2021, <https://ssrn.com/abstract=3762971> (dostęp: 20.09.2024 r.), s. 20.

¹¹⁵⁰ T. Streinz, *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, edited by P. Craig, G. de Búrca, Oxford 2021, <https://ssrn.com/abstract=3762971> (dostęp: 20.09.2024 r.), s. 20.

¹¹⁵¹ T. Streinz, *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, edited by P. Craig, G. de Búrca, Oxford 2021, <https://ssrn.com/abstract=3762971> (dostęp: 20.09.2024 r.), s. 26.

na niezwykle dużą liczbę aktów prawnych regulujących dane i liczbę podmiotów administrujących ustanowionych na ich podstawie, co powodowałoby do braku waloru skuteczności, jaka mogłaby zostać związana z takim wydzieleniem z przyczyn wskazanych w analizie „prawa ochrony danych osobowych” jako „prawa wszystkiego”. Kryterium przedmiotowe w postaci danych należy uznać za przydatne z tej przyczyny, że pojęcie „danych” jest klarowniejsze (ponieważ jest szersze) niż pojęcie „danych osobowych”; wymagałoby jednak uzupełnienia o dodatkowe kryteria, które konwencjonalnie ograniczałyby szeroki zakres tak wyodrębnionego „unijnego prawa danych”¹¹⁵².

Przegląd stanowisk w literaturze prowadzi do konkluzji, że dokonanie spójnego i trwałego wydzielania aktów prawnych w obszarze przetwarzania danych osobowych do odrębnej kompleksowej gałęzi prawa stanowi wyzwanie, ponieważ jej granice, struktura i nazwa nie są rozumiane jednolicie¹¹⁵³, w tym brak jest zgody co do sposobu dokonania wydzielenia tak, aby zapewnić możliwie szeroką ochronę prawa podstawowych (czego konsekwencją jest szerokie pojęcie danych osobowych), a jednocześnie zachować spójność takiej gałęzi. Z drugiej strony, takie działania wydają się niezbędne dla uporządkowania chaotycznej siatki pojęciowej w obszarze przetwarzania danych osobowych, ustalenia znaczenia relacji *lex generalis* - *lex specialis* między aktami prawnymi w tym obszarze¹¹⁵⁴ i stabilnego instrumentarium współpracy między podmiotami administrującymi z nadrzędną rolą organów ochrony danych osobowych, których istnienie i niezależność chroni KPP, co było podkreślane. Brak konsekwentnego wyodrębnienia kompleksowej gałęzi prawa w tym obszarze pogłębia niepewność co do pozycji organów ochrony danych osobowych względem innych podmiotów administrujących w tym obszarze. Ta niepewność będzie wzrastać wraz z nowymi aktami prawnymi, które będą przyjmowane. Takie wyodrębnienie wymagałoby to ustalenia idei przewodniej umożliwiającej holistyczną i koherentną analizę¹¹⁵⁵.

Wyodrębnienie prawa danych jako kompleksowej gałęzi prawa stanowi pierwszy postulat *de lege ferenda* niniejszej rozprawy doktorskiej (por. podrozdział 5.7.1.). Brak jasności co do sposobu wyodrębnienia kompleksowej gałęzi prawa w tym obszarze stanowi problem dla stanowienia, stosowania i wykładni prawa, który narastał będzie wraz ze zwiększeniem liczby

¹¹⁵² Por. podrozdział 5.7.1. niniejszej rozprawy.

¹¹⁵³ Pogląd Eberharda Schmidta-Almanna przytoczony za G. Szpor, *Wprowadzenie* [w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 7-8.

¹¹⁵⁴ Por. podrozdział 4.4.1. niniejszej rozprawy.

¹¹⁵⁵ G. Szpor, *Wprowadzenie* [w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 7-8.

aktów prawnych, pogłębiając istniejący już chaos¹¹⁵⁶. Konsekwentne wyodrębnienie kompleksowej gałęzi jest zatem niezbędne dla zmniejszenia negatywnych skutków zjawiska krzyżowania się kompetencji, ponieważ umożliwiało to będzie zmniejszenie tego chaosu i zwiększenie spójności¹¹⁵⁷ m.in. przez wyznaczenie granic ujednolicenia siatki pojęciowej. Pozwoliłoby to także wyznaczyć granice tej gałęzi, a następnie w ramach tych granic przyjąć jej zasady, które pomagałyby w jednolitej wykładni, i ustalić kompetentne podmioty administrujące. W konsekwencji pozwoliłoby to przyznać pogłębione kompetencje współpracy między nimi, jak i między podmiotami administrującymi w kompleksowych gałęziach prawnych, które jednak są zakresowo zbliżone (patrz postulat *de lege ferenda* nr 3 poniżej). Konsekwentne wyodrębnienie kompleksowej gałęzi prawa prowadziłoby również do wyodrębnienia kompleksowej dziedziny nauk prawnych, co miałoby porządkującą wartość dla dydaktyki i badań naukowych, dając możliwość syntetycznej analizy nowych zjawisk o naturze prawnej wykraczającej poza granice dotychczas wyodrębnionych gałęzi¹¹⁵⁸.

5.6. PRZYCZYNA NR 5: WYWAŻENIE RÓŻNYCH CELÓW PRZEZ PODMIOTY ADMINISTRUJĄCE

Jak wskazane zostało w rozdziale 1 niniejszej rozprawy (podrozdział 1.5.4.), cele wyznaczają długoterminowy pożądany efekt działania podmiotu administrującego¹¹⁵⁹, a postać normatywna norm celowościowych często zawiera odwołanie do obranego dobra lub wartości¹¹⁶⁰. Konsekwentnie, weryfikacja realizacji norm celowościowych przez podmioty administrujących dokonywana może być z perspektywy osiągnięcia tego celu, zatem

¹¹⁵⁶ Por. także tezy przedstawione w artykule Laurena E. Elricka o potrzebie stworzenia spójnego „ekosystemu” dla ochrony prawa do prywatności z uwagi na mnogość interesariuszy i konieczność balansowania z innymi prawami podstawowymi (L. E. Elrick, *The ecosystem concept: a holistic approach to privacy protection*, Int. Rev. Law Comput. Technol. 2021, Vol. 35, No. 1, DOI: 10.1080/13600869.2020.1784564) (dostęp: 20.09.2024 r.).

¹¹⁵⁷ M. Guihot, *Coherence in technology law*, Law Innov. Technol. 2019, Vol. 11, No. 2, s. 9.

¹¹⁴³ *Publiczne prawo gospodarcze*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2018, s. 21.

¹¹⁵⁹ M. Szyrski, § 1. *Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń*, II. *Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania. Zastosowanie pojęć teoretycznych w ustawach o dostępie do informacji publicznej oraz o ochronie informacji niejawnych*, 2. *Zadanie i cel*, [w:] *Jawność i jej ograniczenia. Zadania i kompetencje*, t. 9, red. G. Szpor, B. Szmulik, Warszawa 2015, Legalis. Por. także G. Szpor, 2. *Cele i zadania w nauce prawa administracyjnego* [w:] *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza*, red. A. Matan, Warszawa 2022, SIP LEX.

¹¹⁶⁰ M. Maciejewski, *Normy celowościowe i normy zadaniowe w prawie administracyjnym. Dobra chronione jako ustawowe cele organów administracji* [w:] *Dobra chronione w prawie administracyjnym*, red. Z. Duniewska, Łódź 2014, s. 55.

z perspektywy pojęcia skuteczności administracji publicznej¹¹⁶¹. W badanym obszarze ustanowionym organom administracji publicznej można przypisać określony cel, który albo wskazany został w przepisach ustanawiających dany podmiot, albo może być wywiedziony z celów danego aktu prawnego¹¹⁶². Przykładowo, celem organów ochrony danych osobowych jest „ochrona podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii” (art. 51 ust. 1 RODO), cel organów do spraw cyberbezpieczeństwa ustanowionych na podstawie Dyrektywy NIS 2 można zidentyfikować jako „osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego” (art. 1 ust. 1 Dyrektywy NIS 2) a cel działalności GIIF to „przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu” (art. 1 pkt 1 Ustawy o AML)¹¹⁶³.

Wszystkie te cele współlistnieją i realizowane są w ramach jednego systemu administracji publicznej. Ich jednoznaczne określenie może okazać się w praktyce trudne z powodu ewoluujących zewnętrznych okoliczności¹¹⁶⁴. Cele te stanowią – z uwagi na to, że analizowane akty prawne są albo aktami prawa unijnego albo stanowią ich krajową implementację – emanację celów Unii ustanowionych w art. 3 TUE. Niektóre z tych celów powiązane są bezpośrednio z prawami podstawowymi, na przykład cele organów ochrony danych osobowych powiązane są bezpośrednio z prawem do prywatności (art. 7 KPP) i prawem do ochrony danych osobowych (art. 8 KPP)¹¹⁶⁵, podczas gdy cele organów do spraw cyberbezpieczeństwa można pośrednio powiązać z tymi samymi prawami, jak i prawem do wolności i bezpieczeństwa osobistego (art. 6 KPP) a cele GIIF należy uznać za słabo związane z prawami podstawowymi (możliwe byłoby powiązanie z przywołanym art. 6 KPP), a silnie z celem należycie funkcjonującego rynku wewnętrznego (art. 3 ust. 3 TUE).

¹¹⁶¹ M. Maciejewski, Normy celowościowe i normy zadaniowe w prawie administracyjnym. Dobra chronione jako ustawowe cele organów administracji [w:] *Dobra chronione w prawie administracyjnym*, red. Z. Duniewska, Łódź 2014, s. 57, 61.

¹¹⁶² Więcej w przedmiocie celów w prawie unijnym i pojęcia skuteczności prawa unijnego: J. Wegner-Kowalska, 2. *Determinanta celów interwencji prawnej* [w:] *Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej*, Warszawa 2017, SIP LEX.

¹¹⁶³ W Dyrektywie AML 5: „zapobieganie wykorzystywaniu unijnego systemu finansowego do prania pieniędzy i finansowania terroryzmu” (art. 1 ust. 1).

¹¹⁶⁴ J. Wegner-Kowalska, 3. *Problem oceny skutków interwencji prawnej* [w:] *Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej*, Warszawa 2017.

¹¹⁶⁵ Prawo do prywatności (art. 7 KPP) i prawo do ochrony danych osobowych (art. 8 KPP), które na poziomie konstytucyjnym objęte są ochroną w art. 47 i 51 Konstytucji RP, stanowią odrębne, ale powiązane ze sobą prawa. Ich relacja jest przedmiotem badania w literaturze, na przykład O. Lynskey, *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order*, „International & Comparative Law Quarterly” 2014, Vol. 63, Iss. 3, s. 569-597. R. Gellert, S. Gutwirth, *The legal construction of privacy and data protection*, CLSR 2013, Vol. 29, No. 5.522-530.

Ostatecznie wszystkie te cele są komplementarne względem siebie, ponieważ służą jednemu dobru wspólnemu, jednak w odizolowaniu istnieje ryzyko, że realizacja jednego z nich może odbywać się kosztem drugiego w ujęciu prakseologicznym¹¹⁶⁶. Przykładowo, z perspektywy osiągnięcia odizolowanego celu „przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu” zasadne byłoby możliwie szerokie przetwarzanie wszystkich danych osobowych klientów instytucji finansowych, w tym także kopiowanie wszystkich dokumentów tożsamości, podczas gdy z perspektywy osiągnięcia odizolowanego celu „ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych” zasadne byłoby ograniczenie przetwarzania danych osobowych wyłącznie do niezbędnego minimum (zasada minimalizacji w art. 5 ust. 1 lit. c RODO). Ponieważ cele te nie są od siebie jednak normatywnie odizolowane, powinny być realizowane tak, aby osiągnięcie jednego celu dokonywane było z poszanowaniem drugiego celu. Wymaga to balansowania między tymi celami przez podmioty administrujące w procesie wykonywania kompetencji prowadzących do realizacji celu, z którego osiągnięcia podmioty administrujące są rozliczane. Prawodawca dostarcza normatywnych podstaw do tego balansowania, na przykład z jednej strony przez unormowanie, że wykonanie określonych aktów prawnych powinno pozostawać „bez uszczerbku dla” RODO¹¹⁶⁷, z drugiej zaś przez dopuszczenie ograniczeń zakresu obowiązków administratorów i podmiotów przetwarzających oraz praw podmiotów danych w prawodawstwie unijnym lub krajowym zgodnie z art. 23 ust. 1-2 RODO. Prawo do ochrony danych osobowych nie jest bowiem prawem bezwzględny, powinno być postrzegane „w kontekście jego funkcji społecznej”, a przetwarzanie danych osobowych „należy zorganizować w taki sposób, aby służyło ludzkości” (motyw 4 RODO), aby zapewnić „swobodny przepływ danych osobowych między państwami członkowskimi” (art. 1 ust. 1 RODO). Nadto, działalność podmiotów administrujących podlega sądowej kontroli administracji, co pozwala sądom administracyjnym w zakresie ich kognicji dokonywać aktów balansowania w indywidualnych sprawach.

Wyzwanie stanowi, w jaki sposób podmioty administrujące powinny dokonać tego balansowania w konkretnych sprawach. Jest to dodatkowo utrudnione z uwagi na wybór techniki prawodawczej spowodowany potrzebą zapewnienia neutralności technologicznej, czego konsekwencją jest regulacja przy pomocy zasad, terminów nieostrych i podejścia

¹¹⁶⁶ Co nie jest charakterystyczne tylko do aktów prawnych w obszarze ochrony danych osobowych, lecz właściwe jest dla całego prawa administracyjnego materialnego, które jest obszerne i reguluje rozmaite obszary życia społecznego.

¹¹⁶⁷ Rozważania w przedmiocie klauzuli „bez uszczerbku” w podrozdziale 4.4.

opartego na ryzyku¹¹⁶⁸. Jak zostało wykazane, oznacza to przeniesienie zasadniczej części konkretyzacji prawa na podmioty administrujące w trakcie wykonywania przez nie kompetencji w trakcie stosowania prawa, w tym przy wykorzystaniu reguł celowościowych wykładni, gdzie cel stanowi argument interpretacyjny¹¹⁶⁹. Z perspektywy podmiotów nadzorowanych, które objęte są zakresem podmiotowym wszystkich tych aktów prawnych i ryzykiem nałożenia sankcji przez każdy z tych podmiotów administrujących z osobna oznacza to prowadzenie działalności w zwiększonej niepewności prawnej w odniesieniu do sytuacji, w których stosowanie prawa wymaga od podmiotów administrujących dokonania balansowania tych celów. Stąd też to balansowanie (wyważenie) przez sam fakt jego istnienia powoduje wzmocnienie negatywnych skutków wywołanych zjawiskiem krzyżowania się kompetencji podmiotów administrujących w tym obszarze. Aby złagodzić negatywne skutki wynikające z konieczności balansowania celów, konieczne jest ustanowienie efektywnych instrumentów współpracy między podmiotami administrującymi¹¹⁷⁰.

Balansowanie celów przy wykonywaniu kompetencji przez podmioty administrujące winno mieć podstawę prawną. Może nią być w szczególności unormowanie o pozostawianiu danego aktu prawnego „bez uszczerbku” dla RODO lub też to, że podmiot administrujący w określonej konfiguracji sam jest administratorem danych osobowych, a zatem zobowiązany jest do wykonywania obowiązków w RODO. Obowiązek państw członkowskich ustanowienia efektywnego balansowania celów między podmiotami administrującymi może być wyprowadzony także z zasady lojalnej współpracy UE i państw członkowskich zgodnie z art. 4 ust. 3 TUE,¹¹⁷¹. Pośrednio obowiązek balansowania celów może być również wywiedziony z art. 51 ust. 1 KPP, który rozstrzyga o wiążącym charakterze KPP wobec organów państw członkowskich „wyłącznie w zakresie, w jakim stosują one prawo”¹¹⁷² w zakresie, w jakim cele tych organów związane są z zapewnieniem ochrony praw podstawowych, o których mowa w KPP, co w obszarze przetwarzania danych osobowych będzie miało miejsce z zasady.

¹¹⁶⁸ Por. podrozdział 5.3. powyżej.

¹¹⁶⁹ L. Leszczyński, Rozdział VI. Wykładnia celowościowo-funkcjonalna przepisów prawa administracyjnego, [w:] Wykładnia w prawie administracyjnym, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2015, s. 286-288.

¹¹⁷⁰ Por. postulat *de lege ferenda* przedstawiony w podrozdziale 5.7.3 rozprawy.

¹¹⁷¹ Por. analizę wyroku TS z 4.07.2023 r., C-252/21 w podrozdziale 2.6.3.1. rozprawy. Por. Wyrok TS z 4.07.2023 r., C-252/21, Meta Platforms Inc., Anciennement Facebook Inc. I In. przeciwko Bundeskartellamt, SIP LEX nr 3576613

¹¹⁷² Komentarz do art. 51, pkt 2, nb 2 [w:] Karta Praw Podstawowych Unii Europejskiej. Komentarz, red. A. Wróbel Warszawa 202.

Ustalenie istnienia obowiązku balansowania celów przez podmioty administrujące prowadzi do zagadnienia, w jaki sposób to balansowanie powinno zostać dokonane w konkretnych sprawach. Chociaż nie wszystkie cele działalności podmiotów administrujących w obszarze referencyjnym związane są bezpośrednio z ochroną praw podstawowych chronionych także na podstawie Konstytucji RP, to fakt, że niektóre z nich tą ochroną są objęte (jak prawo do prywatności i prawo do ochrony danych osobowych¹¹⁷³)¹¹⁷⁴, znaczy, że możliwe jest zastosowanie do tego balansowania testu proporcjonalności z art. 31 ust. 3 Konstytucji RP razem z testem ograniczenia w korzystaniu praw i wolności w art. 52 ust. 1 KPP¹¹⁷⁵ rozumianych jako „mechanizm usuwania kolizji norm” w konkretnym stanie faktycznym bez apriorycznego rozstrzygania o pierwszeństwie jednej zasady wobec drugiej¹¹⁷⁶. Powinien to być pierwszy etap balansowania, który prowadziłby do kierunkowego ustalenia, w jaki sposób cele mogłyby zostać wyważone. To winno prowadzić do drugiego etapu, w którym kryterium stanowiłoby ustalenie, w jaki sposób w konkretnym stanie faktycznym nastąpiłoby ograniczenie zasad przetwarzania danych osobowych ustanowione w RODO (art. 5 RODO) i jakie byłoby dla tego uzasadnienie¹¹⁷⁷. Taką trafną koncepcję zaproponowała M. Sakowska-Baryła w odniesieniu do wyważania zasad prawa w kontekście realizacji prawa do ochrony danych osobowych oraz praw dostępowych (przede wszystkim prawa dostępu do informacji publicznej)¹¹⁷⁸. Można ją zastosować do balansowania celów przez podmioty administrujące.

Art. 52 ust. 1 KPP normuje, że wszelkie ograniczenia w korzystaniu z praw i wolności muszą być przewidziane przez prawo, szanować istotę prawa lub wolności, odpowiadać celom interesu ogólnego uznanym przez UE (lub potrzebie ochrony praw i wolności innych osób) oraz spełniać test konieczności i proporcjonalności. Z kolei, zgodnie z art. 31 ust. 3 Konstytucji RP, „ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być

¹¹⁷³ O konstytucjonalizacji prawa do ochrony danych osobowych por. Rojszczak, Marcin. (2023). Konstytucjonalizacja prawa do ochrony danych osobowych – proces trwający czy zakończony?. Przegląd Konstytucyjny. 75-111. 10.4467/25442031PKO.23.011.18277.

¹¹⁷⁴ P. Sarnecki [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 2, red. L. Garlicki, M. Zubik, Warszawa 2016, art. 51.

¹¹⁷⁵ Analizą nie objęto EKPCz. W odniesieniu do tego zagadnienia por. przykładowo: M. Michalska, *Zasada proporcjonalności w orzecznictwie TK i ETPC–analiza prawno-porównawcza*, „Krytyka Prawa” 2022, Vol. 14, No. 2 (2022): 80-98.

¹¹⁷⁶ M. Sakowska-Baryła, 5.2. Zagadnienie wyważania zasad prawa [w:] *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022, SIP LEX.

¹¹⁷⁷ M. Sakowska-Baryła, 5.6. Wyważanie zasad w ujęciu warstwowym przy współstosowaniu RODO, ustawy o dostępie do informacji publicznej i ustawy o otwartych danych [w:] *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

¹¹⁷⁸ M. Sakowska-Baryła, 5.6. Wyważanie zasad w ujęciu warstwowym przy współstosowaniu RODO, ustawy o dostępie do informacji publicznej i ustawy o otwartych danych [w:] *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób”, przy czym „nie mogą naruszać istoty wolności i praw”. Zarówno z zestawienia brzmienia tych przepisów, jak i analizy poglądów doktryny wynika, że oba testy limitujące różnią się od siebie¹¹⁷⁹. Analiza każdego z nich z osobna¹¹⁸⁰, jak i ich wzajemnej relacji¹¹⁸¹ jest przedmiotem analiz w literaturze, które pozostają poza zakresem tej rozprawy (należy zaznaczyć jednak, że dla spełnienia testu z Konstytucji RP nie jest wystarczające samo spełnienie testu z KPP¹¹⁸²).

Na potrzeby tej rozprawy w odniesieniu do balansowania celów podmiotów administrujących, wskazać należy w uproszczeniu, że oba te testy obejmują zbadanie co najmniej trzech elementów: 1) naruszenia istoty prawa lub wolności; 2) proporcjonalności ingerencji; 3) niezbędności¹¹⁸³ (konieczności) ingerencji¹¹⁸⁴. Pojęcie istoty prawa lub wolności odnosi się do elementu podstawowego, którego brak powodowałby nieistnienie tego prawa lub wolności, co oceniać należy z perspektywy historycznego rozwoju danego prawa lub wolności¹¹⁸⁵. Przesłanka proporcjonalności w orzecznictwie TK obejmuje trzy kryteria: niezbędności („muszą być one niezbędne do ochrony interesu, z którym są powiązane”¹¹⁸⁶), przydatności („środki zastosowane przez prawodawcę muszą być w stanie doprowadzić do zamierzonych celów”¹¹⁸⁷) i proporcjonalności *sensu stricto* („ich efekty muszą pozostawać w proporcji do ciężarów nakładanych na obywatela”¹¹⁸⁸)¹¹⁸⁹. Wreszcie, w odniesieniu do elementu konieczności wskazać należy, że chodzi o takie rozwiązania, które ze wszystkich

¹¹⁷⁹ Komentarz do art. 51, nb 8 [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel Warszawa 2020,.

¹¹⁸⁰ Przykładowo dla art. 52 ust. 1 KPP: K. Lenaerts, *Limits on limitations: the essence of fundamental rights in the EU*, „German Law Journal” 2019, Vol. 20, No. 6., s. 779-793. Przykładowo dla art. 31 ust. 3 Konstytucji RP: L. Bosek, M. Szydło, *Komentarz do art. 31 [w:] Konstytucja RP, t. 1: Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, SIP Legalis.

¹¹⁸¹ Przykładowo: E. H. Morawska, *Prawa konstytucyjne człowieka i obywatela w Rzeczypospolitej Polskiej a prawa podstawowe Unii Europejskiej. Analiza porównawcza*, Prz.Sejm. 2009, nr 1, s. 31-54.

¹¹⁸² L. Bosek, M. Szydło, *Komentarz do art. 31 [w:] Konstytucja RP, t. 1: Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, nb 83, SIP Legalis.

¹¹⁸³ W KPP element niezbędności jest, samodzielną przesłanką, która nie jest uzależniona od celów ograniczeń tak jak w art. 31 ust. 3 Konstytucji RP; por. *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2020, Komentarz do art. 51, nb 18.

¹¹⁸⁴ E. H. Morawska, *Prawa konstytucyjne człowieka i obywatela w Rzeczypospolitej Polskiej a prawa podstawowe Unii Europejskiej. Analiza porównawcza*, Prz.Sejm. 2009, nr 1, s. 31-54, s. 41-42.

¹¹⁸⁵ L. Bosek, M. Szydło, *Komentarz do art. 31 [w:] Konstytucja RP, t. 1: Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, nb 153, SIP Legalis.

¹¹⁸⁶ Wyrok TK z 21.04.2004 r., K 33/03, OTK-A 2004, nr 4, poz. 31.

¹¹⁸⁷ Wyrok TK z 21.04.2004 r., K 33/03, OTK-A 2004, nr 4, poz. 31.

¹¹⁸⁸ Wyrok TK z 21.04.2004 r., K 33/03, OTK-A 2004, nr 4, poz. 31.

¹¹⁸⁹ L. Garlicki, K. Wojtyczek [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 2, red. M. Zubik, Warszawa 2016, art. 31, nb 45, SIP LEX.

dostępnych do osiągnięcia danego celu są najmniej uciążliwe¹¹⁹⁰, co oznacza, że element ten stanowi część szeroko rozumianej proporcjonalności, przynajmniej w polskim prawie konstytucyjnym¹¹⁹¹. Odniesienie tej uproszczonej w założeniu analizy do problemu balansowania celów przy wykonywaniu poszczególnych kompetencji przez podmioty administrujące prowadzi do wniosku, że akt balansowania winien być dokonywany tak, aby jego wynik nie doprowadził do naruszenia istoty innego celu. Powinno to następować przez dobór środków w taki sposób, aby doprowadziły do zamierzonego celu, ale jednocześnie były możliwie mało ingerujące w inny cel, a potencjalne wynikające z nich korzyści dla realizacji danego celu powinny być w proporcji do ograniczeń w realizacji innego celu.

Na marginesie należy wskazać, że ustanowienie komplementarnych, ale odrębnych celów działalności podmiotów administrujących wywiera wpływ na kulturę organizacyjną obsługujących je urzędów rozumianą w literaturze jako zespół cech cenionych przez uczestników organizacji pozwalający na odróżnienie jej od innych organizacji¹¹⁹² lub też jako „zespół odkrytych, ustanowionych i rozwiniętych przez grupę reguł postępowania”¹¹⁹³. Chociaż jest to zjawisko będące przedmiotem badania nauki o administracji, nie pozostaje bez wpływu na zjawisko krzyżowania się kompetencji organów analizowane w nauce prawa administracyjnego. Kultura organizacyjna powstaje jako efekt systematycznego działania organizacji realizowanego przez jej uczestników przy pomocy ustalonych wzorców zachowania, które prowadzą do pożądaných rezultatów, w konsekwencji wzmacniając te wzorce, co określane jest jako „idealizacja wspólnego doświadczenia”¹¹⁹⁴. Ponieważ normy celowościowe rozliczane są przez weryfikację realizacji tych celów (co z kolei wpływa na sposób wykonywania kompetencji przez podmioty administrujące¹¹⁹⁵), wpływają także na kulturę organizacyjną urzędów obsługujących podmioty administrujące, którym te cele zostały wyznaczone. Do kultury organizacyjnej urzędów obsługujących podmioty administrujące

¹¹⁹⁰ Komentarz do art. 51, nb 18 [w:] *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2020.

¹¹⁹¹ L. Bosek, M. Szydło, *Komentarz do Art. 31 [w:] Konstytucja RP*, t. 1: *Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, nb 109, SIP Legalis.

¹¹⁹² Pogląd S.P. Robbinsa. Przywołanie za E. Głowacka, *Kultura organizacyjna w procesie zarządzania administracją publiczną*, materiały Studenckiej Konferencji Naukowej, Rzeszów 2011, nr 1, <https://wspia.eu/media/bo3n1kzk/11-g%C5%82owacka-edyta.pdf> (dostęp: 20.09.2024 r.), s. 428–430.

¹¹⁹³ Pogląd E.H. Schein. Przywołanie za D. Bąk-Grabowska, *Kształtowanie kultury organizacyjnej w urzędach administracji samorządowej*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Nauki Społeczne” 2010, t. 2, nr 129, s. 256. E.H. Schein, *Organizational Culture and Leadership*, San Francisco-London: Jossey-Bass A Wiley Imprint 1986, s. 142-157.

¹¹⁹⁴ E. Głowacka, *Kultura organizacyjna w procesie zarządzania administracją publiczną*, materiały Studenckiej Konferencji Naukowej, Rzeszów 2011, nr 1, <https://wspia.eu/media/bo3n1kzk/11-g%C5%82owacka-edyta.pdf> (dostęp: 20.09.2024 r.), s. 66.

¹¹⁹⁵ Por. Z. Leoński, *Nauka administracji*, Warszawa 2010, s. 15, 38-40.

można zaliczyć m.in. przekonania urzędników na temat optymalnych reguł wykładni, w tym celowościowych i funkcjonalnych, oraz na temat zasadności nawiązywania współpracy z innymi podmiotami administrującymi. Znaczenie tych przekonań urzędników dla negatywnych skutków zjawiska krzyżowania się kompetencji (przede wszystkim niepewności prawnej po stronie podmiotów nadzorowanych) wzrasta w związku z technikami prawodawczymi zastosowanymi w obszarze przetwarzania danych osobowych (konkretyzacja prawa pozostawiona jest w znacznej części podmiotom administrującym w procesie jego stosowania) i ustanowieniem nieobligatoryjnych instrumentów współpracy między podmiotami administrującymi. Od tych przekonań zależy bowiem w jaki sposób wykonywane będą kompetencje podmiotów administrujących nakierowane na zwiększenie spójności między poszczególnymi aktami (byłoby to pożądane) bądź też raczej na szybszą realizację celów wynikających z właściwych im norm celowościowych z ograniczonym balansowaniem albo z pominięciem balansowania tych celów z innymi celami, co mogłoby być skorygowane dopiero na etapie sądowej kontroli administracji, jednak najpierw doprowadziłoby do pogłębienia niepewności prawnej.

5.7. POSTULATY *DE LEGE FERENDA*

W perspektywie tak scharakteryzowanych przyczyn zjawiska krzyżowania się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych, w odniesieniu do przedstawionego problemu badawczego sformułowano cztery postulaty *de lege ferenda*, które omówione zostaną z osobna niżej: 1) wyodrębnienie prawa danych jako odrębnej kompleksowej gałęzi prawa; 2) centralizacja struktury stosowania RODO wobec największych podmiotów nadzorowanych i ustanowienie organów ochrony danych jako organów właściwych dla stosowania aktów prawnych w obszarze przetwarzania danych osobowych; 3) wprowadzenie efektywnych instrumentów współpracy między podmiotami administrującymi stosującymi akty prawne w obszarze przetwarzania danych osobowych; 4) wprowadzenie rozwiązania typu klauzula „*safe harbour*” dla podmiotów nadzorowanych. Realizacja tych postulatów nie doprowadziłaby do całkowitego wyeliminowania tego problemu, ponieważ, jak wskazano, jego przyczyny mają charakter strukturalny, a przez ich realizację nie można tych strukturalnych przyczyn wyeliminować. Ich realizacja pozwoliłaby jednak zmniejszyć negatywne skutki spowodowane zjawiskiem krzyżowania się kompetencji i umożliwiłoby dalszy rozwój tego obszaru regulacji w sposób dojrzały i efektywniejszy.

5.7.1. POSTULAT NR 1: WYODRĘBNIE NIE PRAWA DANYCH JAKO ODREBNEJ KOMPLEKSOWEJ GAŁĘZI PRAWA

Zarówno zasadność, jak i kryterium wyodrębniania kompleksowych gałęzi prawa to skomplikowane zagadnienie teorii prawa dotyczące taksonomii dyscyplin prawa, a poglądy na jego temat są dalekie od jednoznacznych¹¹⁹⁶. Jednocześnie to teoretycznoprawne zagadnienie jest przedmiotem zainteresowania w szczegółowych naukach prawnych z powodu jego praktycznej użyteczności. Dlatego też było i pozostaje przedmiotem wielokrotnych ożywionych dyskusji w dogmatyce prawa, np. w odniesieniu do prawa gospodarczego, prawa energetycznego¹¹⁹⁷, czy prawa ochrony środowiska¹¹⁹⁸. Z uwagi na przedmiot tej rozprawy, postuluje się w niej, aby jako kompleksową gałąź prawa wyodrębnić „unijne prawo danych” (za T. Streinz)¹¹⁹⁹, a jako kryterium wyodrębnienia przyjąć, zgodnie z monistycznymi teoriami¹²⁰⁰, przedmiot regulacji – przetwarzanie danych (osobowych i nieosobowych), o ile jest to przeważający przedmiot regulacji. Poniżej uzasadniony zostanie wybór kryterium, a następnie przedstawione zostaną korzyści z tego wyodrębnienia dla zmniejszenia skutków krzyżowania się kompetencji.

Jako kryterium wyodrębnienia wybrane zostało przetwarzanie danych (osobowych i nieosobowych), o ile jest to przeważający przedmiot regulacji¹²⁰¹. Jest to dwojako nieostre kryterium. Po pierwsze, dlatego, że pojęcia danych osobowych i nieosobowych, w tym we wzajemnej ich relacji, są szerokie i niejasne¹²⁰². Nadto, na skutek postępu technicznego dane nieosobowe mogą stać się danymi osobowymi, a wiele zbiorów danych ma charakter mieszany – zawiera dane osobowe i nieosobowe¹²⁰³. Stąd też dokonanie takiego wyboru zmniejszałoby niepewności co do konieczności każdorazowej dystynkcji między danymi osobowymi

¹¹⁹⁶ G. Góralczyk, *Samodzielność pojęciowa prawa gospodarczego jako problem analitycznej teorii prawa*, „Acta Universitatis Wratislaviensis. Prawo” 2011, t. 312, nr 3337, s. 135-145.

¹¹⁹⁷ E. Kosiński, Czy istnieje prawo energetyczne?: Część 1: Przedmiot, podmioty i metoda regulacji prawa energetycznego, „Acta Universitatis Wratislaviensis. Prawo” 2022, nr 334, s. 787-790.

¹¹⁹⁸ J. Ciechanowicz-McLean, *Prawo ochrony środowiska jako kompleksowa dziedzina prawa – ustawa organiczna?* [w:] *Zagadnienia systemowe prawa ochrony środowiska*, red. P. Korzeniowski, Łódź 2015.

¹¹⁹⁹ T. Streinz, *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, edited by P. Craig, G. de Búrca, Oxford 2021, <https://ssrn.com/abstract=3762971> (dostęp: 20.09.2024 r.). Natomiast wyodrębnienie dokonane zostanie w inny sposób niż dokonał tego ten autor (scharakteryzowano powyżej).

¹¹⁸⁵ *Publiczne prawo gospodarcze*, red. R. Hauser, Z. Niewiadowski, A. Wróbel, Warszawa 2018, s. 19-20.

¹²⁰¹ Por. art. 3 ust. 3 1/2003.

¹²⁰² Scharakteryzowano w podrozdziale 2.3. rozprawy.

¹²⁰³ T. Streinz, *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, edited by P. Craig, G. de Búrca, Oxford 2021, <https://ssrn.com/abstract=3762971> (dostęp: 20.09.2024 r.), s. 22-23.

i nieosobowymi¹²⁰⁴. Po drugie, dlatego, że również ocenne jest ustalenie tego, co stanowi przeważający przedmiot regulacji. Jeżeli jednak celem jest dokonanie wyodrębnienia, które będzie miało wartość poznawczą i praktyczną, to takie ograniczenie musi być wprowadzone, ponieważ liczba aktów prawnych, które incydentalnie regulują przetwarzanie danych, jest w systemie prawnym zbyt duża (przykładowo, wyszukanie terminu „dane osobowe” w SIP LEX w samych tylko obowiązujących polskich ustawach daje wynik 559 pozycji¹²⁰⁵). Przy ocenie przeważającego przedmiotu regulacji należy uwzględnić trzy kryteria: 1) zakres spraw regulowanych aktem prawnym i podmiotów, których akt ten dotyczy, co powinno zostać określone w przepisach ogólnych aktu (por. § 21 ust. 1 pkt 1 Zasad Techniki Prawodawczej); 2) stosunek liczby jednostek redakcyjnych aktu prawnego, które dotyczą przetwarzania danych względem ogólnej liczby jednostek redakcyjnych tego aktu (do zakwalifikowania do prawa danych stosunek ten powinien przekraczać 50%); 3) na poziomie unijnym dodatkowym kryterium mogłaby stanowić podstawa prawna, na podstawie której przyjęty został dany akt, to jest czy tę podstawę stanowi art. 16 TFUE dotyczący ochrony danych osobowych (tak jak jest w przypadku AI Act w odróżnieniu od DMA i DSA, które oparto tylko na art. 114 TFUE). Jeżeli przynajmniej jedno z powyższych kryteriów byłoby spełnione, akt prawny powinien być zaliczony do prawa danych. Tak sformułowane kryterium oznacza, że do tej kompleksowej gałęzi prawa zaliczone zostaną normy prawa administracyjnego, cywilnego (np. art. 82 RODO ustanawiający podstawę roszczenia odszkodowawczego w wyniku naruszenia RODO) i karnego (art. 107 §1-2 UODO penalizujący nielegalne przetwarzanie danych osobowych), co nie jest jednak zjawiskiem wyjątkowym dla tego typu kompleksowych gałęzi, na przykład podobnie jest w prawie ochrony środowiska¹²⁰⁶.

Tak sformułowane kryteria oznaczają, że poza tą gałęzią prawa danych znalazłyby się akty prawne, które miałyby większy niż tylko incydentalny wpływ na przetwarzanie danych osobowych. W odniesieniu do nowych aktów prawnych w obecnym stanie prawnym byłoby to w szczególności DMA i DSA. Samo niezaliczenie tych aktów do prawa danych nie oznacza jednak, że wobec krzyżowania się kompetencji się podmiotów administrujących ustanowionych na podstawie tych aktów i organów ochrony danych nie można zgłosić postulatów. Takie postulaty zostaną zgłoszenie niżej. Oznacza to natomiast, że prawo danych

¹²⁰⁴ W odniesieniu do danych nieosobowych, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Tekst mający znaczenie dla EOG.) PE/53/2018/REV/1 Dz. Urz. UE L 303, 28.11.2018, p. 59–68.

¹²⁰⁵ Na dzień 14 stycznia 2024 r.

¹²⁰⁶ B. Rakoczy, Prawo ochrony środowiska w styku z innymi obszarami systemu prawa [w:] Zagadnienia systemowe prawa ochrony środowiska, red. P. Korzeniowski, Łódź 2015, s. 71.

powinno być rozumiane raczej wąsko, co pozwoli wprowadzić dalej idące rozwiązania zapewniające spójność, co w szerszym rozumieniu prawa danych byłoby trudne bez podporządkowania innych celów, np. zapewnienia konkurencyjnego rynku celom ochrony danych osobowych i prywatności.

Jak wskazano wyżej, nawet w przypadku braku pełnej jasności co do klasyfikacji określonego aktu prawnego do prawa danych, wyodrębnienie takiej kategorii wciąż byłoby pomocne. W prawie danych aktem prawnym o charakterze *lex generalis* jest RODO, a kluczowymi organami – organy ochrony danych osobowych z powodu ich roli wynikającej z KPP. Wyodrębnienie tej odrębnej „gałęzi” umożliwiłoby ujednolicenie terminologii, to jest „danych”, „danych osobowych”, „danych nieosobowych” i relacji zakresu podmiotowego RODO („administrator”, „współadministrator” i „podmiot przetwarzający”) do zakresu podmiotowego innych aktów tego prawa, w tym DGA, Data Act oraz kolejnych aktów ustanowionych dla europejskich przestrzeni danych. Ułatwione byłoby jednolite stosowanie zasad przetwarzania w RODO we wszystkich tych aktach, z uwzględnieniem specyfiki ich zastosowania do danych nie-osobowych, co ułatwiałoby dokonywanie spójnej wykładni prawa. Pozwoliłoby to także zwiększyć pewność prawną w odniesieniu do stosowania zakazu *ne bis in idem* przez możliwość przyjęcia, że akty prawne w tak wyodrębnionej kompleksowej gałęzi prawa realizują tożsamy cel, co umożliwiałoby powoływanie się na za zakaz *ne bis in idem* w rozumieniu ukształtowanym przez TSUE i TK. Dodatkowo, mogłoby to stanowić punkt odniesienia dla ustalenia właściwości wyspecjalizowanych sądów w obszarze przetwarzania danych osobowych, których powołanie postulowane jest przez przedstawicieli doktryny (np. Arwida Mednisa ¹²⁰⁷) z uwagi na konieczność posiadania specjalistycznej wiedzy do prawidłowego orzekania. Sądy te, wydzielone według kryterium przedmiotowego, w założeniu mogłyby przypominać strukturą i właściwością sądy orzekające w sprawach ochrony konkurencji i konsumenta (por. art. 479²⁸ i nast. ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego¹²⁰⁸).

W odniesieniu natomiast do relacji podmiotów administrujących w prawie danych względem organów ochrony danych, zasadne byłoby wprowadzenie instrumentów zacieśnionej

¹²⁰⁷ Wypowiedź Arwida Mednisa w trakcie dyskusji podczas: Sejm Rzeczypospolitej Polskiej, Transmisje Archiwalne: Podkomisja stała do spraw sztucznej inteligencji i przejrzystości algorytmów, Informacja na temat ochrony praw podstawowych oraz danych osobowych (w tym danych profilowych) w kontekście korzystania ze sztucznej inteligencji i algorytmów cyfrowych – przedstawia Prezes Urzędu Ochrony Danych Osobowych, https://www.sejm.gov.pl/sejm10.nsf/transmisje_arch.xsp?unid=378673CBF43C9FCFC1258B1500323AED (dostęp: 15.09.2024 r.).

¹²⁰⁸ T.j. Dz. U. z 2023 r. poz. 1550 z późn. zm.

współpracy zaproponowanych w postulacie nr 3 poniżej, w której decydującą rolę odgrywałyby organy ochrony danych.

**5.7.2. POSTULAT NR 2: CENTRALIZACJA STRUKTURY STOSOWANIA RODO
WOBEC NAJWIĘKSZYCH PODMIOTÓW NADZOROWANYCH I USTANOWIENIE
ORGANÓW OCHRONY DANYCH JAKO ORGANÓW WŁAŚCIWYCH DLA
STOSOWANIA AKTÓW PRAWNYCH W OBSZARZE PRZETWARZANIA DANYCH
OSOBOWYCH**

Realizacja postulatów wyodrębnienia prawa danych osobowych jako kompleksowej gałęzi prawa pozwoliłaby uporządkować siatkę pojęciową w obszarze przetwarzania danych osobowych, zasady tego prawa, co mogłoby ułatwić dokonywanie wykładni oraz dawałoby ramy do dyskusji o relacji tej gałęzi prawa do innych kompleksowych gałęzi, które zakresowo mogą być stykowe (np. prawo konkurencji). Chociaż te postulaty mogą pomóc, to nie rozwiązują dwóch istotnych problemów w wymiarze prawa ustrojowego.

Po pierwsze, wyodrębnienie kompleksowej gałęzi prawa nie rozwiązuje ryzyka ustanowienia różnych (innych niż organy ochrony danych osobowych) organów jako krajowych organów właściwych na podstawie DSA, Data Act, DGA i AI Act zgodnie z zasadą autonomii instytucjonalnej państw członkowskich zarówno w ramach jednego państwa, jak i w innych państwach. Tytułem przykładu, wskutek operacjonalizacji DSA przez poszczególne państwa członkowskie jako koordynatorów ds. usług cyfrowych¹²⁰⁹ w Niemczech ustanowiono *Federal Network Agency (Bundesnetzagentur*, czyli organ regulacyjny m.in. w sektorze telekomunikacyjnym), we Francji – *Autorité de régulation de la communication audiovisuelle et numérique* (nowopowstały Organ Regulacyjny do spraw Komunikacji Audiowizualnej i Cyfrowej), na Łotwie – *Consumer Rights Protection Centre* (Centrum Ochrony Praw Konsumentów, czyli organ ochrony praw konsumentów), w Hiszpanii – *National Commission for the Markets and Competition* (Krajowa Komisja do spraw Rynków i Konkurencji, czyli hiszpański krajowy organ prawa konkurencji). Ta niejednorodność prowadziła będzie do rozdrobnienia struktury organów, które będą działały równocześnie w różnych sieciach administracyjnych na poziomie unijnym i współpracowały z różnymi unijnymi podmiotami. Takie rozdrobnienie nie przyczyni się do zwiększenia spójności stosowania zarówno tych

¹²⁰⁹ Ustalenia na podstawie: H. Lovells, *EU Digital Services Act: List of Digital Services Coordinators*: <https://www.engage.hoganlovells.com/knowledgeservices/eu-digital-services-act-list-of-digital-services-coordinators> (dostęp: 15.09.2024 r.).

aktów prawnych, jak I RODO. Stąd też postulowane jest, aby państwa członkowskie w procesie operacjonalizacji aktów prawnych w obszarze referencyjnym, to jest DSA, Data Act, DGA i AI Act, jak i innych aktów prawnych, które zaliczane będą do unijnego prawa danych jako organy właściwe do ich stosowania, wyznaczały ten sam podmiot administrujący w strukturze administracji. Z uwagi na chronioną traktatowo niezależność organów ochrony danych osobowych powinny to być organy nadzorcze ustanowione na podstawie RODO. Jeżeli kompetencje wynikające ze wszystkich tych aktów prawnych będą przyznane tylko jednemu organowi, w założeniu można zakładać większą spójność w stosowaniu tych aktów prawnych i RODO, co powinno ułatwić także horyzontalną i wertykalną współpracę w UE.

Z ustanowieniem organów ochrony danych osobowych związane są jednak problemy. Pierwszym jest konieczność zapewnienia adekwatnych zasobów finansowych i osobowych, aby wykonywać nowe kompetencje. Jak wskazano w rozdziale 3. rozprawy, organy ochrony danych osobowych nie mają wydzielonych odpowiednich zasobów nawet po to, aby stosować RODO. Jeżeli nowe akty prawne mają być efektywnie przez nie stosowane, konieczne byłoby szybkie i znaczne zwiększenie ich budżetów. Nadto, w zależności od ukształtowania struktury administracji publicznej poszczególnych państw, dokonanie takiej koncentracji kompetencji w jednym organie z traktatowo zagwarantowaną niezależnością mogłoby doprowadzić do sytuacji, w której ten organ otrzymałby zbyt duże władztwo w stosunku do tej niezależności w tym sensie, że stwarzałoby to ryzyko do nadużyć przez piastuna organu do partykularnych celów (np. politycznych). Można jednak argumentować również w drugim kierunku, twierdząc, że wykorzystanie tej niezależności mogłoby wzmocnić skuteczność i spójność stosowania tych aktów prawa unijnego w całej UE przez ograniczenie możliwości wpływu krajowej administracji rządowej na te organy. Finalnie, z perspektywy nauki o administracji można twierdzić, że kultura organizacyjna urzędów działających przy organach ochrony danych osobowych nakierowana jest na ochronę prawa do ochrony danych osobowych, podczas gdy cele organów ustanowionych na podstawie innych aktów – chociaż zasadniczo komplementarne względem tego podstawowego celu – mogą być nakierowane na realizację innych celów, np. wymianę danych w europejskich przestrzeniach danych, które pozostają w pewnym napięciu z tym podstawowym celem. W konsekwencji, w praktyce stosowania tych aktów w sytuacji napięcia między różnymi celami i dyskrecjonalności, mogłoby dochodzić do faworyzowania ochrony prawa do ochrony danych osobowych względem innych celów

Po drugie, efektywność stosowania RODO w sprawach transgranicznych jest przedmiotem krytyki,¹²¹⁰ w tym z uwagi na skomplikowanie postępowań spowodowanych różnicami proceduralnymi w państwach członkowskich, jak i obawę o rzeczywistą (nie tylko postulowaną) niezależność tych organów, zarówno wobec organów administracji rządowej, jak i największych podmiotów gospodarczych¹²¹¹. *Remedium* (przynajmniej częściowym) na różnice proceduralne ma w założeniu być ujednolicenie niektórych elementów procedur w projektowanym rozporządzeniu unijnym ustanawiającym dodatkowe przepisy proceduralne dotyczące egzekwowania RODO¹²¹², który to projekt spotkał się już z krytyką organizacji społecznych jako „atak na prawa podmiotów danych”¹²¹³. W tej rozprawie zagadnienie ujednolicenia procedur w postępowaniach przed organami ochrony danych w sprawach transgranicznych nie będzie przedmiotem pogłębionej analizy, niemniej dyskusja na ten temat jest niezbędna, a dokonanie takiego ujednolicenia jest potrzebne i byłoby komplementarne do sformułowanych w rozprawie postulatów.

W odniesieniu do proceduralnych wyzwań ze sprawami transgranicznymi i ryzyka niezależności krajowych organów nadzorczych, w literaturze podnosi się postulat częściowej centralizacji stosowania RODO przez przyznanie bardziej rozbudowanych kompetencji proceduralnych i naprawczych organom (agencjom regulacyjnym) na poziomie unijnym (np. EROD lub EIOD) w odniesieniu do przetwarzania danych osobowych przez największe podmioty gospodarki cyfrowej, które z natury rzeczy mają charakter transgraniczny¹²¹⁴. Jest to słuszny postulat. Warte odnotowania jest, że postulat centralizacji stosowania przepisów o ochronie danych osobowych w sytuacjach transgranicznych formułowany był już na początku historii ochrony danych osobowych w UE w Rezolucji Parlamentu Europejskiego w sprawie ochrony praw osób fizycznych w związku z rozwojem technicznym przetwarzania danych z 1979 r., zgodnie z którą (część III pkt 13): „Cross-frontier transmissions of personal

¹²¹⁰ Por. podrozdział 3.4.1. rozprawy.

¹²¹¹ Por. P. Litwiński, Krajowy, czy europejski organ nadzorczy w sprawach ochrony danych osobowych?, dodatek MoP 2020, nr 28 (23), s. 54-59, SIP Legalis; F. Brito Bastos, P. Pałka, Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?, „European Constitutional Law Review” 2023, s. 487-517.

¹²¹² Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679, COM/2023/348 final.

¹²¹³ nyob, *GDPR Procedures Regulation: Commission Proposal is an attack on users' rights in GDPR procedure*, <https://noyb.eu/en/gdpr-procedures-regulation-stripping-citizens-procedural-rights> (dostęp: 15.09.2024 r.).

¹²¹⁴ Por. P. Litwiński, Krajowy, czy europejski organ nadzorczy w sprawach ochrony danych osobowych?, dodatek MoP 2020, nr 28 (23), s. 54-59, SIP Legalis; F. Brito Bastos, P. Pałka, Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?, „European Constitutional Law Review” 2023, s. 487-517.

data intended for a recipient in another Member State or originating in another Member State shall not be subject to special arrangements within the Community. They shall be reported to the control body of the European Community” („Transgraniczne przekazywanie danych osobowych przeznaczonych dla odbiorcy w innym Państwie Członkowskim lub pochodzących z innego Państwa Członkowskiego nie powinno podlegać specjalnym uzgodnieniom w ramach Wspólnoty. Powinny one być zgłaszane organowi kontrolnemu Wspólnoty Europejskiej.”)¹²¹⁵.

Model częściowej centralizacji wprowadzono w DSA ¹²¹⁶. W odniesieniu do przetwarzania danych osobowych, wyzwaniem stanowił będzie wybór kryterium, które rozstrzygało będzie o wspólnotowym charakterze sprawy, ponieważ z perspektywy ochrony danych osobowych nie jest istotna tylko liczba przetwarzanych danych, czy liczba użytkowników, ale także wrażliwość danych, która jest trudna do zmierzenia. Pomimo tego, kryterium powinno być ilościowe, ponieważ każde inne kryterium doprowadziłoby do sporów o to, jaki organ jest kompetentny. Negatywnym skutkiem związanym ze „sztywnym” kryterium ilościowym może być to, że niektóre sprawy, które będą dotyczyły danych wrażliwych ilościowo znajdujących się nieznacznie poniżej progu, będą rozstrzygane na poziomie krajowym, podczas gdy podnoszone będzie, że sprawy te są na tyle istotne ze względu na swój charakter, że powinny być rozstrzygane na poziomie unijnym. Jest to trudność nierozwiązywalna, ponieważ konsekwencją jednoznaczności rozwiązań jest zasadniczo brak ich elastyczności.

Postulat ten jest w praktyce trudny do realizacji, ponieważ w unijnym procesie legislacyjnym wymagałby decyzji Rady UE (reprezentującej rządy państw członkowskich) o przekazaniu kompetencji z poziomu państw członkowskich na poziom unijny, co stanowiło będzie wyzwanie. Dyskusyjny byłby w tym kontekście także zakres przyznania agencji takich kompetencji (i ich dyskrecjonalność) w świetle doktryny *Meroni* i problemów związanych z niejasną pozycją ustrojową unijnych agencji regulacyjnych¹²¹⁷.

¹²¹⁵ Dostęp do tekstu uzyskano przez archiwum internetowe prowadzone przez prof. Glorię González Fuster, *History of data protection: An online anthology*, https://glgonzalezfuster.files.wordpress.com/2022/05/oj-joc_1979_140_resolutionrecommendations.pdf. Resolution of 8 May 1979 on the protection of the rights of the individual in the face of technical developments in data processing (Dz. Urz. UE C140, 5.6.1979, 34-38) (dostęp: 15.09.2024 r.).

¹²¹⁶ Scharakteryzowano w podrozdziałach 3.4.1. i 3.5.5.

¹²¹⁷ Por. F. Brito Bastos, P. Pałka, Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?, „European Constitutional Law Review” 2023, s. 28-30.

5.7.3. POSTULAT NR 3: WPROWADZENIE INSTRUMENTÓW WSPÓŁPRACY MIĘDZY ORGANAMI ADMINISTRACJI PUBLICZNEJ STOSUJĄCYMI AKTY PRAWNE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Oprócz rozwiązań w prawie materialnym i ustrojowym możliwe jest także wprowadzenie rozwiązań o konsekwencjach proceduralnych, które stanowiłyby instrumentarium efektywnej współpracy między organami administracji publicznej stosującymi akty prawne w obszarze przetwarzania danych osobowych. Zasadne byłoby, aby omówione niżej instrumenty zostały ustanowione w prawie unijnym, co wymagałoby jednak ograniczenia autonomii proceduralnej państw członkowskich, a zatem musiałyby zostać dokonane z uwzględnieniem traktatowych ograniczeń prawodawcy unijnego. Stąd też postulat ten kierowany jest również do prawodawców krajowych. Istotne jest, że poniższa analiza dotyczy instrumentów współpracy na poziomie krajowym i unijnym między podmiotami administrującymi ustanowionymi na podstawie innych aktów prawnych, a nie dotyczy współpracy horyzontalnej między podmiotami administrującymi ustanowionymi w różnych państwach członkowskich na podstawie tego samego aktu prawnego. W ustanowieniu instrumentów współpracy pomogłoby wyodrębnienie unijnego prawa danych jako odrębnej kompleksowej gałęzi prawa. Ułatwiłoby to oddzielenie podmiotów administrujących na podstawie aktów prawnych tej gałęzi od podmiotów administrujących w innych gałęziach, które mogą także incydentalnie rozstrzygać zagadnienia przetwarzania danych osobowych (np. prawo konkurencji). W pierwszej kolejności omówione zostaną instrumenty współpracy między krajowymi podmiotami administrującymi, a następnie – na poziomie unijnym.

W odniesieniu do krajowych podmiotów administrujących na podstawie aktów prawnych stanowiących unijne prawo danych proponowane jest wprowadzenie normy proceduralnej, zgodnie z którą do rozstrzygnięcia sprawy na podstawie aktu unijnego prawa danych wymagane jest uzyskanie uprzedniego stanowiska organu ochrony danych wiążącego dla organu rozstrzygającego sprawę. Natomiast w odniesieniu do spraw prowadzonych przez podmioty administrujące na podstawie aktów prawnych innych gałęzi prawa (np. prawie konkurencji) proponowane jest wprowadzenie normy proceduralnej, zgodnie z którą do rozstrzygnięcia sprawy, dla której niezbędne jest rozstrzygnięcie zagadnienia dotyczącego przetwarzania danych (osobowych lub nieosobowych) wymagane jest uzyskanie niewiążącej, uprzedniej opinii organu ochrony danych. Wprowadzenie tych dwóch norm powinno, z jednej strony, zapewnić spójność rozstrzygnięć w samym unijnym prawie danych, a z drugiej powinno wzmocnić pozycję organów ochrony danych w rozstrzyganiu spraw w innych

gałęziach prawa, które dotyczą danych osobowych, jednak bez ograniczania niezależności decyzyjnej innych organów. Powinny być one uzupełnione o jednoznaczne normy umożliwiające wymianę informacji i dokumentów między organami na potrzeby prowadzonej współpracy. Należy mieć na względzie, że wszystkie te rozstrzygnięcia mogą podlegać następnie kontroli sądowej.

W odniesieniu do wydawania tak zwanych aktów prawa miękkiego na podstawie kompetencji doradczych, informacyjnych i edukacyjnych zasadne byłoby ustanowienie na poziomie krajowym podmiotów administrujących o funkcji koordynującej, które byłyby podmiotami kolegalnymi, w których skład wchodziłby przedstawiciele organu ochrony danych osobowych, inne podmioty administrujące ustanowione na podstawie unijnego prawa danych i podmioty administrujące w stykowych gałęzi prawa (np. prawa konkurencji, organy właściwe do spraw cyberbezpieczeństwa, nadzoru nad rynkiem finansowym i do spraw AML). Wszystkie te podmioty współpracowałyby w ramach podmiotu o funkcjach koordynacyjnych nad wypracowaniem wspólnych aktów prawa miękkiego, a także mogłyby koordynować kierunki podejmowanych działań, np. wybór sektora do przeprowadzenia kontroli w danym roku. Chociaż ustanowienie takiego podmiotu o funkcji koordynującej nie powodowałoby, że podmioty administrujące nie mogłyby wydawać własnych aktów prawa miękkiego, to należy jednak założyć, że zarówno podmioty administrujące w unijnym prawie danych, jak i w stykowych gałęziach byłyby zainteresowane udziałem w pracach takiego podmiotu koordynującego, ponieważ przy rozstrzyganiu spraw i tak musiałyby uzyskać albo wiążące stanowisko, albo opinię organu ochrony danych osobowych. Byłoby to w istocie rozwiązanie podobne do rozwiązań wprowadzonych w ostatnich latach – w Królestwie Niderlandów przez ustanowienie the Cooperative Platform for Digital Supervision (w skład wchodzi: Authority for Consumers and Markets (ACM), the Authority for the Financial Markets (AFM), the Data Protection Authority (AP), and the Media Authority) ¹²¹⁸ i w Wielkiej Brytanii przez ustanowienie The Digital Regulation Cooperation Forum ¹²¹⁹ (w skład wchodzi: the Competition and Markets Authority, the Financial Conduct Authority, the Information Commissioner's Office and Ofcom), które odgrywają rolę takich podmiotów koordynujących między organami ochrony danych, organami prawa konkurencji i ochrony konsumentami oraz organami nadzoru nad sektorem finansowym.

¹²¹⁸ *The Digital Regulation Cooperation Platform (SDT)*, <https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt> (dostęp: 15.09.2024 r.).

¹²¹⁹ *About the DRCF*, <https://www.drcf.org.uk/about-us> (dostęp: 15.09.2024 r.).

W odniesieniu do podmiotów unijnych proponowana jest współpraca w wykonywaniu kompetencji doradczych, informacyjnych i edukacyjnych. Chociaż można byłoby sformułować także postulaty dotyczące współpracy w wykonywaniu kompetencji proceduralnych i naprawczych, ich wdrożenie byłoby obecnie utrudnione z uwagi na rozbudowaną, kolegialną strukturę EROD jako kluczowej agencji unijnej¹²²⁰ w obszarze przetwarzania danych osobowych. W przypadku ustanowienia bardziej scentralizowanego modelu stosowania RODO zasadne byłoby wprowadzenie instrumentów współpracy w wykonywaniu kompetencji proceduralnych i naprawczych między EROD (lub inną agencją unijną stosującą RODO) a Komisją jako organem unijnego prawa konkurencji wyposażonym w rozbudowane kompetencje na podstawie DMA I DSA.

Po pierwsze, postulowane jest, aby przedstawiciele EROD i EIOD byli członkami z prawem głosu wszystkich unijnych organów kolegialnych ustanowionych w unijnym prawie danych i kompleksowych gałęziach prawa zakresowo stykowych. W obecnym stanie prawnym tak nie jest. Przedstawiciele EROD i EIOD nie są członkami, np. Europejskiej Rady ds. Usług Cyfrowych. Samo to ich członkostwo umożliwiłoby uwzględnienie stanowiska EROD i EIOD, które pozwoliłoby wziąć pod uwagę perspektywę RODO w opiniach i wytycznych, w tym w przedmiocie stosowania poszczególnych rozwiązań w tych aktach (np. DSA) w sposób zharmonizowany ze stosowaniem rozwiązań w RODO.

Po drugie, zasadne jest poparcie postulatu EIOD sformułowanego w „Opinii w sprawie spójnego egzekwowania praw podstawowych w erze dużych zbiorów danych” z 2016 r.,¹²²¹ zgodnie z którym celowe byłoby ustanowienie unijnej agencji o nazwie „Cyfrowa Izba Rozliczeniowa” („Digital Clearing House”). Pojęcie izb rozliczeniowych powiązane jest z obrotem instrumentami finansowymi. Przykładowo, Dyrektywa 98/26/WE Parlamentu Europejskiego i Rady z dnia 19 maja 1998 r. w sprawie zamknięcia rozliczeń w systemach płatności i rozrachunku papierów wartościowych¹²²² definiuje termin „izby rozliczeniowe” w art. 2 lit. f jako „podmiot ponoszący odpowiedzialność za wyliczenie pozycji netto instytucji, partnera centralnego¹²²³ i/lub agenta rozrachunkowego, jeżeli tacy występują”. Oznacza to, że izby rozliczeniowe to zaufany centralny podmiot między instytucjami w systemie, którego

¹²²⁰ Określenie EROD jako agencji unijnej jest kontrowersyjne z uwagi na szczególny charakter niezależności przyznanej organom ochrony danych osobowych w prawie pierwotnym UE. Zasadne byłoby rozważenie klasyfikowania EROD jako unijnej agencji (albo unijnego organu) *sui generis*.

¹²²¹ *Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (dostęp: 15.09.2024 r.).

¹²²² Dz. Urz. UE L 166, 11.6.1998, p. 45–50.

¹²²³ Zgodnie art. 2 lit. c) jest to: „podmiot umiejscowiony między instytucjami w systemie, który działa jako wyłączny kontrahent tych instytucji odnośnie do ich zleceń transferu”.

funkcją jest wymiana informacji lub pomoc, przy czym takie podmioty ustanowiono także w innych sektorach, np. transporcie kolejowym i edukacji¹²²⁴. Digital Clearing House jest pomyślany w opinii EIOD jako sieć punktów kontaktowych w organach regulacyjnych w „sektorze cyfrowym” (w tym także sektor telekomunikacyjny) na poziomie krajowym i unijnym z dwoma kryteriami członkostwa: wspólnym celem wspierania spójnego wykonywania swoich kompetencji i wolą do współpracy oraz wymiany informacji¹²²⁵. Digital Clearing House miałby, zgodnie ze stanowiskiem EIOD, pięć zadań: 1) dyskusja o wyborze stosowania najodpowiedniejszego aktu prawnego na potrzeby konkretnych spraw (lecz niedecydowanie o tym) i unijna koordynacja stosowania poszczególnych aktów; 2) wykorzystywanie prawa danych i prawa ochrony konsumenta do formułowania teorii szkody na potrzeby prawa konkurencji; 3) dyskusja o działaniach organów tam, gdzie dane osobowe stanowią kluczowe aktywy jako alternatywy dla nowej legislacji dla tego sektora; 4) konsultowanie konsekwencji stosowania kompetencji naprawczych w poszczególnych sprawach; 5) wspieranie nieformalnej współpracy między europejskimi sieciami administracyjnymi, np. Europejskiej Sieci Konkurencji i Europejskiej Sieci Ochrony Konsumentów¹²²⁶.

Wyzwaniem dla ustanowienia tego podmiotu jest zidentyfikowanie obszaru regulacji, który uznać można byłoby za „sektor cyfrowy”, a tym samym ustalenie, jakie organy mogłyby być członkami Digital Clearing House. Jest to refleks problemu wynikającego z niejasnego pojęcia danych osobowych, czego konsekwencją jest teza, że prawo danych osobowych jest „prawem wszystkiego”. Skoro jednak ten podmiot pomyślany jest jako nie-obligatoryjny, a członkostwo w nim ma charakter otwarty, nie ma przeszkód, aby użyty w opinii EIOD termin „sektora cyfrowego” rozumieć w sposób możliwie szeroki, a jako członków przyjmować także, np. krajowe urzędy patentowe i Urząd Unii Europejskiej ds. Własności Intelektualnej, aby osiągnąć synergii także w relacji z prawem własności intelektualnej kluczowym przecież dla zabezpieczenia rozwoju innowacji.

¹²²⁴ *Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (dostęp: 15.09.2024 r.), s. 22.

¹²²⁵ *Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (dostęp: 15.09.2024 r.), s. 15.

¹²²⁶ *Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (dostęp: 15.09.2024 r.), s. 15. Po przyjęciu tej opinii w ramach inicjatywy Digital Clearing House zrealizowano szereg spotkań z udziałem przedstawicieli środowisk akademickich i niektórych organów, przy czym zakres tych spotkań i prac z nimi związanych nie stanowił pełnej realizacji postulatów w opinii.

5.7.4. POSTULAT NR 4: WPROWADZENIE ROZWIĄZAŃ TYPU KLAUZULA *SAFE HARBOUR*

Powyższe postulaty wymagają wprowadzenia modyfikacji w prawie (przede wszystkim unijnym), które należy ocenić jako daleko idące, ponieważ oznaczałyby zmianę podstawowych elementów modelu regulacji przetwarzania danych osobowych w UE. Stąd też zasadne byłoby postulatywnie rozwiązań o mniej spektakularnym charakterze, które jednak mogłyby osiągnąć (przynajmniej częściowo) cel, czyli zminimalizowanie negatywnych skutków zjawiska krzyżowania się kompetencji¹²²⁷. Takim istotnym skutkiem jest niepewność po stronie podmiotów nadzorowanych, w jaki konkretnie sposób mają wypełniać obowiązki nałożone przez poszczególne akty prawne w sytuacji, w której różne podmioty administrujące mogą niezależnie stosować wobec nich kompetencje naprawcze, np. przez nakładanie administracyjnych kar pieniężnych.

Z perspektywy podmiotów nadzorowanych zmniejszenie tej niepewności mogłoby nastąpić przez zmiany w prawie polegające na wprowadzeniu przepisu, zgodnie z którym wypełnienie obowiązku (O1) w sposób zgodny z jednym z aktów prawnych (A1) i stanowiskiem podmiotu administrującego ustanowionego na podstawie tego aktu (P1) oznaczałoby jednocześnie spełnienie obowiązku (O2) nałożonego przez inny akt prawny (A2), przy czym oba te obowiązki musiałyby być zasadniczo ekwiwalentne (równoważne)¹²²⁸. Konsekwencją przyjęcia automatycznego spełnienia obu obowiązków (O1=O2) byłoby, że podmiot administrujący (P2) zgodnie z drugim z aktów prawnych (A2) nie mógłby nałożyć sankcji za naruszenie tego obowiązku (O2). W tej rozprawie zaproponowano, aby takie rozwiązanie określić jako klauzulę *safe harbour* (bezpieczna przystań)¹²²⁹. Z uwagi na zagwarantowaną w unijnym prawie pierwotnym niezależność organów ochrony danych, to właśnie organy nadzorcze ustanowione na podstawie RODO musiałyby pełnić funkcję podmiotów administrujących P1, czyli tych, których stanowisko rozstrzygałoby o automatycznym spełnieniu obu obowiązków (O1=O2).

¹²²⁷ Skutki zjawiska krzyżowania się kompetencji scharakteryzowane zostały w podrozdziale 4.5. rozprawy.

¹²²⁸ Inspirację dla tego postulatu stanowił pogląd przedstawiony przez prof. Cary'ego Coglianese w publikacji *Easy fix for federal regulatory overlap*, <https://eu.onlineathens.com/story/opinion/2015/04/02/coglianese-easy-fix-federal-regulatory-overlap/15498581007/>

¹²²⁹ Jest to termin używany w odniesieniu do rozwiązań o podobnym charakterze, np. w prawie podatkowym w odniesieniu do cen transferowych (Podatki.gov.pl, *Safe harbour dla pożyczek – metodyka kalkulacji przy ujemnej stopie referencyjnej*, <https://www.podatki.gov.pl/ceny-transferowe/wyjasnienia/safe-harbour-dla-pozyczek-metodyka-kalkulacji-przy-ujemnej-stopie-referencyjnej/>).

Dyskusyjne jest, jakie konkretnie obowiązki pozwalałaby na wprowadzenie takiego rozwiązania. Scharakteryzowany zostanie jeden przykład – obowiązki związane z wdrożeniem odpowiednich środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa przetwarzania. Obowiązek taki nakłada wprost art. 32 ust. 1 RODO, nakazując administratorowi i podmiotowi przetwarzającemu wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, przy uwzględnieniu m.in. stanu wiedzy technicznej i kosztu wdrażania. RODO nie rozstrzyga, jakie dokładnie środki są odpowiednie, aby wypełnić ten obowiązek, wskazując jedynie przykłady, np. pseudonimizację i szyfrowanie danych. Ostatecznie zdecydować ma o tym sam administrator i podmiot przetwarzający. Jednocześnie, zgodnie z art. 21 ust. 1 Dyrektywy NIS 2, podmioty kluczowe i ważne zobowiązane są do wprowadzenia m.in. odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty¹²³⁰. Podmioty kluczowe i ważne mogą być jednocześnie administratorami i podmiotami przetwarzającymi, zatem obowiązek, o którym mowa w art. art. 21 ust. 1 Dyrektywy NIS 2 może z perspektywy tych podmiotów współistnieć z obowiązkiem z art. 32 ust. 1 RODO.

Pytaniem jest, czy oba te obowiązki – podobne do siebie *prima facie* – są zasadniczo ekwiwalentne (równoważne). Należy to ocenić z perspektywy celu ich ustanowienia. W pierwszym z nich punktem odniesienia jest ryzyko „naruszenia praw lub wolności osób fizycznych”, a w drugim – ryzyko „dla bezpieczeństwa sieci i systemów informatycznych”. Można argumentować, że naruszenie drugiego z obowiązków będzie co do zasady stanowiło naruszenie pierwszego, podczas gdy naruszenie pierwszego nie zawsze będzie oznaczało naruszenie drugiego. Nie zawsze bowiem (choć w praktyce zazwyczaj) ryzyko „naruszenia praw lub wolności osób fizycznych” jest spowodowane brakiem „bezpieczeństwa sieci i systemów informatycznych”. Oznacza, że zakresy obu tych obowiązków pokrywają się tylko w odniesieniu do takiego ryzyka „naruszenia praw lub wolności osób fizycznych”, które spowodowane jest brakiem „bezpieczeństwa sieci i systemów informatycznych”. W konsekwencji, w odniesieniu do proponowanego rozwiązania typu klauzula *safe harbor*

¹²³⁰ Dalsza część ustępu 1: „Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należy uwzględnić stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze”.

zasadniczą ekwiwalentność obowiązku z art. 32 ust. 1 RODO i obowiązku z art. 21 ust. 1 Dyrektywy NIS² można byłoby stwierdzić tylko w zakresie, w jakim ryzyko „naruszenia praw lub wolności osób fizycznych” spowodowane brakiem „bezpieczeństwa sieci i systemów informatycznych”.

Przy tak sformułowanej ekwiwalentności obowiązków kolejnym problemem jest ustalenie, w jaki sposób podmioty nadzorowane mogłyby nabrać przekonania, że wypełniają obowiązek z art. 32 ust. 1 RODO. Punktem odniesienia w analizie tej kwestii powinno być naruszenie ochrony danych osobowych (art. 4 pkt 12 RODO) jako zdarzenie, które w praktyce najczęściej powoduje weryfikowanie wypełnienia tego obowiązku przez organy ochrony danych. W przypadku prowadzenia postępowania przez organy ochrony danych w związku z takim naruszeniem zajmowałyby one stanowisko wobec praktyki podmiotu nadzorowanego przez podejmowanie czynności procesowych, np. wydanie decyzji nakładającej administracyjną karę pieniężną. Nie zmniejszałoby to jednak niepewności w sytuacjach, kiedy do naruszenia nie dochodzi (czyli w większości przypadków). Niepewność mogłoby zmniejszyć wprowadzenie odpowiednich mechanizmów certyfikacji zgodnie z art. 42-43 RODO, które mogłyby uwzględniać uznane standardy cyberbezpieczeństwa¹²³¹, w tym powstawać w porozumieniu z podmiotami administrującymi ustanowionymi na podstawie aktów prawnych regulujących cyberbezpieczeństwo. Ze względów pragmatycznych zasadne jest wykorzystywanie istniejącego instrumentarium prawnego¹²³². Chociaż uzyskanie certyfikacji przez administratora lub podmiot przetwarzający nie spowodowałoby uchylecia odpowiedzialności za naruszenie RODO, to może wpłynąć, np. na wysokość administracyjnej kary pieniężnej (art. 83 ust. 2 lit. j RODO). Zasadniczo jednak stanowiłoby wskazówkę dla administratora lub podmiotu przetwarzającego, że wykonuje on obowiązek z art. 32

¹²³¹ Por. np. S. D. D. Ferguson, *European Cybersecurity Certification Schemes and Cybersecurity in the EU Internal Market*, „International Cybersecurity Law Review” 2022, Vol. 3, No. 1, s. 51-114; I. Nwankwo, M. Stauch, P. Radoglou-Grammatikis et al., *Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector*, „Electronics” 2022; Vol. 11, Iss. 6, <https://doi.org/10.3390/electronics11060965> (dostęp: 20.09.2024 r.); K. Hovhannisyan, P. Bogacki, C. A. Colabuono et al., *Towards a Healthcare Cybersecurity Certification Scheme* [in:] *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers IEEE 2021, <https://doi.org/10.1109/CyberSA52016.2021.9478255> (dostęp: 20.09.2024 r.).

¹²³² Więcej w przedmiocie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i art. 43 RODO: EROD, *Wytoczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia*, Wersja 3.0 4.06.2019 r., https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_p1.pdf; por. także: E. Koulourakis, *Certification as Guidance for Data Protection by Design*, Int. Rev. Law Comput. Technol. 2024, Vol. 38, No. 2, <https://doi.org/10.1080/13600869.2023.2269498>, (dostęp: 7.09.2024 r.).

ust. 1 RODO w sposób należyty, co, w połączeniu z klauzulą *safe harbor*, zmniejszałoby niepewność.

Wymaga uwagi, że art. 4 ust. 1 Dyrektywy NIS 2 wprowadza podobne do postulowanego rozwiązanie w odniesieniu do równoważnego traktowania spełnienia obowiązku przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów w unijnych sektorowych aktach prawnych względem spełnienia obowiązków z Dyrektywy NIS 2. Zgodnie z art. 4 ust. 1 Dyrektywy NIS 2, „w przypadku gdy na podstawie sektorowych aktów prawnych Unii wymaga się od podmiotów kluczowych lub ważnych przyjęcia środków zarządzania ryzykiem w cyberbezpieczeństwie lub zgłaszania poważnych incydentów i w przypadku gdy wymogi te są co najmniej równoważne pod względem skutku obowiązkowi określonym w niniejszej dyrektywie, nie stosuje się do takich podmiotów odpowiednich przepisów niniejszej dyrektywy, w tym przepisów dotyczących nadzoru i egzekwowania (...)”. Skoro zatem prawodawca unijny dostrzega możliwość wprowadzenia podobnego rozwiązania w odniesieniu do sektorowych aktów prawnych, nie ma przeszkód, aby podobne rozwiązanie było wprowadzone w odniesieniu do obowiązków ustanowionych na podstawie RODO. Analiza zastosowania tego typu klauzuli *safe harbor* dla obowiązku dotyczącego środków technicznych i organizacyjnych jest tylko przykładem. Zasadne byłoby rozważenie rozszerzenia zastosowania tego typu klauzuli także do innych obowiązków. Przedmiotem refleksji powinno być najpierw, jakie kryterium należy wybrać przy wyborze takich obowiązków.

5.8. PODSUMOWANIE

W niniejszym rozdziale scharakteryzowano przyczyny występowania zjawiska krzyżowania się kompetencji podmiotów administrujących w obszarze przetwarzania danych osobowych. Te przyczyny to: nieadekwatność odpowiedzi prawodawcy na socjo-techniczne zmiany spowodowane transformacją cyfrową; wybór techniki legislacyjnej przez prawodawcę, aby obszar ten uregulować za pomocą zasad, terminów nieostrych metody opartej na ryzyku w celu zapewnienia neutralności technologicznej; niejasność taksonomiczna w odniesieniu do prawa ochrony danych osobowych; proces europeizacji prawa administracyjnego prowadzący do złożonej struktury podmiotów administrujących bez wyraźnych hierarchicznych relacji między nimi; konieczność balansowania celów wyznaczonych poszczególnym podmiotom. Przyczyny te są złożone, pozostają ze sobą powiązane i wzajemnie się umacniają, co utrudnia zaproponowanie adekwatnych rozwiązań dla badanego w tej rozprawie problemu.

Przykładowo, jak zostało wykazane, balansowanie celów potęguje negatywne skutki zjawiska krzyżowania się kompetencji z powodu obranej techniki legislacyjnej, której konsekwencją jest, że to podmioty administrujące w zasadniczej części dokonują konkretyzacji prawa trakcie jego stosowania, co zwiększa ich dyskrejonalność, a tym samym z zasady poszerza zakres spraw (lub daje więcej możliwych sposobów ich załatwiania), poszerzając skalę zjawiska krzyżowania się kompetencji.

W drugiej części rozdział sformułowano postulaty *de lege ferenda*: 1) wyodrębnienie prawa danych jako odrębnej kompleksowej gałęzi prawa; 2) centralizacja struktury stosowania RODO wobec największych podmiotów nadzorowanych i ustanowienie organów ochrony danych jako organów właściwych dla stosowania aktów prawnych w obszarze przetwarzania danych osobowych; 3) wprowadzenie efektywnych instrumentów współpracy między podmiotami administrującymi stosującymi akty prawne w obszarze przetwarzania danych osobowych; 4) wprowadzenie rozwiązania typu klauzula „safe harbour” dla podmiotów nadzorowanych. Jak zostało wskazane, nie należy oczekiwać, że ich realizacja nie doprowadzi do całkowitego wyeliminowania negatywnych skutków zjawiska krzyżowania się kompetencji organów. Pozwoliłaby jednak zredukować niektóre problemy w tym obszarze, co zwiększyłoby efektywność ochrony praw podstawowych (zwłaszcza postulat nr 1 i 2), a jednocześnie zmniejszyłoby niepewność prawną po stronie podmiotów administrujących, podmiotów nadzorowanych i podmiotów danych (zwłaszcza postulat nr 3 i 4).

ZAKOŃCZENIE

Celem tej rozprawy była weryfikacja hipotezy badawczej, zgodnie z którą w obszarze przetwarzania danych osobowych ustanowione zostały organy administracji publicznej, których kompetencje krzyżują się, co prowadzi do niepewności prawnej, a brak jest instrumentów, mogących ten problem skutecznie rozwiązać. Hipotezę tę zweryfikowano pozytywnie. W tym celu dokonano analizy krzyżowania się zakresu przedmiotowego RODO i wybranych aktów prawnych regulujących przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu, cyberbezpieczeństwo, prawo konkurencji, Akt o Rynkach Cyfrowych i Akt o Usługach Cyfrowych, sztuczną inteligencję oraz europejskie przestrzenie danych (Akt w Sprawie Zarządzania Danymi i Akt w Sprawie Danych), aby następnie zbadać kompetencje organów ustanowionych przez te akty prawne.

RODO – będąc podstawowym aktem prawnym normującym przetwarzanie danych osobowych w UE – jest rozporządzeniem prawa unijnego o skutku bezpośrednim, o szerokim zakresie obowiązywania w wymiarze przedmiotowym, podmiotowym i terytorialnym. W RODO przyjęta została nieostra definicja danych osobowych, która jest interpretowana rozszerzająco w orzecznictwie TSUE. Podobnie nieostro rozumiane są kluczowe terminy wyznaczające zakres podmiotowy RODO, to jest pojęcie administratora i współadministratora danych osobowych. Nieprzewidzianą (jak się zdaje) i nieuchronną konsekwencją tak szerokiego i nieostrego zakresu przedmiotowego oraz podmiotowego RODO w połączeniu ze wszechobecnością danych osobowych w gospodarce cyfrowej jest to, że zakres przedmiotowy RODO krzyżuje się z innymi aktami prawnymi w systemie prawa administracyjnego, w tym sektorowymi aktami prawnymi (np. w sektorze ochrony zdrowia). Niektóre z tych aktów przyjęte zostały w odpowiedzi na transformację cyfrową (np. regulujące cyberbezpieczeństwo), a niektóre służyły jeszcze przed transformacją cyfrową innym celom, których osiągnięcie w odniesieniu do tej transformacji wymaga działań związanych z przetwarzaniem danych osobowych (np. prawo konkurencji).

Analiza aktów prawnych w obszarze referencyjnym tej rozprawy prowadzi do konkluzji, że ich wejście w życie stwarza ryzyko ustanowienia aż do 250 różnych organów administracji publicznej w całej UE¹²³³ w obszarze przetwarzania danych osobowych. Należy zastrzec, że liczba ta może być ostatecznie niższa, ponieważ prawodawcy krajowi mogą wyznaczyć organy nadzorcze ustanowione w celu stosowania RODO jako właściwe organy do stosowania tych

¹²³³ Licząc organy, które mogą zostać ustanowione w państwach członkowskich, i kolegalne organy na poziomie unijnym.

aktów na poziomie krajowym. Zależało to będzie jednak od sposobu wdrożenia tych aktów prawnych do porządków krajowych. Niezależnie od ostatecznego kształtu struktur organów ustanowionych w celu stosowania tych aktów, liczba ta będzie znaczna, co w konsekwencji doprowadzi do spotęgowania problemów spowodowanych krzyżowaniem się kompetencji organów w tym obszarze. Na poziomie unijnym zbadano następujące organy i ich kompetencje: Europejska Rada Ochrony Danych, Urząd ds. AI i Europejską Radę ds. Sztucznej Inteligencji, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, Komisja Europejska jako organ unijnego prawa konkurencji, Grupa Wysokiego Szczebla, Europejska Rada ds. Usług Cyfrowych, Europejska Rada ds. Innowacji w zakresie Danych i Europejska Rada ds. Sztucznej Inteligencji oraz Europejski Urząd ds. Sztucznej Inteligencji. Z kolei na poziomie krajowym scharakteryzowano następujące organy: Prezes Urzędu Ochrony Danych Osobowych, Generalny Inspektor Informacji Finansowej, organy właściwe do spraw cyberbezpieczeństwa, Prezes Urzędu Ochrony Konkurencji i Konsumenta jako organ krajowego prawa konkurencji, organy właściwe w Akcie o usługach cyfrowych, organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych, organy właściwe w Akcie w sprawie danych i organy właściwe w AI Act.

Aby zachować neutralność technologiczną i spowodować, że akty prawne regulujące transformację cyfrową podlegają horyzontalnemu stosowaniu, prawodawca preferuje wybór regulowanie przez normy o charakterze zasad (np. zasady dotyczące przetwarzania danych osobowych w art. 5 RODO), szerokie wykorzystanie terminów nieostrych i użycie metody regulacji opartej na ryzyku (*risk-based approach*). Ceną za prawo, które nie jest anachroniczne i możliwe do zastosowania we wszystkich sektorach, jest to, że zasady i znaczenia terminów nieostrych konkretyzowane są dopiero na etapie stosowania prawa przez organy administracji publicznej, a następnie kontrolę sądową. W konsekwencji, to na organach stosujących te akty prawne spoczywa znaczna dyskretywność przy konkretyzacji tego prawa. Nakłada się to na problem relacji prawa unijnego i krajowego w kontekście zasady autonomii proceduralnej i instytucjonalnej państw członkowskich. W konsekwencji ma to negatywne skutki dla podmiotów nadzorowanych (administratorów i współadministratorów danych osobowych) i podmiotów danych, prowadząc do niepewności prawnej, która jest fundamentalnym skutkiem zjawiska nazwanego w tej rozprawie krzyżowaniem się kompetencji organów administracji publicznej w obszarze przetwarzania danych osobowych.

W rozprawie sformułowano definicję tego zjawiska, jego typologię i zbadano przykłady, ustalając, że jako nieefektywne należy ocenić instrumenty prawne, które mogłyby służyć do zmitygowania jego skutków. Zjawisko to zdefiniowano jako sytuację prawną, w której co

najmniej dwóm organom administracji publicznej w porządku krajowym lub unijnym przyznane zostały kompetencje w tej samej sprawie albo w odniesieniu do tego samego zagadnienia w taki sposób, że może prowadzić to do rozstrzygnięcia tej samej sprawy lub tego samego zagadnienia odmiennie. Do pewnego stopnia istnieje możliwość zredukowania negatywnych skutków tego zjawiska przez dokonanie przez prawodawcę krajowego wyboru, aby, operacjonalizując prawo unijne w ramach autonomii instytucjonalnej, konsekwentnie ustanawiać ten sam organ jako kompetentny do ich stosowania. Za niewielkie należy uznać jednak prawdopodobieństwo, że taka jednolitość zostanie zachowania nie tylko w Polsce, ale również w innych jurysdykcjach.

Kwestię krzyżowania się kompetencji należy rozpatrywać z perspektywy zasady legalizmu i zakazu domniemania kompetencji organów administracji publicznej. Analiza tego zjawiska prowadzi do wniosku, że brak jest skutecznych instrumentów prawnych, aby rozwiązać problemy nim spowodowane. Dotyczy to zarówno instrumentów prawnych w wymiarze prawa materialnego (np. tzw. klauzule „bez uszczerbku”), jak i prawa procesowego (np. rozstrzyganie sporów o właściwość i instrumenty współpracy na poziomie krajowym i unijnym). Przykładowo, instrumenty prawne w prawie administracyjnym procesowym umożliwiają rozstrzyganie sporów o właściwość między organami administracji publicznej na gruncie skonkretyzowanych spraw. Tymczasem zjawisko krzyżowania się kompetencji organów administracji publicznej nie dotyczy tylko takich spraw. Dotyczy bowiem także sytuacji, w których organy administracji publicznej w obszarze przetwarzania danych osobowych wydają instrumenty typu *soft law*. Spory o właściwość między organami administracji publicznej w obszarze przetwarzania danych osobowych nie mogą być także rozstrzygnięte na podstawie Konstytucji RP, ponieważ w tym trybie mogą być rozstrzygane jedynie spory między centralnymi konstytucyjnymi organami, do których nie zalicza się analizowanych organów.

Zjawisko to skutkuje ryzykiem istnienia równoległych struktur podmiotów administrujących, w których te podmioty mogą procedować te same sprawy lub rozstrzygać o tych samych kwestiach w odmienny sposób, bez efektywnej współpracy między nimi. To prowadzi do niepewności prawnej zarówno po stronie organów administracji publicznej, podmiotów nadzorowanych i podmiotów danych w odniesieniu do podziału kompetencji między organami i wykładni aktów prawnych w obszarze przetwarzania danych osobowych. Stanowi także zagrożenie dla realizacji zasady *ne bis in idem* w odniesieniu do rozstrzygania tej samej sprawy przez różne organy administracji publicznej. Odmienna wykładnia aktów prawnych w tym obszarze w poszczególnych państwach członkowskich może prowadzić także

do tzw. *forum shopping*. Stanowi to problem dla integralności rynku wewnętrznego UE. Zjawisko to prowadzi także do zagrożenia dla ochrony praw podstawowych, ponieważ dla poszczególnych organów administracji publicznej w obszarze przetwarzania danych osobowych wyznaczono cele, których pełna realizacja prowadzi do rozbieżności także na poziomie zbalansowanej realizacji prawa do prywatności i ochrony danych osobowych względem innych praw podstawowych.

W perspektywie skutków ekonomicznych, dynamika spowodowana dwojakim charakterem danych osobowych (jako przedmiotu ochrony praw podstawowych i jako kluczowego aktywa w gospodarce cyfrowej) doprowadziła (w pewnym uproszczeniu) do sformułowania dwóch odmiennych poglądów na skutki aktów prawnych w obszarze przetwarzania danych osobowych. Jedni uważają, że akty te hamują innowacyjność i wzrost gospodarczy w UE, ponieważ są zbyt skomplikowane i nakładają zbyt duże obowiązki. Drudzy, wychodząc z perspektywy troski o ochronę praw podstawowych, stoją na stanowisku, że akty te, zwłaszcza na etapie ich stosowania, są niewystarczająco restrykcyjne w stosunku do administratorów danych osobowych, zwłaszcza tzw. gigantów cyfrowych. Źródła tych różnic należy doszukiwać się w odmiennych podejściach do innowacyjności i odmiennych zapatrywaniach etycznych na regulację zmian socjo-technicznych spowodowanych transformacją cyfrową. Zajęcie stanowiska wobec tych poglądów wymagałoby wyjścia poza metody badawcze i przedmiot tej rozprawy. Nie należy jednak zapominać, że prawo administracyjne, stanowiąc system sam w sobie (będąc jednocześnie podsystemem prawa), wywiera także skutki ekonomiczne, społeczne i polityczne wykraczające poza ten system.

Obecny stan prawny jest efektem działań prawodawcy unijnego i krajowego zasadniczo w pierwszych dwóch dekadach XXI wieku. Ustanowione akty prawne w obszarze przetwarzania danych osobowych nie stanowią jeszcze ostatecznej odpowiedzi prawodawcy na transformację cyfrową. Regulacja w obszarze przetwarzania danych osobowych jest sama w sobie relatywnie nowa, liczy bowiem od swoich początków najwyżej pięćdziesiąt lat (od pierwszych aktów prawnych w Szwecji i Niemczech, których celem była ochrona danych osobowych w latach 70. XX wieku). Transformacja cyfrowa wciąż trwa, co powodowało będzie nowe ryzyka i stwarzało nowe szanse, wobec czego można przyjąć, że odpowiedź prawodawcy na nie będzie ewoluować. Dlatego też w najbliższej dekadzie można spodziewać się nowych inicjatyw prawodawczych nie tylko prawodawcy krajowego i unijnego, ale także w innych jurysdykcjach, w wymiarze globalnym.

Dla kompletności wywodu nie jest wystarczające skonstatowanie, że zjawisko krzyżowania się kompetencji organów istnieje i ustalenie jego przyczyn oraz skutków, ale

potrzebne jest także zaproponowanie rozwiązań. Mając na względzie przyczyny tego zjawiska krzyżowania, sformułowano cztery postulaty *de lege ferenda*: 1) Wyodrębnienie prawa danych jako odrębnej kompleksowej gałęzi prawa; 2) Centralizacja struktury stosowania RODO wobec największych podmiotów nadzorowanych i ustanowienie organów ochrony danych jako organów właściwych dla stosowania aktów prawnych w obszarze przetwarzania danych osobowych; 3) Wprowadzenie efektywnych instrumentów współpracy między podmiotami administrującymi stosującymi akty prawne w obszarze przetwarzania danych osobowych; 4) Wprowadzenie rozwiązania typu klauzula „safe harbour” dla podmiotów nadzorowanych. Realizacja tych postulatów nie doprowadziłaby do całkowitego wyeliminowania tego problemu, ponieważ, jak wskazano, jego przyczyny mają charakter strukturalny, a przez ich realizację nie można tych strukturalnych przyczyn wyeliminować. Chociaż te postulaty należy ocenić jako trudne do realizacji, nie powinno to jednak zaskakiwać. Gdyby problem można było łatwo rozwiązać, to zostałby już rozwiązany.

Sformułowanie postulatów *de lege ferenda*, które, pragmatycznie patrząc, mogłyby mieć szansę realizacji, stanowi w tym przypadku szczególne wyzwanie. Jest tak, ponieważ przyczyny tego zjawiska są strukturalne (rozdział 5. rozprawy). Przyczyny te wynikają nie z ewentualnych błędów w procesie legislacyjnym popełnionych przez prawodawcę unijnego czy krajowego, lecz z procesów, które dotyczą immanentnej trudności związanej z adekwatną odpowiedzią prawodawców na bardzo dynamiczne zmiany socjo-techniczne (rozłączenie regulacyjne scharakteryzowane w podrozdziale 5.2. rozprawy). Co więcej, ta odpowiedź wpisana jest w proces europeizacji prawa administracyjnego (podrozdział 5.4. rozprawy), który ze swej natury prowadzi do powstania wielopoziomowych struktur podmiotów administrujących, bez ustanowienia jasnych hierarchicznych relacji między nimi, czego konsekwencją jest i pozostanie multicentryczność. Właśnie te dwie przyczyny czynią trudnym formułowanie postulatów, które byłyby możliwe do wdrożenia bez konieczności uprzedniego rozstrzygnięcia, jaki powinien być optymalny stosunek prawodawcy do innowacji, i w którym momencie jej rozwoju należy interweniować, ani też bez dyskusji o zmianie traktatów unijnych, aby umożliwić uczynienie zarządzania administracyjnego w UE efektywniejszym oraz adekwatnym do nowych wyzwań. Obie te kwestie wykraczają poza naukę prawa administracyjnego, obejmując zagadnienia z prawa konstytucyjnego, etyki, informatyki i nauk ekonomicznych. Kwestie te mają jednak fundamentalne znaczenie i warte są dyskusji w ujęciu systemowym, która powinna odbyć się z udziałem ekspertów z każdej z tych dyscyplin razem, a także psychologów, socjologów i lekarzy. Chociaż dyskusja ta jest trudna, to nie należy od niej odstąpić; zadecyduje bowiem, jak wyglądały będą dalsze etapy transformacji cyfrowej

i miejsce, jakie zajmie w niej jednostka. Stawką jest dojrzały i efektywniejszy model regulacji przetwarzania danych osobowych w UE i w Polsce.

Ambicją tej rozprawy było, aby zaproponować ramy teoretyczne do dyskusji o tym zjawisku. Przeprowadzenie tej dyskusji jest potrzebne dla ustanowienia optymalnego modelu regulacji przetwarzania danych osobowych w UE i w Polsce. Problem ten nie dotyczy wyłącznie UE, lecz ma wymiar globalny i ze swojej istoty transgraniczny tak jak sama transformacja cyfrowa i procesy automatycznego przetwarzania danych. Zgodnie z informacjami Konferencji Narodów Zjednoczonych ds. Handlu i Rozwoju (UNCTAD), 137 na 194 państw przyjęło akty prawne w celu ochrony danych osobowych i prywatności¹²³⁴. Z perspektywy podmiotów nadzorowanych prowadzących działalność globalnie zwiększenie liczby tych aktów prawnych w różnych jurysdykcjach w ostatnich dwóch dekadach stanowi wyzwanie operacyjne, ponieważ wymaga dostosowania tych samych procesów przetwarzania do obowiązków wynikających z różnych aktów i odpowiadania względem różnych podmiotów administrujących. Chociaż przynajmniej niektóre te akty inspirowane są RODO¹²³⁵ i Konwencją 108¹²³⁶, to jednak różnią się między sobą¹²³⁷. Niekiedy różnice wynikają z czynników pozaprawnych, na przykład odmiennego stosunku do prywatności jako wartości w społeczeństwach indywidualistycznych i kolektywnych¹²³⁸. Prowadzi to do sformułowania pytań w odniesieniu do globalnej regulacji przetwarzania danych osobowych¹²³⁹: 1) Czy ustanowienie wielu podobnych, ale nie tożsamy standardów ochrony danych osobowych

¹²³⁴ UNCTAD, Data Protection and Privacy Legislation Worldwide, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>; por. także: G. Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey, „Privacy Laws & Business International Report” 2017, Iss. 145, <https://ssrn.com/abstract=2993035> (dostęp: 20.09.2024 r.).

¹²³⁵ Por. A. Bradford, The Brussels effect: how the European Union rules the world, Oxford 2020. N. Martin, F. Ebberts, When Regulatory Power and Industrial Ambitions Collide: The 'Brussels Effect,' Lead Markets, and the GDPR. [in:] Privacy Symposium 2022: Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT), Cham 2022.

¹²³⁶ Por. L. A. Bygrave, The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects, CLSR 2021, Vol. 40; A. Mantelero, The Future of Data Protection: Gold Standard vs. Global Standard, CLSR 2021, Vol. 40.

¹²³⁷ Zobacz przykładowo: H. Mukiri-Smith, R. Leenes, Beyond the 'Brussels Effect'? Kenya's Data Protection Act (DPA) 2019 and the European Union's General Data Protection Regulation (GDPR) 2018, EDPL 2021, Vol. 7, Iss. 4, s. 502-519.

¹²³⁸ Por. S. Basu, *Privacy Protection: A Tale of Two Cultures*, „Masaryk University Journal of Law and Technology” 2012, Vol. 6, No. 1, s. 1-34; H. Cho, B. Knijnenburg, A. Kobsa et al., *Collective Privacy Management in Social Media: A Cross-Cultural Validation*, „ACM Transactions on Computer-Human Interaction (TOCHI)” 2018, Vol. 25, No. 3, s.1-33.

¹²³⁹ Należy zaznaczyć, że sama dyskusja o globalnej regulacji przetwarzania danych osobowych nie jest nowa. Przykładowo, M. L. Rustad, T. H. Koenig, *Towards a Global Data Privacy Standard*, „Florida Law Review” 2019, Vol. 71, No. 2, s. 365-454; G. Greenleaf, *Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi*, „UNSW Law Research Paper” 2018, No. 18-56, <https://ssrn.com/abstract=3184548> (dostęp: 20.09.2024 r.).

w poszczególnych jurysdykcjach jest optymalne? 2) Czy możliwe i potrzebne jest ustanowienie jednego globalnego standardu ochrony danych osobowych, który jednocześnie umożliwiłby interoperacyjność¹²⁴⁰ tych danych w celach służących ludzkości, np. naukowych badaniach medycznych? 3) W jaki sposób podmioty administrujące w różnych jurysdykcjach mogłyby współpracować, aby zoptymalizować zmniejszenie ryzyk i wykorzystanie szans transformacji cyfrowej? ¹²⁴¹ Pytania te wyznaczają interesujący i ważny obszar do dalszych badań naukowych. To, że na pytania te wciąż nie ma odpowiedzi satysfakcjonującej z pragmatycznej perspektywy, oznacza, że regulacja przetwarzania danych osobowych tak w wymiarze regionalnym, jak i globalnym (co powiązać można z ideą globalnego prawa administracyjnego¹²⁴²) jest wciąż na względnie wczesnym etapie rozwoju.

¹²⁴⁰ *Interoperacyjność*, [hasło w:] *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, red. G. Szpor, L. Grochowski, Warszawa 2021, s. 228-230.

¹²⁴¹ Zaznaczyć należy, że istnieje nieformalna współpraca między tymi podmiotami, np. Global Privacy Enforcement Network, <https://www.privacyenforcement.net/> (dostęp: 15.09.2024 r.). Więcej na temat takich instrumentów: EDPB, *International Cooperation & Cooperation with Other Authorities* https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/international-cooperation-cooperation-other_en (dostęp: 15.09.2024 r.).

¹²⁴² Por. R. Tripathi, *Concept of Global Administrative Law: An Overview*, „India Quarterly” 2011, Vol. 67, No. 4, <http://www.jstor.org/stable/45073012> (dostęp: 20.09.2024 r.).

SPIS ILUSTRACJI

Schemat 1 Porównanie graficzne zakresu NIS a NIS 2.....	111
Schemat 2. Schemat organizacyjny krajowego systemu cyberbezpieczeństwa	218

WYKAZ ŹRÓDEŁ

AKTY PRAWNE

Prawo międzynarodowe

1. Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.).
2. Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 z późn. zm.).
3. Protokół Dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, sporządzony w Strasburgu dnia 8 listopada 2001 r. (Dz. U. z 2006 r. Nr 3, poz. 15).

Prawo Unii Europejskiej

4. Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 115 2008 r., s. 47).
5. Traktat o Unii Europejskiej (wersja skonsolidowana: Dz. Urz. UE C 202 2016 r., s. 13).
6. Karta praw podstawowych (wersja skonsolidowana: Dz. Urz. UE C 202 2016 r., s. 389).
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1 z późn. zm.).
8. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE L 201, s. 37 z późn. zm.).
9. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub

finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. Urz. UE L 141, s. 73 z późn. zm.) wraz z późniejszymi zmianami.

10. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337, s. 35 z późn. zm.).
11. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Tekst mający znaczenie dla EOG) PE/86/2018/REV/1 (Dz. Urz. L 151, s. 15).
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Tekst mający znaczenie dla EOG) PE/17/2022/REV/1 (Dz. Urz. L 265, s. 1).
13. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Tekst mający znaczenie dla EOG) PE/30/2022/REV/1 (Dz. Urz. L 277, s. 1).
14. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) PE/49/2023/REV/1 (Dz. Urz. L 2023/2854, s.1)
15. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Tekst mający znaczenie dla EOG) PE/85/2021/REV/1 (Dz. Urz. L 152, s. 1).

16. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1781 z dnia 13.09.2023 w sprawie ustanowienia ram dotyczących środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników oraz zmiany rozporządzenia (UE) 2021/694 (akt w sprawie czipów) (Dz. Urz. UE L 229, s. 1).
17. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1288/2013 z dnia 11 grudnia 2013 r. ustanawiające „Erasmus+”: unijny program na rzecz kształcenia, szkolenia, młodzieży i sportu oraz uchylające decyzje nr 1719/2006/WE, 1720/2006/WE i 1298/2008/WE (Dz. Urz. UE L 347, s. 50 z późn. zm.).
18. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/241 z dnia 12 lutego 2021 r. ustanawiające Instrument na rzecz Odbudowy i Zwiększania Odporności, (Dz. Urz. UE L 57, s. 17 z późn. zm.).
19. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/695 z dnia 28 kwietnia 2021 r. ustanawiające program ramowy w zakresie badań naukowych i innowacji Horyzont Europa oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie oraz uchylające rozporządzenia (UE) nr 1290/2013 i (UE) nr 1291/2013, (Dz. Urz. UE L 170, s. 1).
20. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Tekst mający znaczenie dla EOG) PE/31/2018/REV/1 (Dz. Urz. UE L 295, s. 39).
21. Rozporządzenie Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 1, 2003 r., s. 1).
22. Rozporządzenie Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu + Rozporządzenie Rady (WE) nr 139/2004 z dnia 20 stycznia 2004 r. w sprawie kontroli koncentracji przedsiębiorstw.

23. Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylecia decyzji Komisji 2009/78/WE (Dz. Urz. UE L 331, 2010 r., s. 12).
24. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/942 z dnia 5 czerwca 2019 r. ustanawiające Agencję Unii Europejskiej ds. Współpracy Organów Regulacji Energetyki (przekształcenie) (Tekst mający znaczenie dla EOG) PE/83/2018/REV/1 (Dz. Urz. UE L 158, s. 22).
25. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333, s. 1).
26. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257, s. 73).
27. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1620 z dnia 31 maja 2024 r. w sprawie ustanowienia Urzędu ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010. Tekst mający znaczenie dla EOG. PE/35/2024/INIT (Dz. Urz. UE L 2024/1620, s. 1).
28. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu. (Tekst mający znaczenie dla EOG) PE/36/2024/REV/1 (Dz. Urz. UE L 2024/1624, s. 1).
29. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1 z dnia 11 grudnia 2018 r. mająca na celu nadanie organom ochrony konkurencji państw członkowskich uprawnień w celu skuteczniejszego egzekwowania prawa i zapewnienia należytego funkcjonowania rynku wewnętrznego (Tekst mający znaczenie dla EOG) PE/42/2018/REV/1 (Dz. Urz. UE L 11, 2019 r., s. 3).

30. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Tekst mający znaczenie dla EOG) PE/53/2018/REV/1 (Dz. Urz. UE L 303, s. 59).
31. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257, s. 73).
32. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1620 z dnia 31 maja 2024 r. w sprawie ustanowienia Urzędu ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010. (Tekst mający znaczenie dla EOG) PE/35/2024/INIT (Dz. Urz. L 2024/1620, s. 1).
33. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu. (Tekst mający znaczenie dla EOG) PE/36/2024/REV/1 (Dz. Urz. L 2024/1624, s. 1).
34. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337, s. 35 z późn. zm.).
35. Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz. Urz. UE L 95, s. 29 z późn. zm.).
36. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE i uchylająca dyrektywę 1999/44/WE (Dz. Urz. UE L 136, s. 28 z późn. zm.).
37. Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady

- 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady (dyrektywa o nieuczciwych praktykach handlowych) (Dz. Urz. UE L 149, s. 22 z późn. zm.).
38. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. Urz. UE L 130, s. 92).
39. Dyrektywa 2006/114/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca reklamy wprowadzającej w błąd i reklamy porównawczej (wersja ujednolicona) (Dz. Urz. UE L 376, s. 21).
40. Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz. Urz. UE L 304, s. 64 z późn. zm.).
41. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333, s. 164).
42. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 172, s. 56).
43. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca dyrektywę (UE) 2019/1937 oraz zmieniająca i uchylająca dyrektywę (UE) 2015/849 (Tekst mający znaczenie dla EOG) PE/37/2024/INIT. (Dz. Urz. UE L 2024/1640, s. 1).
44. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady

- (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. Urz. UE L 141, s. 73 z późn. zm.).
45. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Tekst mający znaczenie dla EOG) PE/72/2017/REV/1 (Dz. Urz. UE L 156, s. 43–74).
 46. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1673 z dnia 23 października 2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych (Dz. Urz. UE L 284, s. 22).
 47. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE L 201, s. 37 z późn. zm.).
 48. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119, s. 89).
 49. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281, s. 31 z późn. zm.).
 50. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194, s. 1).
 51. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE)

2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Tekst mający znaczenie dla EOG) PE/32/2022/REV/2 (Dz. Urz. UE L 333, s. 80).

Prawo krajowe (polskie)

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.).
2. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 r. poz. 1257 z późn. zm.).
3. Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2019 r. poz. 2325 z późn. zm.).
4. Ustawa z dnia 22 maja 2003 r. o nadzorze ubezpieczeniowym i emerytalnym (t.j. Dz. U. z 2019 r. poz. 207).
5. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2019 r. poz. 2460 z późn. zm.).
6. Ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym (t.j. Dz. U. z 2019 r. poz. 1871 z późn. zm.).
7. Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. Dz. U. z 2020 r. poz. 180 z późn. zm.).
8. Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2019 r. poz. 369 z późn. zm.).
9. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2020 r. poz. 794).
10. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2020 r. poz. 971).
11. Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. Dz. U. z 2019 r. poz. 1292 z późn. zm.).
12. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r. poz. 1369).

13. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).
14. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. poz. 730).
15. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2019 r. poz. 730 ze zm.).
16. Uchylona ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2018 r. poz. 723).
17. Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (t.j. Dz. U. z 2022 r. poz. 2512 z późn. zm.).
18. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r. poz. 1206).
19. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. poz. 730).
20. Ustawa z dnia 7 lipca 2023 r. o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli (Dz. U. poz. 1369).
21. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2023 r. poz. 2488 z późn. zm.).
22. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2023 r. poz. 1545 z późn. zm.).
23. Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2023 r. poz. 1550 z późn. zm.).

24. Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą "Program Rozwoju Kompetencji Cyfrowych" (M. P. z 2023 r. poz. 318).

Prawo innych jurysdykcji krajowych

1. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Francuska ustawa nr 78-17 z dnia 6 stycznia 1978 r. o przetwarzaniu danych, zbiorach danych i swobodach osobistych).
2. UK Data Protection Act 2018 ,
<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
3. Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 <https://www.legislation.gov.uk/uksi/2019/419/contents>, (dostęp: 20.09.2024 r.).
4. Dutch General Data Protection Regulation Implementation Act. Unofficial translation, https://www.dataguidance.com/sites/default/files/dutch_general_general_data_protection_regulation_implementation_act.pdf

Projekty aktów prawnych

1. Uzasadnienie do wniosku „Dyrektywa parlamentu europejskiego i rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148”, COM/2020/823 final.
2. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679”, COM/2023/348 final.
3. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)”, COM/2012/011 final - 2012/0011 (COD).
4. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające Urząd ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu i zmieniające

rozporządzenia (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010”, COM/2021/421 final.

5. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy lub finansowania terroryzmu”, COM/2021/420 final.
6. Wniosek „Dyrektywa Parlamentu Europejskiego i Rady w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić, mających na celu zapobieganie wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz uchylająca dyrektywę (UE) 2015/849”, COM/2021/423 final.
7. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020”, COM/2022/454 final;
8. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi)”, COM/2020/767 final
9. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia”, COM/2022/197 final.
10. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) 1095/2010 i (UE) 2022/2554”, COM/2023/360 final.
11. Wniosek „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych)”, COM/2022/68 final.

ORZECZNICTWO

Orzecznictwo TSUE

1. Wyrok TSUE z 9.03.2010 r., C-518/07, Komisja Europejska przeciwko Republice Federalnej Niemiec, EU:C:2010:125.
2. Wyrok TSUE z 16.10.2012 r., C-614/10, Komisja Europejska przeciwko Republice Austrii, EU:C:2012:631.

1. Wyrok TSUE z 8.04.2014 r., C-288/12, Komisja Europejska przeciwko Węgrom, EU:C:2013:816.
2. Wyrok TSUE z 1.10.2015 r., C-230/14, Weltimmo s.r.o. przeciwko Nemzeti Adatvédelmi és Információszabadság Hatóság, EU:C:2015:639.
3. Wyrok TSUE z 5.06.2018 r., C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH, EU:C:2018:388.
4. Wyrok TSUE z 22.11.2022 r., C-37/20, WM przeciwko Luxembourg Business Registers, EU:C:2022:912.
5. Wyrok TSUE z 23.11.2006 r., C-238/05, Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL przeciwko Asociación de Usuarios de Servicios Bancarios (Ausbanc), EU:C:2006:734.
6. Wyrok TSUE z 4.07.2023 r., C-252/21, Meta Platforms Inc., Meta Platforms Ireland Ltd, Facebook Deutschland GmbH przeciwko Bundeskartellamt przy udziale Verbraucherzentrale Bundesverband eV, EU:C:2023:537.
7. Wyrok TSUE z 23.04.1991 r., C-41/90, Klaus Höfner i Fritz Elser przeciwko Macrotron GmbH, EU:C:1991:161.
8. Wyrok TSUE z 6.11.2003 r., C-101/01, Bodil Lindqvist, EU:C:2003:596.
9. Wyrok TSUE z 3.05.2018 r., T-653/16, Republika Malty przeciwko Komisji Europejskiej, EU:T:2018:241.
10. Wyrok TSUE z 13.05.2014 r., C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi, EU:C:2014:317.
11. Wyrok TSUE z 6.10.2015 r., C-362/14, Maximillian Schrems przeciwko Data Protection Commissioner, EU:C:2015:650.
12. Wyrok TSUE z 20.12.2017 r., C-434/16, Peter Nowak przeciwko Data Protection Commissioner, EU:C:2017:994.

13. Wyrok TSUE z 9.11.2010 r., C-92/09 i C-93/09, Volker und Markus Schecke GbR (C-92/09) i Hartmut Eifert (C-93/09) przeciwko Land Hessen, EU:C:2010:662.
14. Wyrok TSUE z 29.07.2019 r., C-40/17, Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV, EU:C:2019:629.
15. Wyrok TSUE z 19.10.2016 r., C-582/14, Patrick Breyer przeciwko Bundesrepublik Deutschland, EU:C:2016:779.
16. Wyrok TSUE z 9.11.2023 r., C-319/22, Gesamtverband Autoteile-Handel eV przeciwko Scania CV AB, EU:C:2023:837.
17. Wyrok TSUE (Sądu) z 26.04.2023 r., T-557/20, Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji (SRB) przeciwko Europejskiemu Inspektorowi Ochrony Danych (EIOD), EU:T:2023:219.
18. Wyrok TSUE z 13.06.1958 r., 9-56, Meroni & Co., Industrie Metallurgiche, SpA przeciwko Wysokiej Władzy EWWiS, EU:C:1958:7.
19. Wyrok TS z 22.03.2022 r., C-117/20, bpost SA przeciwko Autorité belge de la concurrence, EU:C:2022:202.
20. Wyrok TS z 18.11.2008 r., C-158/07, Jacqueline Förster przeciwko Hoofddirectie van de Informatie Beheer Groep, EU:C:2008:630.
21. Wyrok TSUE z 7.12.2023 r., C-634/24, SCHUFA OQ przeciwko Land Hessen, przy udziale SCHUFA Holding AG, EU:C:2023:957.

Orzecznictwo TK

1. Wyrok TK z 21.04.2004 r., K 33/03, OTK-A 2004/4, poz. 31.
2. Wyrok TK z 21.02.2001 r., P 12/00, OTK 2001/3, poz. 47.
3. Wyrok TK z 13.03.2007 r., K 8/07, OTK-A 2007/3, poz. 26.
4. Wyrok TK z 20.06.2017 r., P 124/15, OTK-A 2017, poz. 50.
5. Wyrok TK z 21.04.2015 r., P 40/13, OTK-A 2015/4, poz. 48.

6. Wyrok TK z 21.10.2014 r., P 50/13, OTK-A 2014/9, poz. 103.
7. Wyrok TK z 1.12.2016 r., K 45/14, OTK-A 2016, poz. 99.

Orzecznictwo polskich sądów administracyjnych

1. Wyrok NSA z 26.09.2018 r., I OSK 11/17, SIP LEX nr 2573629.
2. Wyrok NSA z 5.12.2017 r., II OSK 346/17, SIP LEX nr 2449251.
3. Wyrok NSA z 6.05.2015 r., I OSK 2287/13, SIP LEX nr 1773636.
4. Wyrok WSA w Warszawie z 5.05.2021 r., II SA/Wa 2222/20, SIP LEX nr 3209095.
5. Wyrok WSA w Warszawie z 13.04.2017 r., VII SA/Wa 1069/16, CBOSA.
6. Wyrok WSA w Warszawie z 25.04.2014 r., II SA/Wa 30/14, CBOSA.
7. Wyrok WSA w Warszawie z 22.04.2021 r., II SA/Wa 1865/20, SIP LEX nr 3178526.
8. Wyrok WSA w Warszawie z 23.02.2022 r., II SA/Wa 1128/21, SIP LEX nr 3349591.
9. Wyrok WSA w Warszawie z 18.11.2022 r., II SA/Wa 193/22, SIP LEX nr 3457484.
10. Wyrok NSA z 17.10.2022 r., II GSK 1971/21, SIP LEX nr 3442475.

Orzecznictwo sądów innych jurysdykcji krajowych

1. VG Köln, Urt. v. 16.2.2017 – 13 K 6093/15.
2. OVG 3Nordrhein-Westfalen, 19.10.2017 – 16 A 770/17.

DECYZJE ADMINISTRACYJNE, OPINIE I DOKUMENTY URZĘDOWE

1. Commission Nationale Informatique et Libertes, Status & Composition, <https://www.cnil.fr/en/cnil/status-composition> (dostęp: 20.09.2024 r.).
2. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. BfDI, About us. https://www.bfdi.bund.de/EN/DerBfDI/UeberUns/ueberuns_node.html (dostęp: 20.09.2024 r.).
3. BfDI, Data Protection Authorities of the Federal States (Länder) <https://www.bfdi.bund.de/EN/Service/Anschriften/Laender/Laender-node.html> (dostęp: 20.09.2024 r.).
4. Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities (5.08.2021),

- https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf (dostęp: 20.09.2024 r.).
5. EROD, Wytyczne 8/2022 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (28.03.2023), https://edpb.europa.eu/system/files/2023-10/edpb_guidelines_202208_identifying_lsa_targeted_update_pl.pdf (dostęp: 20.09.2024 r.).
 6. EROD, Wytyczne 02/2022 w sprawie stosowania art. 60 RODO (14.03.2022), https://www.edpb.europa.eu/system/files/2022-10/guidelines_202202_on_the_application_of_article_60_gdpr_pl.pdf (dostęp: 20.09.2024 r.).
 7. UODO, Sprawozdanie z działalności Prezesa UODO w roku 2022, <https://uodo.gov.pl/pl/file/4404> (dostęp: 20.09.2024 r.).
 8. UODO, Procedura Weryfikacji Pasażerów Linii Ryanair. UODO Reaguje (28.08.2023): <https://uodo.gov.pl/pl/138/2815> (dostęp: 20.09.2024 r.).
 9. UODO. O Ochronie Danych Osobowych. Między Teorią a Praktyką (31.03.2023): <https://uodo.gov.pl/pl/138/2652> (dostęp: 20.09.2024 r.).
 10. European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM (2020) 65 final.
 11. Komisja, Cyfrowa dekada Europy: Komisja wyznacza kierunek w celu utworzenia do 2030 r. Europy opartej na technologiach cyfrowych. Komunikat prasowy z dnia 9.03.2021, https://ec.europa.eu/commission/presscorner/detail/pl/IP_21_983. (dostęp: 20.09.2024 r.).
 12. Komisja, Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie, COM/2021/118 final.
 13. European Data Protection Supervisor, Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection

- in the Digital Economy. (2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (dostęp: 20.09.2024 r.).
14. EDPB, International Cooperation & Cooperation with Other Authorities, https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/international-cooperation-cooperation-other_en (dostęp: 20.09.2024 r.).
 15. Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43. Rozporządzenia. Wersja 3.0 (4.06.2019 r.), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pl.pdf (dostęp: 20.09.2024 r.).
 16. Decision of 23.3.2023 on setting up the High-Level Group for the Digital Markets Act, C (2023) 1833 final, https://competition-policy.ec.europa.eu/system/files/2023-03/High_Level_Group_on_the_DMA_0.pdf (dostęp: 20.09.2024 r.).
 17. Rada Europy, Full List of Signatures and Ratifications – Convention 223 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=223> (dostęp: 20.09.2024 r.).
 18. EROD, RODO: wytyczne, zalecenia, najlepsze praktyki, https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_pl (dostęp: 20.09.2024 r.).
 19. Komisja Europejska, Opinions and recommendations, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (dostęp: 20.09.2024 r.).
 20. Opinion 03/2013 on purpose limitation, WP 203 (2.04.2013), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (dostęp: 20.09.2024 r.).
 21. Opinion 15/2011 on the definition of consent, WP 187 (13.06.2011), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (dostęp: 20.09.2024 r.).
 22. Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, wersja 1.1, (04.05.2020 r.),

- https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consult_pl.pdf (dostęp: 20.09.2024 r.).
23. EROD, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217 (9.04.2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (dostęp: 20.09.2024 r.).
 24. EROD, Opinia 08/2024 w sprawie ważnej zgody w kontekście modeli „wyraż zgodę albo zapłacić” stosowanych przez duże platformy internetowe (Przyjęta 17 kwietnia 2024 r.), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consultorpay_pl.pdf (dostęp: 15.09.2024 r.).
 25. EROD, Guidelines on transparency under Regulation 2016/679. Adopted on 29 November 2017. As last Revised and Adopted on 11 April 2018, WP 260 rev.01, <https://ec.europa.eu/newsroom/article29/items/622227/en> (dostęp: 20.09.2024 r.).
 26. EROD, Guidelines on Data Protection Impact Assessment (DPIA) WP 248 rev.01 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711 (dostęp: 20.09.2024 r.).
 27. Guidelines on Personal data breach notification under Regulation 2016/679. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018, WP 250 rev.01, <https://ec.europa.eu/newsroom/article29/items/612052/en> (dostęp: 20.09.2024 r.).
 28. Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679. Wersja 2.0 (4.06. 2019 r.) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_code_of_conduct_pl.pdf (dostęp: 20.09.2024 r.).
 29. Guidelines on the right to data portability, Adopted on 13 December 2016. As last Revised and adopted on 5 April 2017, WP 242 rev.01, <https://ec.europa.eu/newsroom/article29/items/611233/en> (dostęp: 20.09.2024 r.).
 30. Wytyczne 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3). Wersja 2.0, (12.11.2019 r.) https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_pl.pdf (dostęp: 20.09.2024 r.).

31. Obwieszczenie Komisji Europejskiej dotyczące zasad dostępu do akt Komisji w sprawach na mocy art. 81 i 82 Traktatu WE, art. 53, 54 i 57 Porozumienia EOG oraz rozporządzeniem Rady (WE) nr 139/2004 (Tekst mający znaczenie dla EOG) (Dz. Urz. UE C 325, 2005 r., s. 7).
32. Opinion No. 4/2007 on the concept of personal data – WP 136 (20.06.2007), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (dostęp: 20.09.2024 r.).
33. Opinion 05/2014 on Anonymisation Techniques, WP 216 (10.04.2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (dostęp: 20.09.2024 r.).
34. Komisja Europejska, A Europe fit for the digital age. Empowering people with a new generation of technologies, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en (dostęp: 20.09.2024 r.).
35. EIOD, Opinions, https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_en
36. Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities Adopted on 12 March 2019, https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf (dostęp: 20.09.2024 r.).
37. Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive Adopted on 14 November 2023, https://edpb.europa.eu/system/files/2023-11/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_en.pdf (dostęp: 20.09.2024 r.).
38. Opinia 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych (12.03.2019), https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_pl.pdf (dostęp: 20.09.2024 r.).

39. Anti-money laundering and countering the financing of terrorism legislative package (20.07.2021), https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en?prefLang=pl (dostęp: 20.09.2024 r.).
40. Opinion on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals (21.09.2022), https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf (dostęp: 20.09.2024 r.).
41. EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations (28.03.2023), https://edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf (dostęp: 20.09.2024 r.).
42. Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing (13.06.2011), 01008/2011/EN WP 186, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf (dostęp: 20.09.2024 r.).
43. ENISA, Handbook on Security of Personal Data Processing (29.01.2018), <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing> (dostęp: 20.09.2024 r.).
44. Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (9.11.2022), https://edps.europa.eu/system/files/2022-11/2022-0921_d2649_opinion_en.pdf (dostęp: 20.09.2024 r.).
45. Oświadczenie Europejskiej Rady Ochrony Danych w sprawie wpływu koncentracji gospodarczych na ochronę danych, (27.08.2018 r.), https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_pl.pdf (dostęp: 20.09.2024 r.).

46. Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf. (dostęp: 20.09.2024 r.).
47. Bundeskartellamt, *Bundeskartellamt prohibits Facebook from combining user data from different sources* (7.02.2019) https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (dostęp: 20.09.2024 r.).
48. Bundeskartellamt, Case Summary. Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing, (15.02.2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4 (dostęp: 20.09.2024 r.).
49. Statement on the Digital Services Package and Data Strategy Adopted on 18 November 2021, https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf (dostęp: 20.09.2024 r.).
50. Opinion 2/2021 on the Proposal for a Digital Markets Act (10.02.2021 r.), https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf (dostęp: 20.09.2024 r.).
51. Opinion 1/2021 on the Proposal for a Digital Services Act (10.02.2021 r.), https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf (dostęp: 20.09.2024 r.).
52. Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space (12.07.2022), https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en_.pdf (dostęp: 20.09.2024 r.).
53. Wspólna opinia EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu i Rady europejskiego danymi (akt zarządzania danymi) Wersja 1.1 (9.06.2021 r.), https://edpb.europa.eu/system/files/2021-09/edpb-edps_joint_opinion_dga_pl_0.pdf (dostęp: 20.09.2024 r.).
54. Wspólna opinia EROD i EIOD 2/2022 na temat wniosku Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do

- danych i ich wykorzystywania (akt w sprawie danych) (4.05.2022 r.), https://edpb.europa.eu/system/files/2023-03/edpb-edps_jointopinion_2022-02_data_act_proposal_pl.pdf (dostęp: 20.09.2024 r.).
55. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0 (07.07.2021 r.), pkt 14, s. 10, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (dostęp: 20.09.2024 r.).
56. Decyzja PUODO, ZSPR.027.306.2019, SIP LEX nr 3285140.
57. UODO, *Czy instytucje finansowe mogą kopiować dowody osobiste?* (16.08.2022 r.), <https://uodo.gov.pl/pl/138/2476#:~:text=W%20ostatnim%20czasie%20w%20związku,w%20tym%20zakresie%20pozostają%20niezmienne> (dostęp: 20.09.2024 r.).
58. Pismo GIIF z 4.02.2020 r. nr IF6.701.29.2019 do PUODO.
59. Opinia Rzecznika Generalnego w sprawie C-582/14, (12.05.2016), EU:C:2016:339.
60. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) Adopted on 4 April 2017, WP 247, <https://ec.europa.eu/newsroom/article29/redirection/item/610140> (dostęp: 20.09.2024 r.).
61. Wytyczne w sprawie oceny horyzontalnego połączenia przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw (Dz. Urz. UE C 31, 2004 r., s. 5).
62. Wytyczne w sprawie oceny niehoryzontalnych połączeń przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw (Dz. Urz. UE C. 265, 2008 r., s. 6).
63. Komunikat Komisji Europejskiej – wytyczne w sprawie priorytetów, którymi Komisja będzie się kierować przy stosowaniu art. 82 Traktatu WE w odniesieniu do szkodliwych działań o charakterze praktyki wyłączającej, podejmowanych przez przedsiębiorstwa dominujące (Dz. Urz. UE C 45, 2009 r., s. 7 z późn. zm.).
64. Obwieszczenie Komisji Europejskiej w sprawie definicji rynku właściwego do celów wspólnotowego prawa konkurencji (Dz. Urz. UE C 372, 1997 r., s. 5).

65. Decyzja Komisji Europejskiej, Brak sprzeciwu wobec zgłoszonej koncentracji (Sprawa M.7217 – Facebook/WhatsApp) (Tekst mający znaczenie dla EOG) (Dz. Urz. UE C 417, 2014 r., s.4).
66. Decyzja Komisji Europejskiej, Zgłoszenie zamiaru koncentracji (sprawa M.8124 – Microsoft/LinkedIn) (Tekst mający znaczenie dla EOG) (Dz. Urz. UE C 388, 2016 r., s.4).
67. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia w zakresie danych COM(2020) 66 final.
68. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev. 01,(4.04.2017), <https://ec.europa.eu/newsroom/article29/items/611236> (dostęp: 20.09.2024 r.).
69. Statement on enforcement cooperation. Adopted on 28 April 2022, [edpb_statement_20220428_on_enforcement_cooperation_en.pdf](#) (dostęp: 20.09.2024 r.).
70. EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level, [edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf](#) (dostęp: 20.09.2024 r.).
71. Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (dostęp: 20.09.2024 r.).
72. Objasnienia prawne z dnia 23 stycznia 2019 r. wydane przez Ministra Cyfryzacji na podstawie art. 33 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców na wniosek Rzecznika Małych i Średnich Przedsiębiorców, [dostęp: https://mc.bip.gov.pl/objasnienia-prawne/objasnienia-prawne.html](https://mc.bip.gov.pl/objasnienia-prawne/objasnienia-prawne.html) (dostęp: 20.09.2024 r.).

73. Memorandum of Understanding on increasing cooperation between the European Data Protection Supervisor and the European Union Agency for Cybersecurity, https://www.edps.europa.eu/system/files/2022-11/22-11-30_edps_enisa_mou_en.pdf (dostęp: 20.09.2024 r.).
74. Porozumienie o współpracy w zakresie naruszeń prawa związanych z przetwarzaniem danych osobowych pacjentów zawarte w Warszawie, 7 grudnia 2023 roku pomiędzy UODO a Głównym Inspektorem Farmaceutycznym,, <https://uodo.gov.pl/pl/file/4537> (dostęp: 20.09.2024 r.).
75. Opinia EIOD 12/2021 w sprawie pakietu legislacyjnego dotyczącego przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (AML/CFT) (22.09.2021 r.), https://www.edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf#page=7.57 (dostęp: 20.09.2024 r.).
76. First EDPS Orientations for EUIs using Generative AI, (3.06.2024), https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en (dostęp: 20.09.2024 r.).
77. CNIL, *AI: CNIL publishes its first recommendations on the development of artificial intelligence systems*. (7.06.2024) <https://www.cnil.fr/en/ai-cnil-publishes-its-first-recommendations-development-artificial-intelligence-systems> (dostęp: 20.09.2024 r.).
78. Garante per la protezione dei dati personali, 'Provvedimento dell'11 aprile 2023 [9874702]' (Garante per la protezione dei dati personali, 11.04.2023) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702> (dostęp: 20.09.2024 r.).
79. Restricted Committee Deliberation No SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf (dostęp: 20.09.2024 r.).
80. Komisja Europejska. *Nowe Ramy Legislacyjne* https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en?prefLang=pl (dostęp: 20.09.2024 r.).

81. EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (18.06.2021 r.).
82. Decyzja Komisji Europejskiej z dnia 24 stycznia 2024 r. ustanawiająca Europejski Urząd ds. Sztucznej Inteligencji, Bruksela, C(2024) 390 final.
83. EDPB Statement 2024/03 on DPAs Role in AI Act.
https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf (dostęp: 20.09.2024 r.).
84. EDPB's Letter to the European Commission concerning Guidelines on the Interplay between Digital Markets Act (DMA) and GDPR (18.07.2024),
https://www.edpb.europa.eu/system/files/2024-07/edpb_letter_reply_com_gls_interplay_dma_gdpr_en.pdf (dostęp: 20.09.2024 r.).
85. EROD, Dokument EROD w sprawie ram skoordynowanego egzekwowania prawa na mocy rozporządzenia 2016/679 (przyjęty 20 października 2020 r.),
https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_documents_20201020_coordinatedenforcementframework_pl.pdf (dostęp: 10.09.2024 r.).
86. Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą,
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pl.pdf (dostęp: 20.09.2024 r.).
87. Zarządzenie Nr 13/2024 Prezesa Urzędu Ochrony Danych Osobowych z dnia 4 czerwca 2024 r. w sprawie: ustanowienia Społecznego Zespołu Ekspertów przy Prezesie Urzędu Ochrony Danych Osobowych,
<https://uodo.gov.pl/583#:~:text=Spo%C5%82eczny%20Zesp%C3%B3%C5%82%20Ekspert%C3%B3w%20przy%20Prezesie%20Urz%C4%99du%20Ochrony%20Danych%20Osobowych%20zosta%C5%82,cia%C5%82em%20opiniodawczo%2Ddoradczym%20Prezesa%20Urz%C4%99du> (dostęp: 20.09.2024 r.).

LITERATURA

1. Accetto M., *The Principle of Effectiveness: Rethinking Its Role in Community Law*, „European Public Law” 2005, Vol. 11, Iss. 3, <https://doi.org/10.54648/euro2005030> (dostęp: 20.09.2024 r.).
2. Adamiak B., Borkowski J., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2022, SIP Legalis.
3. Affre J., Witek K., *Soft law Prezesa UOKiK na przykładzie „Informacji o sposobie składania wniosków o ograniczenie prawa wglądu w postępowaniach”*, „IKAR” 2020, nr 5.
4. Aghion Ph., Jones B. F., Jones Ch. I., *Artificial intelligence and economic growth* [in:] *The economics of artificial intelligence: An agenda*, edited by A. K. Agrawal, J. Gans, A. Goldfarb, Chicago and London: University of Chicago Press 2019.
5. Ajdukiewicz K., *Zarys logiki*, Warszawa: Państwowe Zakłady Wydawnictw Szkolnych 1958.
6. Allen D. W. E., Berg A., Berg Ch. et al. *Some Economic Consequences of the GDPR*, „Economics Bulletin” 2019, Vol. 39, No. 2, <https://ssrn.com/abstract=3160404> (dostęp: 20.09.2024 r.).
7. Arnould R. J., Grabowski H., *Auto Safety Regulation: An Analysis of Market Failure*, „The Bell Journal of Economics” 1981, Vol. 12, No. 1.
8. Ausloos J., *The Right to Erasure in EU Data Protection Law*, Oxford: Oxford University Press 2020.
9. Babis H. (red.), Flaga-Gieruszyńska K. (red.), *Rynek usług telekomunikacyjnych*, Warszawa: Wolters Kluwer Polska 2011.
10. Baets A. de, *A historian's view on the right to be forgotten*, Int. Rev. Law Comput. Technol. 2016, Vol. 30, No. 1-2, <http://dx.doi.org/10.1080/13600869.2015.1125155> (dostęp: 20.09.2024 r.).
11. Baldwin R. (ed.), Cave M. (ed.), Lodge M. (ed.), *The Oxford Handbook of Regulation*, Oxford: Oxford University Press 2010.

12. Baldwin R. (ed.), Cave M.(ed.), Lodge M. (ed.), *Understanding Regulation: Theory, Strategy, and Practice*, Oxford: Oxford University Press 2012, <https://doi.org/10.1093/acprof:osobl/9780199576081.003.0007> (dostęp: 10.02.2024 r.).
13. Banasiński C, Bychowska M., *Kompetencje decyzyjne Komisji Europejskiej i Prezesa UOKiK wynikające z rozporządzenia Rady UE nr 1/2003 w świetle zasady równoległego stosowania wspólnotowego i krajowego prawa antymonopolowego*, „Przegląd Prawa Handlowego” 2009, nr 3.
14. Banasiński C., Aziewicz D., Bielecki A. M. et al., *Polskie prawo antymonopolowe: zarys wykładu*, Warszawa: Wolters Kluwer Polska 2018.
15. Bania K., *Fitting the Digital Markets Act in the existing legal framework: the myth of the “without prejudice” clause*, „European Competition Journal” 2023, Vol.19, No. 1.
16. Barcentewicz M., *Interpreting the EU Digital Markets Act Consistently With the EU Charter’s Rights to Privacy and Protection of Personal Data*, „Bocconi University. MediaLaws.eu” 2023, 3.08.2023, <https://ssrn.com/abstract=4531383> (dostęp: 020.09.2024 r.).
17. Barkhuysen T., Ouden W., Schuurmans Y. E., *The law on administrative procedures in the Netherlands*, „Netherlands Administrative Law Library” 2012, dostęp: <https://www.nall.nl/tijdschrift/nall/2012/06/NALL-D-12-00004.pdf> (dostęp: 020.09.2024 r.).
18. Bartosiewicz A., Bieniasz J., Szczypiorski K., *Kompendium cyberbezpieczeństwa. Cz. I: Poradnik cyberbezpieczeństwa dla środowisk edukacyjnych i przedsiębiorstw*, Warszawa: PARP. Grupa PFR. Sektorowa Rada ds. Kompetencji. Telekomunikacja i Cyberbezpieczeństwo, 2023.
19. Basu S., *Privacy Protection: A Tale of Two Cultures*, „Masaryk University Journal of Law and Technology” 2012, Vol. 6, No. 1.
20. Bauer M.W., Trondal J., *The Palgrave Handbook of the European Administrative System. European Administrative Governance*, New York: Palgrave Macmillan 2015.

21. Bąk-Grabowska D., *Kształtowanie kultury organizacyjnej w urzędach administracji samorządowej*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Nauki Społeczne” 2010, t. 2, nr 129.
22. Bennett Moses L., *Regulating in the Face of Sociotechnical Change* [in:] *The Oxford Handbook of Law, Regulation and Technology*, edited by R. Brownsword, E. Scotford, K. Yeung, Oxford: Oxford University Press 2017, <https://doi.org/10.1093/oxfordhb/9780199680832.013.49> (dostęp: 31.12.2023 r.).
23. Besiekierska A. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.
24. Biega A. J., Potash P., Daumé H. et al., *Operationalizing the Legal Principle of Data Minimization for Personalization*, [in:] *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20)*, New York: Association for Computing Machinery 2020, <https://doi.org/10.1145/3397271.3401034> (dostęp: 20.09.2024 r.).
25. Bielak-Jomaa E., Lubasz D., *RODO. Ogólne Rozporządzenie o Ochronie Danych. Komentarz*, Warszawa: Wolters Kluwer Polska 2018, SIP LEX.
26. Black J., *The Rise, Fall and Fate of Principles Based Regulation*, „LSE Legal Studies Working Paper” 2010, No. 17, <http://dx.doi.org/10.2139/ssrn.1712862> (dostęp: 20.09.2024 r.).
27. Blind K., Niebel C., Rammer Ch., *The Impact of the EU General Data Protection Regulation on Innovation in Firms*, „ZEW - Centre for European Economic Research Discussion” 2022, No. 22-047, <http://dx.doi.org/10.2139/ssrn.4257740> (dostęp: 20.09.2024 r.).
28. Błachnio-Parzych A., *Zbieg odpowiedzialności karnej i administracyjno-karnej jako zbieg reżimów odpowiedzialności represyjnej*, Warszawa: Wolters Kluwer Polska 2016, SIP LEX.
29. Błachucki M., *System postępowania antymonopolowego w sprawach kontroli koncentracji przedsiębiorców*, Warszawa: Urząd Ochrony Konkurencji i Konsumentów 2012.

30. Błachucki M., *Współdziałanie organów administracji publicznej a obowiązek dokonywania urzędowej interpretacji przepisów. Glosa do wyroku Naczelnego Sądu Administracyjnego z 17.10.2022 r., II GSK 1971/21*), PPP 2024, nr 4.
31. Błaś A. (red.), *Pewność sytuacji prawnej jednostki w prawie administracyjnym*, Warszawa: Wolters Kluwer Polska 2012, SIP LEX.
32. Bobev T., Dessers V. K., Ducuing. Ch. et al., *White Paper on the Definition of Data Intermediation Services*, „CiTiP Working Paper Series” 2023, <http://dx.doi.org/10.2139/ssrn.4589987> (dostęp: 20.09.2024 r.).
33. Boć J., *Prawo administracyjne*, Wrocław: Kolonia Limited 2002.
34. Bois J., Van Cleynenbreugel P., *National Institutional Autonomy and EU law: time to reframe the stakes of interdisciplinary scholarship?*, „EUDAMONIA Working Paper” 2021, No. 1.
35. Bolecki A. et al., *Prawo konkurencji*, Warszawa: LexisNexis 2012, SIP LEX.
36. Bonnici J., *Exploring the non-absolute nature of the right to data protection*, Int. Rev. Law Comput. Technol. 2014, No. 28, <https://doi.org/10.1080/13600869.2013.801590> (dostęp: 20.09.2024 r.).
37. Bontridder N., Pouillet Y., *The role of artificial intelligence in disinformation*, „Data & Policy” 2021, Vol. 3, No. e32, <https://doi.org/10.1017/dap.2021.20>, (dostęp: 20.09.2024 r.).
38. Borgesius F.J.Z., *Singling out people without knowing their names—Behavioural targeting, pseudonymous data, and the new Data Protection Regulation*, CLSR 2016, No. 32(2).
39. Borkowski J., *Decyzja administracyjna*, Łódź-Zielona Góra: Zachodnie Centrum Organizacji 1999.
40. Börzel T. A., Heard-Lauréote K., *Networks in EU multi-level governance: concepts and contributions*, „Journal of Public Policy” 2009, No. 29(2).

41. Botta M., Wiedemann K., *The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey*, „The Antitrust. Bulletin 64” 2019, No. 3.
42. Boughey J., *Administrative Law: The Next Frontier For Comparative Law*, „International and Comparative Law Quarterly” 2013, No. 62(1), <https://doi.org/10.1017/S0020589312000553> (dostęp: 20.09.2024 r.).
43. Bounfour A., *From IT to Digital Transformation: A Long Term Perspective*, [in:] *Digital Futures, Digital Transformation: From Lean Production to Acceluction*, Cham etc: Springer 2016.
44. Bradford A. *The Brussels Effect: How the European Union Rules the World*, Oxford: Oxford University Press 2020.
45. Brewczyńska M., *A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation* [in:] *Research handbook on EU data protection law*, Cheltenham: Edward Elgar Publishing 2022.
46. Brewczyńska M., *Financial Intelligence Units: Reflections on the applicable data protection legal framework*, CLSR 2021, No. 43.
47. Brewczyńska M., Kosta E., *From the Fight Against Money Laundering and Financing of Terrorism Towards the Fight for Fundamental Rights: Role of Data Protection*, „Tilburg Law School Research Paper” 2023, No. 2, <https://ssrn.com/abstract=4328464> (dostęp: 20.09.2024 r.).
48. Brito Bastos F., Pałka P., *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?*, „European Constitutional Law Review” 2023, No. 19(3).
49. Brownsword R., *'The Challenge of Regulatory Connection', Rights, Regulation, and the Technological Revolution*, Oxford: Oxford University Press 2008, <https://doi.org/10.1093/acprof:oso/9780199276806.003.0006>, (dostęp: 7.02.2024 r.).
50. Brzozowski W., *Współdziałanie władz publicznych*, PiP 2010, nr 2.

51. Brzozowski W., *Zwalczanie przestępczości zorganizowanej w aspekcie finansowym*, Kraków: Zakamycze 2004.
52. Buchanan J. M., *Opportunity cost* [in:] *The world of economics*, edited by J. Eatwell, London: Palgrave Macmillan UK 1991.
53. Bułakowski J., *O kompetencjach organów administracji morskiej z perspektywy teorii prawa administracyjnego*, „Kortowski Przegląd Prawniczy” 2018, nr 3.
54. Burgess M., *How GDPR is failing*, 23.05.2022, <https://www.wired.co.uk/article/gdpr-2022> (dostęp: 20.09.2024 r.).
55. Bursztynowicz M., Sługocka M., *Postępowanie administracyjne dla jednostek samorządu terytorialnego. Komentarz*, Warszawa: Wolters Kluwer Polska 2020, SIP LEX.
56. Butenko A., Larouche P., *Regulation for Innovativeness or Regulation of Innovation?*, „TILEC Discussion Paper” 2015, No. 2015-007, <https://ssrn.com/abstract=2584863> (dostęp: 20.09.2024 r.).
57. Butenko A., *Sharing Energy: Dealing with Regulatory Disconnect in Dutch Energy Law*, 2016, <https://ssrn.com/abstract=2847590> (dostęp: 5.09.2024 r.).
58. Bygrave L. A., *The ‘Strasbourg Effect’ on Data Protection in Light of the ‘Brussels Effect’: Logic, Mechanics and Prospects*, CLSR 2021, Vol. 40.
59. Can A. T. İ. K., *Horizontal intervention, sectoral challenges: Evaluating the data act's impact on agricultural data access puzzle in the emerging digital agriculture sector*, CLSR 2023, Vol. 51.
60. Cappai M., Colangelo G., *Applying ne bis in idem in the Aftermath of bpost and Nordzucker: The Case of EU Competition Policy in Digital Markets*, „Market Law Review” 2023, <https://ssrn.com/abstract=4344075> or <http://dx.doi.org/10.2139/ssrn.434407> (dostęp: 20.09.2024 r.).
61. Carrapico H., Barrinha A., *The EU as a Coherent (Cyber)Security Actor*, „Journal of Common Market Studies” 2017, Vol. 55, No. 6.

62. Caveltly M., Smeets M., *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority*, J. Eur. Public Policy 2023, No. 30(7).
63. Celeste R. (ed.), Costello E. A. (ed.), Harbinja E. (ed.) et al., *Data Protection and Digital Sovereignty Post-Brexit*, Oxford: Hart Publishing 2023, <http://dx.doi.org/10.5040/9781509966516.ch-008> (dostęp: 20.09.2024 r.).
64. Chakraborty S. K., Koshy A. K., Raghunath A., *Data As Property: Towards a Property Based Model?*, „Global Privacy Law Review” 2023, Vol. 4, Iss. 4, <https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/4.4/GPLR2023025> (dostęp: 20.09.2024 r.).
65. Chamon M., *EU Agencies: Does the Meroni Doctrine Make Sense?*, „Maastricht Journal of European and Comparative Law” 2010, nr 17(3). <https://doi.org/10.1177/1023263X1001700304> (dostęp: 20.09.2024 r.).
66. Chemlali L., *The competence of non-lead supervisory authority under the EU GDPR'S one-stop-shop mechanism: CJEU judgment in Facebook and Others (C-645/19)*, „Journal of Media Law” 2022, Vol. 14, No. 2, <https://doi.org/10.1080/17577632.2022.2109852> (dostęp: 20.09.2024 r.).
67. Cherka M. (red.), Gołaszewski P. (red.), Piecha J. (red.) et al., *Kryzys, stagnacja, renesans? Prawo administracyjne przyszłości. Księga jubileuszowa profesora dr hab. Jacka Jagielskiego*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.
68. Cho H., Knijnenburg B., Kobsa A. et al., *Collective Privacy Management in Social Media: A Cross-Cultural Validation*, „ACM Transactions on Computer-Human Interaction (TOCHI)” 2018, Vol. 25, No. 3.
69. Ciechanowicz-McLean J., *Prawo ochrony środowiska jako kompleksowa dziedzina prawa – ustawa organiczna?* [w:] *Zagadnienia systemowe prawa ochrony środowiska*, red. P. Korzeniowski, Łódź: Wydawnictwo Uniwersytetu Łódzkiego 2015.
70. Cilak M., *Problem krzyżowania się kompetencji nadzorczych wojewody i regionalnych izb obrachunkowych w sferze działalności gospodarczej samorządu terytorialnego*, „Finanse Komunalne” 2013, nr 1-2.

71. Coglianese C., *Easy fix for federal regulatory overlap*, <https://eu.onlineathens.com/story/opinion/2015/04/02/coglianese-easy-fix-federal-regulatory-overlap/15498581007/> (dostęp: 20.09.2024 r.).
72. Colangelo G., Maggiolino M., *Data protection in attention markets: protecting privacy through competition?*, „Journal of European Competition Law & Practice” 2017, Vol. 8, No. 6.
73. Comandé G., *Elgar Encyclopedia of Law and Data Science*, Cheltenham: Edward Elgar Publishing 2022.
74. Costa-Cabral F., Lynskey O., *Family ties: the intersection between data protection and competition in EU Law*, „Common Market Law Review” 2017, Vol. 54, No. 11.
75. Council of Europe, *Handbook on European Data Protection Law: 2018 edition*, 2018.
76. Craig P. P., *Shared Administration and Networks: Global and EU Perspectives*, „Oxford Legal Studies Research Paper” 2009, No. 6, <https://ssrn.com/abstract=1333557> (dostęp: 20.09.2024 r.).
77. Crepax T., Gaur M., da Rosa Lazarotto B., *Measuring data access and re-use in the European Legal Framework for Data, from the General Data Protection Regulation (GDPR) law to the Proposed Data Act: the case of vehicle data*, „Open Research Europe” 2023, 3:192, <https://doi.org/10.12688/openreseurope.16468.1> (dostęp: 20.09.2024 r.).
78. Curtin D., Manucharyan T., *Legal acts and hierarchy of norms in EU law* [in:] *The Oxford Handbook of European Union Law* edited by Arnall A., Chalmers D., Oxford: Oxford University Press 2015.
79. Custers B., Malgieri G., *Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data*, CLSR 2022, Vol. 45.
80. Czaplicki K., Gryszczyńska A., Szpor G., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa: Wolters Kluwer Polska 2019, SIP LEX.
81. Czarnomska-Bokowy U., *Prawo konkurencji a projekt rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym—kto przypilnuje strażników?*, iKAR 2022, t. 11, nr 1.

82. Czerniawski M. (red.), Kawecki M. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2019.
83. Czerniawski M., *Odpowiedzialność administratora fanpage'a na Facebooku za przetwarzanie danych osobowych. Glosa do wyroku TS z dnia 5 czerwca 2018 r., C-210/16*, SIP LEX 2018.
84. Czerniawski M., *Pisemne odpowiedzi egzaminowanego oraz komentarze egzaminatora jako dane osobowe. Glosa do wyroku TS z dnia 20 grudnia 2017 r., C-434/16*, SIP LEX 2018.
85. Czerniawski M., *Rozdział II. Instytucja współadministrowania a pojęcie „ustalania” celów i sposobów przetwarzania danych osobowych – zarys problemu* [w:] *Rok RODO*, red. W. Wiewiórowski, H. Wolska, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.
86. Ćwiertnia M., *Charakter prawny kompetencji administracyjnych organów egzekucyjnych*, PPP 2018, nr 5.
87. Dacar R., *Is the Essential Facilities Doctrine Fit for Access to Data Cases? The Data Protection Aspect*, „Croatian Yearbook of European Law & Policy” 2022, Vol. 18, No. 1.
88. D'Amato A., *Legal Uncertainty*, „California Law Review” 1983, Vol. 71, No. 1.
89. Danek M., *Korzyści efektywnościowe w kontroli koncentracji przedsiębiorstw w systemach ochrony konkurencji Unii Europejskiej i Stanów Zjednoczonych Ameryki - porównanie prawno-ekonomiczne*, ZNUJ 2012, nr 3.
90. Davola A., Malgieri G., *Data, Power, and Competition Law: The (Im)possible Mission of the DMA?* [in:] *The Economics and Regulation of Digital Markets*, edited by F. Fagan, J. Langenfeld, Leeds: Emerald Publishing Limited 2023, <https://doi.org/10.1108/S0193-589520240000031003> (dostęp: 20.09.2024 r.).
91. Dawidowicz W., *Polskie prawo administracyjne*, Warszawa: Państwowe Wydawnictwo Naukowe 1980.
92. Demircan M., *The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions* [in:] *Privacy and Identity Management. Privacy and*

- Identity*, red. F. Bieker, J. Meyer, S. Pape, Cham: Springer 2022, https://doi.org/10.1007/978-3-031-31971-6_1 (dostęp: 20.09.2024 r.).
93. Derdak M.K., *Problem uwzględniania pozaekonomicznych czynników oceny koncentracji przez Prezesa UOKiK na przykładzie pluralizmu mediów*, iKAR 2022, nr 4.
94. Didenko A. N., *Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond*, „Uniform Law Review” 2020, Vol. 25, No. 1, <https://ssrn.com/abstract=3533664> (dostęp: 20.09.2024 r.).
95. Dimitrakopoulos D.G., *The Transposition of EU Law: ‘Post-Decisional Politics’ and Institutional Autonomy*, „European Law Journal” 2001, Vol. 7, No. 4, <https://doi.org/10.1111/1468-0386.00137> (dostęp: 20.09.2024 r.).
96. Długosz T., *Kompetencja w publicznym prawie gospodarczym*, Warszawa: Wydawnictwo C.H. Beck 2021, SIP Legalis.
97. Dmochowska A., Piotrowska A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2018, SIP Legalis.
98. Dmochowska A., Zadrożny M., *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warszawa: Wydawnictwo C.H. Beck 2016, SIP Legalis.
99. Dobkowski J., *Kompetencja administracyjna (niektóre uwagi na kanwie pracy A. Matczaka „Kompetencja organu administracji publicznej”, Kraków 2004)*, [w:] *Studia z zakresu nauk prawnoustrojowych*, t. 1: *Minesclinea*, red. J. Sługocki, Bydgoszcz: Wydawnictwo Kujawsko-Pomorska Szkoła Wyższa w Bydgoszczy 2008.
100. Dobosz P. (red.), Skrzydło-Niżnik I. (red.), *Jednolitość systemu prawa a jednolitość orzecznictwa sądowno-administracyjnego i administracyjnego w sprawach samorządowych*, Kraków: Zakamycze 2001.
101. Doczekalska A., *Język prawny w tworzeniu i transpozycji prawa Unii Europejskiej. Procesy hybrydyzacji*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.
102. Dorfleitner G., Hornuf L., Kreppmeier J., *Promise not fulfilled: FinTech, data privacy, and the GDPR*, „Electronic Markets” 2023, Vol. 33, No. 1.

103. Ducuing Ch., *Data as infrastructure? A study of data sharing legal regimes*, „Competition and Regulation in Network Industries” 2020, Vol. 21, No 2.
104. Duniewska Z. (red.), *Dobra chronione w prawie administracyjnym*, Łódź: Wydawnictwo Uniwersytetu Łódzkiego 2014.
105. Duniewska Z. (red.), Krakala A. (red.), Stahl M. (red.), *Zasady w prawie administracyjnym. Teoria, praktyka, orzecznictwo*, Warszawa: Wolters Kluwer Polska 2018, SIP LEX.
106. Duniewska Z., Lewicka R., Lewicki M., *Władza w przestrzeni administracji publicznej*, Warszawa: Wolters Kluwer Polska 2020.
107. Dymitruk M., *Akt o usługach cyfrowych w czasach ChatGPT: czy dostawcy generatywnej AI są pośrednikami internetowymi?*, „Prawo Nowych Technologii” 2023, nr 3.
108. Easterbrook F. H., *Cyberspace and the Law of the Horse*, „The University of Chicago Legal Forum” 1996, Vol. 1996, No 1.
109. Eberle E. J., *The Methodology of Comparative Law*, „Roger Williams University Law Review” 2011, Vol. 16, No. 1, http://docs.rwu.edu/rwu_LR/vol16/iss1/2 (dostęp: 20.09.2024 r.).
110. Ebers M., Sein K., *Data-driven Technologies – Challenges for Privacy and EU Data Protection Law* [in:] *Privacy, Data Protection and Data-driven Technologies*, red. M. Ebers, K. Sein, Abingdon: Routledge 2024, <https://ssrn.com/abstract=4823823> (dostęp: 20.09.2024 r.).
111. Egeberg M., Trondal J., *Agencification of the European Union Administration: Connecting the Dots*, „TARN Working Paper” 2016, No. 1, <https://ssrn.com/abstract=2754716> (dostęp: 20.09.2024 r.).
112. El Khoury A., *Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger’s Cat*, Eur. J. Risk Regul. 2017, Vol. 8, No. 1, (dostęp: 20.09.2024 r.).
113. El Khoury A., *Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data through Quantum Mechanics*, „Erasmus Law Review” 2018, Vol. 11, No 3.

114. Eliantonio M. (ed.), Korkea-aho E. (ed.), Mörtz U. (ed.), *Research Handbook on Soft Law*, Cheltenham: Edward Elgar Publishing Limited 2023.
115. Elrick L. E., *The ecosystem concept: a holistic approach to privacy protection*, Int. Rev. Law Comput. Technol. 2021, Vol. 35, No. 1, DOI: 10.1080/13600869.2020.1784564 (dostęp: 20.09.2024 r.).
116. Elżanowski F. M., *Prawnoprocesowa sytuacja przedsiębiorstwa energetycznego w sprawach z zakresu regulacji energetyki*, Warszawa: Wolters Kluwer Polska 2015, SIP LEX.
117. Erdos D. O., *The Development of European Data Protection Law and Regulation* [in:] tegoż, *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?*, Oxford: Oxford University Press 2019.
118. Ertel W., *Introduction to artificial intelligence*, Cham: Springer 2018.
119. Etteldorf C., *Data Protection Authorities Try to Fill the Gap between GDPR and e-Privacy Rules*, EDPL 2018, Vol. 4, No. 2.
120. Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: Wolters Kluwer Polska 2022, SIP LEX.
121. Fajgielski P., Mednis A., Gałęzowska K. et al., *Prywatność a jawność: bilans 25-lecia i perspektywy na przyszłość*, Warszawa: Wydawnictwo CH Beck 2016, SIP Legalis.
122. Fajgielski P., *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa: Wolters Kluwer Polska 2019.
123. Fajgielski P., *Rola Europejskiego Inspektora Ochrony Danych w kształtowaniu i wykładni przepisów o ochronie danych osobowych*, MoP 2021, nr 23.
124. Ferguson S. D. D., *European Cybersecurity Certification Schemes and Cybersecurity in the EU Internal Market*, „International Cybersecurity Law Review” 2022, Vol. 3, No. 1.

125. Finck M., Pallas F., *They who must. not be identified—distinguishing personal from non-personal data under the GDPR*, Int. Data Priv. Law 2020, Vol.10, Iss. 1, <https://doi.org/10.1093/idpl/ipz026> (dostęp: 20.09.2024 r.).
126. Fischer B., *Prawne aspekty norm technicznych. Normalizacja jako wsparcie legislacji administracyjnej*, Warszawa: Wolters Kluwer Polska 2017.
127. Flaga-Gieruszyńska K. (red.), Gołaczyński J. (red.), Szostek D. (red.), *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.
128. Flaga-Gieruszyńska K. (red.), Gołaczyński J. (red.), Arkuszewska A. M. (red.), et al., *Prawo nowych technologii*, Warszawa: Wolters Kluwer Polska 2021.
129. Flisek K., *Europejska współpraca administracyjna*, PPP 2020, nr 6.
130. Fox E. M., Gerard D., *EU Competition Law. Cases, Textes and Context*, Cheltenham: Edward Elgar 2023.
131. Frenz W., *Handbook of EU competition law*, Berlin: Springer 2016.
132. Fuster G. G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham: Springer 2014.
133. Gajewski S., *Tryb i forma rozstrzygania sporów o właściwość na gruncie kodeksu postępowania administracyjnego oraz jego sądowoadministracyjna kontrola*, PPP 2016, nr 11.
134. Galetta D. U., *Procedural autonomy of EU Member States: paradise lost?: a study on the „functionalized procedural competence” of EU Member States*, Cham: Springer 2010.
135. Gallese C., *Web scraping and Generative Models training in the Directive 790/19*, „Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale” 2023, Vol. 16, No. 2.
136. Gałęzowska K., *Dane biometryczne a dane behawioralne*, MoP 2022, nr 21.
137. Garlicki L. (red.), Zubik M. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 2, Warszawa: Wydawnictwo Sejmowe 2016, SIP LEX.

138. Gawroński M., *Prezentacja w czasie Konferencji Urzędu Ochrony Danych Osobowych „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów”*, <https://uodo.gov.pl/pl/file/4249> (dostęp: 20.09.2024 r.).
139. Gellert R., Gutwirth S., *The legal construction of privacy and data protection*, CLSR 2013, Vol. 29, No. 5.
140. Gellert R., *The risk-based approach to data protection*, Oxford: Oxford University Press 2020, <https://doi.org/10.1093/oso/9780198837718.001.0001> (dostęp: 10.02.2024 r.).
141. Gentile G., Lynskey O., *Deficient by Design? The Transnational Enforcement of the GDPR*, „International and Comparative Law Quarterly” 2022, Vol. 71, No. 4.
142. Genus, A., Stirling A., *Collingridge and the dilemma of control: Towards responsible and accountable innovation*, „Research policy” 2018, Vol. 47, No. 1.
143. Giurgiu A., Larsen T. A., *Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?*, EDPL 2016, Vol. 2, No. 3.
144. Głowacka E., *Kultura organizacyjna w procesie zarządzania administracją publiczną*, materiały Studenckiej Konferencji Naukowej, Rzeszów: WSPiA 2011, nr 1, <https://wspia.eu/media/bo3n1kzk/11-g%C5%82owacka-edyta.pdf> (dostęp: 20.09.2024 r.).
145. Goldberg S., Johnson G., Shriver S., *Regulating Privacy Online: An Economic Evaluation of the GDPR*, „Law & Economics Center at George Mason University Scalia Law School Research Paper Series” 2022, No. 22-025, <http://dx.doi.org/10.2139/ssrn.3421731> (dostęp: 20.09.2024 r.).
146. Krzywka K. [w:] *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. M. Dyl, M. Królikowski, Warszawa: Wydawnictwo C.H. Beck 2021, SIP Legalis.
147. Gołaczyński J. (red.), *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, Warszawa: Wydawnictwo C.H. Beck 2022.

148. Gołaczyński J. (red.), Skibicki R.(red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa: Wolters Kluwer Polska 2024.
149. Góral U., *Europejska Rada Ochrony Danych – proces transformacji Grupy Roboczej Art. 29*, MoP 2017, nr 20, dodatek.
150. Góralczyk G., *Samodzielność pojęciowa prawa gospodarczego jako problem analitycznej teorii prawa*, „Acta Universitatis Wratislaviensis. Prawo” 2011, t. 312, nr 3337.
151. Góralczyk W., *Zasada kompetencyjności w prawie administracyjnym*, Warszawa: Wydawnictwa UW 1986.
152. Graef I., Clifford D., Valcke P., *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, Int. Data Priv. Law 2018, Vol. 8, No. 3, <https://ssrn.com/abstract=3216198> (dostęp: 20.09.2024 r.).
153. Graef I., *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, PhD summary, Kluwer Law International 2016, <https://ssrn.com/abstract=3635378> (dostęp: 08.09.2024 r.).
154. Graef I., Husovec M., Purtova N., *Data portability and data control: lessons for an emerging concept in EU law*, „German Law Journal” 2018, Vol. 19, No. 6.
155. Greenberg B. A., *Rethinking Technology Neutrality*, „Minnesota Law Review 100” 2016, No. 4.
156. Greenleaf G., *Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi*, „UNSW Law Research Paper” 2018, No. 18-56. <https://ssrn.com/abstract=3184548> (dostęp: 20.09.2024 r.).
157. Greenleaf G., *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, „Privacy Laws & Business International Report” 2017, Iss. 145, <https://ssrn.com/abstract=2993035> (dostęp: 20.09.2024 r.).
158. Grochowski M. (red.), *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2024, SIP Legalis.

159. Gruszecka D., *Pojęcie dobra prawnego w prawie karnym*, „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie” 2008.
160. Gryszczyńska A. (red.), Szpor G. (red.), Wiewiórowski W. R. (red.), *Internet. Globalne gry. Global Games*, Warszawa: Wydawnictwo C.H. Beck 2022, SIP Legalis.
161. Gryszczyńska A., G. Szpor, W.R. Wiewiórowski (red.), *Internet Hacking*, Warszawa 2023, SIP Legalis, C.H. Beck.
162. Grzeszak J., Łukasik K., Święcicki I., *Ile warte są nasze dane?*, Warszawa: Polski Instytut Ekonomiczny 2021, https://pie.net.pl/wp-content/uploads/2022/01/PIE-Raport_Wartosc_danych.pdf (dostęp: 20.09.2024 r.).
163. Grzybowski T., Sarnowiec-Cisłak M., *Ważenie zasad prawa w orzecznictwie sądów administracyjnych*, ZNAS 2018, nr 6.
164. Guihot M., *Coherence in technology law*, Law Innov. Technol. 2019, Vol. 11, No. 2.
165. Gunst S., De Ville F., *The Brussels effect: how the GDPR conquered Silicon Valley*, „European Foreign Affairs Review” 2021, Vol. 26, Iss. 3, <https://doi.org/10.54648/eerr2021036> (dostęp 07.09.2024 r.).
166. Hacker P., Cordes J., Rochon J., *Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and Beyond* <http://dx.doi.org/10.2139/ssrn.4316944> (dostęp: 20.09.2024 r.).
167. Hacket E. J. (ed.) et al., *The handbook of science and technology studies*, Cambridge, MA: The MIT Press 2008, <https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-wyatt-2007b.pdf> (dostęp: 20.09.2024 r.).
168. Hahn I., *Purpose Limitation in the Time of Data Power: Is There a Way Forward?*, EDPL 2021, Vol. 7, Iss. 1, <https://doi.org/10.21552/edpl/2021/1/7> (dostęp: 09.09.2024 r.).
169. Hajduk P., *A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research* [in:] Forthcoming, 18th IFIP Privacy and Identity Management 2023 – Sharing (in) a Digital World, Springer, <https://ssrn.com/abstract=4673534> (dostęp: 20.09.2024 r.).

170. Hajduk P., *Divergence between authorities on publicly available spatial data in Poland*, „GIS Odyssey Journal” 2022, Vol. 2, No. 2.
171. Hajduk P., *The Powers of the Supervisory Body in the GDPR as a Basis for Shaping the Practices of Personal Data Processing*. RECoL 2021, Vol. 45, No. 2, <https://doi.org/10.31743/recl.10733> (data dostępu 7.09.2024 r.).
172. Harcourt A., *Data Protection and Privacy Post-Brexit* [in:] eadem, *Brexit and the Digital Single Market*, Oxford: Oxford University Press 2023; <https://doi.org/10.1093/oso/9780192899378.003.0010>, (dostęp: 12.02.2024 r.).
173. Hauser R. (red.), Niewiadowski Z. (red.), Wróbel A. (red.), *Europeizacja prawa administracyjnego*, Warszawa: Wydawnictwo C.H. Beck. Instytut Nauk Prawnych PAN 2014, Legalis.
174. Hauser R. (red.), Niewiadowski Z. (red.), Wróbel A. (red.), *Instytucje prawa administracyjnego*, Warszawa: Wydawnictwo C.H. Beck. Instytut Nauk Prawnych PAN 2015, SIP Legalis.
175. Hauser R. (red.), Niewiadowski Z. (red.), Wróbel A. (red.), *Podmioty administrujące*, Warszawa: Wydawnictwo C.H. Beck. Instytut Nauk Prawnych PAN 2011, SIP Legalis.
176. Hauser R. (red.), Niewiadowski Z. (red.), Wróbel A. (red.), *Prawne formy działania administracji*, Warszawa: Wydawnictwo C.H. Beck. Instytut Nauk Prawnych PAN 2013.
177. Hauser R. (red.), Niewiadowski Z. (red.), Wróbel A. (red.), *Publiczne prawo gospodarcze*, Warszawa: Wydawnictwo C.H. Beck. Instytut Nauk Prawnych PAN 2018, SIP Legalis.
178. Hauser R. (red.), Niewiadowski Z. (red.), Wróbel A. (red.), *Wykładnia w prawie administracyjnym*, Warszawa: Wydawnictwo C.H. Beck. Instytut Nauk Prawnych PAN 2015, SIP Legalis.
179. Hauser R. (red.), Wierzbowski M. (red.), *Kodeks postępowania administracyjnego. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2020, SIP Legalis.
180. Hauser R. (red.), Wierzbowski M. (red.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.

181. He Y., *The importance of artificial intelligence to economic growth*, „Korea Journal of Artificial Intelligence” 2019, Vol. 7, No. 1.
182. He Z., *From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law*, „Digital Society” 2023, Vol. 2, <https://doi.org/10.1007/s44206-023-00043-5> (dostęp: 20.09.2024 r.).
183. Hemphill T. A., *The Innovation Governance Dilemma: Alternatives to the Precautionary Principle*, „Technology in Society” 2020, Vol. 63, <https://doi.org/10.1016/j.techsoc.2020.101381>. (dostęp: 20.09.2024 r.).
184. Herbet W., Racka K., *Definiowanie rynku właściwego w sektorze farmaceutycznym w sprawach antymonopolowych – rola Obwieszczenia KE w sprawie definicji rynku właściwego do celów wspólnotowego prawa konkurencji*, iKAR 2020, nr 5.
185. Hert P. de, Czerniawski M., *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, Int. Data Priv. Law 2016, Vol. 6, No. 3, <https://doi.org/10.1093/idpl/ipw008> (dostęp: 20.09.2024 r.).
186. Hert P. de, Hajduk P., *Governance of Digital Technologies in the EU: Cross-Regime Enforcement, Redundancy and Interdependence*.
187. Hert P. de, Lazcoz G., *When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance*, EDPL 2022, Vol. 8, No. 31-40.
188. Hert P. de, *Post-GDPR Lawmaking in the Digital Data Society: Mimesis without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law*, [in:] *Data at the Boundaries of European Law*, edited by D. Curtin, M. Catanzariti, Oxford: Oxford University Press 2023, <https://doi.org/10.1093/oso/9780198874195.003.0004> (dostęp: 30.01.2024 r.).
189. Hertrich-Woleński J., *Nieostrość i definicje regulujące*, [w:] *Odmiany współczesnej nauki o polityce*, red. P. Borowiec, R. Kłosowicz, P. Ścigaj, Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego 2014.

190. Hofmann H. C. H., *Multi-Jurisdictional Composite Procedures - The Backbone to the EU's Single Regulatory Space*, „University of Luxembourg. Law Working Paper” 2019 No. 003-2019, <https://ssrn.com/abstract=3399042> (dostęp: 20.09.2024 r.).
191. Hofmann H. C. H., *Seven challenges for EU administrative law*, „Review of European Administrative Law” 2009, Vol. 2, No. 2.
192. Hofmann H. C. H., Mapping the European administrative space, „West European Politics” 2008, Vol. 31, Iss. 4, <https://doi.org/10.1080/01402380801905918> (dostęp: 20.09.2024 r.).
193. Homplewicz J., *Zarządzenia administracyjne: studium z zakresu nauki prawa administracyjnego*, Kraków: nakładem Uniwersytetu Jagiellońskiego 1970.
194. Hovhannisyan K., Bogacki P., Colabuono C. A. et al., *Towards a Healthcare Cybersecurity Certification Scheme* [in:] *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers IEEE 2021: <https://doi.org/10.1109/CyberSA52016.2021.9478255> (dostęp: 7.09.2024 r.).
195. Hughes T, *History of Technology* [in:] *International Encyclopedia of the Social & Behavioral Sciences*, edited by N. J. Smelser, P. B. Baltes, Amsterdam: Elsevier. Pergamon 2001, <https://doi.org/10.1016/B0-08-043076-7/02648-6> (dostęp: 20.09.2024 r.).
196. Ishwara Bhat P., *Comparative Method of Legal Research: Nature, Process, and Potentiality* [in:] idem, *Idea and Methods of Legal Research*, New Delhi: Oxford University Press 2020, <https://doi.org/10.1093/oso/9780199493098.003.0009> (dostęp: 28.12.2023 r.).
197. Jagielski J., Wierzbowski M., *Prawo administracyjne*, Warszawa: Wolters Kluwer Polska 2020.
198. Jakimowicz W. (red.), *Aktualność pojęć prawa administracyjnego. XI Krakowsko-Wrocławskie Spotkanie Naukowe Administratywistów*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.

199. Jakimowicz W., *Normatywne uwarunkowania realizowania kompetencji prawodawczych*, „Ruch Prawniczy Ekonomiczny i Socjologiczny” 2015, nr 3.
200. Jakimowicz W., *Wykładowia w prawie administracyjnym*, Kraków: Kantor Wydawniczy Zakamycze. Wolters Kluwer Polska 2006, SIP LEX.
201. Jakubowski A., *Zasada ciągłości administracji publicznej a właściwość rzeczowa organów (studium przypadku)*, PiP 2015, nr 12.
202. Jančiūtė L., *European Data Protection Board: a nascent EU agency or an ‘intergovernmental club’?*, Int. Data Priv. Law 2020, Vol. 10, No. 1.
203. Jarentowski M. G., *Legislacyjne aspekty ustroju centralnych organów administracji rządowej*, PPP 2011, nr 5.
204. Jaroszyński T., *Rozporządzenie Unii Europejskiej jako składnik systemu prawa obowiązujące w Polsce*, Warszawa: Wolters Kluwer Polska 2011, SIP LEX.
205. Jasiński W. (red.), *Standardy rzetelności postępowania w sprawach z zakresu ochrony konkurencji i konsumentów*, Warszawa: Wolters Kluwer Polska 2016, SIP LEX.
206. Jaśkowska M., Wilbrandt-Gotowicz M., Wróbel A., *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.
207. Jaśkowski M., *Sądowa kontrola legalności aktów administracyjnych Unii Europejskiej*, Warszawa: Wolters Kluwer Polska 2016, SIP LEX.
208. Jędrzejczak M., *Ochrona danych osobowych w prawie publicznym*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.
209. Johnson G., *Economic Research on Privacy Regulation: Lessons From the GDPR and Beyond* [in:] *The Economics of Privacy*, edited by A. Goldfarb, C. Tucker, Chicago: University of Chicago Press 2024, <http://dx.doi.org/10.2139/ssrn.4290849> (dostęp: 20.09.2024 r.).
210. Józefowicz A., *Problem rozstrzygania sporów kompetencyjnych*, „Przegląd Legislacyjny” 2004, nr 4.

211. Jurkowska-Gomułka A. (red.), Piszcz A. (red.), *Prawo konkurencji*, Warszawa: Wydawnictwo C.H. Beck 2024.
212. K. Czaplicki (red.), A. Gryczyńska (red.), G. Szpor (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa: Wolters Kluwer Polska 2019, SIP LEX.
213. Kaczyńska-Kral A. M., *Spór kompetencyjny Ministra Cyfryzacji oraz Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 33 Prawa przedsiębiorców*, „Studia Iuridica” 2018, t. 77, <https://studiaiuridica.pl/article/131866/pl> (dostęp 8.09.2024 r.).
214. Kamara I., Hert P. de, *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, „Brussels Privacy Hub” 2018, Vol. 4, No. 12, <https://ssrn.com/abstract=3228369>. (dostęp: 20.09.2024 r.).
215. Kapica W. (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu*, Warszawa: Wolters Kluwer Polska 2020, SIP LEX.
216. Kapica W. (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik*, Warszawa: Wolters Kluwer Polska 2018, SIP LEX.
217. Karpiuk M. (red.), Krzykowski P. (red.), Skóra A. (red.), *Kodeks postępowania administracyjnego. Komentarz do art. 1-60*, t. 1, Olsztyn: Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego w Olsztynie 2020, SIP LEX.
218. Karwala D., Zdancrwich-Leśniak A., *Numer umowy kredytowej jako dana osobowa. Glosa do wyroku WSA z dnia 22 kwietnia 2021 r., II SA/Wa 1865/20*, „Monitor Prawa Bankowego” 2022, nr 2.
219. Kawecki M. (red.), Osiej T. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa: Wydawnictwo C.H. Beck 2017, SIP Legalis.
220. Kening-Witkowska M. (red.), *Prawo instytucjonalne Unii Europejskiej*, Warszawa: Wydawnictwo C.H. Beck 2011.
221. Kerber W., *Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives*, „GRUR International”, Vol. 72, Iss. 2, <https://doi.org/10.1093/grurint/ikac107> (dostęp: 7.09.2024 r.).

222. Kerber W., Zolna K. K., *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law*, „European Journal of Law and Economics” 2022, Vol. 54, <http://dx.doi.org/10.2139/ssrn.3719098> (dostęp: 7.09.2024 r.).
223. Kettemann C. M. (ed.), Peukert A. (ed.), Spiecker gen. Döhmman I. (ed.), *The Law of Global Digitality*, Taylor & Francis 2022.
224. Kędzierski D. V., (2018). Metodologia i paradygmat polskich szczegółowych nauk prawnych, „Transformacje prawa prywatnego” 2018, nr 3, <https://www.doi.org/10.26106/0p55-br71> (dostęp: 21. 09.2024 r.).
225. Kindylidi I., *The Data Protection Implications of the EU AML Framework: A Critical Overview & the Case of AI*, [in:] *Annual Privacy Forum*, edited by A. Gryszczyńska, P. Polański, N. Gruschka et al., Cham: Springer International Publishing 2022.
226. Kira B., Sinha V., Srinivasan S., *Regulating digital ecosystems: bridging the gap between competition policy and data protection*, „Industrial and Corporate Change” 2021, Vol. 30, No. 5.
227. Kisała M., *Układy kompetencyjne w samorządzie terytorialnym*, autoreferat, Lublin 2019, https://www.kul.pl/files/1418/public/habilitacje/dr_magdalena_kisaa/dr_M._Kisala_-_autoreferat.pdf (dostęp: 1.09.2024 r.).
228. Kisała M., *Układy kompetencyjne w samorządzie terytorialnym*, Lublin: Wydawnictwo KUL 2018.
229. Kitler W. (red.), Taczkowska-Olszewska J. (red.), Radoniewicz F. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.
230. Klimas T., Vaiciukaite J., *The Law of Recitals in European Community Legislation*, „ILSA Journal of International & Comparative Law” 2008, Vol. 15, No. 1, <https://ssrn.com/abstract=1159604> (dostęp 12.09.2024 r.).
231. Kłosowska K., *Czynności faktyczne jako prawna forma działania administracji*, Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego 2009.

232. Kmiecik Z., *Idea badań prawnoporównawczych Franciszka Longchamps de Bérér*, PiP 2019, R. 74, z. 5.
233. Kmiecik Z., *Ogólne zasady prawa i postępowania administracyjnego*, Warszawa: Wydawnictwa Prawnicze PWN 2000.
234. Knetsch J., *The compensation of non-pecuniary loss in GDPR infringement cases*, special issue of „European Journal of Privacy Law & Technologies” 2020, <https://doi.org/10.1515/jetl-2022-0008> (dostęp 7.09.2024 r.).
235. Knysiak-Sudyka H. (red.), *Kodeks postępowania administracyjnego. Komentarz*, Warszawa: Wolters Kluwer Polska 2019, SIP LEX.
236. Kohutek K., *Komentarz do rozporządzenia nr 139/2004 w sprawie kontroli koncentracji przedsiębiorstw*, SIP LEX 2013.
237. Kohutek K., *Naruszenie przepisów o ochronie danych osobowych (RODO) a nadużycie pozycji dominującej w rozumieniu art. 102 TFUE – glosa do wyroku Trybunału Sprawiedliwości z 4.07.2023 r., C-252/21, Meta Platforms Inc. (dawniej Facebook Inc.) przeciwko Bundeskartellamt*, „Europejski Przegląd Sądowy” 2023, nr 10.
238. Kokott J., Sobotta Ch., *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, Int. Data Priv. Law, Vol. 3, Iss. 4, <https://doi.org/10.1093/idpl/ipt017> (dostęp: 20.09.2024 r.).
239. Konarski X., *Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenia o ochronie danych osobowych (RODO)*, MoP 2017, nr 20.
240. Konarski X., *Podstawy prawne korzystania z „ciasteczek” internetowych (cookies) jako przykład wzajemnej relacji przepisów RODO oraz przepisów o ochronie prywatności w sektorze łączności elektronicznej*, MoP 2018, nr 22.
241. Korczak J. (red.), *Układ administracji publicznej*, Warszawa: Wolters Kluwer Polska 2020, SIP LEX.
242. Korn K., *Określanie rynku właściwego w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej w latach 1997-2010*, ZNUJ 2012, z. 116.

243. Kornhauser, L., *The Economic Analysis of Law*, [in:] *The Stanford Encyclopedia of Philosophy*, edited by E. N. Zalta, (Spring 2022 Edition), <https://plato.stanford.edu/archives/spr2022/entries/legal-econanalysis/> (dostęp: 20.09.2024 r.).
244. Kornobis-Romanowska D. (red.), Grzeszczak R. (red.), *Traktat o Unii Europejskiej. Komentarz*, Warszawa: Wolters Kluwer Polska 2023, SIP LEX.
245. Korzeniowski P., *Zasady prawne ochrony środowiska*, Łódź: Wydawnictwo Uniwersytetu Łódzkiego 2010.
246. Kosiński E., *Czy istnieje prawo energetyczne?: Część 1: Przedmiot, podmioty i metoda regulacji prawa energetycznego*, „Acta Universitatis Wratislaviensis. Prawo” 2022, nr 334.
247. Kosta E., *A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon* (October 4, 2021). <http://dx.doi.org/10.2139/ssrn.3935730> (dostęp: 20.09.2024 r.).
248. Koulierakis E., *Certification as Guidance for Data Protection by Design*, Int. Rev. Law Comput. Technol. 2024, Vol. 38, No. 2, <https://doi.org/10.1080/13600869.2023.2269498>, (dostęp: 20.09.2024 r.).
249. Kowalczyk B., *Zasada terytorializmu działania administracji a transgraniczność spraw administracyjnych*, [w:] *Współpraca transgraniczna w administracji publicznej*, red. R. Kusiak-Winter, Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, http://repozytorium.uni.wroc.pl/Content/79066/PDF/10_Barbara_Kowalczyk.pdf (dostęp: 20.09.2024 r.).
250. Kozak M., *Glosa do wyroku Sądu Ochrony Konkurencji i Konsumentów z 12 maja 2022 r. w sprawie XVII AmA 61/21*, iKAR 2022, t. 11, nr 4.
251. Kozak M., *Raz, dwa, trzy, niezależny będziesz ty... O konieczności szerszego spojrzenia na niezależność polskiego organu antymonopolowego w świetle dyrektywy ECN+*, iKAR 2019, t. 8, nr 6.

252. Kramcsák P. T., *Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?*, CLSR 2023, Vol. 48.
253. Krawczyk M., *Podstawy władztwa administracyjnego*, Warszawa: Wolters Kluwer Polska 2016, SIP LEX.
254. Krawczyk M., *Zakres kognicji Naczelnego Sądu Administracyjnego w rozstrzyganiu sporów kompetencyjnych i o właściwość*, „Samorząd Terytorialny” 2023, nr 6.
255. Kruś M. (red.), Staniszevska L. (red.), Szewczyk M. (red.), *Kierunki rozwoju jurysdykcji administracyjnej*, Warszawa: Wolters Kluwer Polska 2022, SIP LEX.
256. Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa: Wydawnictwo C.H. Beck 2016, SIP Legalis.
257. Kuba M., *Zasada przejrzystości przetwarzania danych osobowych jako instrument ochrony autonomii informacyjnej pracownika*, MoP 2020, nr 12, doi:10.32027/MOPR.20.12.2.
258. Kubiak-Cyrul A., *Rekomendacje OECD jako ramy etyczne i prawne dla rozwoju sztucznej inteligencji*, „Studia Prawnicze: rozprawy i materiały” 2022, t. 26, nr. 1.
259. Kuczkowska E., *Glosa aprobuująca do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13 kwietnia 2021 r., sygn. akt II SA/Wa 1898/20*, „Roczniki Administracji i Prawa” 2021, nr 3.
260. Kuczma E, Kuczma P., *Generalny Inspektor Ochrony Danych Osobowych jako organ kontroli i ochrony prawa*, „Zeszyty Naukowe Dolnośląskiej Wyższej Szkoły Przedsiębiorczości i Techniki w Polkowicach. Studia z Nauk Społecznych” 2013, nr 6.
261. Kuczma E., *Generalny Inspektor Ochrony Danych Osobowych jako organ ochrony prawa do prywatności*, Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora” 2018.
262. Kulkarni M., Mondal A., Singh K. K., *GDPR: A Bibliometric Analysis*, [in]: *Proceedings of the International Conference on Cognitive and Intelligent Computing. Cognitive Science and Technology*, edited by A. Kumar, G. Ghinea, S. Merugu et al., Singapore: Springer 2022, https://doi.org/10.1007/978-981-19-2350-0_1 (dostęp: 20.09.2024 r.).

263. Kuner Ch. et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford: Oxford University Press 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001> (dostęp: 17.01.2024 r.).
264. Kunysz J., *Skuteczność prawa: (zagadnienia wybrane)*, „Administracja: Teoria, Dydaktyka, Praktyka” 2014, nr 2.
265. Kupiec M., *Uprawnienie do uzyskania od administratora informacji o odbiorcach lub o kategoriach odbiorców a cele prawa dostępu do danych. Glosa do wyroku TS z dnia 12 stycznia 2023 r., C-154/21 (RW przeciwko Österreichische Post AG)*, „Europejski Przegląd Sądowy” 2023, nr 6.
266. Kurek J., Taczowska-Olszewska J., *Status ustrojowy PUODO [w:] eidem, Ochrona danych osobowych jako realizacja zadań w obszarze bezpieczeństwa państwa*, Wydawnictwo C.H. Beck 2020, SIP Legalis.
267. Lachaud E., *Adhering to GDPR codes of conduct: A possible option for SMEs to GDPR certification*, „Journal of Data Protection & Privacy” 2019, Vol. 3, No. 1.
268. Lai L. (red.), M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa: Wydawnictwo C.H. Beck 2020, SIP Legalis.
269. Lalova-Spinks T., Meszaros J., Huys I., *The application of data altruism in clinical research through empirical and legal analysis lenses*, „Frontiers in Medicine” 2023, Vol. 10.
270. Landerer L. M., *The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention: A Flawed Comparison?*, „Eu crim – the European Criminal Law Associations' Forum” 2022, Iss. 01.
271. Laurie, G., Sethi N., *Towards Principles-Based Approaches to Governance of Health-Related Research Using Personal Data*, Eur. J. Risk Regul. 2013, Vol. 4, No. 1.
272. Lee J., Schoenherr D., Starmans J., *The Economics of Legal Uncertainty*, „European Corporate Governance Institute – Law Working Paper” 2022, No. 669/2022, <http://dx.doi.org/10.2139/ssrn.4276837> (dostęp: 20.09.2024 r.).
273. Lenaerts K., *Limits on limitations: the essence of fundamental rights in the EU*, „German Law Journal” 2019, Vol. 20, No. 6.

274. Leoński Z., *Nauka administracji*, Warszawa: Wydawnictwo C.H. Beck 2010.
275. Lessig L., *The Law of the Horse: What CyberLaw Might Teach*, „Harvard Law Review” 1999, Vol. 113, No. 2.
276. Leszczyński L. (red.), *Wykładnia prawa Unii Europejskiej*, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.
277. Levi-Faur D., *Regulatory networks and regulatory agencification: towards a Single European Regulatory Space*, J. Eur. Public Policy 2011, Vol. 18, Iss. 6, <https://doi.org/10.1080/13501763.2011.593309> (dostęp: 20.09.2024 r.).
278. Li W., Li Z., Li W. et al., *Mapping the Empirical Evidence of the GDPR (In-) Effectiveness: A Systematic Review*, arXiv:2310.16735, 2023, <https://doi.org/10.48550/arXiv.2310.16735> (dostęp: 20.09.2024 r.).
279. Lievens E., Verdoodt V., *Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation*, CLSR 2018, Vol. 34, No. 2.
280. Lindseth P. L., *What's in a Label? The EU as 'Administrative' and 'Constitutional'* [in:] *Comparative Administrative Law*, edited by S. Rose-Ackerman, P. L. Lindseth, B. Emerson, Cheltenham: Edward Elgar Publishing 2017.
281. Lipowicz I. (ed.), Szpor G. (ed.), Syrt A. (ed.), *Instruments of Public Law: Digital Transformation During the Pandemic*, London: Taylor & Francis (Routledge) 2022.
282. Lipowicz I. (red.), *System prawa samorządu terytorialnego, t. 1: Podstawowe pojęcia i podstawy prawne funkcjonowania*, Warszawa: Wolters Kluwer Polska 2022, SIP LEX.
283. Lipowicz I. (red.), *System prawa samorządu terytorialnego, t. 3: Samodzielność samorządu terytorialnego – granice i perspektywy*, Warszawa: Wolters Kluwer Polska 2023, SIP LEX.
284. Lipowicz I., *Europeizacja administracji publicznej*, RPEiS 2008, R. LXX, z. 1.
285. Litwiński P. (red.), *Ochrona danych osobowych w sektorze publicznym*, Warszawa: Wydawnictwo C.H. Beck 2022, SIP Legalis.

286. Litwiński P. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2021, SIP Legalis.
287. Litwiński P., *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych. Glosa do wyroku TS z dnia 19 października 2016 r., C-582/14*, EPS 2017, nr 5.
288. Lubasz D. (red.), Namysłowska M.(red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa: Wolters Kluwer Polska 2024, SIP LEX.
289. Lubasz D. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: Wolters Kluwer Polska 2019, SIP LEX.
290. Lubasz D., Szkurlat A., *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, MoP 2021, nr 23.
291. Lubasz D., Szkurlat A., *Relacja aktu o sztucznej inteligencji i ogólnego rozporządzenia o ochronie danych*, MoP 2022, nr 21.
292. Lynskey O., *Complete and Effective Data Protection*, „Current Legal Problems” 2023, Vol. 76, Iss. 1, <https://doi.org/10.1093/clp/cuad009> (dostęp: 20.09.2024 r.).
293. Lynskey O., *Deconstructing data protection: the ‘added-value’ of a right to data protection in the EU legal order*, „International & Comparative Law Quarterly” 2014, Vol. 63, Iss. 3.
294. Lynskey O., *The foundations of EU data protection law*, Oxford: Oxford University Press 2015.
295. Łaszczyca G. (red.), Kmiec A. (red.), *System prawa administracyjnego procesowego*, t. 1: *Zagadnienia ogólne*, Warszawa: Wolters Kluwer Polska 2017, SIP LEX.
296. Łaszczyca G., Matan A., Martysz C., *Kodeks postępowania administracyjnego. Komentarz*, t. 1, *Komentarz do art. 1-103*, Warszawa: Wolters Kluwer Polska 2010, SIP LEX.

297. Macenaite M., *The “Riskification” of European Data Protection Law through a two-fold Shift*, Eur. J. Risk Regul. 2017, Vol. 8, Iss. 3, <https://doi.org/10.1017/err.2017.40> (dostęp: 20.09.2024 r.).
298. Maciariello E., *EU Agencies and the Issue of Delegation: Conferral, Implied Powers and the State of Exception*, „European Papers-A Journal on Law and Integration” 2019, Vol. 4, No. 3.
299. Magiera A., Wyczyk J., *Akt o AI w kontekście ochrony danych*, „ABIExpert”, styczeń-marzec 2023.
300. Magierska M., *Three EDPB Binding Decisions in the Art. 65 GDPR Procedure and Two Major Questions for the Future*, EDPL 2023, Vol. 9, No. 1.
301. Majcher K., *Coherence between Data Protection and Competition Law in Digital Markets*, Oxford: Oxford University Press 2023.
302. Malgieri, G., *The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation*, Proceedings of FAT* '20, January 27–30, 2020, ACM, New York, NY, USA, <https://ssrn.com/abstract=3517264>. (dostęp: 20.09.2024 r.).
303. Małobęcka-Szwast I., *Big Data and the Abuse of a Dominant Position by Data-Driven Online Platforms under EU Competition Law*, Warszawa: Wydawnictwo C.H. Beck 2021, SIP Legalis.
304. Małobęcka-Szwast I., *Naruszenie prawa ochrony danych osobowych jako nadużycie pozycji dominującej? Postępowanie Bundeskartellamt przeciwko Facebookowi*, iKAR 2018, nr 8.
305. Mantelero A., *The Future of Data Protection: Gold Standard vs. Global Standard*, CLSR 2021, Vol. 40.
306. Marcinkowski B. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: Wolters Kluwer Polska 2018.
307. Markiewicz R., *ChatGPT i prawo autorskie Unii Europejskiej*, ZNUJ 2023, nr 2.

308. Markopoulou D., Papakonstantinou V., De Hert P., *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, CLSR 2019, Vol. 35, Iss. 6.
309. Martin N., Ebbers F., *When Regulatory Power and Industrial Ambitions Collide: The 'Brussels Effect,' Lead Markets, and the GDPR.*, [in:] *Privacy Symposium 2022: Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)*, Cham: Springer International Publishing 2022.
310. Martin, N., Matt Ch., Niebel C. et al., *How data protection regulation affects startup innovation*, „Information systems frontiers” 2019, Vol. 21.
311. Martinsen D. S., Mastenbroek E., Schrama R., *The power of 'weak' institutions: assessing the EU's emerging institutional architecture for improving the implementation and enforcement of joint policies*, J. Eur. Public Policy 2022, Vol. 29, No. 10, <https://doi.org/10.1080/13501763.2022.2125046> (dostęp: 20.09.2024 r.).
312. Martysz C. (red.), *Skuteczność w prawie administracyjnym*, Warszawa: Wolters Kluwer Polska 2022, SIP LEX.
313. Mastenbroek E., Sindbjerg Martinsen D., *Filling the gap in the European administrative space: the role of administrative networks in EU implementation and enforcement*, J. Eur. Public Policy 2018, Vol. 25, Iss. 3, <https://doi.org/10.1080/13501763.2017.1298147> (dostęp: 20.09.2024 r.).
314. Matan A. (red.), *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza*, Warszawa: Wolters Kluwer; Katowice: Uniwersytet Śląski w Katowicach 2022, SIP LEX.
315. Matan A.(red.), *System Prawa Administracyjnego Procesowego*, t. 4: *Postępowania autonomiczne i szczególne. Postępowania niejurysdykcyjne*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.
316. Matczak M., *Kompetencja organu administracji publicznej*, Kraków: Zakamycze 2004.
317. Mazurkiewicz D., *Pojęcie kompetencji w prawie administracyjnym*, PiP 1988, nr 3.
318. McCullagh K., *Post-Brexit UK Data Protection: Maintaining Alignment with or Diverging from the GDPR?* [in:] *Data Protection and Digital Sovereignty Post-Brexit*,

- edited by E. Celeste , R. Costello , E. Harbinja et al., Oxford: Hart Publishing 2023, <http://dx.doi.org/10.5040/9781509966516.ch-002> (dostęp: 13.02.2024 r.).
319. Mednis A. (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa: Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW 2013.
320. Mednis A., *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, Wrocław: PRESSCOM 2019.
321. Mednis A., *Ustawa o ochronie danych osobowych*, Warszawa: Wydawnictwo Prawnicze 1999, SIP LEX.
322. Miąsik D. (red.), Półtorak N. (red.), Wróbel A. (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I (art. 1-89)*, Warszawa: Wolters Kluwer Polska 2012, SIP LEX.
323. Michaels R., *The Functional Method of Comparative Law* [in:] *The Oxford Handbook of Comparative Law*, 2nd edn, edited by M. Reimann, R. Zimmermann, Oxford: Oxford University Press 2019, <https://doi.org/10.1093/oxfordhb/9780199296064.013.0011> (dostęp: 12.02.2024 r.).
324. Michalska M., *Zasada proporcjonalności w orzecznictwie TK i ETPC – analiza prawno-porównawcza*, „Krytyka Prawa” 2022, t. 14, nr 2.
325. Mik B., *Glosa do uchwały SN z dnia 14 listopada 2007 r., BSA-4110-5/07*, „Prokuratura i Prawo” 2008, nr 6.
326. Minčičová M., *Digital Skills in the Workplace and Training of Jobseekers and Employees*, „Technium Social Sciences Journal” 2020, Vol. 12.
327. Molfetas B, Grava L., *Risk-Based Approaches to Business Regulation*, Washington, DC: World Bank Group 2020, <https://documents1.worldbank.org/curated/en/880271603464018549/pdf/A-Note-for-Reformers.pdf> (dostęp: 20.09.2024 r.).
328. Monarcha-Matlak A., *Obowiązki administracji w komunikacji elektronicznej*, Warszawa: Wolters Kluwer Polska 2008, SIP LEX.

329. Morawska E. H., *Prawa konstytucyjne człowieka i obywatela w Rzeczypospolitej Polskiej a prawa podstawowe Unii Europejskiej. Analiza porównawcza*, „Przegląd Sejmowy” 2009, nr 1 (90).
330. Moreno Bellosa N., Petit N., *The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove*, „European Law Review” 2023, Vol. 48, No. 4, <https://ssrn.com/abstract=4411743> (dostęp: 20.09.2024 r.).
331. Mostowik M., *Ochrona danych osobowych w Internecie rzeczy w prawie UE*, Warszawa: Wydawnictwo C.H. Beck 2022, SIP Legalis.
332. Mühlhoff R., *Predictive privacy: Collective data protection in the context of AI and Big Data*, „Big Data & Society” 2023, Vol. 10, No. 1.
333. Mukiri-Smith H., Leenes R., *Beyond the 'Brussels Effect'? Kenya's Data Protection Act (DPA) 2019 and the European Union's General Data Protection Regulation (GDPR) 2018*, EDPL 2021, Vol. 7, Iss. 4.
334. Mulders S., *The relationship between the principle of effectiveness under Art. 47 CFR and the concept of damages under Art. 82 GDPR*, Int. Data Priv. Law 2023, Vol. 13, Iss. 3.
335. Murphy C., *Lon Fuller and the Moral Value of the Rule of Law*, „Law and Philosophy” 2005, t. 24, nr 3.
336. Mutiro B., *The Future of EU Data Protection Law for Collectives: A Reverse Brussels Effect*, EDPL 2023, Vol. 9, Iss. 4, <https://doi.org/10.21552/edpl/2023/4/7> (dostęp: 20.09.2024 r.).
337. Nadolska A., *Komisja Nadzoru Finansowego w nowej instytucjonalnej architekturze europejskiego nadzoru finansowego*, Warszawa: Wolters Kluwer Polska 2014, SIP LEX.
338. Naef T., *Data Protection Without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, Cham: Springer International Publishing 2023.
339. Namysłowska M., Bieda R., Budrewicz P., et al., *O etycznych, prawnych i społecznych konsekwencjach stosowania systemów sztucznej inteligencji w państwach członkowskich*

- Unii Europejskiej. Uwagi na tle projektu rozporządzenia w sprawie sztucznej inteligencji*, „Przegląd Sejmowy” 2023, 6 (179).
340. Naudts L. et al., *Meaningful Transparency through Data Rights: A Multidimensional Analysis*, „Amsterdam Law School Research Paper” 2022, No. 37, <https://dx.doi.org/10.2139/ssrn.3949750> (dostęp: 20.09.2024 r.).
 341. Niczyporuk J., *Kompetencja administracyjna*, „Annales UMCS” 1999, vol. XLVI.
 342. Niczyporuk J., *Regulacja kompetencji administracji leśnej*, BSP 2015, nr 18.
 343. Niebel C., *The impact of the general data protection regulation on innovation and the global political economy*, CLSR 2021, Vol. 40.
 344. Niedźwiedź M., *Doktryna Meroni i jej znaczenie dla europejskiego prawa administracyjnego - wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.06.1958 r., 9/56, Meroni & Co., Industrie Metallurgiche, SpA przeciwko Wysokiej Władzy EWWiS*, EPS 2020, nr 1.
 345. Niedźwiedź M., *Zakres sądowej kontroli decyzji administracyjnych wydanych w związku z wykonaniem wniosku o przekazanie informacji w ramach współpracy administracyjnej w sprawach podatkowych – wprowadzenie i wyrok Trybunału Sprawiedliwości z 16.05.2017 r., C-682/15, Berlioz Investment Fund S.A. przeciwko Directeur de l'administration des Contributions directes*, EPS 2020, nr 10.
 346. Niewiadomski Z., Cieślak Z., Lipowicz I. et al., *Prawo administracyjne*, Warszawa: LexisNexis 2011.
 347. Noga-Bogomilska J., *Kto może kontrolować podmioty w zakresie ochrony danych osobowych?*, SIP LEX 2019.
 348. *Law of Administrative Procedure of the European Union: European Added Value Assessment (+ Annexes I-III)* (2012). https://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/dv/eav_lawofadm_inprocedure_/EAV_LawofAdminprocedure_EN.pdf (dostęp: 20.09.2024 r.).
 349. Novelli C., Hacker P., Morley J. et al., *A Robust. Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, Eur. J. Risk Regul. 2024, <https://ssrn.com/abstract=4817755>. (dostęp: 20.09.2024 r.).

350. Nowakowski, M. (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa: Wolters Kluwer Polska 2023, SIP LEX.
351. Nowicki M., *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.
352. Nwankwo I., Stauch M., Radoglou-Grammatikis P. et al., *Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector*, „Electronics” 2022; Vol. 11, Iss. 6, <https://doi.org/10.3390/electronics11060965> (dostęp: 20.09.2024 r.).
353. O'Callaghan L., *The Intersection between Data Protection and Competition Law: How To Incorporate Data Protection, as a Non-Economic Objective, into EU Competition Analysis*, „Trinity College Law Review” 2018, Vol. 21.
354. O'Leary T., Armfield T., *Adapting to the Digital Transformation*, „Alberta Law Review” 2020, Vol. 58, No. 2.
355. Olsen J., *Towards a European administrative space?* J. Eur. Public Policy 2003, Vol. 10, Iss. 4.
356. Partyk A., Partyk T., *Numer rejestracyjny pojazdu jako dane osobowe*, 2020, SIP LEX.
357. Patrascu, C., Schin, G.: *Challenges of the EU administrative space: convergence of national administrations to the European administrative law*, „Union of Jurists of Romania. Law Review” 2017, Vol. 7, Iss. 2.
358. Pavlidis G. , *The birth of the new anti-money laundering authority: harnessing the power of EU-wide supervision*, „Journal of Financial Crime” 2024, Vol. 31 No. 2, <https://doi.org/10.1108/JFC-03-2023-0059>. (dostęp: 20.09.2024 r.).
359. Peers S., Hervey T., Kenner J. et al. (Eds.), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing 2021.
360. Peukert Ch., Bechtold S., Batikas M. et al., *Regulatory spillovers and data governance: Evidence from the GDPR*, „Marketing Science” 2022, Vol. 41, No. 4.

361. Pichlak M., Gaczoł K. *Refleksyjna regulacja ryzyka w ochronie danych osobowych. Podstawy teoretyczne i praktyka działalności Prezesa UODO*, Łódź: Wydawnictwo Uniwersytetu Łódzkiego 2022.
362. Piech M., *One stop shop. Mechanizmy podejmowania decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE*, MoP 2016, nr 20.
363. Piechocki A., Gorzkowska, K., *Problematyka stosowania prawa autorskiego do dzieł stworzonych przy udziale tzw. generatywnej sztucznej inteligencji*, „Prawo Nowych Technologii” 2023, nr 1.
364. Pietrzak A. (red), *Prawo przedsiębiorców. Komentarz*, Warszawa: Wolters Kluwer Polska 2019, SIP LEX.
365. Pietrzyk M., *Soft law i hard law w europejskim prawie administracyjnym: relacja alternatywy, uzupełnienia, wykluczenia oraz przejścia* [w:] *Administracja publiczna wobec wyzwań i oczekiwań społecznych*, red. M. Giełda, R. Raszevska-Skałeczka, Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego 2015, <http://www.bibliotekacyfrowa.pl/publication/73349> (dostęp: 20.09.2024 r.).
366. Piszcz A., *Niezależność Prezesa Urzędu Ochrony Konkurencji i Konsumentów a dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1*, „Przegląd Ustawodawstwa Gospodarczego” 2022, nr 10.
367. Piszcz A., *Objaśnienia prawne według ustawy z 6.3.2018 r. – Prawo przedsiębiorców*, MoP 2018, nr 13.
368. Piwowarczyk A. J., *Kompetencje komunikacji międzykulturowej: Rozwój kompetencji przyszłych ekonomistów i menedżerów*, Warszawa: Wydawnictwo CH Beck 2020.
369. Podkowik J., Rybski R., Zubik M., *Judicial dialogue on data retention laws: A breakthrough for European constitutional courts?*, „International Journal of Constitutional Law” 2021, Vol. 19, Iss. 5, <https://doi.org/10.1093/icon/moab132>. (dostęp: 20.09.2024 r.).
370. Podsiad A., *Słownik terminów i pojęć filozoficznych*, Warszawa: Instytut Wydawniczy PAX 2001.

371. Porcedda M. G., *Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*, CLSR 2018, Vol. 34, No. 5.
372. Post R. C., *Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere*, „Duke Law Journal” 2018, Vol. 67, No. 5.
373. Potjewijd G., Yakovleva S., Carvalho F. de et al., *Mass damage claims for GDPR infringements: multi-jurisdictional perspective*, „Mass Claims: An International Journal with European Focus” 2021, nr 1.
374. Prabucki, R. T., Syrociak D., *Cyberbezpieczeństwo na fali regulacyjnej*, „ABI Expert: prawne i techniczne aspekty ochrony danych informacji” 2023, nr 1.
375. Prokop M., *Typologia reżimów hybrydalnych. Ujęcie teoretyczno-metodologiczne*, „Historia i Polityka” 2017, t. 28, nr 21.
376. Przybysz P., *Instytucje prawa administracyjnego*, Warszawa: Wolters Kluwer Polska 2020, SIP LEX.
377. Purtova N., *The Illusion of Personal Data as No One's Property*, Law Innov. Technol. 2015, Vol. 7, No. 1, <https://doi.org/10.1080/17579961.2015.1052646> (dostęp: 20.09.2024 r.).
378. Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, Law Innov. Technol. 2018, Vol. 10, No. 1 <https://doi.org/10.1080/17579961.2018.1452176> (dostęp: 20.09.2024 r.).
379. Pyziak M., *Rozstrzyganie sporów kompetencyjnych na ziemiach polskich. Od Rady Stanu Księstwa Warszawskiego do współczesności*, „Studia z Dziejów Państwa i Prawa Polskiego” 2010, t. 13.
380. Quelle C., *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach*, Eur. J. Risk Regul. 2018, Vol. 9, Iss. 3, <https://doi.org/10.1017/err.2018.47> (dostęp: 20.09.2024 r.).
381. Rabska T. (red.), Łętowski J. (red.), *System prawa administracyjnego*, t. 3, Wrocław: Ossolineum 1978.

382. Radwanowicz–Wanczewska J., Fortunato N., *Niewładcze formy działania administracji publicznej w postępowaniu egzekucyjnym w administracji*, BSP 2021, t. 26, nr 5.
383. Rakoczy B. (red.), *Prawo o odpadach. Wybrane problemy*, Warszawa: Wolters Kluwer Polska 2019, SIP LEX.
384. Rakoczy B., *Prawo ochrony środowiska w styku z innymi obszarami systemu prawa* [w:] *Zagadnienia systemowe prawa ochrony środowiska*, red. P. Korzeniowski, Łódź: Wydawnictwo Uniwersytetu Łódzkiego 2015.
385. Reimann M, Zimmermann R. (eds), *The Oxford Handbook of Comparative Law*, 2nd edn, Oxford: Oxford University Press 2019 <https://doi-org.tilburguniversity.idm.oclc.org/10.1093/oxfordhb/9780198810230.013.40> (dostęp: 12.02.2024).
386. Reitz J. C, *How to Do Comparative Law*, „American Journal of Comparative Law” 1998, Vol. 46, No. 4.
387. Ribera Martínez A., *The Decentralisation of the DMA's System of Enforcement*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4857232 (dostęp: 20.09.2024 r.).
388. Robb L., Candy T., Deane F., *Regulatory overlap: A systematic quantitative literature review*, „Regulation & Governance” 2023, Vol. 17, No. 4, <https://doi.org/10.1111/rego.12504> (dostęp: 20.09.2024 r.).
389. Robbins S. P., *Zachowania w organizacji*, Warszawa: Polskie Wydawnictwo Ekonomiczne 2004.
390. Rojszczak M., *Konstytucjonalizacja prawa do ochrony danych osobowych – proces trwający czy zakończony?*, „Przegląd Konstytucyjny” 2023, nr 2, <https://doi.org/10.4467/25442031PKO.23.011.18277> (dostęp: 20.09.2024 r.).
391. Rojszczak M., *Odpowiedzialność za przetwarzanie danych przez portal społecznościowy. Glosa do wyroku TS z dnia 5 czerwca 2018 r., C-210/16*, EPS 2018, nr 10.
392. Rojszczak M., *Reforma Krajowych Przepisów o Ochronie Danych a Kwestia Niezależności Organów Nadzorczych na Tle Rozporządzenia 2016/679 i Dyrektywy 2002/58–Uwagi Krytyczne*, iKAR 2018, t. 7, nr 4.

393. Rojszczak M., *Sztuczna inteligencja w innowacjach finansowych–aspekty prawne i regulacyjne*, iKAR 2020, t. 9, nr 2.
394. Rojszczak M., *The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content*, „Institutiones Administrationis-Journal of Administrative Sciences” 2023, Vol. 3, No. 2.
395. Rokita K. (2016). *Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych*, EPS 2016, nr 7.
396. Rosas A., *The Court of Justice of the European Union: A Human Rights Institution?*, „Journal of Human Rights Practice” 2022, Vol. 14, Iss. 1, <https://doi.org/10.1093/jhuman/huac020> (dostęp: 20.09.2024 r.).
397. Roszkiewicz J., *Zakaz domniemywania kompetencji i wyjątki od tego zakazu. Studium publicznoprawne*, Warszawa: Wydawnictwo C.H. Beck 2022, SIP Legalis.
398. Rubin J. , *Restrictions on the Printing Press* [in:] *Rulers, Religion, and Riches: Why the West Got Rich and the Middle East Did Not*, Cambridge: Cambridge University Press 2017.
399. Rudnicki M., Sobieraj K., *Skuteczność prawa administracyjnego na przykładzie regulacji z zakresu międzynarodowego przemieszczania odpadów*, RPEiS 2013, t. 75, z. 2.
400. Rustad M. L., Koenig T. H., *Towards a Global Data Privacy Standard*, „Florida Law Review” 2019, Vol. 71, No. 2.
401. Rzepiński T., *Konstruowanie typologii i klasyfikacji wielowymiarowych dla potrzeb*, „Zagadnienia Naukoznawstwa” 2016, t. 2, nr 208.
402. Safjan M. (red.), Bosek L. (red.), *Konstytucja RP, t. I: Komentarz do art. 1–86*, Warszawa: Wydawnictwo C.H. Beck 2016, SIP Legalis.
403. Sajfert J., Quintel T., *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* <http://dx.doi.org/10.2139/ssrn.3285873>. (dostęp: 20.09.2024 r.).
404. Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2018, SIP Legalis.

405. Sakowska-Baryła M., *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa: Wolters Kluwer Polska 2022.
406. Schein E.H., *Organizational Culture and Leadership*, San Francisco-London: Jossey-Bass A Wiley Imprint 1986.
407. Schmidt-Aßmann E.berhard, *Dogmatyka prawa administracyjnego. Bilans rozwoju, reformy i przyszłych zadań*, Warszawa: Wolters Kluwer Polska 2022.
408. Schneider J.-P., *A Common Framework for Decentralized EU Agencies and the Meroni Doctrine*, Special Issue of „Administrative Law Review” 2009, Vol. 61.
409. Schuurmans Y. E., Barkhuysen T., Willemien W. den, *Codification of Administrative Law in the Netherlands* [in:] *Codification of Administrative Law: A Comparative Study on the Sources of Administrative Law*, edited by F. Uhlmann, London: Bloomsbury Academic, 2023.
410. Sieradzka M., Kohutek K., *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa: Wolters Kluwer Polska 2014, SIP LEX.
411. Sikora M., *Relacje Między Prawem Administracyjnym a Konstytucyjnym – Perspektywa angielska* [w:] *Comparative perspectives for public administration and administrative law*, red. D. Cendrowicz, A. Chrisidu-Budnik, Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego 2018
http://www.repozytorium.uni.wroc.pl/Content/92950/PDF/03_01_M_Sikora_Administrative_Law_and_Constitutional_Matrix-English_Perspective.pdf (dostęp: 20.09.2024 r.).
412. Singh K., Mishra S., *Mapping the Inter-Relation of Abuse of Dominant Position and Merger Control Regime vis-a-vis Big Data: The Curious Case of WhatsApp Privacy Policy*, „Journal of National Law University Delhi” 2020, Vol. 7, Iss. 1-2.
413. Singh K., Mishra S., *Interplay of Data in Digital Economy and Merger Control Regime: A Conundrum without Solutions*, „Law, State and Telecommunications Review” 2022, Vol. 14, No. 2.

414. Sismondo S., *The Prehistory of Science and Technology Studies* [in:] *An Introduction to Science and Technology Studies*, Malden: Blackwell Publishing, Wiley 2011, <https://books.google.pl/books?id=TsEfNbMtSmoC&lpg=PA1&hl=pl&pg=PP1#v=onepage&q&f=false> (dostęp: 04.09.2024 r.).
415. Skoczny T. (red.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2014, SIP Legalis.
416. Skoczny T., *Zgody szczególne w prawie kontroli koncentracji*, Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 2012.
417. Skoczylas A.P., *Rozstrzyganie sporów kompetencyjnych i o właściwość przez NSA*, Warszawa: Wydawnictwo LexisNexis 2008, SIP LEX.
418. Sloot Bart van de, *Home Is Where the Heart Is: The Household Exemption in the 21st Century*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law” 2023, Vol. 14, No. 1.
419. Solove D. J., *Data is what data does: Regulating based on harm, and risk instead of sensitive data*, GWU Legal Studies Research Paper 2023, No. 2023-22.
420. Sołtys A., *Obowiązek wykładni prawa krajowego zgodnie z prawem unijnym jako instrument zapewniania efektywności prawa Unii Europejskiej*, Warszawa: Wolters Kluwer Polska 2015.
421. Stahl M. (red.), *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, Warszawa: Wolters Kluwer Polska 2013, SIP LEX.
422. Stankiewicz R., *Koordinacja w prawie administracyjnym*, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.
423. Stawicki A. (red.), Stawicki E. (red.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa: Wolters Kluwer Polska 2016, SIP LEX.
424. Stefaniuk M. E., *Skuteczność prawa i jej granice*, „Studia Iuridica Lublinensia” 2011, t. 16.

425. Streeel A. de, Monti G., *Improving Institutional Design to Better Supervise Digital Platforms*, Bruxelles: CERRE, 2022, <https://pure.unamur.be/ws/portalfiles/portal/62618173/8834.pdf> (dostęp: 20.09.2024 r.).
426. Streinz T., *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, 3rd edn, edited by P. Craig, G. de Búrca, Oxford: Oxford University Press 2021, <https://ssrn.com/abstract=3762971> (dostęp: 20.09.2024 r.).
427. Supernat J., *Restatements – koncepcja i zastosowanie*. [w:] *Administracja publiczna pod rządami prawa: księga pamiątkowa z okazji 70-lecia urodzin prof. zw. dra hab. Adama Błasia*, red. J. Korczak, Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego 2016.
428. Suwaj R., *Zasady nakładania administracyjnych kar pieniężnych*, Warszawa: Wolters Kluwer Polska 2021, SIP LEX.
429. Szczepański M., *Is Data the New Oil? Competition Issues in the Digital Economy*, European Parliamentary Research Service 2020, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf) (dostęp: 20.09.2024 r.).
430. Szkurlat A., *Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych*, iKAR 2020, t. 9, nr 2.
431. Szmigielski A., *Nowe formy nadużycia pozycji dominującej w świetle zasady pewności prawa – rozważania na kanwie sprawy Google Search*, EPS 2019, nr 10.
432. Szmit J., *Konstytucyjny wzorzec reżimu zatrudnienia członków korpusu służby cywilnej*, Warszawa: Wolters Kluwer Polska 2024, SIP LEX.
433. Szpor G. (red.), Grochowski L. (red.), *Wielka encyklopedia prawa*, t. 22: *Prawo informatyczne*, Warszawa: Fundacja Ubi Societas Ibi Ius 2021.
434. Szpor G. (red.), Szmulik B. (red.), *Jawność i jej ograniczenia. Zadania i kompetencje*, t. 9, Warszawa: Wydawnictwo C.H. Beck 2015, SIP Legalis.
435. Szpor G. (red.), *Internet. Ochrona wolności, własności i bezpieczeństwa*, Warszawa: Wydawnictwo C.H. Beck 2011.

436. Szpor G., Hajduk P., *Digital Competences and Digital Skills in the Legal Regulation of the Digital Transformation of the European Union*, RECoL 2024, Vol. 56, No. 1, <https://doi.org/10.31743/recl.17139> (dostęp: 20.09.2024 r.).
437. Szpor G., *Jawność i jej ograniczenia*, t. I.: *Idee i pojęcia*, Warszawa: Wydawnictwo C.H. Beck 2016.
438. Szpor G., *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland*, RECoL 2021, Vol. 46, No. 3, <https://doi.org/10.31743/recl.12645> (dostęp: 20.09.2024 r.).
439. Szpor G., *Wymogi związane z Dyrektywą INSPIRE. Zakres regulacji zagospodarowania przestrzennego*, numer specjalny „Kontroli Państwowej” 2016, nr 2.
440. Szpyrka M., *Znacznie niezależności Prezesa UKE dla realizacji unijnych praw podstawowych na przykładzie postępowania karowego prowadzonego na podstawie prawa telekomunikacyjnego*, iKAR 2023, t. 12, nr 4.
441. Szydło M., *Zapobieganie forum shopping w europejskim prawie upadłościowym*, PiP 2008, nr 9.
442. Targański B., *Definiowanie rynków produktowych w gospodarce cyfrowej w świetle projektu Zawiadomienia Komisji w sprawie definicji rynku właściwego do celów unijnego prawa konkurencji z 8 listopada 2022 roku*, iKAR 2023, nr 1.
443. Tarno J.P., *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa: LexisNexis 2006, SIP LEX.
444. Terwangne C. de, *Privacy and data protection in Europe: Council of Europe's Convention 108+ and the European Union's GDPR* [in:] *Research Handbook on Privacy and Data Protection Law*, edited by G. Gonzalez, R. van Brakel, P. de Hert, Cheltenham: Edward Elgar Publishing 2022.
445. Trescakova D., *Digital Transformation of Business Entities under the Current Conditions - Reality or Utopia?*, „EU and Comparative Law Issues and Challenges Series” 2020, Vol. 4.
446. Tripathi R., *Concept of Global Administrative Law: An Overview*, „India Quarterly” 2011, Vol. 67, No. 4, <http://www.jstor.org/stable/45073012> (dostęp: 20.09.2024 r.).

447. Tucker E. W., *The morality of law, by Lon L. Fuller*, „Indiana Law Journal” 1965, Vol. 40, no. 2.
448. Turner B., Wiber M. G., *Legal Pluralism and Science and Technology Studies: Exploring Sources of the Legal Pluriverse*, „Science, Technology, & Human Values” 2023, Vol. 48, Iss. 3, <https://doi.org/10.1177/01622439211069659> (dostęp: 20.09.2024 r.).
449. Uhlmann F. (ed.), *Codification of Administrative Law: A Comparative Study on the Sources of Administrative Law*, Londo: Bloomsbury Academic 2023.
450. Ukrow J., *Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108*, European Data Protection Law Review 2018, Vol. 4, Iss. 2.
451. Ura E., *Prawo administracyjne*, Warszawa: LexisNexis 2009.
452. Van Alsenoy, B., *Reconciling the (Extra)Territorial Reach of the GDPR with Public International Law* [in:] *Data Protection and Privacy Under Pressure. Transatlantic Tensions, EU Surveillance and Big Data*, edited by G. Vermeulen, E. Lievens, Antwerpen: Maklu, 2018.
453. Van Cleynenbreugel P., *BPost and Nordzucker: Searching for the Essence of Ne Bis in Idem in European Union Law: ECJ 22 March 2022, Case C-117/20, BPost v Autorité belge de la concurrence Case C-151/20, Bundeswettbewerbsbehörde v Nordzucker AG e.a.*, „European Constitutional Law Review” 2022, Vol. 18, Iss. 2, <https://doi.org/10.1017/S1574019622000190> (dostęp: 20.09.2024 r.).
454. Van Eecke P., Šimkus A., *Article 64 Opinion of the Board*, [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. C. Kuner. Et al., New York: Oxford University Press 2020, <https://doi.org/10.1093/oso/9780198826491.003.0108> (dostęp: 20.09.2024 r.).
455. Vanberg A. D., *Coordinating digital regulation in the UK: is the digital regulation cooperation forum (DRCF) up to the task?*, Int. Rev. Law Comput. Technol. 2023, Vol. 37, Iss. 2, <https://doi.org/10.1080/13600869.2023.2192566> (dostęp: 20.09.2024 r.).
456. Vandezande N., *Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor*, CLSR 2024, Vol. 52.

457. Varona D., Suárez J. L., *Discrimination, Bias, Fairness, and Trustworthy AI*, „Applied Sciences” 2022, Vol. 12, Iss. 12.
458. Véliz C. (ed.), *Oxford Handbook of Digital Ethics*, Oxford: Oxford University Press 2023, <https://doi.org/10.1093/oxfordhb/9780198857815.001.0001> (dostęp: 19.12.2023 r.).
459. Vestlund N.M. *Pooling administrative resources through EU regulatory networks*, J. Eur. Public Policy 2017, Vol. 24, No. 1.
460. Vial G., *Understanding digital transformation: A review and a research agenda* [in:] *Managing digital transformation*, edited by A. Hinterhuber, T. Vescovi, F. Checchinato, Abingdon, New York: Routledge 2021.
461. Vieriu D., *Legal Requests of the Authority Administrative Act*, special issue of „Journal of Law and Administrative Sciences” 2015.
462. Volmar M., Helmdach K., *Protecting Consumers and Their Data Through Competition Law? Rethinking Abuse of Dominance in Light of the Federal Cartel Office's Facebook Investigation*, „European Competition Journal”, 2018, Vol. 14, No. 2-3, <https://doi.org/10.1080/17441056.2018.1538033> (dostęp: 20.09.2024 r.).
463. Voss W. G., *First the GDPR, Now the Proposed ePrivacy Regulation*, „Journal of Internet Law” 2017, Vol. 21, No. 1, <https://ssrn.com/abstract=3008765> (dostęp: 20.09.2024 r.).
464. Vuorikari R., Kluzer S., Punie Y., *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*, Luksemburg: Urząd Publikacji Unii Europejskiej 2022, <https://publications.jrc.ec.europa.eu/repository/handle/JRC128415> (dostęp: 20.09.2024 r.).
465. Wasastjerna M. C., *The implications of big data and privacy on competition analysis in merger control and the controversial competition-data protection interface*, „European Business Law Review” 2019, Vol. 30, No. 3.
466. Wasilewski R., *Postępowanie dowodowe przed Prezesem Urzędu Ochrony Konkurencji i Konsumentów*, Warszawa: Wydawnictwo C.H. Beck 2020, SIP Legalis.

467. Wegner J., Wojtuń M., Kmiecik Z., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa: Wolters Kluwer Polska 2023, SIP LEX.
468. Wegner-Kowalska J., *Skuteczność unijnego prawa administracyjnego na przykładzie ochrony weterynaryjnej*, Warszawa: Wolters Kluwer Polska 2017, SIP LEX.
469. Weitzenboeck E. M., Lison P., Cydecka M. et al., *The GDPR and unstructured data: is anonymization possible?*, Int. Data Priv. Law 2022, t. 12, nr 3, <https://doi.org/10.1093/idpl/ipac008>. (dostęp: 20.09.2024 r.).
470. West S.M., Whittaker M., Crawford K., *Discriminating Systems: Gender, Race and Power in AI*, AI Now Institute 2019, <https://ainowinstitute.org/publication/discriminating-systems-gender-race-and-power-in-ai-2> (dostęp: 20.09.2024 r.).
471. Wierczyński G., *Redagowanie i ogłaszanie aktów normatywnych. Komentarz*, Warszawa: Wolters Kluwer Polska 2016, SIP LEX.
472. Wierzbowski M. (red.), Wiktorowska A. (red.), *Kodeks postępowania administracyjnego. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2023, SIP Legalis.
473. Wierzbowski M. (red.), *Prawo administracyjne*, Warszawa: LexisNexis 2011.
474. Wiewiórowski W., *Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych*, EPS 2017, nr 5.
475. Wiewiórowski W., *Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią*, EPS 2020, nr 6.
476. Wilbrandt-Gotowicz M., *Europeanisation of Administrative Proceedings Law – Opportunities and Risks*, BSP 2018, nr 2.
477. Winczorek P. (red.), *Teoria i praktyka wykładni prawa*, Warszawa: Wydawnictwo Liber, 2005.
478. Wojciechowski M., *Stwierdzane niezgodności norm wyższego i niższego rzędu a pojęcia niezgodności norm*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji” 2016, nr 3718.

479. Wolwiak I., *Zakończenie postępowania rozpoznawczego*, Warszawa: Wydawnictwo C.H. Beck 2019, SIP Legalis.
480. Wong J., Henderson T., *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, Int. Data Priv. Law 2019, t. 9, nr 3, <https://doi.org/10.1093/idpl/ipz008> (dostęp: 6.09.2024 r.).
481. Woś M. (red.), *Postępowanie administracyjne*, Warszawa: Wolters Kluwer Polska 2017, SIP LEX.
482. Wronkowska, S., Zieliński M., Ziemiński Z., „Zasady prawa” w perspektywie teorii prawa oraz szczegółowych nauk prawnych, RPEiS 1974, t. 36, z. 2.
483. Wróbel A., *Autonomia proceduralna państw członkowskich. Zasada efektywności i zasada efektywnej ochrony sądowej w prawie Unii Europejskiej*, RPEiS 2005, t. 67, z. 1.
484. Wróbel A. (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa: Wydawnictwo C.H. Beck 2020, SIP Legalis.
485. Wróbel A., Wróbel P., *Wyrok TS z dnia 14 września 2023 r. w sprawie C-55/22 NK przeciwko Bezirkshauptmannschaft Feldkirch*, ZNAS 2023, nr 5.
486. Wróblewski J., *Prawo obowiązujące a „ogólne zasady prawa”*, „Zeszyty Naukowe UŁ Nauki humanistyczno-społeczne, seria I” 1965, z. 42.
487. Wróblewski J., *Sądowe i pozasądowe stosowanie prawa – problemy teorii i ideologii*, „Studium Prawno-Ekonomiczne” 1981, t. 26.
488. Wszolek P., *O metodach badawczych stosowanych w nauce prawa administracyjnego dla poznania prawa jako wypowiedzi normatywnej*, PPP 2011, nr 7-8.
489. Wybraniec-Skardowska U., *O konceptualizacji wiedzy nieostrej*, „Filozofia Nauki” 1996, t. 4, nr 3.
490. Yaraghi N., *A case against the General Data Protection Regulation*, <https://www.brookings.edu/articles/a-case-against-the-general-data-protection-regulation/> (dostęp: 20.09.2024 r.).
491. Yesilkagit K., Jordana J., *Entangled agencies and embedded preferences: National Regulatory Agencies in multi-level European governance*, J. Eur. Public

- Policy 2022, Vol. 29, No. 10, <https://doi.org/10.1080/13501763.2022.2103170> (dostęp: 20.09.2024 r.).
492. Zafir-Fortuna G., *Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package* [in:] *Two decades of personal data protection. What next?*, Brussels: European Data Protection Supervisor 2024, https://www.edps.europa.eu/system/files/2024-06/edps_20thanniversary-book_en.pdf (dostęp: 20.09.2024 r.).
493. Zapadka P. (red.), Mikos-Sitek A. (red.), Nowak-Far A. (red.), *Prawo obrotu pieniężnego. Komentarz*, Warszawa: Wolters Kluwer Polska 2023, SIP LEX.
494. Zieliński M., *Clara non sunt interpretanda – mity i rzeczywistość*, ZNAS 2012, nr 6.
495. Zieliński M., *Wykładni prawa. Zasady, reguły, wskazówki*, Warszawa: LexisNexis 2008.
496. Zientara A., *Prawnokarna ochrona przed nieuczciwą konkurencją w ustawie o zwalczaniu nieuczciwej konkurencji*, Warszawa: Wolters Kluwer Polska 2023, SIP LEX.
497. Zimmermann J. (red.), *Koncepcja systemu prawa administracyjnego*, Warszawa: Wolters Kluwer Polska 2007.
498. Zimmermann J., *Aksjomaty prawa administracyjnego*, Warszawa: Wolters Kluwer Polska 2013.
499. Zimmermann J., *Alfabet prawa administracyjnego*, Warszawa: Wolters Kluwer Polska 2022, SIP LEX.
500. Zimmermann J., *Prawo administracyjne*, Kraków: Wolters Kluwer Polska 2012.
501. Zimmermann J., *Prawo administracyjne*, Warszawa: Wolters Kluwer Polska 2020.
502. Zimmermann J., *Z problematyki sporów kompetencyjnych między organami administracji państwowej a sądami*, PiP 1989, nr 3.
503. Zingales N., *Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law*, CLSR 2017, Vol. 33, No. 4.

504. Ziwei J. et al., *Survey of Hallucination in Natural Language Generation* „ACM Computing Surveys” 2023, t. 55, nr 12 <https://doi.org/10.1145/3571730>. (dostęp: 20.09.2024 r.).
505. Zopf F., *Two Worlds Colliding - The GDPR in between Public and Private Law*, EDPL 2022, Vol. 8, No. 2.
506. Zuiderveen Borgesius F., *Discrimination, artificial intelligence, and algorithmic decision-making*, Strasbourg: Council of Europe, Directorate General of Democracy 2018, <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> (dostęp: 4.09.2024 r.).
507. Zwierz M., *Zakaz ne bis in idem w prawie administracyjnym*, [Rozprawa doktorska, Uniwersytet Warszawski], Repozytorium Uniwersytetu <https://repozytorium.uw.edu.pl//handle/item/3660> (dostęp: 20.09.2024 r.).
508. Żukowski L. J., *Spółeczna skuteczność prawa administracyjnego (zarys koncepcji)*, PiP 2017, nr 5.
509. Żuradzki P., *Spory kompetencyjne na tle regulacji ustawy z 20.07.2017 r. – Prawo wodne*, „Samorząd Terytorialny” 2019, nr 7-8.
510. Żyrek S., *Pojęcie administratora danych w przypadku9 wspólnego ich przetwarzania przez portal społecznościowy i podmioty korzystające z jego usług - wprowadzenie i wyrok Trybunału Sprawiedliwości z 5.06.2018 r., C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, EPS 2019, nr 7.

STRONY INTERNETOWE

1. House of Lords Library, N. Newson, *Digital regulation*, <https://lordslibrary.parliament.uk/digital-regulation/#heading-4> (dostęp: 20.09.2024 r.).
2. Business Insider, *Uciążliwe telefony od telemarketerów. Jest nowy pomysł, jak z nimi walczyć* (12.11.2019), <https://businessinsider.com.pl/walka-z-telefonami-od-telemarketerow-dzialania-uke-uokik-i-uodo/23pbryg> (dostęp: 20.09.2024 r.).
3. *Kompetencja*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/sjp/kompetencja;2564077> (dostęp: 20.09.2024 r.).

4. *Competence*, [hasło w:] *Cambridge Dictionary* [online], <https://dictionary.cambridge.org/dictionary/english/competence> (dostęp: 20.09.2024 r.).
5. Britannica, *What is the plural form of "competence"?* <https://www.britannica.com/dictionary/eb/qa/what-is-the-plural-form-of-competence> (dostęp: 20.09.2024 r.).
6. *Zwizczywać*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/slowniki/zwizczany.html> (dostęp: 20.09.2024 r.).
7. [podatki.gov.pl](https://www.podatki.gov.pl), *Safe harbour dla pożyczek – metodyka kalkulacji przy ujemnej stopie referencyjnej*, <https://www.podatki.gov.pl/ceny-transferowe/wyjasnienia/safe-harbour-dla-pozyczek-metodyka-kalkulacji-przy-ujemnej-stopie-referencyjnej/> (dostęp: 20.09.2024 r.).
8. nyob, *GDPR Procedures Regulation: Commission Proposal is an Attack on Users' Rights in GDPR Procedure*, <https://noyb.eu/en/gdpr-procedures-regulation-stripping-citizens-procedural-rights> (dostęp: 20.09.2024 r.).
9. G. González Fuster, *History of Data Protection: An Online Anthology*, https://glgonzalezfuster.files.wordpress.com/2022/05/oj-joc_1979_140_resolutionrecommendations.pdf (dostęp: 20.09.2024 r.).
10. UNCTAD, *Data Protection and Privacy Legislation Worldwide*, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> (dostęp: 20.09.2024 r.).
11. Global Privacy Enforcement Network. [Online]. Available: <https://www.privacyenforcement.net/> (dostęp: 20.09.2024 r.).
12. Lovells H., *EU Digital Services Act: List of Digital Services Coordinators*, <https://www.engage.hoganlovells.com/knowledgeservices/eu-digital-services-act-list-of-digital-services-coordinators> (dostęp: 20.09.2024 r.).
13. Rovilos V., Zafir-Fortuna G., *EU's Digital Services Act just became applicable: outlining ten key areas of interplay with the GDPR*, Future of Privacy Forum, <https://fpf.org/blog/eus-digital-services-act-just-became-applicable-outlining-ten-key-areas-of-interplay-with-the-gdpr/> (dostęp: 20.09.2024 r.).

14. *Elastyczny*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/sjp/elastyczny%3B2556392> (dostęp: 20.09.2024 r.).
15. EP Legislative Carriage, <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age> (dostęp: 20.09.2024 r.).
16. Legislative Train Schedule, Proposal for a regulation on privacy and electronic communications, <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform> (dostęp: 20.09.2024 r.).
17. TSUE, Komunikat Prasowy nr 188/22, 22.10.2022, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188pl.pdf> (dostęp: 20.09.2024 r.).
18. Pieńkosz P., *Prezes UODO: kopiowanie dowodów osobistych przez instytucje finansowe jest uzasadnione*, „Dziennik Gazeta Prawna”, 11.07.2022, <https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8489919,czy-mozna-kopiowac-dowody-osobiste.html> (dostęp: 20.09.2024 r.).
19. *Prezes UODO ws. kopiowania dokumentów tożsamości: konieczne wytyczne dla banków*, „Rzeczpospolita” 14.04.2020, <https://www.rp.pl/dane-osobowe/art776041-prezes-uodo-ws-kopiowania-dokumentow-tozsamosci-konieczne-wytyczne-dla-bankow> (dostęp: 20.09.2024 r.).
20. Nagranie wideo panelu „FUTURE TREND: THE CONFLICT BETWEEN CYBERSECURITY AND PRIVACY”, który odbył się w czasie konferencji CPDP w Brukseli w roku 2023 r. <https://www.youtube.com/watch?v=LgCWRZYb040> (dostęp: 20.09.2024 r.).
21. Komisja, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 (dostęp: 20.09.2024 r.).
22. Komisja, <https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers> (dostęp: 20.09.2024 r.).
23. Google Scholar (dane na 20.09.2024 r.), https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=The+law+of+everything.

- +Broad+concept+of+personal+data+and+future+of+EU+data+protection+law&btnG= (dostęp: 20.09.2024 r.).
24. Sidley Austin LLP, *Unpacking Digital Data Laws Across Europe: Addressing the Digital Markets Act*, <https://datamatters.sidley.com/2023/01/24/unpacking-digital-data-laws-across-europe-addressing-the-digital-markets-act/> (dostęp: 20.09.2024 r.).
 25. Komisja, *Keynote of EVP Vestager at the European Competition Law Tuesdays: A Principles Based approach to Competition Policy*, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_6393 (dostęp: 20.09.2024 r.).
 26. About TILT, <https://www.tilburguniversity.edu/about/schools/law/departments/tilt/about> (dostęp: 20.09.2024 r.).
 27. nyob, *European Center for Digital Rights, GDPR: a culture of non-compliance? Numbers of evidence-based enforcement efforts*, https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance_2.pdf (dostęp: 20.09.2024 r.).
 28. UE, *Decentralised agencies*, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/types-institutions-and-bodies_en (dostęp: 20.09.2024 r.).
 29. IAPP, *Global AI Legislation Tracker By IAPP Research and Insights*, 25.08.2023, https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf (dostęp: 20.09.2024 r.).
 30. Rada Europy, *Glossary* <https://www.coe.int/en/web/artificial-intelligence/glossary> (dostęp: 20.09.2024 r.).
 31. OpenAI, ChatpGPT, <https://openai.com/blog/chatgpt> (dostęp: 20.09.2024 r.).
 32. *Sytuacja*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/slowniki/sytuacja.html> (dostęp: 20.09.2024 r.).
 33. *Krzyżować się*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/szukaj/krzyżować%20się.html> (dostęp: 20.09.2024 r.).

34. *Nakładać się*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/slowniki/nakladać%20się.html> (dostęp: 20.09.2024 r.).
35. *Zagadnienie*, [hasło w:] *Słownik języka polskiego PWN* [online], <https://sjp.pwn.pl/sjp/zagadnienie;2542263.html> (dostęp: 20.09.2024 r.).
36. UODO, *Oświadczenie Prezes UODO w związku z planowaną konferencją Ministerstwa Cyfryzacji*, dostęp w archiwum internetowym: <http://web.archive.org/web/20210228125035/http://https://uodo.gov.pl/pl/138/672> (ten komunikat usunięto ze strony internetowej PUODO) (dostęp: 20.09.2024 r.).
37. Nowakowski M., *Jeśli nie ma umowy kredytowej to dane klienta pozyskane w toku procesu oceny zdolności kredytowej powinny zostać usunięte?*, Bank.pl, 12.07.2022, <https://bank.pl/jesli-nie-ma-umowy-kredytowej-to-dane-klienta-pozyskane-w-toku-procesu-oceny-zdolnosci-kredytowej-powinny-zostac-usuniete/> (dostęp: 20.09.2024 r.).
38. Lesner D., *WSA: Bank i Biuro Informacji Kredytowej muszą usunąć dane osobowe niedoszłego kredytobiorcy*, <https://www.prawo.pl/biznes/czy-bank-moze-przetwarzac-dane-osobowe-niedoszlego-kredytobiorcy,515830.html>, Prawo.pl 05.07.2022. (dostęp: 20.09.2024 r.).
39. *Sądy raz każą usuwać, raz zachowywać dane. Niejasne przepisy ws. przetrzymywania informacji o klientach*, „Dziennik Gazeta Prawna” 13.09.2022 r., <https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8535477,rodo-uodo-dane-przetrzymywanie-danych.html> (dostęp: 20.09.2024 r.).
40. UODO, *Skarga kasacyjna od wyroku WSA ws. przetwarzania danych osobowych klienta banku*, 13.01.2022, <https://uodo.gov.pl/pl/138/2379>. (dostęp: 20.09.2024 r.).
41. *Efficiency*, [hasło w:] *Cambridge Dictionary* [Online], <https://dictionary.cambridge.org/dictionary/english/efficiency#> (dostęp: 20.09.2024 r.).
42. *Optymalny*, [hasło w:] *Słownik języka polskiego PWN*, <https://sjp.pwn.pl/slowniki/optymalny.html> (dostęp: 20.09.2024 r.).
43. *Niepewny*, [hasło w:] *Słownik języka polskiego PWN*, <https://sjp.pwn.pl/slowniki/niepewność.html> (dostęp: 20.09.2024 r.).

44. *SDT members to expand their collaboration regarding digital regulation*, <https://www.acm.nl/en/publications/sdt-members-expand-their-collaboration-regarding-digital-regulation>, Autoriteit Consument & Markt (ACM) (dostęp: 20.09.2024 r.).
45. *Samenwerkingsplatform Digitale Toezichhouders (SDT)*, <https://www.acm.nl/nl/organisatie/samenwerking/nationale-samenwerking/samenwerkingsplatform-digitale-toezichhouders-sdt> (dostęp: 20.09.2024 r.).
46. Commissariaat voor de Media, English summary Dutch Media Authority, <https://www.cvdm.nl/english-summary-dutch-media-authority/> (dostęp: 20.09.2024 r.).
47. *Dutch regulators strengthen oversight of digital activities by intensifying cooperation*, Autoriteit Consument & Markt (ACM), <https://www.acm.nl/en/publications/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation> (dostęp: 20.09.2024 r.).
48. Judiciary, *The justice system and the constitution*, <https://www.judiciary.uk/about-the-judiciary/our-justice-system/jud-acc-ind/justice-sys-and-constitution/#:~:text=The%20United%20Kingdom%20has%20three,of%20Union%201707%20and%201800.> (dostęp: 20.09.2024 r.).
49. Government of the Netherlands, *What is Brexit?*, <https://www.government.nl/topics/european-union/question-and-answer/what-is-brexit> (dostęp: 20.09.2024 r.).
50. UODO, *Brexit*, <https://uodo.gov.pl/pl/535/2509#:~:text=Możliwość%20swobodnego%20przekazywani a%20danych%20do,przepisami%20o%20ochronie%20danych%20osobowych.&text=O bie%20decyzje%20weszły%20w%20życie,czas%20określony%20wynoszący%20czter y%20lata.> (dostęp: 20.09.2024 r.).
51. Council of Europe, *United Kingdom*, <https://www.coe.int/en/web/data-protection/united-kingdom> (dostęp: 20.09.2024 r.).
52. UK legislation, *Data Protection Act 2018*, <https://www.legislation.gov.uk/ukpga/2018/12/contents> (dostęp: 20.09.2024 r.).

53. ICO, *Who we are*, <https://ico.org.uk/about-the-ico/who-we-are/> (dostęp: 20.09.2024 r.).
54. ICO, *Digital Regulation Cooperation Forum*, <https://ico.org.uk/about-the-ico/what-we-do/digital-regulation-cooperation-forum/> (dostęp: 20.09.2024 r.).
55. DCRF, *DRCF Terms of Reference*, https://www.drcf.org.uk/__data/assets/pdf_file/0030/258573/DRCF-Terms-of-Reference.pdf (dostęp: 20.09.2024 r.).
56. DCRF, *DRCF to pilot new advisory service as part of Government's plans for AI*, <https://www.drcf.org.uk/news-and-events/news/drcf-to-pilot-new-advisory-service-as-part-of-governments-plans-for-ai> (dostęp: 20.09.2024 r.).
57. Hajduk P., *AI Act and GDPR: on the path towards overlap of the enforcement structures*, 1.10.2023, <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/?cn-reloaded=1&cn-reloaded=1> (dostęp: 20.09.2024 r.).
58. UE, *Kraje UE, Holandia*, https://european-union.europa.eu/principles-countries-history/country-profiles/netherlands_pl#:~:text=W%20UE%3A%20od%201%20stycznia,Waluta%3A%20euro. (dostęp: 20.09.2024 r.).
59. De Autoriteit Consument & Markt (ACM) https://www.acm.nl/sites/default/files/old_publication/publicaties/15446_dutch-general-administrative-law-act.pdf (dostęp: 20.09.2024 r.).
60. Komisja, *Akt prawny o usługach cyfrowych: Komisja Europejska przyjmuje pierwszy zestaw aktów delegowanych*, 20 października 2024 r., https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689. (dostęp: 20.09.2024 r.).
61. Datatilsynet, *Wniosek o opinię EDPB w sprawie zgody lub zapłaty*, <https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/> (dostęp: 20.09.2024 r.).
62. Sejm Rzeczypospolitej Polskiej, *Transmisje Archiwalne: Podkomisja stała do spraw sztucznej inteligencji i przejrzystości algorytmów. Informacja na temat ochrony praw podstawowych oraz danych osobowych (w tym danych profilowych) w kontekście*

- korzystania ze sztucznej inteligencji i algorytmów cyfrowych – przedstawia Prezes Urzędu Ochrony Danych Osobowych*
https://www.sejm.gov.pl/sejm10.nsf/transmisje_arch.xsp?unid=378673CBF43C9FCFC1258B1500323AED. (dostęp: 20.09.2024 r.).
63. Parlament Europejski, *Walka z praniem pieniędzy: Parlament przyjął nowe przepisy*, 19.04.2024, <https://www.europarl.europa.eu/news/pl/press-room/20240419IPR20586/walka-z-praniem-pieniedzy-parlament-przyjal-nowe-przepisy> (dostęp: 20.09.2024 r.).
64. Bureau Européen des Unions de Consommateurs, *Consumer groups file complaint against Meta's unfair pay-or-consent model*, <https://www.beuc.eu/press-releases/consumer-groups-file-complaint-against-metas-unfair-pay-or-consent-model> (dostęp: 15.09.2024 r.).
65. Komisja, *Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act*, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_1689/IP_24_1689_EN.pdf (dostęp: 15.09.2024 r.).
66. Komisja, *Komisja wysyła do Meta wnioski o udzielenie informacji na podstawie aktu o usługach cyfrowych*, <https://digital-strategy.ec.europa.eu/pl/news/commission-sends-request-information-meta-under-digital-services-act-1> (dostęp: 15.09.2024 r.).
67. Komisja, *Komisja z zadowoleniem przyjmuje przyjęcie przez Parlament Europejski europejskiej przestrzeni danych dotyczących zdrowia oraz rozporządzenia w sprawie substancji pochodzenia ludzkiego*, 24.04.2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2250. (dostęp: 20.09.2024 r.).
68. Rada UE, *Przeciwdziałanie praniu pieniędzy: Rada przyjmuje pakiet przepisów*, 30.05.2024, <https://www.consilium.europa.eu/pl/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/pdf/> (dostęp: 20.09.2024 r.).
69. Vale S. B., *Training Large Generative AI Models Based on Publicly Available Personal Data: A GDPR Conundrum that the AI Act Could Solve*, „The Digital Constitutionalist”, 14.04.2023. <https://digi-con.org/training-large-generative-ai-models-based-on-publicly->

- available-personal-data-a-gdpr-conundrum-that-the-ai-act-could-solve/ (dostęp: 20.09.2024 r.).
70. J Nelson, *ChatGPT Wrongly Accuses Law Professor of Sexual Assault*, Yahoo Finance 7.042023, https://finance.yahoo.com/news/chatgpt-wrongly-accuses-law-professor-184500778.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGNAz_Mo-_4Ditq9q0FPgivJrr74PwDjb23HfsDzy7qhphC7XJVskisu-ZHDAfIlxnWa3MxcHC_pjz2zv2kBV7yGt_VZaUsv2OVzjDIV2CApvmQ5K9AgIW8pIvv2NJyswyvP9sM8jUBfYGc3N5Eo_lgZc4EwBQ9w_izzBHBCc46j (dostęp: 20.09.2024 r.).
 71. Grupa Robocza ds. AI, *Analysis of the Relationship of the Act on Artificial Intelligence with Selected and Proposed Regulations*, 3.08.2023, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjB08fnpNiGAxUjSPEDHea4DEoQFnoECBsQAQ&url=https%3A%2F%2Fwww.gov.pl%2Fattachment%2F8b2bed43-a24c-4d10-b341-a7372e702455&usg=AOvVaw04PjC_uudrNAIYqcldj5BV&opi=89978449 (dostęp: 20.09.2024 r.).
 72. *Data Protection Commission, Data Protection Commission publishes 2022 Annual Report*, <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commissionpublishes-2022-annual-report> (dostęp: 12.02.2024 r.).
 73. *Digital Cluster Bonn*, <https://www.digitalclusterbonn.de/DCB/start.html> (dostęp: 12.02.2024 r.).
 74. *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. UK Statutory Instruments 2019 No. 419*, ustanowione 28.02.2019, <https://www.legislation.gov.uk/uksi/2019/419/contents> (dostęp: 20.09.2024 r.).
 75. *Explanatory Memorandum to The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. UK Statutory Instruments 2019 No. 419*, https://www.legislation.gov.uk/uksi/2019/419/pdfs/uksiem_20190419_en.pdf.org/media/pdf/resource_center/eu_ai_act_stakeholder_map.pdf (dostęp: 20.09.2024 r.).

76. European Banking Authority: <https://www.eba.europa.eu/polski> (dostęp: 20.09.2024 r.).

⁷¹⁵ K. Ajdukiewicz, *Zarys logiki*, Warszawa 1958, s. 30.