Uniwersytet Jana Kochanowskiego w Kielcach
Wydział Prawa i Nauk Społecznych
Instytut Stosunków Międzynarodowych i Polityk Publicznych

Mgr Tomasz Osypowicz

Wpływ standardów Rady Europy i Unii Europejskiej na zapewnienie bezpieczeństwa danych osobowych w państwach członkowskich

Dysertacja doktorska z dziedziny nauk społecznych, dyscyplina: nauki o polityce i administracji

Promotor:
Prof. dr hab. Jerzy Jaskiernia
Promotor pomocniczy:
Dr Kamil Spryszak

Kielce 2021

Spis treści

Wykaz skrótów……...…….4

Wprowadzenie ……....6

Rozdział 1: Ogólna charakterystyka bezpieczeństwa danych osobowych

1.1. Geneza koncepcji bezpieczeństwa danych osobowych …….……..19
1.2. Rozumienie pojęcia „bezpieczeństwo danych osobowych” ……....24
1.3. Bezpieczeństwo danych osobowych a inne typy bezpieczeństwa
1.3.1. Bezpieczeństwo militarne …….…….31
1.3.2. Bezpieczeństwo energetyczne……...…….33
1.3.3. Bezpieczeństwo socjalne ……...……37
1.3.4. Bezpieczeństwo informatyczne……..38
1.3.5. Bezpieczeństwo polityczne …….…...40
1.3.6. Bezpieczeństwo demokratyczne ……..……..42
1.4. Rodzaje zagrożeń dla bezpieczeństwa danych osobowych …….43
1.5. Ogólne zasady związane z zapewnieniem bezpieczeństwa danych osobowych…..45
1.6. Standardy międzynarodowe w obszarze bezpieczeństwa danych osobowych
1.6.1. Standardy uniwersalne ……..……47
1.6.2. Standardy regionalne ……51

Rozdział 2: Bezpieczeństwo danych osobowych w systemie aksjologicznym Rady Europy i mechanizmy jego realizacji w państwach członkowskich

2.1. Ogólna charakterystyka Rady Europy ……...……..53
2.2. Bezpieczeństwo danych osobowych w systemie aksjologicznym RE
2.2.1. Standardy prawnie wiążące……..…….57
2.2.2. Standardy o charakterze tzw. „miękkiego prawa”…….……63

2.3. Mechanizmy egzekwowania standardów dotyczących bezpieczeństwa danych osobowych w państwach członkowskich

2.3.1. Procedura akcesyjna ……72

2.3.2. Procedura monitoringowa ……76

Rozdział 3: Bezpieczeństwo danych osobowych w systemie aksjologicznym Unii Europejskiej i mechanizmy jego realizacji w państwach członkowskich

3.1. Ogólna charakterystyka Unii Europejskiej ……81

3.2. Bezpieczeństwo danych osobowych w systemie aksjologicznym Unii Europejskiej

3.2.1 Standardy prawnie wiążące ……86

3.2.2. Standardy o charakterze tzw. „miękkiego prawa”……110

3.3. Mechanizmy egzekwowania standardów dotyczących bezpieczeństwa danych osobowych w państwach członkowskich

3.3.1. Faza procedury akcesyjnej ……113

3.3.2. Faza członkostwa ……116

Rozdział 4: Realizacja standardów bezpieczeństwa danych osobowych w państwach członkowskich Rady Europy i Unii Europejskiej

4.1. Przekształcenia w obszarze ustawodawstwa ……123

4.2. Przekształcenia w obszarze kreowania polityki bezpieczeństwa danych osobowych ……146

4.3. Przekształcenia w obszarze mechanizmów kontrolnych bezpieczeństwa danych osobowych ……151

4.4. Ocena efektywności wdrażania bezpieczeństwa danych osobowych w państwach członkowskich Rady Europy i Unii Europejskiej ……159

Zakończenie ……171

Bibliografia 175

Wykaz skrótów

CJ–PD – Komitet Ekspertów ds. Ochrony Danych

CNIL – Krajowa Komisja Informatyki i Wolności

CPDP – Komisja Ochrony Danych Osobowych

CSCE – Conference on Security and Cooperation in Europe

EDPB – Europejska Rada Ochrony Danych

EIOD - Europejski Inspektor Ochrony Danych

ENISA - The European Union Agency for Cybersecurity (Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji)

EROD – Europejska Rada Ochrony Danych

EURATOM - Europejska Wspólnota Energii Atomowej

EWG - Europejska Wspólnota Gospodarcza

EWWiS - Europejska Wspólnota Węgla i Stali

GDPR - General Data Protection Regulation (EU) 2016/679

GIODO - Generalny Inspektor Danych Osobowych

KBWE – Konferencja Bezpieczeństwa i Współpracy w Europie

KPP- Karta Praw Podstawowych

MPPOiP - Międzynarodowy Pakt Praw Obywatelskich i Politycznych

MŚP- małe i średnie przedsiębiorstwa

NAIH - Węgierski Krajowy Urząd ds. Ochrony Danych i Wolności Informacji

OBWE – Organizacja Bezpieczeństwa i Współpracy w Europie

OECD - Organizacji Współpracy Gospodarczej i Rozwoju

OSCE – Organization of Security and Cooperation in Europe

PACE – Parliamentary Assembly of the Council of Europe

RE – Rada Europy

SIS – System Informacyjny Schengen

TA – Traktat Amsterdamski

TFUE – Traktat o funkcjonowaniu Unii Europejskiej

TL – Traktat z Lizbony

TFUE – Traktat o funkcjonowaniu Unii Europejskiej

TSUE – Trybunał Sprawiedliwości Unii Europejskiej

TUE – Traktat o Unii Europejskiej

UE – Unia Europejska

ZPRE – Zgromadzenie Parlamentarne Rady Europy

Wprowadzenie

Zapewnienie bezpieczeństwa danych osobowych znalazło się w ostatnich latach w centrum zainteresowań badawczych[1]. Jest to wyrazem reakcji na skalę zagrożeń jakie współczesny rozwój cywilizacyjny przyniósł w zakresie przetwarzania danych osobowych[2]. Dostęp do danych osobowych uważanych jest za jeden z kluczowych czynników prowadzenia współczesnej działalności gospodarczej[3]. Rozwój technik informatycznych stał się z jednej strony źródłem wzrostu gospodarczego i szybszego rozwiązywania problemów społecznych, a z drugiej strony otworzył pole do nienotowanej uprzednio w takiej skali cyberprzestępczości[4]. Wymaga to poszukiwania nowych metod ochrony danych, w związku z coraz bardziej wyrafinowanymi typami występujących tu zagrożeń[5].

Ochronę danych osobowych uznaje się jako element prawa do prywatności[6]. Bezsporne jest to, że każdy człowiek powinien mieć zagwarantowane prawo do prywatności[7]. Prawo to, czerpiąc wiedzę z łaciny (z łac. prywatność – *privatus*), oznacza „oddzielony od reszty"[8]. Prawo do prywatności określane jest jako należące do jednego z praw człowieka[9]. W przypadku zderzenia prawa do prywatności i ochrony danych mówi się jednak o „niełatwej miłości"[10]. Ustawodawcy dążą do zabezpieczenia

[1] Por. *Security and privacy in cyber-physical systems: foundations, principles, and applications*, red. H. Song, G.A. Fink, S. Jeschke, *Security and privacy in cyber-physical systems : foundations, principles, and applications*, John Wiley & Sons, Chichester – Hoboken 2019.
[2] Zob. M. Betkier, *Privacy online, law and the effective regulation of online services*, Intersentia, Cambridge 2019, s. 48.
[3] Por. *Personal data in competition, consumer protection and intellectual property law : towards a holistic approach?*, red. M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Sulbryte-Namavičiene, Springer, Berlin 2018.
[4] Zob. R. Pittiglio, F. Reganati, F. Ricci, C. Tedeshi, [w:] *The Palgrave Handbook of Corporate Sustainability in the Digital Era*, Springer International Publishing, Cham 2020, s. 131.
[5] Zob. N.A. Hassan, R. Hijazi, H. Salminen, *Data hiding techniques in Windows OS: a practical approach to investigation and defense*, Syngress, Amsterdam 2017, s. 38.
[6] Szerzej: P. Sobczyk, *Ochrona danych osobowych jako element prawa do prywatności,* „Zeszyty Prawnicze UKSW" 2009, nr 9, s. 299 – 318.
[7] Zob. R. Mochocki, *Prawnokarna ochrona danych osobowych,* [w:] *Nowe wyzwania i rozwiązania w polskim systemie ochrony praw człowieka,* red. J. Jaskiernia, K. Spryszak, Wydawnictwo Adam Marszałek, Toruń 2018, s. 368.
[8] Zob. M. Puwalski, *Prawo do prywatności osób publicznych,* Wydawnictwo TNOiK, Toruń 2003, s. 14.
[9] Zob. O. Diggelmann, M.N. Cleis, *How to Right to Privacy Became a Human Right,* "Human Rights Law Review" 2014, vol. 14, s. 441-458.
[10] M. Merill, *An Uneasy Love Triangle Between Alexa, Your Personal Life, and Data Security: Exploring Privacy in the Digital New Age*, "Mercer Law Review", 2020, nr 2, s. 637.

prywatności[11]. Kluczowe znaczenie ma tu zapewnienie instrumentów kontrolnych ze strony kompetentnych organów władzy publicznej[12]. Jest to jednak złożony cel w sytuacji stałego doskonalenia technologii informatycznych, a w tym także technik inwigilacyjnych[13]. Samo więc zagwarantowanie prawa do prywatności na poziomie konstytucyjnym, jak na to wskazują np. doświadczenia Federacji Rosyjskiej, nie jest wystarczające w zderzeniu z nowymi wyzwaniami, jakie niesie rozwój metod informatycznych i muszą być tu ustawicznie weryfikowane zarówno rozwiązania rangi ustawowej, a także przepisy wykonawcze[14]. Również doświadczenia Stanów Zjednoczonych wskazują, że nie można poprzestać na gwarancji konstytucyjnej, a ochrona danych osobowych powinna być objęta precyzyjną regulacją ustawową[15].

Dane osobowe są dziś przetwarzane w nienotowanej skali zarówno w sferze publicznej, jak i prywatnej. Gdyby poprzestać na przykładzie Facebooka, który jest drugim co o wielkości światowym medium społecznościowym, to notuje on cotygodniowy wzrost rzędu 3% i staje się atrakcyjnym przedmiotem ataków dla tych, którzy chcą pozyskać dane dotyczące jego użytkowników[16]. Wiąże się z tym ryzyko w zakresie zapewnienia bezpieczeństwa tych danych, którego identyfikacja stanowi podstawę do podejmowania działań ochronnych[17]. Rozwój technologii cyfrowych i ich szerokie zastosowanie w różnych obszarach życia społecznego, politycznego i gospodarczego[18] w sposób bezpośredni oddziałuje na zapewnienie bezpieczeństwa w procedurach przetwarzania danych osobowych[19]. Ta technologiczna rewolucja w dziedzinie technologii cyfrowych z jednej strony niesie nowe możliwości w zglobalizowanym świecie w sferze nauki i życia gospodarczego, ale też wiąże się z

[11] Zob. U. Jackowiak, *Ochrona danych osobowych w prawie pracy,* „Prawo i Zabezpieczenie Społeczne" 1998, nr 7-8, s. 31.
[12] Zob. Z.-Y. Du, *Personal Data Security and Supervision in the Age of Large Data*, "Intelligent Automation and Soft Computing" 2019, nr 1, s. 1.
[13] Por. *Law, policy and the Internet*, red. L. Edwards, Hart, London 2019.
[14] Zob. A.K. Zharova, V.M. Elin, *The use of Big Data: A Russian perspective of personal data security*, "The Computer Law and Security Report", 2017-08, nr 4, s. 482.
[15] Zob. J. Desiree Dodd, *Data security law—state statutory requirements for protecting personal data*, "The American Journal of Trial Advocacy", 2015-04-01, nr 3, s. 623.
[16] Zob. I.M. Vlad, *Security of Personal Data in Social Networks*, "International Journal of Information Security and Cybercrime (IJISC)", 2018, nr 2, s.14.
[17] Zob. S.C. Cha, K.-H. Yeh, *A Data-Driven Security Risk Assessment Scheme for Personal Data Protection*, Institute of Electrical and Electronics Engineers (IEEE) Access, 2018, vol. 6, s. 505.
[18] Por. *Digital transformation in business and society: theory and cases*, red. P.B. George, J. Paul, Palgrave Macmillan, Cham 2020.
[19] Por. *Digital Transformation*, red. R. Neugebauer, Springer, Berlin-Heidelberg 2019.

pojawieniem się nowego typu zagrożeń dla ochrony praw człowieka[20]. Następuje przy tym odejście od subiektywnego i mniej ustrukturowanego przetwarzania danych osobowych do jego form zautomatyzowanych. W wyniku tego może dochodzić do niekontrolowanej cyrkulacji o ludziach, ich upodobaniach, preferencjach i stylu życia[21]. Rodzi to szereg obaw w obszarze ochrony praw człowieka, bo może nieść praktyki dyskryminacyjne w zakresie dostępu do kredytów, ubezpieczenia, edukacji, a nawet ochrony zdrowia[22].

Istotnym obszarem zagrożeń dla ochrony danych osobowych stała się służba zdrowia. Wiążę się to m.in. z dokonującym się procesem decentralizacji usług medycznych, a także coraz szerszym wykorzystaniem technik informatycznych, co w sposób zasadniczy zwiększyło niebezpieczeństwo bezprawnego dostępu do danych pacjentów[23].

Przetwarzanie danych osobowych otwiera też drogę do manipulacji cenami na rynku drogą adresowania ofert do precyzyjnie zaadresowanej grupy potencjalnych klientów[24]. Przetwarzanie danych musi się więc stać przedmiotem regulacji prawnych, uwzględniających odpowiednie mechanizmy ochronne[25]. Trwają poszukiwania rozwiązań technologicznych, które umożliwiałyby zapewnienie standardów ochronnych w procesie przetwarzania danych osobowych[26]. Poważnym wyzwaniem stało się zapewnienie prawa do bycia zapomnianym, istotne dla ochrony praw człowieka w dobie szerokiego zastosowania Internetu[27]. Wdrażanie nowych technologii wiąże się z niepewnością, w jakim celu będą one wykorzystywane[28]. Tworzy to zasadniczy problem

[20] Por. *Edge Computing From Hype to Reality*, red. F. Al-Turjman, Springer International Publishing, Cham 2019.
[21] Zob. D. Lee, N. Park, G. Kim, J. Jin, S. Jo, J. Han, *De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment*, "Peer-to-Peer Networking and Applications", 2018-11, nr 6, s. 1299.
[22] Por. *Consumer informatics and digital health: solutions for health and health care*, red. M. Edmunds, E. Holve, Springer, Cham 2019; *Personalized Medicine in Healthcare Systems Legal, Medical and Economic Implications*, red. N. Bodriga-Vukobrat, D. Rukavina, K. Pavelić, G.G. Sander, Springer International Publishing, Cham 2019.
[23] Zob. J.K. Lynch, M. Fisk, *mHealth, Trust and the Security of Personal Data*, "Mobile e-Health", 2 December 2017, s. 237.
[24] Zob. Y. Liu, C. Greene, *The Dark Side of Big Data: Personal Privacy, Data Security, and Price Discrimination*, "Digital Transformation in Business and Society", 15 October 2019, s. 145.
[25] Zob. A. Drożdż, *Protection of natural persons with regard to automated individual decision-making in the GDPR*, Kluwer Law International, Alpen aan den Rijn 2020, s. 44.
[26] Por. *Trusting records in the Cloud*, red. L. Duranti, C. Rogers, Facet, London 2019.
[27] Zob. P. Lambert, *The right to be forgotten: interpretation and practice*, Bloomsbury, London 2019, s. 63.
[28] Por. *Regulating new technologies in uncertain times*, red. L. Reins, Asser Press, Springer, The Hague 2019.

dla prawnych działań regulacyjnych, gdyż prawodawca nie zawsze potrafi przewidzieć wszystkie konsekwencje, jakie może przynieść zastosowanie nowych technologii.

Globalny charakter mediów społecznościowych powoduje, że problemy ochrony danych osobowych mają istotne prawne i polityczne znaczenie nie tylko dla mieszkańców Europy i Ameryki, ale też Azji, Afryki[29] oraz Australii i Oceanii. Choć cel w postaci zabezpieczenia danych osobowych pozostaje wszędzie tam w zasadzie ten sam, to jednak dają o sobie znać specyficzne podejścia w zakresie instrumentów przeciwdziałania, nawiązujące do kultury politycznej, kultury prawnej oraz tradycji. Widać to np. w odniesieniu do Konwencji Unii Afrykańskiej o cyberbezpieczeństwie i ochronie danych osobowych z 27 czerwca 2014[30].

Bezpieczeństwo danych osobowych stanowi dziś jeden z istotnych elementów polityki państw[31]. Jest to reakcja na – jak to określono – „kryzys w zakresie ochrony danych osobowych"[32]. Internet przyniósł bowiem nowe możliwości i zagrożenia, jakie wiążą się m.in. z dynamicznym kształtowaniem się rynku danych osobowych[33]. Ludzie zdają sobie bowiem coraz bardziej sprawę z tego, na jakie niebezpieczeństwa narażone są ich dane osobowe w sytuacji funkcjonowania wyrafinowanych metod inwigilacyjnych, jakie niosą nowoczesne formy komunikowania się i oczekują od władz państwowych podejmowania adekwatnych środków zaradczych[34]. Dotyczy to zwłaszcza Internetu, który gromadzi – uwzględniając różne formy mediów społecznościowych – miliardy użytkowników, zabieganie o dane osobowe których staje się biznesem o skali globalnej[35]. Stąd poszukiwanie skutecznych mechanizmów ochrony tych danych urasta do rangi jednego z najważniejszych wyzwań współczesności[36]. Zapewnieniu tej ochrony

[29] Zob. R. Alunge, *Africa's Multilateral Legal Framework on Personal Data Security: What Prospects for the Digital Environment?*, "e-Infrastructure and e-Services for Developing Countries", 14 February 2020, s. 38.
[30] Zob. K.M. Ball, *African Union Convention on Cyber Security and Personal Data Protection*, "International Legal Materials" 2017, nr 1, s. 164; eadem, *Introductory note to African Union convention on cyber security and personal data protection*, "International Legal Materials", 2017, nr 1, s. 164.
[31] Szerzej: T. Osypowicz, *Standardy uniwersalne w obszarze bezpieczeństwa danych osobowych,* „Przegląd Prawno-Ekonomiczny" 2019, nr 46.
[32] L. Keshu, S. Meixia, *Personal Information Security Crisis in the Era of Big Data*, "Journal of physics. Conference series", 2020, vol. 1486, s. 52002.
[33] Por. *Competition law for the digital economy*, red. B. Lundquist, M.S. Gal, Edward Elgar Publishing, Cheltenham-Northampton 2019.
[34] Zob. P. Arora, *The Next Billion Users: Digital Life Beyond the West*, Harvard University Press, Cambridge 2019, s. 29.
[35] Por. *Data protection in the Internet*, red. D.M. Vincente, P.S. de Vasconelos Casimiro, Springer, Cham 2020.
[36] Por. *Ubiquitous Computing and Computing Security of IoT*, red. J. Jeyjanyhi, A. Abraham, H. Mcheick, Springer International Publishing, Cham 2019.

służą w szczególności zawierane porozumienia dotyczące przetwarzania danych osobowych[37].

Nowe typy zagrożeń bezpieczeństwa informacji wiążą się z użytkowaniem komputerów przenośnych i smartfonów[38].

Zagrożenia w zakresie zarządzania danymi osobowymi zwiększyły zainteresowanie dla tworzenia Systemów Zarządzania Danymi Osobowymi (Personal Data Management Systems - PDMS), oferowanych jednostkom dla ochrony całokształtu ich obecności w świecie cyfrowym[39]. Eksponuje się zarówno walory takich systemów, jak i zagrożenia, które niosą. Stawiane są bowiem pytania, na ile zwykli ludzie będ mieli faktyczny dostęp do zbioru danych i potrafili nimi zarządzać[40].

Żyjemy w czasach globalnej współzależności, gdzie problemy bezpieczeństwa związane z terroryzmem mają charakter ponadgraniczny, a zglobalizowane sieci informatyczne i handlowe e-platformy zmieniły kształt światowej gospodarki. W tych warunkach załamaniu uległy wcześniejsze systemy regulacyjne, a tworzenie nowych musiało uwzględniać konflikty powstające na styku wolności i bezpieczeństwa. Nasiliły się one od chwili zamachu na World Trade Centre w dniu 11 września 2001 r., co spowodowało wymóg udostępniania listy pasażerów linii lotniczych[41], czy w związku z rewelacjami przekazanymi przez Snowdena[42]. Wywołało to globalne działania, w których zaangażowane są państwowe agencje bezpieczeństwa, ministrowie spraw wewnętrznych, prywatne organizacje pozarządowe (NGOs), biurokraci, a także inni aktorzy, próbujący eksploatować tego typu wydarzenia do osiągania swych celów w skali transatlantyckiej[43].

---

[37] Zob. J.B. Weiss, *Data processing agreements: coordination, drafting & negotiation*, International Association of Privacy Professionals IAPP, Portsmouth 2019, s. 34.

[38] Zob. E. Pshehotskaya, *Theft Preventive Measures for Interconnected Personal Computer Devices as Proactive Physical Security of Data*, "International Journal of Embedded and Real-Time Communication Systems (IJERTCS)", 2018, nr 2, s. 97.

[39] Zob. N. Anciaux, L. Buganim, P. Pucheral, I.S. Popa, G. Scerri, *Personal Database Security and Trusted Execution Environments: A Tutorial at the Crossroads,* [w:] *Proceedings of the VLDB Endowment*, 28 August 2019, s. 14.

[40] Zob. N. Anciaux, P. Bonnet, L. Bauganim, B. Nguen, P. Pucheral, I. Sandu Popa, G. Scerri, *Personal Data Management Systems: The security and functionality standpoint, "*Information Systems" 2019, vol. 80, s. 13.

[41] Zob. O. Mironenko Enerstvedt, *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*, Springer International Publishing, Cham 2017, s. 32.

[42] Zob. E. Snowden, *Mémoires vives*, Éditions du Seuil, Paris 2019, s. 34.

[43] Zob. H. Farrell, A. Newman, *Of privacy and power: the transatlantic struggle over freedom and security*, Princeton University Press, Princeton – Oxford 2019, s. 66.

Zarządzanie bezpieczeństwem informatycznym stało się obszarem działalności państwowej, które wymaga stałego dostosowania instrumentów prawnych do nowych wyzwań[44]. Wymaga ono innowacyjnego spojrzenia na zadania państwa w dobie rewolucji informatycznej[45]. Chodzi o przeciwdziałanie zagrożeniom, jakie związane są z cyberterroryzmem[46]. Ma ono zarówno wymiar wewnętrzny, w kontekście konstytucyjnie gwarantowanych praw i wolności obywateli, jak też wymiar zewnętrzny, w kontekście ochrony praw człowieka, zarówno w skali powszechnej, jak i regionalnej. Dotyczy to w szczególności zarządzania incydentami w systemie bezpieczeństwa[47]. Wiążą się one m.in. z atakami hakerów zorientowanych na pozyskanie danych osobowych[48]. Mają one na celu kradzież danych lub wykorzystywanie ich do innych działań przestępczych. Problem jest jednak złożony, bo niektóre przedsiębiorstwa używają techniki hakowania do ograniczenia ryzyka w podejmowanej działalności gospodarczej, np. w sferze ubezpieczeń[49].

Stąd próbuje się szukać zabezpieczeń prywatności w stosunku do cyber-fizycznych systemów (Cyber-Physical Systems – CPS), w ramach różnych form ich zastosowania, m.in. uwzględniających techniki kryptograficzne. CPS stanowią nową generację systemów, które łączą techniki komputerowe z możliwościami powiązań występujących w świecie fizycznym w procesie monitorowania i kontroli jednostek. Umożliwia to gromadzenie olbrzymiej liczby informacji i ich wykorzystanie w procesach decyzyjnych w różnych dziedzinach[50].

Koncepcja Chmur Danych Osobowych (Personal Data Clouds - PDCs) związana jest z zapewnieniem pożądanych metod gromadzenia danych osobowych, a zarazem z dostępem do tych danych osób, których one dotyczą. Daje to osobom zainteresowanym prawo do zarządzania tymi danymi. Ma to istotne znaczenie dla zapewnienia

[44] Zob. A. Volchkov, *Information security governance : framework and toolset for CISOs and decision makers*, CRS Press. Boca Raton 2019, s. 43.
[45] Zob. J. Ladley, *Data governance : how to design, deploy and sustain an effective data governance program*, Academic Press, London 2020, s. 54.
[46] Zob. Z.-H. Pang, G.-P. Liu, D. Zhou, D. Sun, *Networked Predictive Control of Systems with Communication Constraints and Cyber Attacks*, Springer, Singapore 2019, s. 44.
[47] Zob. M. Pemble, W. Goucher, *CIO's guide to security incident management*, CRS Press, New York 2019, s. 38.
[48] Zob. M.J. Carey, Tribe *of hackers : cybersecurity advice from the best hackers in the world Cybersecurity advice from the best hackers in the world*, Wiley, Indianopolis 2019, s. 54.
[49] Zob. P. Burkat, T. McCourt, *Why Hackers Win : Power and Disruption in the Network Society*, University of California Press, Berkeley 2020, s. 56.
[50] Zob. M. Pan, J. Wang, S.M. Errapotu, X. Zhang, J. Ding, Z. Han, *Big Data Privacy Preservation for Cyber-Physical Systems*, Springer International Publishing, Cham 2019, s. 44.

bezpieczeństwa tych danych, a także kontroli zasadności ich gromadzenia i przetwarzania[51]. Dotyczy to m.in. chmur obliczeniowych[52]. Wskazuje się jednak, że ochrona danych osobowych w systemie Cloud Computing jest szczególnie trudnym wyzwaniem[53].

Współczesna globalizacja, poczynając od lat 70. XX w., przyniosła rewolucję w zakresie elektronicznych technik przetwarzania informacji. Obszar aktywności społecznej, politycznej i gospodarczej przeniósł się do Internetu w tak dużej skali, że zaczęły być gromadzone o ludziach informacje we wszystkich dziedzinach ich życia, również w ujęciu ponadgarnicznym, na ochronę których to informacji nie znajdowano w odpowiednim czasie odpowiednich instrumentów. Zaczęto wówczas podejmować analizy rozwiązań prawnych zarówno w skali krajowej, jak i regionalnej[54]. Wzrosło też znaczenie badań porównawczych zastosowanych rozwiązań prawnych[55]. Wiąże się to z tym – gdyby nawiązać do doświadczeń choćby Stanów Zjednoczonych i Unii Europejskiej – że strategie zapewnienia ochrony danych osobowych bywają zróżnicowane[56].

Istotne wyzwania dla bezpieczeństwa danych osobowych pojawiają się wraz z rozwojem robotyzacji i powstawaniem nowych technologii informacyjnych[57], m.in. w zakresie sztucznej inteligencji[58]. Pojawia się tam bowiem niebezpieczeństwo użycia danych niekompletnych lub nieprawdziwych, które mogą stać się powodem działań dyskryminacyjnych[59]. Nieprzypadkowo więc Agencja Praw Podstawowych UE podjęła

[51] Zob. *Privacy and security in personal data clouds: final report*, ENISA, Heraklion 2016, s. 9.
[52] Zob. A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Wolters Kluwer Polska Warszawa 2018, s. 32. Por. A. Biczysko-Pudełko, *Administrator danych osobowych i przetwarzający dane na zlecenie a chmura obliczeniowa - problemy interpretacyjne*, „Prawo Mediów Elektronicznych" 2016, nr 1, s. 49.
[53] Zob. L. Kumar, V. Rishival, *Design of Retrievable Data Perturbation Approach and TPA for Public Cloud Data Security*, "Wireless Personal Communications", 2019, nr 1, s.235.
[54] Por. *Regulating industrial internet through IPR, data protection and competition law*, red. R.M. Ballardini, I. Pitkänen, P. Kuoppamäki, Kluwer Law International, Alphen aan den Rijn 2019.
[55] Zob. R. Walters, L. Trakman, B. Zeller, *Data Protection Law A Comparative Analysis of Asia-Pacific and European Approaches*, Springer, Singapore 2019, s. 33.
[56] Zob. A. Fleischmann, *Personal Data Security: Divergent Standards in the European Union and the United States*, "Fordham International Law Journal" 1995, nr 1, s. 143.
[57] Por. *AI in Cybersecurity*, red. L.F. Sikos, Springer International Publishing, Cham 2019.
[58] Por. *Security in Smart Cities: Models, Applications, and Challenges*, red. A.E. Hassanien, M. Elhoseny, S.H. Ahmed, A.K. Singh, Springer International Publishing 2019.
[59] Por. *AI Love You Developments in Human-Robot Intimate Relationships,* red. Y. Zhou, M.H. Fischer, Springer International Publishing, Cham 2019.

działania na rzecz poszukiwania rozwiązań, które prowadziłyby do oparcia się na rzetelnych danych w systemach opartych ma „sztucznej inteligencji”[60].

Poszukiwanie doskonalszych metod ochrony danych osobowych ma też znaczenie dla władz lokalnych[61]. Projektowanie „inteligentnych miast” ma uwzględniać ochronę danych osobowych w sytuacji, gdy narasta liczba zagrożeń dla zapewnienia bezpieczeństwa w tym zakresie[62]. Ma to istotne znaczenie dla zapewnienia ochrony praw człowieka w procedurach, które mają zapewnić bezpieczeństwo społeczności lokalnych[63].

Nowe wyzwania dla ochrony danych osobowych niesie zastosowanie technologii 5G[64]. Trwają więc poszukiwania zabezpieczeń, które mogłoby zrealizować wymóg bezpieczeństwa informatycznego w odniesieniu do tej technologii, która stanie się w najbliższych latach istotnym segmentem nowoczesnej komunikacji społecznej[65].

Władze państwowe z jednej strony dążyły do ochrony danych osobowych obywateli, a z drugiej strony zmuszone były udostępniać informacje o nich ze względu na wymogi bezpieczeństwa, stosowania prawa czy dostępu obywateli do korzyści wynikających z funkcjonowania systemu opieki społecznej. Szczególne wyzwanie wiązało się z sytuacjami, gdy dochodziło do ponadgranicznego przepływu informacji. Powstawało wówczas pytanie: jakie prawo ma zastosowanie. Sprawa ta stała się przedmiotem porozumień międzypaństwowych, a także o charakterze multilateralnym, przyjmowanych w ramach organizacji międzynarodowych, takich jak OECD czy APEC[66].

Przedmiotem szczególnego zainteresowania jest kwestia wzajemnych relacji bezpieczeństwa i ochrony danych osobowych, zwłaszcza w kontekście możliwej

---

[60] Zob. *Data quality and artificial intelligence: mitigating bias and error to protect fundamental rights*, Publication Office, Luxembourg 2019, s. 8.

[61] Zob. R. Schifreen, *Data Protection and Security for Personal Computers: A manager's guide to improving the confidentiality, availability and integrity of data on Personal Computers and Local Area Networks*, Elsevier Science, Amsterdam 2014, s. 39.

[62] Por. *Smart Cities of Today and Tomorrow Better Technology, Infrastructure and Security*, red. J.P. Pelton, I.B. Singh, Springer International Publishing, Cham 2019.

[63] Por. *Digital Twin Technologies and Smart Cities*, red. M. Farsi, A. Daneskhah, A. Hoseinian-Far, H. Jahankhani, Springer International Publishing, Cham 2020.

[64] Por. *5G Enabled Secure Wireless Networks*, red. D.N.K. Jayakody, K. Srinivasan, V. Sharma, Springer International Publishing, Cham 2019.

[65] Zob. S.-J. Kim, K.-J. Suh, H.-J. Lee, H.-I. Yu, J.-H. Park, H.-J. Lee, *Apparatus and method for enhancing personal information data security*, ESP, Cenet 2019, s. 45.

[66] Zob. J.W. Kropf, N. Cohen, *U.S. government practice on global sharing of personal information*, 3rd ed., International Association of Privacy Professionals IAPP, Portsmouth 2000, s. 23.

inwigilacji elektronicznej obywateli[67]. Narasta bowiem napięcie pomiędzy swobodą informacji, traktowanej jako jeden z najważniejszych standardów ochrony praw człowieka, a ochroną danych osobowych, co rzutuje zarówno na działalność tradycyjnej prasy, jak i na coraz bardziej żywiołowo rozwijające się tzw. nowe media. Poszukiwanie równowagi w tym zakresie określane bywa niekiedy „balansowaniem na linie"[68].

Jeszcze do niedawna nie każdy zauważał lub być może nie był świadomy tego, że jego dane osobowe podlegają przetwarzaniu. Do dziś nadal wiele osób nie wie lub nie zdaje sobie sprawy z ważności danych osobowych, które są wprowadzane do obiegu społecznego[69]. Często też obywatel sam wyraża na to zgodę nie zdając sobie sprawy z konsekwencji takiej decyzji[70]. Zdarza się także, iż przepisy prawa świadomie nie są przestrzegane, są lekceważone i pomijane przez osoby, z którymi są one związane[71]. Z tej motywacji przyjęte zostało rozporządzenia UE dotyczącego ochrony danych osobowych (RODO), określane w kategoriach „zharmonizowanego obowiązku" i „dzielonej odpowiedzialności"[72]. Dlatego ustawodawca państwa członkowskiego UE, wdrażając to rozporządzenie UE[73], powinien dążyć do stworzenia coraz skuteczniejszej ochrony danych osobowych[74]. Każde działanie w kierunku wykreowania lepszej ochrony tych danych można określać jako bezcenne zarówno dla każdego człowieka, jak i całej społeczności[75].

Bezpieczeństwo danych osobowych stało się szczególnie istotnym zagadnieniem zarówno na poziomie krajowym jak i międzynarodowym. Szybki rozwój technologii

---

[67] Zob. S. Sharpe, *National security, personal privacy and the law: surveying electronic surveillance and data acquisition*, Routlege, London-New York 2020, s. 34.

[68] D. Erdos, *European data protection regulation, journalism and traditional publishers: balancing on a tightrope?*, Oxford University Press, Oxford 2019, s. 8.

[69] Zob. A.M. Dzięgiel, *Naruszenie dóbr osobistych w Internecie,* „Jurysta" 2017, nr 1, s. 29 – 32.

[70] Zob. K. Dygasiewicz, *Kradzież tożsamości w czasach społeczeństwa informacyjnego,* [w:] *Internet. Strategie bezpieczeństwa. Security strategy,* red. G. Szpor, A. Gryszczyńska, Wydawnictwo C.H. Beck, Warszawa 2017, s. 251 – 258.

[71] Por. T. Banyś, A.J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Presscom, Wrocław 2017.

[72] P.T.J. Wolters, *The security of personal data under the GDPR. A harmonized duty or a shared responsibility?*, "International Data Privacy Law", 2017, nr 3, s. 165

[73] Por. *The EU general data protection regulation (GDPR): a commentary*, red. C. Kuner, Oxford University Press, Oxford 2019.

[74] Zob. P.T.J. Wolters, *The Security of Personal Data under the GDPR: a harmonized duty or a shared responsibility?,* „International Data Privacy Law" 2017, Vol. 7, s. 165 – 178.

[75] Por. M. Balcerzak, *Kategoria jawności i prawo do informacji z perspektywy orzecznictwa Europejskiego Trybunału Praw Człowieka,* [w:] *Jawność i jej ograniczenia,* red. G. Szpor, C. Mik, t. 11. *Standardy europejskie*, Wydawnictwo Beck, Warszawa 2016, s. 67 – 93.

informacyjnych zwiększył, bowiem potrzebę solidniejszej ochrony danych osobowych zarówno w systemie aksjologicznym Unii Europejskiej (UE), jak i Rady Europy (RE). Zapewnienie tej ochrony zaczęto wiązać z nowymi i poważnymi wyzwaniami, ponieważ postęp technologiczny rozszerzył granice takich obszarów jak nadzór, przechwytywanie informacji i przechowywanie danych[76]. Dotyczy do m.in. bezpieczeństwa danych w związku z masowym stosowaniem kart kredytowych[77].

Na tle realizacji instrumentów prawnych pojawiło się szereg trudnych kwestii teoretycznych. Z podobną sytuacją mamy do czynienia w Unii Europejskiej, gdzie podnoszony jest np. problem wzajemnej relacji art. 17 RODO oraz art. 8 Karty Praw Podstawowych, gwarantującego prawo do ochrony danych osobowych[78].

Celem dysertacji doktorskiej jest ustalenie, jaki jest wpływ standardów Rady Europy i Unii Europejskiej na zapewnienie bezpieczeństwa danych osobowych w państwach członkowskich. Zasadność podjęcia się tej analizy badawczej wiąże się z tym, że zarówno RE, która ma znaczące doświadczenie w regulowaniu ochrony danych, a także dąży do ustanowienia regionalnych standardów w tej dziedzinie, ale też Unia Europejska, która wprowadza przełomowe zmiany w tym obszarze, w zasadniczy sposób przyczyniają się do tworzenia nowych warunków przetwarzania danych w dzisiejszym zglobalizowanym świecie. Zasadnym jest więc podjęcie analizy, jak te dwie ważne organizacje międzynarodowe oddziałują na ochronę danych osobowych w państwach członkowskich. Problem ten nie doczekał się dotychczas monograficznego opracowania, stąd niniejsza dysertacja jest próbą wypełnienia tej luki.

Analiza w dysertacji doktorskiej przeprowadzona została w ramach 4 rozdziałów.

Rozdział 1 dotyczy ogólnej charakterystyki bezpieczeństwa danych osobowych. Zamiarem tego rozdziału było ukazanie: genezy koncepcji bezpieczeństwa danych osobowych, jak również rozumienia tego pojęcia. Autor skoncentrował się również na bezpieczeństwie danych osobowych w odniesieniu do innych typów bezpieczeństwa tj.: bezpieczeństwa militarnego, bezpieczeństwa energetycznego, bezpieczeństwa socjalnego, bezpieczeństwa informatycznego, bezpieczeństwa politycznego, czy też

[76] Szerzej: *Handbook on European Data Protection Law – 2018 edition,* Publications Office of the European Union, Luxembourg 2018.

[77] Por. *PCI compliance : understand and implement effective PCI data security standard compliance. Understand and implement effective PCI data security standard compliance*, red. B.R. Wiliams, A.A. Chuvakin, D. Milroy, Syngress, Waltham 2015.

[78] Zob. J. Ausloos, *The right to erasure in EU data protection law : from individual rights to effective protection, Oxford University Press*, Oxford 2020, s. 54.

bezpieczeństwa demokratycznego. Ukazane zostały także rodzaje zagrożeń oraz ogólne zasady związane z zapewnieniem bezpieczeństwa danych osobowych. Poza tym zaprezentowane zostały standardy uniwersalne i regionalne w tym obszarze.

W rozdziale 2 zostało przedstawione bezpieczeństwo danych osobowych w systemie Rady Europy i mechanizmy jego realizacji w państwach członkowskich. Przedmiotem niniejszego rozdziału była analiza standardów prawnie wiążących, jak i tych o charakterze tzw. „miękkiego prawa". Celem analizy było też zaprezentowanie mechanizmów egzekwowania standardów dotyczących bezpieczeństwa danych osobowych w państwach członkowskich (procedura akcesyjna, procedura monitoringowa).

W rozdziale 3 zostało przedstawione bezpieczeństwo danych osobowych w systemie Unii Europejskiej i mechanizmy jego realizacji w państwach członkowskich. Odniosłem się w analizie zarówno do standardów prawnie wiążących, jak i standardów o charakterze „miękkiego prawa", jak również zaprezentowałem mechanizmy egzekwowania standardów w tym obszarze podczas fazy akcesyjnej i fazy członkostwa.

W rozdziale 4 dokonana została analiza realizacji standardów bezpieczeństwa danych osobowych w państwach członkowskich Rady Europy i Unii Europejskiej W związku z tym przedstawiłem przekształcenia w trzech obszarach: ustawodawstwa, kreowania polityki bezpieczeństwa danych osobowych, oraz w obszarze mechanizmów kontrolnych. Podjąłem się także oceny efektywności wdrażania bezpieczeństwa danych osobowych w państwach członkowskich RE i UE.

W pracy podjęto weryfikacji następujące **hipotezy badawcze:**

Hipoteza 1. Pod wpływem standardów Rady Europy i Unii Europejskiej dokonano podniesienia bezpieczeństwa danych osobowych do rangi konstytucyjnie chronionego prawa. Oddziaływanie tych standardów zaowocowało nie tylko stworzeniem odpowiedniego ustawodawstwa, ale i podjęciem prac legislacyjnych w celu jego skutecznego dostosowania do norm międzynarodowych.

Hipoteza 2. Nacisk, jaki na państwa członkowskie od wielu lat kładą Rada Europy i Unia Europejska w kontekście bezpieczeństwa danych osobowych, sprawił, iż w każdym z tych państw zagadnienia to stało się przedmiotem regulacji prawnych.

Potwierdza to monitoring prowadzony zarówno w systemie RE, jak i UE, który daje możliwość uchwycenia stopnia realizacji standardów międzynarodowych w tym zakresie. Doświadczenia zgromadzone w państwach członkowskich RE i UE wskazują jednak, że istnieje potrzeba identyfikowania coraz to nowych zagrożeń powstających w systemie ochrony danych osobowych. Mogą one skłaniać do modyfikacji standardów międzynarodowych, a także do odpowiedniego dostosowania do nich ustawodawstwa krajowego.

Hipoteza 3. Współcześnie zasadniczy krok w kwestii bezpieczeństwa danych osobowych dokonała Unia Europejska. Tworząc RODO założyła, iż głównym celem będzie zapewnienie spójnego stopnia ochrony danych osób fizycznych w Unii oraz zapobiegnięcie rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym. Standardy te mają także gwarantować podmiotom gospodarczym pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten dam poziom prawnie egzekwowalnych praw i obowiązków. Wdrażanie rozporządzenia RODO w państwach członkowskich UE przyniosło jednak szereg obserwacji i doświadczeń, które powinny zachęcać do ponownego przemyślenia niektórych zawartych w nim rozwiązań. Chodzi o to, by system ten był skuteczny, a jednocześnie nie rodził nadmiernej uciążliwości po stronie podmiotów, do których jest adresowany.

W pracy uwzględniono następujące **metody badawcze**:

Jako podstawową metodę badawczą wykorzystałem **metodę instytucjonalno-prawną,** wykorzystaniem której dokonał analizy aktów prawnie wiążących, jak i dokumentów o charakterze „miękkiego prawa", zawierających w swej treści standardy dotyczące bezpieczeństwa danych osobowych.

W pracy ujęta została również **metoda historyczna,** która posłużyła zarówno do przedstawienia genezy Rady Europy jak i Unii Europejskiej, oraz rozwoju bezpieczeństwa danych osobowych w systemach aksjologicznych tychże organizacji międzynarodowych. Stworzyło to możliwość ukazania relacji występujących pomiędzy poszczególnymi systemami.

Przy zastosowaniu **metody analizy systemowej,** możliwe było zaprezentowanie wysiłków RE i UE jako dwóch odrębnych systemów. Stworzyło to warunki do przedstawienia relacji pomiędzy nimi w kontekście bezpieczeństwa danych osobowych.

Badając przykłady oddziaływania Rady Europy i Unii Europejskiej na bezpieczeństwo danych osobowych w państwach członkowskich z wykorzystaniem **metody politologicznej**, analizą objęto piśmiennictwo krajowe, jak i zagraniczne.

Rozdział 1: Ogólna charakterystyka bezpieczeństwa danych osobowych

1.1. Geneza koncepcji bezpieczeństwa danych osobowych

Genezy koncepcji bezpieczeństwa danych osobowych należy upatrywać w szeroko rozumianym prawie do prywatności, o którym wzmianki zawarte były już w prawie starożytnych państw. Szczęście utożsamiano wówczas z poczuciem własności czy też braku zagrożenia. W literaturze powtarza się pogląd, iż współcześnie, w czasach cywilizacji informacyjnej prywatność coraz trudniej jest zachować. Bronić jej ma natomiast prawo o ochronie danych osobowych[79]. Pojawiają się tu jednak coraz to nowsze wyzwania w związku z rozwojem technologii informacyjnych[80].

Ustawodawstwo o ochronie danych osobowych pojawiło się na przełomie lat 60. i 70. XXI w. jako wyraz ówczesnych obaw nie tyle przed gromadzeniem i wykorzystywaniem informacji o osobach (co niewątpliwie czyniono już wcześniej)[81], ile przed użyciem w tym celu komputerów[82]. Komputer nie był wówczas tak „oswojonym" narzędziem pracy jak obecnie. Posługiwała się nim wąska grupa specjalistów, względy techniczne i trudności w obsłudze ograniczały dostępność maszyn cyfrowych (jak je dawniej nazywano). Ograniczenie dostępności i charakter nowości wywołały obawy, a nawet strach przed wszechmocą nowych urządzeń[83].

Erich Fromm pisał wówczas: „*dziś jesteśmy świadkami początków drugiej rewolucji przemysłowej, dla której charakterystyczne jest zastępowanie człowieka przez „myślące" maszyny. Cybernetyka i automatyzacja (komputeryzacja) umożliwiają bowiem budowanie maszyn, które działają szybciej i precyzyjniej niż ludzki mózg, udzielają odpowiedzi na ważne organizacyjne pytania. Komputeryzacja daje możliwość stworzenia nowego rodzaju struktury gospodarczej i społecznej. Stosunkowo niewielka*

[79] M. Krasińska, *Ochrona danych osobowych – prawo a rzeczywistość,* „Gazeta Bankowa" 2007, nr 7, s. 38.
[80] Zob. M. Zubik, J. Podkowik, R. Rybski, *Prywatność. Wolność u progu D-day*, „Gdańskie Studia Prawnicze" 2018, t. XL, s. 391.
[81] Zob. M. Barański, *Informacja w ujęciu prawnym przez pryzmat zagadnień terminologicznych*., Uniwersytet Śląski, Katowice 2017, s. 34.
[82] Zob. A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej,* „Państwo i Prawo" 1997, z. 6, s. 29.
[83] Tamże.

liczba gigantycznych przedsiębiorstw zaczyna stanowić centrum maszyny gospodarczej i w niedalekiej przyszłości będzie nią całkowicie zarządzać". I dalej: „*wszystko wskazuje na to, że społeczeństwem przyszłości będzie odczłowieczone społeczeństwo technotroniczne"*[84].

Od tego czasu w stosunku ludzi do komputerów zaszły jednak duże zmiany. Miały one dwojaki charakter. Przede wszystkim informatyka stała się nieodłącznym elementem naszego życia codziennego, komputer jest dla wielu osób zwykłym narzędziem pracy. Jednocześnie okazało się, iż pierwotne obawy, że komputer pomoże zawładnąć sferą życia prywatnego i intymnego jednostki, były nadmiernie wyolbrzymione[85]. Przyjęte początkowo w wielu ustawach administracyjnoprawne środki ograniczające możliwość przetwarzania danych osobowych (np. konieczność uzyskania zezwolenia na wykorzystywanie takich danych) hamują działalność gospodarczą podmiotów posługujących się informacjami osobowymi, mimo, że w wielu przypadkach działalność taka nie jest żadnym zagrożeniem dla praw jednostki[86]. Z drugiej strony nie neguje się jednak i tego, że szerokie wykorzystanie informacji może nieść pewne zagrożenia dla prywatności człowieka, przez ułatwienie osobom nieupoważnionym dostępu do informacji osobowych i możliwości posługiwania się nimi[87]. W tej sytuacji istotnym sposobem przeciwdziałania występującym tu zagrożeniom miały okazać się standardy prawne postępowania celem uniknięcia zagrożeń[88], zarówno o charakterze krajowym[89], jak i międzynarodowym[90]. Były one niezbędne w sytuacji, gdy wiele instytucji, które weszły w posiadanie danych osobowych różnego rodzaju, wykazywało tendencję do przetrzymywania ich w sposób bezterminowy, bez racjonalnego uzasadnienia[91].

---

[84] E. Fromm, *Rewolucja nadziei,* Wydawnictwo Rebis, Poznań 1996, s. 50 i 56.
[85] Por. A. Adamski, S. Redo, *Globalna wioska i gminna rzeczywistość. Ochrona danych osobowych a rządy prawa,* „Rzeczpospolita" 1996, nr 160.
[86] Por. A. Mrózek, *Ochrona danych osobowych w Szwajcarii,* „OMT" 1984, nr 1, s. 26 – 29.
[87] Zob. A. Mrózek, *Zachodnioniemiecka ustawa o ochronie danych osobowych w procesach automatycznego przetwarzania,* „Studia Prawnicze" 1978, nr 1, s. 175 – 195.
[88] Zob. R.R. Williams, A.A. Chuvakin, D. Milroy (red.), *PCI compliance : understand and implement effective PCI data security standard compliance. Understand and implement effective PCI data security standard compliance*, Syngress, Waltham 2015, s. 87.
[89] Zob. M. Bloom, *Protecting personal data: a model data security and breach notification statute*, "St. John's Law Review", 2018, nr 4, s. 977.
[90] Zob. A.M. Dzięgiel, *Naruszenie dóbr osobistych w Internecie*, „Jurysta" 2017, nr 1, s. 29.
[91] Zob. C. Phua, *Protecting organisations from personal data breaches*, "Computer Fraud & Security", 2009, nr 1, s.13.

Poszukiwanie skutecznej ochrony danych osobowych stało się poważnym wyzwaniem nie tylko w kategoriach prawnych, ale też społecznych, gospodarczych i politycznych. Zaczęły się pojawiać systemy ochronne w poszczególnych krajach, a także standardy międzynarodowe w tym zakresie[92]. Musiały one wszakże uwzględniać fakt, że informacja i dostęp do niej jest wiąże się z istotą demokracji[93], a więc wszelkie ograniczenia w dostępie do niej muszą być szczególnie uzasadnione. Ma to istotne znaczenie w kontekście w kontekście działalności administracji publicznej[94].

Geneza ochrony danych osobowych jest łączona z kształtowaniem się prawa do prywatności. Stąd początek prawnej ochrony danych osobowych w obrocie międzynarodowym datuje się na 1948 rok. Przyjęto wówczas Powszechną Deklarację Praw Człowieka, która w art. 12 odwołuje się do zakazu samowolnego ingerowania w cudze życie prywatne, domowe, rodzinne i korespondencję. W podobny sposób do prawa do prywatności odnosi się Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966 r., który w przeciwieństwie do Deklaracji jest wiążącą strony umową międzynarodową. W systemie ONZ problematykę ochrony danych osobowych poruszyła rezolucja 34/169 przyjęta przez Zgromadzenie Ogólne ONZ w 1979 r. – Kodeks postępowania funkcjonariuszy porządku prawnego, nakazujący zapewnienie szczególnej ochrony posiadanym przez funkcjonariuszy poufnym informacjom. Prawo do poszanowania życia prywatnego przewiduje również art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 r. przyjętej przez wszystkie państwa będące członkami Rady Europy.
Za pierwszą na świecie całościową regulację w dziedzinie dotyczącej *stricte* ochrony danych osobowych uznaje się *Datenschutzgesetz* – ustawę przyjętą w 1970 r. w Niemczech przez Hesję, której zakres oddziaływania ograniczony był tylko do tego landu. Natomiast w 1974 r. w USA uchwalono *Privacy Act*, który miał zasięg ogólnopaństwowy, ale podmiotowo zawężony do przetwarzania danych przez

[92] Por. *Privacy and data protection seals*, red. R. Rodrigues, V. Papakonstantinou, T,M.C. Asser Press, The Hague 2018.
[93] Zob. K. Celarek, *Informacja istotą demokracji - szczególna rola administracji publicznej w procesie urzeczywistniania Prawa informacyjnego*, [w:] *Stulecie polskiej administracji. Doświadczenia i perspektywy*, red. W. Federczyk, Krajowa Szkoła Administracji Publicznej, Warszawa 2018, s. 37.
[94] Por. *Bezpieczeństwo informacji w administracji publicznej*, red. D. Fleszer, Wyższa Szkoła Humanitas, Sosnowiec 2017.

amerykańskie agencje federalne[95]. Ochronę danych osobowych uregulowała szwedzka ustawa z 1973 r.[96]

U źródeł potrzeby ochrony danych osobowych był – jak się wydaje – rozwój gospodarczy i związany z tym przepływ danych między państwami oraz jednostkami gospodarczymi[97]. Jak wskazuje J. Sobczak, co najmniej od zakończenia II wojny światowej zaobserwowano poszerzanie się zakresu zbierania przez rozmaite organy i instytucje publiczne, a nieco później także prywatne, informacji odnoszących się zarówno do rozmaitych podmiotów życia gospodarczego i społecznego, jak i poszczególnych obywateli[98]. Na tym tle formułowano szereg pytań szczegółowych – np. czy związki religijne i wyznaniowe maja prawo żądania od kandydatów na ich pracowników informacji o ich wyzwaniu i religii[99].

Początkowo zbieranie tego typu danych uzasadniano w aspekcie politycznym potrzebami bezpieczeństwa, początkowo tylko wewnętrznego[100], a stopniowo waz z pojawieniem się zjawiska terroryzmu międzynarodowego, nasileniem szpiegostwa przemysłowego także bezpieczeństwa międzynarodowego[101].

Wraz z upowszechnieniem stosowania komputerów pojawiły się nowe możliwości zbierania, zapisywania, przetwarzania i udostępniania danych osobowych[102]. Dotyczyło to coraz innych nośników informacji[103]. Sama informacja stopniowo stawała się

---

[95] Zob. E. Roguska, *Systemy ochrony danych osobowych w Unii Europejskiej i Stanach Zjednoczonych*, źródło: https://www.temidium.pl/artykul/systemy_ochrony_danych_osobowych_w_unii_europejskiej_i_stanach_zjednoczonych-5398.html, data dostępu: 26.12.2020.

[96] Zob. J. Sobczak, *Ochrona danych osobowych – standardy unijne i rzeczywistość polska,* [w:] *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka,* red. J. Jaskiernia, t. 2, Wydawnictwo Sejmowe, Warszawa 2013, s. 481.

[97] Zob. G. Gonzalez Fuster, *Security and the future of personal data protection in the European Union,* "Security and Human Rights" 2013, vol. 23, s. 331-342.

[98] Zob. J. Sobczak, *Ochrona danych…,* jw.

[99] Zob. O. Kucharski, P. Wolnicki, *Prawo kościołów i innych związków wyznaniowych do żądania od kandydata na pracownika danych osobowych o jego wyznaniu lub religii*, Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019, nr 2, s. 121.

[100] Por. J. Borecka, *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych,* „Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie" 2006, z. IV, s. 5.

[101] Zob. A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem,* Oficyna a Wolters Kluwer business, Warszawa 2010, s. 272.

[102] Por. G.F. Gonzalez, S. Gutwirth, *Opening up personal data Protection: A conceptual controversy,* "Computer Law & Security Review: The International Journal of Technology Law and Practice" 2013, vol. 29, s. 531-539.

[103] Zob. J. Bronfman, *I'm ready for my close-up, Mr. Spielberg: creating a working model for data security and personal privacy in the use case of unmanned aerial systems in film and video game productions*, "Whittier Law Review", 2018, nr 2, s. 25.

towarem o istotnej, stale zwiększającej się wartości gospodarczej[104]. Istotnym czynnikiem stało się to, z wiele międzynarodowych przedsiębiorstw przeszło na system działalności on-line, co w sposób znaczący podniosło wartość informacji o potencjalnych odbiorcach towarów i dóbr[105]. Jednocześnie konstatowano coraz większe trudności sprawowania przez jednostkę kontroli zarówno treści informacji jej dotyczącej, jak i obiegu takich informacji[106], co skutkowało ograniczeniem szans do samookreślenia informacyjnej autoprezentacji[107], godząc w „prawo do wizerunku własnego życia" i zniechęcając do aktywnego udziału w życiu społecznym[108]. Istotne zagrożenia dla ochrony danych osobowych pojawiły się m.in. w obszarze służby zdrowia, w kontekście dostępu do informacji poufnych dotyczących zdrowia pacjentów[109]. Mnożyły się przypadki naruszania tajemnicy danych osobowych także w innych dziedzinach, zwłaszcza w sferze biznesu[110]. Wymuszało to poszukiwanie bardziej wyrafinowanych rozwiązań, które mogłyby bardziej skutecznie chronić dane osobowe[111].

Odnotować tez należy, że pojawiły się bariery prawne cyfrowych kanałów dystrybucji, obserwowane m.in. w działalności ubezpieczeniowej[112].

Widoczna ewolucja nastąpiła w latach 80. i 90. XX w. kiedy to zaczęto tworzyć rozwiązania prawne oraz techniczne służące implementacji procedur bezpiecznego przetwarzania danych osobowych, w taki sposób, aby nie utrudniać działalności instytucji, w szczególności tych biznesowych[113]. Pełnym dopełnieniem tych działań stała się Dyrektywa 95/46/WE/ Parlamentu Europejskiego i Rady z dnia 24

[104] Zob. E. Tran, M. Atkinson, *Security of personal data across national borders,* "Information Management & Computer Security" 2002, Vol. 10, s. 237-241.
[105] Tamże.
[106] Zob. E. Schultz, *Security views: security breaches threaten personal and financial data*, "Computers & Security", 2004, nr 4, s. 269.
[107] Zob. K. Ceglarek, *Ochrona danych osobowych a rozwój społeczeństwa informacyjnego,* „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2012, nr 88, s. 721.
[108] Tamże.
[109] Zob. A.Y. Zalozhnev, D.A. Andros, V.N. Ginz, A.E. Loktionov, *Information Systems and Network Technologies for Personal Data Cyber Security in Public Health*, [w:] 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019, s. 3.
[110] Zob. F. Feri, N. Jenzsch, *Disclosure oJ personal information under risk of privacy shocks*, "Journal of Economic Behavior & Organization", 2016, vol. 123, s. 138.
[111] Por. *Security with Intelligent Computing and Big-data Services*, red. S.-L. Peng, S.-J. Wang, V.E. Balas, M. Zho, Springer International Publishing, Cham 2018.
[112] Zob. P. Wrzesiński, *Bariery prawne rozwoju cyfrowych kanałów dystrybucji w działalności zakładów ubezpieczeń w Polsce*, „Prawo Asekuracyjne" 2019, nr 2, s. 127.
[113] Zob. *Historia danych osobowych,* źródło: www.ochronainformacji.com.pl/historia-danych-osobowych, data dostępu: 26.06.2018.

października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[114].

W literaturze zwraca się uwagę, że utworzone przepisy chroniące dane osobowe – z jednej strony – zaczęły pełnić funkcję instrumentu stojącego na straży uznanych powszechnie praw i wolności, z drugiej zaś, ich zadaniem stała się ochrona użytkowników najnowszych technologii informatycznych[115] i interesów oraz zapewnienie niezbędnego do ich działań zaufania i bezpieczeństwa[116]. Wiązało się to M.in. z kwestią uzyskiwania przez osoby prywatne danych telekomunikacyjnych i internetowych[117].

Na przestrzeni lat zaczęto także dążyć do równowagi między ochroną danych osobowych, co należy wiązać z ochroną prywatności, a ich przetwarzaniem, które okazało się konieczne w warunkach funkcjonowania wspólnego rynku. Dlatego również pojawiła się potrzeba przyjęcia odpowiednich regulacji na poziomie wspólnotowym, które zostały najpierw ujęte w ww. dyrektywie 95/46/WE[118].

1.2. **Rozumienie pojęcia „bezpieczeństwo danych osobowych”**

Bezpieczeństwo zawsze miało kluczowe znaczenie dla ochrony poufności, integralności i dostępności danych osobowych. By jednak zrozumieć pojęcie „bezpieczeństwo danych osobowych” należy odnieść się do prawa do prywatności przysługującego każdemu obywatelowi[119]. Jak bowiem zauważa M. Jagielski, podstawowym celem (wartością) przyświecającą ochronie danych osobowych jest ochrona prywatności jednostki[120].Cel ten jednoznacznie określają zarówno akty

[114] Dz.U. L 281 z 23.11.1995, s. 31.
[115] Zob. O. Szumski, *Ochrona danych osobowych w społeczeństwie informacyjnym,* „Acta Universitatis. Lodziensis. Folia Oeconomia” 2007, t. 2, s. 187-197.
[116] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz,* Kraków 2004, s. 52.
[117] Zob. A. Lach, *Uzyskiwanie przez osoby prywatne danych telekomunikacyjnych oraz danych internetowych*, „Państwo i Prawo” 2018, nr 6, s. 66.
[118] Por. J. Maliszewska-Nienartowicz, *Ochrona danych osobowych,* „Prawo i Podatki Unii Europejskiej w Praktyce” 2006, nr 10, s. 18-24.
[119] Por. J. Braciak, *Prawo do prywatności,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2002, s. 278.
[120] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie,* Oficyna a Wolters Kluwer business, Warszawa 2010, s. 21.

międzynarodowe[121] i europejskie wyznaczające standardy ochrony danych[122], jak też akty prawa wewnętrznego[123].

Prawo do prywatności (ochrony informacji o życiu prywatnym), rozumiane jest jako prawo do swobodnego rozwoju i nieskrępowanego spełnienia swojej osobowości[124], stanowi jedną z fundamentalnych i powszechnie uznawanych zasad każdego demokratycznego państwa. Nic bowiem nie zasługuje na większą ochronę prawną niż prawo każdego człowieka do zachowania swoich praw tylko dla siebie i samodzielnego decydowania, w jakim zakresie będzie oglądem publicznej obserwacji. Przyczyny tej szczególnej roli prawa do prywatności każdego człowieka są powszechnie znane. Bezpieczeństwo informacji o życiu prywatnym jest bowiem ściśle związane z pojęciem interesu własnego jednostki, jej dobra oraz z aktywnością podejmowaną przez jednostkę na rzecz ochrony tego dobra[125], a za jej źródło należy uznać godność ludzką – przyrodzoną i niezbywalną[126]. Ponadto inne, zarówno normatywne jak i prawnonaturalne wolności i prawa człowieka, jak choćby zapewnienie każdemu obywatelowi świadomego i czynnego udziału w realizacji władzy państwowej, czy wolności wyboru – nie mogą zostać zrealizowane bez zagwarantowania jednostce prawa do ochrony informacji o życiu prywatnym. Tak więc, bez gwarancji realizacji prawa do prywatności, jako dobra autonomicznego (to znaczy nie wymagającego odwoływania się do innych dóbr prawnie chronionych ani innych celów, którym prawo to służy), nie można mówić o istnieniu demokratycznego państwa prawnego[127].

[121] Por. J. Goerick, *Współpraca międzynarodowa organów ochrony danych osobowych państw członkowskich Unii Europejskiej przed wejściem w życie ogólnego rozporządzenia o ochronie danych,* „Przegląd Naukowy. Disputio" 2017, nr 2, s. 19-28.
[122] Zob. A. Gonschior, *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej,* [w:] *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego. Aspekty teoretyczne i praktyczne,* red. D. Kornobis-Romanowska, Uniwersytet Wrocławski, Wrocław 2017, s. 239-287.
[123] Zob. A. Romkowski, *Przepisy karne ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. w kontekście standardów ochrony danych osobowych w rozporządzeniu GOPR (RODO) z dnia 27 kwietnia 2016 r.,* „Przegląd Prawno – Ekonomiczny" 2018, nr 1, s. 268-306.
[124] Zob. P. Hofmański, *Prawo do poszanowania prywatności (art. 17 Paktu i art. 8 Europejskiej Konwencji Praw Człowieka), a rozwiązania polskiego prawa karnego materialnego i procesowego* [w:] *Standardy praw człowieka a polskie prawo karne,* red. J. Skupiński, Warszawa 1995, s. 253.
[125] Por. J. Thomson, *The Right to Privacy,* "Philosophy and Public Affairs" 1975, t. 4, s. 308.
[126] Zob. R. Pelewicz, *Ujawnianie danych osobowych zarejestrowanych w systemie dozoru elektronicznego w kontekście konstytucyjnych i międzynarodowych gwaranci ochrony życia prywatnego,* [w:] *Efektywność europejskiego systemu ochrony praw człowieka. Obszary analizy skuteczności europejskiego systemu ochrony praw człowieka,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2012, s. 433.
[127] Tamże.

Bezpieczeństwo obywatela w społeczeństwie informacyjnym staje się w związku z tym istotnym wyzwaniem regulacyjnym, a także dla praktyki ustrojowej[128].

Akceptując tezę, że prywatność jednostki jest tak doniosła, a z punktu widzenia społecznego, tak dalece podstawowa, to zagwarantowanie jej skuteczności wymaga szeroko zakreślonych gwarancji należytego funkcjonowania. Po pierwsze, dla ochrony społeczeństwa i jednostki przed naruszeniem, po drugie zaś, przed nadużywaniem zagrażającym prawom innych osób[129]. Obok niezbędnych regulacji prawnych niezbędna jest tu wiedza wszystkich użytkowników nowoczesnych technologii informacyjnych w kwestii tego, w jaki sposób można zapewnić poufność, dostępność i integralność informacji, z uwzględnieniem zasad wypracowanych w dziedzinie zarządzania bezpieczeństwem informatycznym[130]. Wiedza ta musi też obejmować sposoby wykorzystywania mediów społecznościowych do upowszechniania fałszywych informacji o osobie (celem np. zdyskredytowania jej w oczach potencjalnych wyborców, czy szantażowania, w związku z posiadanymi przez tę osobę skłonności). Powstają bowiem warunki do podważania dobrego wizerunku, jaki posiadają indywidualne osoby czy organizacje społeczne. Staje się to wówczas potężną bronią wymierzoną przeciwko partom politycznym, organizacjom społecznym czy podmiotom działalności gospodarczej[131].

Poważnym wyzwaniem dla ochrony dóbr osobistych rodzi monitoring wizyjny[132]. Istotne problemu z punktu widzenia prawa do prywatności rodzi też monitorowanie pracownika w miejscu pracy[133].

Jako pierwsi prawo do ochrony danych osobowych, jako element prawa do prywatności opisali amerykańscy prawnicy Samuel D. Warren i Louis D. Brandeis. Zgodnie z ich poglądami prawo to ma charakter autonomicznej wartości, której funkcją

[128] Zob. M. Kontapka, *Bezpieczeństwo obywatela w społeczeństwie informacyjnym - casus profilowania w sieciach handlowych*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Warszawa-Siedlce 2018, s. 11.

[129] Zob. K. Motyka, *Prawo do prywatności,* „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach Seria: Administracja i Zarządzanie" 2010, nr 85, s. 9-35.

[130] Zob. R. Schifreen, *Data Protection and Security for Personal Computers: A Manager's Guide to Improving the Confidentiality, Availability and Integrity of Data on Personal Computers and Local Area Networks*, Elsevier Science & Technology, Kent 1992, s. 34.

[131] Zob. P.B. Lambert, *Security of Personal Data*, [w:] *Essential Introduction to Understanding European Data Protection Rules*, CRS Press, Boca Raton 2018, s. 271.

[132] Zob. G. Tylec, *Monitoring wizyjny jako ingerencja w sferę dóbr osobistych*, „Przegląd Prawno-Ekonomiczny" 2018, nr 2, s. 56.

[133] Zob. D. Kuźnicka, *Monitorowanie pracownika w miejscu pracy a ochrona prywatności*, „Przegląd Prawniczy Uniwersytetu Warszawskiego" 2018, nr 1, s. 53.

jest ochrona „nienaruszalnej osobowości", a także przejawia się ono jako prawo do bycia pozostawionym w spokoju[134]. Z kolei pierwszą powszechną definicję wprost odnoszącą się do ochrony danych osobowych zawarto w Rekomendacji Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z 23 września 1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami, zgodnie z którą: „Dane osobowe oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, która zgodnie z prawem krajowym jest właściwa do rozstrzygania o zawartości i wykorzystaniu danych osobowych, niezależnie od tego, czy takie dane są gromadzone, przechowywane, przetwarzane i rozpowszechniane przez tę stronę, czy przez podmiot w jej imieniu"[135].

Na przestrzeni lat ochrona danych osobowych stała się elementem zarządzania bezpieczeństwem informacji w wielu organizacjach, firmach itp.[136] Informacje stały się bowiem ważnym elementem w strategii organizacji biznesowych[137]. Dlatego też ważnym aspektem stała się jej administracja[138]. Zdaniem M. Gołdy – Sobczak, przetwarzanie danych osobowych oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak. np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie[139].

Na tym tle powstaje szereg problemów prawnych. Ważnym problemem jest odpowiednie zabezpieczenie danych biometrycznych klientów banków[140]. Istotnym wyzwaniem jest odpowiednie zabezpieczenie danych osobowych w kancelarii

[134] Zob. S.D. Warren, L.D. Brandeis, *The Right to Privacy,* "Harvard Law Review" 1890, vol. 4, s. 193.
[135] Recommendation of the Council concerning guidelines governing the Protection of privacy and transborder flows of personal data, OECD 23 September 1980.
[136] Por. J. Łuczak, *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji,* „Studia Oeconomia Posnaniensia" 2016, nr 12, s. 57-73; K. Tor, *Wybrane zagadnienia prawnej ochrony danych osobowych w działalności przedsiębiorstwa,* „Zeszyty Naukowe/Akademia Ekonomiczna w Krakowie" 2004, nr 657, s. 89-105.
[137] Zob. K.M. Siegel, *Protecting the most valuable corporate asset: electronic data, identity theft, personal information, and the role of data security in the information age*, "Penn State law review", 2007, nr 3, s. 779.
[138] Zob. J. Niczyporuk, *Administracja ochrony danych osobowych,* „Zeszyty Naukowe/Wyższa Szkoła Informatyki i Zarządzania" 1999, nr 1, s. 29-35.
[139] Zob. M. Gołda-Sobczak, *Unia Europejska wobec potrzeby ochrony danych osobowych,* [w:] *Europejski system ochrony praw człowieka. Aksjologia-instytucje-efektywność,* red. J. Jaskiernia, t. III, Wydawnictwo Adam Marszałek, Toruń 2015, s. 155.

adwokackiej, radcowskiej, notarialnej czy komorniczej[141]. Istotny jest też problem zgody pracownika na przetwarzanie jego danych osobowych[142]. Chodzi tu również o dane biometryczne[143].

Szczególne znaczenie ma bezpieczeństwo osobowe w systemie ochrony informacji niejawnych[144]. Dotyczy to m.in. działalności organów siłowych, np. Ministerstwa Obrony Narodowej[145].

Powstają też różne szczegółowe problemy w zakresie przechowywania danych osobowych. Dotyczą one np. zasad przetwarzania danych osobowych byłych wyznawców przez kościoły i inne związki wyznaniowe[146].

Za „zbiór danych" uważa się natomiast każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, scentralizowanych, zdecentralizowanych lub rozproszonych funkcjonalnie lub geograficznie. „Administratora danych" definiuje się jako osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych. Jeżeli cele i sposoby przetwarzania danych są określone w przepisach ustawowych i wykonawczych lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe[147]. W rozumieniu Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady „przetwarzający" oznacza osobę fizyczną lub prawną, władzę publiczną, agencje lub inny organ przetwarzający dane osobowe w imieniu administratora danych[148].

---

[140] Zob. S. Cegiełko, *Kultura użytkowa zabezpieczeń biometrycznych klientów banków w Polsce na podstawie sondażu internetowego*, „Bezpieczny Bank" 2018, t. 72, nr 3, s. 164.

[141] Por. *Bezpieczeństwo danych i IT w kancelarii prawnej, radcowskiej, adwokackiej, notarialnej, komorniczej czyli jak bezpiecznie przechowywać dane w kancelarii prawnej*, red. D. Szostek, Warszawa 2018.

[142] Zob. M. Bąba, *Zasada proporcjonalności (adekwatności) a zgoda pracownika na przetwarzanie danych osobowych*, „Praca i Zabezpieczenie Społeczne" 2018, nr 2, s. 19.

[143] Zob. M. Bąba, *Zgoda pracownika jako podstawa legalizująca gromadzenie przez pracodawcę danych biometrycznych pracownika*, „Praca i Zabezpieczenie Społeczne" 2018, nr 1, s. 25.

[144] Zob. M. Karpiuk, *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*., „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, t. 40, nr 1, s. 85.

[145] Zob. R. Kawka, *Kontrola ochrony informacji niejawnych w jednostkach organizacyjnych MON*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski. Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Warszawa - Siedlce 2018, s. 79.

[146] Zob. K. Dyrda, *Prawo i obowiązek przetwarzania danych osobowych byłych wyznawców przez kościoły i inne związki wyznaniowe*, „Studia z Prawa Wyznaniowego" 2018, t. 21, s. 369.

[147] Zob. M. Gołda-Sobczak, *Unia…*, s. 155-156.

[148] Dz.U. L 281 z 23.11.1995. Por. T. Kirkham, S. Winfield, S. Ravet, S. Kellomaki, "IEEE Security & Privacy", 2013, nr 5, s.12.

Za „osobę trzecią" uważa się osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędącym osobom, której dane dotyczą, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego upoważnione są do przetwarzania danych. „Odbierającym dane" jest osoba fizyczna lub prawna, władza publiczna, alegacja lub inny organ, któremu ujawniane są dane, będący lub niebędącym osobą trzecią. Jednakże władze, które mogą otrzymywać dane w ramach konkretnego dochodzenia, nie są uważane za odbiorcę. Przez „zgodę osoby, której dotyczą" rozumie się konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych[149].

Rozumienie bezpieczeństwa danych osobowych ulega ciągłej ewolucji wraz z rozwojem nowych technologii, czy też portali społecznościowych. Bowiem jak zauważa L. Bogucka analizując rolę Facebooka dokonał on „rewolucji w kontaktach interpersonalnych, a posiadanie profilu na tym portalu społecznościowym jest już kwestią powszechnie przyjętą w społeczeństwie", dlatego zasadnicze znaczenia ma również bezpieczeństwo danych osobowych na nim przetwarzanych[150].

Bezpieczeństwo danych osobowych obejmujące dziś wiele różnych systemów[151], należy zatem rozumieć je jako wymóg współczesnych czasów dla bezpieczniejszej przyszłości prawa do prywatności każdego z obywateli. Jednak należy też zaznaczyć, iż bezpieczeństwo to nie polega jedynie na zastosowaniu jednego lub więcej środków, a sam środek bezpieczeństwa nie może zapewnić odpowiedniego poziomu ochrony danych osobowych. Wręcz przeciwnie, bezpieczeństwo danych osobowych musi

[149] Wykładnię pojęcia "zgoda" zawiera Opinia Grupy Roboczej z dnia 13 lipca 2011 r. 01197/11/EN,WP187.

[150] L. Bogucka, *Bezpieczeństwo danych osobowych w świecie Facebooka,* „Zarządzanie Innowacyjne w Gospodarce i Biznesie" 2017, nr 1, s. 23.

[151] Zob. J. Bajorek, *Ochrona i bezpieczeństwo danych osobowych w organizacji,* „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2016, nr 1, s. 40-50; J. Czerniński, *Bezpieczeństwo danych osobowych w aplikacjach umieszczonych w „chmurze",* „Logistyka" 2015, nr 3, s. 871-880; G. Wojarnik, *Bezpieczeństwo przetwarzania danych w modelu cloud computing: uwarunkowania w kontekście ochrony danych osobowych w warunkach prawa polskiego,* „Zeszyty Naukowe. Studia Informatica/Uniwersytet Szczeciński" 2013, nr 33, s. 167-179; W. Wolny, B. Sadecki, *Bezpieczeństwo danych w systemach ERP,* „Prace Naukowe/Akademia Ekonomiczna w Katowicach" 2009, t. 1, s. 257-269; B. Domańska-Szaruga D. Prokopowicz, *Ochrona transferu danych osobowych w cyberprzestrzeni,* „SECRETUM. Służby Specjalne, Bezpieczeństwo i Informacja" 2016, nr 2, s. 122-136; M. Kunasiewicz, *Wybrane aspekty ochrony danych osobowych w systemach informatycznych,* „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2002, nr 955, s. 248-257; K. Szymczyk-Madej, J. Madej, *Bezpieczeństwo informatycznych systemów rachunkowości,* „Zeszyty Naukowe/Akademia Ekonomiczna w Krakowie" 2000, nr 553, s. 161-177.

podlegać dokładnym i stale monitorowanym ramom kontroli, zarówno technicznym, jak i organizacyjnym, dostosowanym do charakteru przetwarzania danych i związanego z nimi ryzyka.

Istotne problemy prawne powstają na tle ochrony informacji telekomunikacyjnej w kontekście analizy NAT jako identyfikacji sprawców[152]. Jest to szerszy problem związane z bezpieczeństwem urządzeń mobilnych w przestrzeni cyfrowej[153].

W świetle ocen formułowanych w Stanach Zjednoczonych, zapewnienie bezpieczeństwa danych staje się jednym z najważniejszych wyzwań dla korporacji międzynarodowych, ale też dla całej polityki publicznej. Dlatego też np. emitenci kart kredytowych wprowadzają tu całe wyrafinowane systemy zabezpieczeń, a czuwa nad tym organ samoregulacji w postaci the Payment Card Industry Security Standards Council. Zwalcza on cyberprzestępczość, a także oferuje standardy postępowania, wypracowane drogą porównania istniejących w tej dziedzinie rozwiązań[154].

Sposoby zagwarantowania bezpieczeństwa informacyjnego mogą się przy tym różnić, a zależne jest to od dziedziny, w której zarządzanie danymi osobowymi ma miejsce[155]. Szczególną specyfiką wyróżnia się tu medycyna, gdyż dostęp do informacji poufnych o ludziach chorujących stanowi cenną wiedzę dla różnych podmiotów (np. firm farmaceutycznych) w zakresie profilowania informacji przesyłanych do poszczególnych osób, charakteryzujących się określonymi dolegliwościami i stanami chorobowymi. Zachęca to do kradzieży danych lub do manipulowania nimi. Istotnym sposobem przeciwdziałania takim patologicznym praktykom staje się w tej sytuacji zastosowanie odpowiedniego typu zabezpieczeń przez administratorów danych osobowych, zgodnych ze standardami krajowymi i międzynarodowymi[156].

[152] Zob. M. Czosnek, G. Piaskowski, *Tajemnica telekomunikacyjna. Analiza NAT jako narzędzie do identyfikacji sprawców*, „Przegląd Policyjny" 2018, nr 4, s. 218.
[153] Zob. H. Świeboda, P. Stobiecki, *Bezpieczeństwo urządzeń mobilnych w przestrzeni cyfrowej*, „Przegląd Policyjny" 2018, nr 4, s. 27.
[154] Zob. T.A. Hemphil, P. Longstreet, *Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards*, "Technology in Society, 2016, vol. 44, s. 30.
[155] Zob. R. Wolters, L. Trakman, B. Zeller, *Personal Data and Cybersecurity*, "Data Protection Law", 5 September 2019, s. 375.
[156] Zob. A. Soluamni, A. Alti, L. Laouamer, *A Blind Image Watermarking Method for Personal Medical Data Security*, [w:] 2019 International Conference on Networking and Advanced Systems (ICNAS),2019, s. 3.

1.3. **Bezpieczeństwo danych osobowych a inne typy bezpieczeństwa**

Bezpieczeństwo danych osobowych przenika do różnych płaszczyzn, tj. militarnej, energetycznej, socjalnej, informatycznej, politycznej oraz demokratycznej. Bowiem w każdej z nich ujawniane są dane, które umożliwiają osiąganie określonych celów, ale również wiąże się to z licznymi zagrożeniami wpływającymi na ich bezpieczeństwo. O kompleksowym charakterze występujących tu zjawisk świadczą np. problemy związane z potrzebą jednoczesnego zapewnienia zdrowia publicznego i ochrony danych osobowych, stosownie do oczekiwań społecznych[157]. Dlatego warto podjąć analizę bezpieczeństwa danych osobowych w przełożeniu na inne typy bezpieczeństwa.

1.3.1. Bezpieczeństwo militarne

Tworzenie krajowych systemów ochrony danych osobowych obywateli świadczy o tym, iż zagadnienie to jest ważne w kontekście bezpieczeństwa państw. Intensywne prace nad zapewnieniem odpowiedniego poziomu ochrony danych osobowych w wielu z nich, ale także na poziomie organizacji międzynarodowych wiązane są z bezpieczeństwem narodowym. Dlatego ochrona danych osobowych dotyczy także płaszczyzny militarnej.

Ewolucja nowych zagrożeń w sferze militarnej wymusza na państwach działania, które skupione są już nie tylko na klasycznych zagrożeniach[158], ale również na tych nowo powstałych, związanych z rozwojem nowoczesnych technologii[159]. Zatem zmienność zagrożeń warunkuje powstawanie szeregu narzędzi służących ich eliminacji w różnych wymiarach bezpieczeństwa państwa a także w skupieniu na nowych elementach tj. na ochronie przetwarzanych danych o ważnym znaczeniu dla funkcjonowania państwa na arenie międzynarodowej[160].

---

[157] Zob. E. Biliri, B. Kokkinakos, A. Michailitsi, D. Papaspyror, J. Tsapelas, S. Mouzakitis, S. Koussouris, Y. Glickaman, F. Kirstein, *Big data analytics in public safety and personal security: Challenges and potential*, [w:] 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), 2017, s. 1382.

[158]Por. S. Jaczyński, *Bezpieczeństwo militarne II Rzeczypospolitej: aspekty wewnętrzne,* „Doctrina. Studia Społeczno-Polityczne" 2016, nr 13, s. 61-74.

[159] Por. W. Furmanek, *Zagrożenia wynikające z rozwoju technologii informacyjnych,* „Dydaktyka Informatyki" 2014, nr 9, s. 20-48.

[160] Zob. M. Trombski, B. Kosowski, *Współczesny wymiar bezpieczeństwa w aspekcie zmienności zagrożeń,* Wyższa Szkoła Zarządzania Ochroną Pracy, Katowice 2010, s. 20.

Militarny wymiar bezpieczeństwa w dobie współczesnej wiązać zatem należy nie tylko z zagrożeniami związanymi wyścigiem zbrojeń[161], ale również z zagrożeniami pozamilitarnymi. Zagrożenia te występują w szczególności w cyberprzestrzeni, gdzie zastosowanie nowoczesnych metod informatycznych może wywoływać określone konsekwencje w systemach obronnych państw, np. gdy dochodzi do hakerskich ataków na systemy bezpieczeństwa w odniesieniu do systemów nuklearnych[162].

Do obszarów zagrożeń w tym zakresie należy zaliczyć zjawisko fal migracyjnych, które mogą nieść zagrożenie bezpieczeństwa zarówno dla poszczególnych państw, jak i całych regionów[163].

W dobie zagrożenia terroryzmem ochrona danych osobowych włączona została jako element przeciwdziałania temu zjawisku. Zostało to wyrażone m.in. w Decyzji Ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[164] w której art. 22 ust. 1 czytamy, iż: „Państwa członkowskie określają, że właściwe organy muszą wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed ich przypadkowym lub nielegalnym zniszczeniem, przypadkową utratą, modyfikacją, nieuprawnionych ujawnieniem lub dostępem do nich – w szczególności gdy przetwarzanie wiąże się z przekazywaniem danych za pomocą sieci lub z udostępnianiem ich przez udzielenie bezpośredniego zautomatyzowanego dostępu do nich – oraz przed wszelkimi innymi niedozwolonymi formami przetwarzania; należy przy tym uwzględnić zwłaszcza ryzyko wiążące się z przetwarzaniem i charakterem danych podlegających ochronie. Biorąc pod uwagę rozwój techniki i koszty ich wdrożenia, środki takie muszą zapewnić poziom bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem i charakterem danych podlegających ochronie”[165].

Nie dziwi zatem fakt, iż walka z terroryzmem międzynarodowym stając się pilnym i niezmiernie ważnym działaniem ze względu na złożoność tego zjawiska oraz ze względu na jej przenikanie do różnych dziedzin życia jednostek, i wykorzystywanie

[161] Zob. K. Zeidler, *W sprawie genezy, dynamiki i charakterystyki współczesnych konfliktów zbrojnych,* „Międzynarodowe Prawo Humanitarne” 2010, t. 1, s. 15.
[162] Zob. A.A. Tsirigotis, *Cybernetics, Warfare and Discourse The Cybernetisation of Warfare in Britain*, Springer International Publishing, Cham 2017, s. 44.
[163] Por. *Security/Mobility Politics of Movement*, red. S. Wittendorp, M. Leese, Manchester University Press, Manchester 2017.
[164] Dz.Urz.UE L 350/60, 30.12.2008.
[165] Tamże.

przeróżnych mechanizmów, zrodziła potrzebę skupienia szczególniejszej uwagi na danych osobowych, których „kradzież" a następnie nieodpowiednie użycie może wiązać się z zasadniczymi konsekwencjami dla bezpieczeństwa militarnego danego państwa.

1.3.2. Bezpieczeństwo energetyczne

W literaturze wskazuje się, iż jednym z elementów prawa obywateli do odpowiedniego poziomu życia jest konieczność zapewnienia tymże obywatelom przez państwo dostaw nośników energii w celu zabezpieczenia paliw płynnych i lotnych wykorzystywanych zarówno w gospodarstwach domowych, jak i przemyśle dóbr konsumpcyjnych. Co więcej poziomy te warunkują posiadanie przez obywateli poczucia bezpieczeństwa, które wyraża się także indywidualnym bezpieczeństwem energetycznym[166].

Bezpieczeństwo energetyczne ma charakter wieloaspektowy i obejmuje uwarunkowania polityczne, ekonomiczne i ekologiczne[167]. Politykę energetyczną często analizuje się jako część składową bezpieczeństwa ekonomicznego państwa. Bezpieczeństwo ekonomiczne należy rozumieć jako stan, w którym gospodarka danego państwa ma zapewnioną niezbędną dla jej funkcjonowania i rozwoju podaż czynników produkcji[168], w tym wystarczalność energetyczną[169]. Elementem bezpieczeństwa ekonomicznego jest bezpieczeństwo surowcowe, żywnościowe, finansowe oraz wiele innych[170]. W aspekcie gospodarczym polityka energetyczna dotyczy głównie kosztów uzyskania energii oraz ciągłość dostaw. Energia jest specyficznym produktem, ponieważ musi być dostępna w sposób ciągły, również w sytuacji kryzysów

[166] Zob. W. Konaszczuk, *Realizacja przez państwo modelu bezpieczeństwa energetycznego jako prawa obywateli do odpowiedniego poziomu życia,* [w:] *Uniwersalny system ochrony praw człowieka. Aksjologia – instytucje – efektywność,* red. J. Jaskiernia, tom I, Wydawnictwo Adam Marszałek, Toruń 2015, s. 383.
[167] Por. R. Bielaszka, *Kształtowanie polskich rozwiązań prawnych przez Unię Europejską w zakresie efektywności energetycznej,* Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2013, s. 187-200.
[168] Zob. H. Lund, *Choice awareness: the Development of technological and institutional choice in the public debate of Danish energy planning,* "Journal of Environmental Policy and Planning" 2000, Vol. 2, s. 249-259.
[169] Zob. K. Księżopolski, *Wpływ rozszerzenia Unii Europejskiej na bezpieczeństwo ekonomiczne państw Europy Środkowej,* „Stosunki Międzynarodowe" 2006, nr 3/4, s. 128-145.
[170] Zob. A. Lubbe, *Bezpieczeństwo ekonomiczne państwa,* „Sprawy Międzynarodowe" 1997, nr 4, s. 61-78.

politycznych lub ekonomicznych[171]. Brak płynności w dostawach energii wiąże się z wysokimi kosztami dla całej gospodarki oraz wpływa bezpośrednio i pośrednio na jakość życia obywateli. Dlatego też surowce energetyczne traktowane są jako produkt strategiczny[172].

Zasadniczą cechą bezpieczeństwa energetycznego jest to, iż jego kształt w przeważającej mierze zależy od państwa, w którym będzie ono realizowane. Zdaniem J. Rotmansa „*rola rządu w zarządzaniu transformacją energetyki jest wieloraką – facyliatora – stymulatora – kontrolera – reżysera. Jest on odpowiedzialny zarówno za formułowanie i realizowanie celów, jak i za organizację samego procesu zmian i za tworzenie jego warunków granicznych – wszystko za pomocą odpowiednich instrumentów*"[173].

Rząd posiada uprawnienia decyzyjne w kwestii polityki energetycznej państwa, które realizuje poprzez przyjmowanie uchwał i dokumentów określających kierunki i sposoby realizacji polityki energetycznej. Prowadzi również działania w tym obszarze, przy wsparciu wyspecjalizowanych instytucji (np. Ministerstwo Gospodarki, Urząd Regulacji Energetyki (URE)[174].

Polityka energetyczna zakorzeniona jest w sektorze energetycznym[175], na który składa się wiele elementów (podsektorów) stanowiących zbiór przedsiębiorstw energetycznych prowadzących działalność gospodarczą w zakresie wytwarzania, przetwarzania, magazynowania, przesyłania oraz dystrybucji paliw, jak również energii oraz obrotu nimi[176]. Pozostaje ona w bliskiej współzależności z koncepcją długookresowego rozwoju kraju oraz unijnych aspiracji[177].

---

[171] Por. A.J. Nehrebecki, *Wspólna polityka energetyczna Unii Europejskiej,* „Stosunki Międzynarodowe" 2009, nr 3/4, s. 125-145.

[172] Zob. P. Kalita, *Bezpieczeństwo energetyczne jako przesłanka poczucia bezpieczeństwa obywateli (doświadczenia Europy i Afryki),* [w:] *Ochrona praw człowieka w Afryce. Aksjologia – instytucje – nowe wyzwania – praktyka,* red. J. Jaskiernia, K. Spryszak, tom II, Wydawnictwo Adam Marszałek, Toruń 2017, s. 137; Por. T. Szubrycht, *Współczesne aspekty bezpieczeństwa państwa,* „Zeszyty Naukowe Akademii Marynarki Wojennej im. Bohaterów Westerplatte" 2006, nr 4, s. 92.

[173] J. Rotmans, R. Kemp, M. van Asselt, *More Evolution than Revolution: Transition Management in Public Policy,* "Foresight" 2001, No. 1, s. 15-31.

[174] Zob. A. Czech, *Uwarunkowania polskiej polityki energetycznej w kontekście postulatu zrównoważonego rozwoju,* „Studia Ekonomiczne. Zeszyty Naukowe" 2016, nr 269, s. 51.

[175] Por. M.A. Waligórski, *Polityka energetyczna państwa jako sektorowa polityka administracyjna,* „Biuletyn Urzędu Regulacji Energetyki" 2008, nr 4, s. 69-74.

[176] Zob. *Energetyka - charakterystyka podstawowa (autor – zespół),* źródło: www.ure.gov.pl/download.php?s=1&d=710, data dostępu: 16.07.2018.

[177] Zob. A. Dobroczyńska, L. Juchniewicz, *Polityka energetyczna Polski,* „Nowe Życie Gospodarcze" 2003, nr 1, s. 4-9.

Biorąc pod rozwagę istotę polityki energetycznej, w literaturze dokonuje się podziału na kilka sposobów jej postrzegania, tj. politykę administracyjną, a co za tym idzie właściwy dobór celów oraz instrumentów ich realizacji a także licznych uwarunkowań a także politykę gospodarczą. Zdaniem Rejmusa, „to istotne spostrzeżenie, bowiem taka polityka administracyjna obejmuje m.in. działanie Prezesa Urzędu Regulacji Energetyki a zwłaszcza stosowane przez niego metody i środki”[178]. F. Elbanowski sprowadza istotę polityki energetycznej do wymiaru gospodarczego. Jak twierdzi: „polityka energetyczna jest programem gospodarczym, którego realizację stanowią przepisy prawa energetycznego”[179]. Polityka energetyczna funkcjonuje na styku tych polityk.

Politykę energetyczną można ujmować również w zakresie szerszym tj. ogół działań podejmowanych przez organy państwowe, których celem jest efektywny rozwój energetyki. A także ujęciu węższym jako dokument opracowany przez ministra właściwego do spraw energetyki i stanowiący program działania[180].

Istnieje pogląd, iż w bezpieczeństwo energetyczne wpisana jest konieczność kreowania wizji przyszłości tego sektora gospodarki w złożonym środowisku społeczno – gospodarczym[181]. Wynika to niewątpliwie z jego specyfiki. Wielu specjalistów w tej dziedzinie tworzy prognozy oparte na analizie tendencji zachodzących zarówno w energetyce UE, jak i na świecie. Przyczynia się to wprowadzania zmian w podejściu do tych regulacji. Co więcej podejścia te opierają się na zrównoważonej polityce energetycznej opartej na podniesieniu standardu życia przy jednoczesnym zmniejszeniu zapotrzebowania na paliwa kopalne, ograniczeniu poziomu zanieczyszczeń i poszanowaniu posiadanych zasobów[182].

Jedną z innowacyjnych przemian w systemie bezpieczeństwa energetycznego są systemy inteligentnych sieci[183]. W 2011 r. Komisja Europejska w swym komunikacie

[178] Zob. M. Rejmus, *Zadania Prezesa Urzędu Regulacji Energetyki a polityka energetyczna państwa,* „Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza” 2014, nr 3, s. 124.
[179] F. Elżanowski, *Polityka energetyczna. Prawne instrumenty realizacji,* Lexis Nexis, Warszawa 2008, s. 72.
[180] M. Rejmus, *Zadania Prezesa…,* jw., s. 124.
[181] Zob. M. Woszczyk, *Bezpieczeństwo dostaw energii elektrycznej – stan obecny i podstawowe wyzwania,* [w:] *W kierunku nowoczesnej polityki energetycznej. Energia elektryczna,* red. M. Swora, Instytut Obywatelski, Warszawa 2011, s. 23.
[182] Zob. T. Skoczkowski, *Zrównoważona polityka energetyczna,* „Przegląd Komunalny” 2004, nr 3, s. 58-59.
[183] Są to zmodernizowane sieci elektroenergetyczne, uzupełnione o system dwustronnej komunikacji cyfrowej między dostawcą a konsumentem oraz inteligentne systemy pomiarów i monitorowania. Zob. P. Olszowiec, *W kierunku inteligentnych sieci. Innowacje i tendencje dla przyszłych systemów*

COM(2011) 202 – „Inteligentne sieci energetyczne" od innowacji do wdrożenia" jako jedną z potrzeb wskazała „zapewnienie odbiorcom bezpieczeństwa danych"[184]. Zagadnienie to zostało podjęte przez Komisję Europejską również w 2012 r., gdzie przy okazji reaktywowania grupy zadaniowej sieci inteligentnych (ang. *Smart Grid Task Force*, SGTF) powołano zespół ekspertów w obszarze poufności i bezpieczeństwa danych[185].

Wskazuje się, iż z punktu widzenia ochrony danych osobowych odbiorcy w związku z wdrożeniem systemu inteligentnych sieci mogą wystąpić następujące zagrożenia:

- kradzież danych identyfikujących podmiot;
- możliwość określenia i śledzenia indywidualnych zachowań odbiorcy;
- możliwość pozyskiwania informacji o urządzeniach przez niego używanych i sterowania nimi;
- pozyskiwanie informacji umożliwiającej precyzyjną napaść;
- umożliwienie cenzurowania działań odbiorcy;
- możliwość modyfikowania danych odbiorcy[186].

System inteligentnych sieci potrafi precyzyjnie określić indywidualne zachowania odbiorców, co z kolei wiąże się z określonym ryzykiem, bowiem w przypadku stosowania niewłaściwych procedur ochronnych tychże danych na różnych etapach ich pozyskiwania może zaistnieć nieuprawniony dostępem do tych danych oraz ich niewłaściwe wykorzystanie, bez zgody podmiotu je zbierającego oraz przetwarzającego[187].

---

elektroenergetycznych, „Automatyka Elektroenergetyczna" 2010, nr 4, s. 32-36.

[184] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów , Inteligentne sieci energetyczne: od innowacji do wdrożenia, SEK(2011) 463, Komisja Europejska, Bruksela, dnia 12.4.2011, KOM (2011) 202 wersja ostateczna.

[185] R. Czyżewski, A. Babś, K. Madajewski, *Sieci inteligentne – wybrane cele i kierunki działania operatora systemu dystrybucyjnego,* „ActaEnergetica", s. 32, źródło: www.actaenergetica_org.pl, data dostępu: 17.07.2018.

[186] Zob. R. Zajdler, *Ochrona danych osobowych a systemy inteligentnych sieci,* Biuletyn URE, źródło: www.wnp.pl/wiadomosci/ochrona-danych-osobowych-a-systemy-inteligentnych-sieci,-6589_1_0.html, data dostępu: 17.07.2018.

[187] Tamże.

1.3.3. Bezpieczeństwo socjalne

Bezpieczeństwo socjalne odgrywa zasadniczą rolę w prawidłowym funkcjonowaniu obywateli, ze względu na ich potrzeby egzystencjonalne oraz jest fundamentalną wartością każdego z nich[188].

Ze względu na ewolucję zagrożeń w tym obszarze podejmowane są działania na rzecz wypracowania najskuteczniejszych mechanizmów ochronnych[189]. Z tego względu obserwuje się zdeterminowaną konieczność podejmowania przez państwo aktywności socjalnej wszędzie tam, gdzie pojawiają się zagrożenia[190].

Dość często bezpieczeństwo socjalne wiązane jest z bezpieczeństwem społecznym, uznając je za pojęcia tożsame. Jednak w literaturze zwraca się uwagę, że jest to wynik wieloaspektowości bezpieczeństwa socjalnego, braku jednej definicji, czy nawet podejmuje się próby udowodnienia, iż występują sprzeczności między tymi pojęciami[191]. Warto jednak zwrócić uwagę na definicję bezpieczeństwa socjalnego stworzoną w systemie Międzynarodowej Organizacji Pracy zgodnie z którą „bezpieczeństwo socjalne stanowi ochronę dostarczaną przez społeczeństwo swoim członkom poprzez zapobieganie ekonomicznej i społecznej nędzy, która może być powodowana redukcją zarobków, chorobą, macierzyństwem, dyskryminacją w sektorze zatrudnienia, bezrobociem, niepełnosprawnością, podeszłym wiekiem”[192]. Głównym podmiotem zapewniającym elementarne warunki egzystencji jest więc tutaj społeczeństwo, głównie w formie rodziny, pojmowanej jako cała sieć krewnych.

Rozwój cywilizacyjny a w związku z tym powstawanie nowych zagrożeń w tym obszarze doprowadził do wprowadzenia w systemie bezpieczeństwa socjalnego państwa nowego elementu w postaci ochrony danych osobowych. Dla przykładu w Polsce w związku z stosowaniem RODO wymaga się m.in., aby ośrodki pomocy społecznej oraz domy pomocy społecznej, będące w posiadaniu danych osobowych przykładały

[188] Zob. I. Sierpowska, *Bezpieczeństwo socjalne jako dobro publiczne,* „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy” 2015, nr 16, s. 45.
[189] Por. Z. Domański, *Bezpieczeństwo socjalne,* „Journal of Modern Science” 2017, nr 2, s. 367 – 384.
[190] Zob. L. Dziewięcka-Bokun, *Bezpieczeństwo socjalne jako podstawa pokoju społecznego,* „Prace Naukowe/Akademia Ekonomiczna w Katowicach” 2003, tom: Bezpieczeństwo socjalne, s. 11-26.
[191] Szerzej: D. Zalewski, *Bezpieczeństwo społeczne i socjalne – kontrowersje wokół pojęć,* „Polityka Społeczna” 2016, nr 10, s. 7-13.
[192] Zob. A.H.M. Leliveld, *Social Security in Developing Countries. Some Theoretical Considerations,* Vrije Universiteit, Amsterdam 1991, s. 3.

szczególną uwagę do ich ochrony[193]. W związku z tym każdy ośrodek pomocy społecznej i dom pomocy społecznej musi odpowiednio zabezpieczyć przetwarzane dane, tak aby uniemożliwić ich nieuprawnione udostępnienie[194]. Tymże wymogiem objęto niemalże wszystkie obszary działalności jednostek w państwie[195].

Przenikanie wymogu ochrony danych osobowych do obszaru obejmującego bezpieczeństwo socjalne świadczyć może o zasadniczym znaczeniu wprowadzenia tejże ochrony dla zapewnienia w pełni socjalnych gwarancji w celu zaspokojenia potrzeb socjalnych ludzi biorąc pod uwagę ryzyko w postaci niewłaściwego administrowania danymi np. w miejscu zatrudnienia[196] czy też w placówkach pomocy społecznej oraz ochrony zdrowia[197].

1.3.4. Bezpieczeństwo informatyczne

W literaturze podkreśla się, iż bezpieczeństwo informatyczne wiąże się z określonym systemem informatycznym[198], w którym zasadniczą rolę odgrywa zarówno informacja, jak też bazy danych dostępnych za jej pośrednictwem[199]. Na jego kształt ma także wpływ szereg czynników związanych z rozwojem technologicznym, cyberprzestrzenią[200] oraz wszystkimi innymi elementami związanymi z sieciami komputerowymi[201]. Bezpieczeństwo informatyczne można jednak dostrzegać w szerszej skali życia społecznego i politycznego, np. w kontekście zapewnienia ochrony danych, które znajdują się w oficjalnym wystąpieniach (np.) petycjach jednostek czy grup

[193] Zob. *GIODO: instytucje socjalne muszą szczególnie dbać o dane osobowe,* źródło: www.lex.pl/czytaj/-/artykul/giodo-instytucje-socjalne-musza-szczegolnie-dbac-o-dane-osobowe, data dostępu: 17.07.2018.
[194] Zob. P. Glen, *Ochrona danych osobowych w pomocy społecznej. Co musisz wiedzieć?,* www.pomocspoleczna24.pl/nr-1/ochrona-danych-osobowych-w-pomocy-spolecznej-co-musisz-wiedziec-55.html, data dostępu: 17.07.2018.
[195] Por. M. Barański, M. Giermak, *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego, (uwagi na tle ferenda),* „Państwo i Prawo" 2017, nr 10, s. 90-99.
[196] Por. K. Aromińska, *Ochrona danych osobowych w procesie rekrutacji i zatrudnienia,* „Bezpieczeństwo Pracy" 2014, nr 3, s. 19-21.
[197] Zob. A. Wierzbicka, *Ochrona danych osobowych w publicznych zakładach opieki zdrowotnej w Polsce,* „Przedsiębiorczość i Zarządzanie" 2014, z. 9, s. 201-217.
[198] Zob. M. Kozioł, *Bezpieczeństwo informacji i ochrona systemów informatycznych w przedsiębiorstwie,* „Zeszyty Naukowe/Uniwersytet Ekonomiczny w Krakowie" 2009, nr 770, s. 7.
[199] Por. Z. Strzyżakowska, *Bezpieczeństwo i ochrona informacji,* „Pomiary, Automatyka, Kontrola" 2005, nr 4, s. 4-5.
[200] Por. M. Grzelak, K. Lidel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe" 2012, nr 22.
[201] Zob. P. Szymczyk, *Bezpieczeństwo systemów i sieci komputerowych,* „Automatyka/Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie" 2003, z. 1-2, s. 291-300.

obywateli do władz publicznych[202]. Istotną rolę odgrywa tu też świadomość społeczna o stanie zagrożeń dla bezpieczeństwa danych osobowych, jakie niesie posługiwanie nowoczesnymi systemami informatycznymi, a zwłaszcza Internetem[203].

Według J. Łuczaka, jednym z elementów zarządzania bezpieczeństwem informacji jest ochrona danych osobowych. Jak twierdzi, „wymagania realizowane w zakresie ochrony danych osobowych są całkowicie zintegrowane z systemem zarządzania jakością i bezpieczeństwem informacji, co gwarantuje odpowiedzialność jednej osoby bezpośrednio przed zarządem. Kluczowe dokumenty związane z nadzorowaniem danych osobowych to polityka ochrony danych osobowych oraz instrukcja nadzoru nad siecią informatyczną – opracowane w ramach procesu zarządzania jakością i bezpieczeństwem informacji, przy czym istotne jest odwoływanie się w nich do wielu dokumentów systemowych"[204].

W literaturze ochronę danych osobowych i politykę bezpieczeństwa informacji zalicza się także w poczet polityk publicznych[205]. Jak również wskazuje się na kwestie prywatności w dobie cyfrowej zaznaczając wzrost znaczenia ryzyka ujawnienia danych osobowych przez osoby niepowołane do dostępu do określonych informacji poufnych znajdujących się w cyberprzestrzeni, ze szczególnym uwzględnieniem ataków hakerskich i terrorystycznych na sieci teleinformatyczne oraz zagrożenia utraty danych osobowych na portalach społecznościowych[206].

Warto także zaznaczyć, iż przepisy zobowiązują do zapewnienia odpowiedniego poziomu bezpieczeństwa danych osobowych firmę lub instytucję korzystającą systemu, a nie dostawcę oprogramowania. Ochrona danych osobowych w systemie bezpieczeństwa informatycznego to temat coraz częściej poruszany, dostrzegany. Stał się priorytetem, gdyż obowiązek ten wynika z prawa i lista wymogów jest określona w przepisach[207]. Jednakże nadal zagadnieniem złożonym jest kwestia wymogów

[202] Zob. E.N. Polyakova, O.I. Filonova, K.G. Prokofjev, S.A. Sutiagin, *Ensuring the information security of personal data when submitting electronic appeals to the public authorities*, "Journal of physics. Conference series", 2019, vol. 1210, s.121.
[203] Zob. E.Y Yildrim, E. Adali, *The threats and risks in personal data security*, [w:] 2017 International Conference on Computer Science and Engineering (UBMK), 2017, s. 610.
[204] J. Łuczak, *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji,* „Studia Oeconomica Posnaniensia" 2016, no. 12, s. 70.
[205] Zob. Ł. Wojciechowski, *Bezpieczeństwo informacji i ochrona danych osobowych jako polityka publiczna – analiza wprowadzania mechanizmów i uregulowań prawnych,* „Polityka i Społeczeństwo" 2016, nr 4, s. 81-93.
[206] Szerzej: B. Domańska-Szaruga, D. Prokopowicz, *Ochrona transferu danych osobowych w cyberprzestrzeni,* „SECRETUM. Służby specjalne, bezpieczeństwo, informacja" 2016, nr 2, s. 122-136.
[207] Por. W. Wolny, B. Sadecki, *Bezpieczeństwo danych …,* s. 257.

stawianych systemom informatycznym na podstawie RODO. Albowiem wskazać można brak szczegółowych i łatwych do weryfikacji wymogów, jednakże analizując treść rozporządzenia o ochronie danych osobowych można wyłonić szereg przesłanek, z których wnioskować można jaką funkcjonalność będą musiały zapewnić systemy informatyczne na potrzeby RODO. Wymogi te można podzielić na: 1) dotyczące interfejsów systemowych użytkownika końcowego 2) funkcjonalności oprogramowania do przetwarzania danych osobowych; 3) oprogramowania do backupu (zapasowa kopia danych); oraz 4) wymaganego poziomu bezpieczeństwa[208].

1.3.5. Bezpieczeństwo polityczne

Bezpieczeństwo polityczne wiąże się z działalnością polityczną państwa, stabilnością rządów, jak również zdolnością do rozwiązywania problemów zgodnie z opracowaną strategią[209].

Zdaniem L. Chojnowskiego „bezpieczeństwo polityczne podmiotu, w ogólnym rozumieniu, to stan pewności przetrwania, suwerennego funkcjonowania oraz rozwoju jego systemu politycznego a wynika ono z braku zagrożeń politycznych lub posiadania zdolności ochrony przed nimi”[210].

Wraz z rozwojem nowoczesnych organizacji, podmiotów gospodarczych, a przede wszystkim państw i ich armii pojawiło się nowe, niezwykle ważne wyzwanie w postaci stworzenia efektywnego systemu bezpieczeństwa politycznego uwzględniającego ochronę danych osobowych[211].

Podstawowe zasady gromadzenia, przetwarzania i przekazywania informacji niejawnych i danych osobowych stały się gwarantem bezpieczeństwa i obronności państwa oraz ochrony prywatności obywateli[212].

---

[208] J. Staśkiewicz, *Wymogi dla systemów informatycznych w RODO,* źródło: www.opensecurity.pl/wymogi-dla-systemow-informatycznych-rodo/, data dostępu: 17.07.2018.
[209] Zob. S. Zalewski, *Strategia jako instrument bezpieczeństwa politycznego państwa,* „DOCTRINA Studia Społeczno-Polityczne” 2009, nr 6, s. 30.
[210] L. Chojnowski, *Polityczny sektor bezpieczeństwa,* „Zeszyty Naukowe WSOWL” 2012, nr 3, s. 108.
[211] Zob. R. Klimek, *Demokracja czy bezpieczeństwo w sieci. Aspekty społeczno-polityczne bezpieczeństwa informacyjnego w XXI wieku,* „Przegląd Naukowo-Metodyczny „Edukacja dla Bezpieczeństwa” 2012, nr 4, s. 58.
[212] Zob. J. Pliżys, *Zarządzanie ochroną informacji w systemach zarządzania kryzysowego,* „DOCTRINA. Studia Społeczno-Polityczne” 2010, nr 7, s. 131-140.

W aktach wyznaczających standardy ochrony danych osobowych umieszczono cel w postaci ochrony o charakterze polityczno – ustrojowym. Jak bowiem zauważa M. Jagielski, pojawiające się już w aktach z lat 80 – tych generalne odwołania do praw człowieka lub zasad przewodnich takich organizacji jak Rada Europy każą uznać, że ów polityczny kontekst ochrony danych osobowych w jakimś stopniu zawsze był obecny[213]. Dopiero jednak dyrektywa 95/46 tego typu wartości przywołuje w swoim tekście *expressis verbis*. Odwołuje się mianowicie do celów Wspólnoty Europejskiej jak takiej, sytuując w ten sposób cele ochrony danych osobowych w tym właśnie kontekście. Tym samym cele ochrony danych osobowych zostały powiązane z takimi wartościami, jak „tworzenie coraz ściślejszego związku między narodami Europy, kształtowanie bliższych stosunków między państwami należącymi do Wspólnoty, zapewnienie postępu gospodarczego i społecznego poprzez wspólne działania na rzecz likwidacji barier dzielących Europę, pobudzania ciągłej poprawy warunków życia jej narodów, ochronę i umacnianie pokoju i wolności oraz wspieranie demokracji”[214].

W systemach aksjologicznych organizacji międzynarodowych wytworzył się pogląd, iż brak odpowiedniej ochrony danych w państwie członkowskim w zasadniczy sposób godzi w godność ludzką i funkcjonowanie jednostki w społeczeństwie. Istnieją jednak przypadki pojawiających się napięć pomiędzy daną organizacją a państwem aspirującym do podpisania porozumienia w tym obszarze. Nie zawsze wiąże się to z pożądanym skutkiem, co do poziomu ochrony danych np. przekazywanych do państwa trzeciego[215]. Dla przykładu w 2008 r. Komisja Europejska zwróciła uwagę na przekazywanie danych osobowych krajom trzecim lub organizacjom międzynarodowym. Jej zdaniem proces ten powinien być ściśle nadzorowany, jak również podlegać każdorazowemu indywidualnemu rozpatrzeniu. Z kolei rolą państw członkowskich jest spełnianie „ostrych kryteriów” w sytuacji, gdy chcą skorzystać z możliwości odstępstwa od wymogu adekwatnej ochrony danych osobowych przekazywanych krajom trzecim. „Ocena, czy kraj trzeci zapewni adekwatną ochronę przekazywanych mu danych osobowych powinna być sporządzana przez niezależny organ”[216].

[213] M. Jagielski, *Prawo do ochrony danych …,* s. 33.
[214] Tamże.
[215] Por. Ch. Kuner, *European Data Protection Law Compliance and Regulation,* Oxford – New York 2007, s. 176.
[216] Zob. *Walka z terroryzmem i ochrona danych osobowych,* źródło: www.europarl.europa.eu/sides/getDoc/do?pubRef=-//EP//TEXT+IM-

1.3.6. Bezpieczeństwo demokratyczne

Analizowanie bezpieczeństwa danych osobowych w kontekście bezpieczeństwa demokratycznego jest bardzo istotne. Bowiem ten rodzaj bezpieczeństwa w zasadniczy sposób kształtuje stabilność danego państwa na arenie międzynarodowej a także odnosi się do wielu aspektów życia obywateli tworząc przesłankę ich zaufania do rządu[217].

Zapewnienie odpowiedniej ochrony praw człowieka, właściwie funkcjonującego wymiaru sprawiedliwości, rządów prawa i niezależności władzy sądowniczej staje się powodem do tworzenia demokratycznych standardów prawnych sprzyjających identyfikacji zagrożeń a także kształtowaniu koncepcji bezpieczeństwa demokratycznego[218].

Dlatego poszukiwanie skutecznych rozwiązań w kwestii zapewnienia podstawowych praw człowieka, w tym prawa do prywatności stanowi wyraz tworzenia mechanizmów służących realizacji celu w postaci radzenia sobie z nowymi zagrożeniami powstającymi w związku z rozwojem nowych technologii i zwiększaniem ich roli w życiu każdego człowieka[219].

Nie ulega wątpliwości, iż szczególne znaczenie dla wzmocnienia ochrony podstawowych praw jednostek w związku z przetwarzaniem danych osobowych mają akty przygotowane przez Radę Europy[220]. Organizację, która dążenie do zapewnienia bezpieczeństwa demokratycznego ma niejako zapisane w statucie. W jego preambule wskazano bowiem, iż państwa powołujące tę organizację potwierdzają „swoje głębokie przywiązanie do duchowych i moralnych wartości stanowiących wspólne dziedzictwo

PRESS+20080901BRI35769+ITEM-003-PL+DOC+XML+VO//PL&language+PL, data dostępu: 16.07.2018; Por. A. Grzelak, *Współpraca między organami ochrony danych osobowych w obszarze współpracy policyjnej i wymiaru sprawiedliwości w sprawach karnych – nadchodzące wyzwania prawne,* [w:] *Wdrożenie ogólnego rozporządzenia o ochronie danych osobowych. Aspekty proceduralne,* red. E. Bielak-Jomaa, U. Góral, Wolters Kluwer Polska, Warszawa 2018, s. 63-80.

[217] J. Robel, *Wpływ Rady Europy na realizację koncepcji bezpieczeństwa demokratycznego w państwach członkowskich.* Wydawnictwo Adam Marszałek, Toruń 2016, s. 97.

[218] Zob. H.P. Furrer, J. Gutzkow, *The Concept of Democratic Security and It's Implementation by the Council of Europe,* "Romanian Journal of International Affairs" 1996, vol. II, s. 28.

[219] Zob. L. Kumar, V. Rishival, *Design of Retrievable Data Perturbation Approach and TPA for Public Cloud Data Security*, "Wireless Personal Communications", 2019, nr 1, s. 235.

[220] Zob. E. Kulesza, *Wpływ regulacji Rady Europy i konwencji dotyczącej ochrony danych osobowych na ustawodawstwo polskie,* [w:] *Polska w Radzie Europy 10 lat członkostwa – wybrane zagadnienia,* red. H. Machińska, Ośrodek Informacji Rady Europy Centrum Europejskiego Uniwersytetu Warszawskiego, Warszawa 2002, s. 238-258.

ich narodów i źródło zasad wolności osobistej, swobód politycznych i praworządności, które stanowią podstawę każdej prawdziwej demokracji”[221].

Z powyższego może wynikać, iż prywatności a w tym ochrona danych osobowych stała się kwestią ważną dla demokracji i wręcz pewną potrzebą do jej realizacji[222]. Dlatego ochronę prywatności traktuje się także, jako zachowanie demokracji[223].

Ochrona danych osobowych stała się jednym z podstawowych praw demokratycznego społeczeństwa i musi być dostępna dla wszystkich na równych zasadach. Co prawda w ewolucji w kierunku społeczeństwa cyfrowego nastąpiło wiele zmian, ale w istocie wydaje się, że niewiele się zmieniło w odniesieniu do zagrożeń dla prywatności w ogóle i ważności podstawowej istoty prawa do prywatności danych[224].

1.4. Rodzaje zagrożeń dla bezpieczeństwa danych osobowych

Zagrożenia dla bezpieczeństwa danych osobowych można pogrupować w następujący sposób:

1. Zagrożenia związane z nieprzestrzeganiem zasad ochrony danych osobowych przez pracowników np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł itd.
2. Zagrożenia wynikające z niewłaściwego zabezpieczenia fizycznego pomieszczeń, urządzeń oraz dokumentów;
3. Zagrożenia związanie z nieodpowiednim zabezpieczeniem sprzętu IT czy też oprogramowania przed wyciekiem lub utratą danych osobowych[225].

Warto zwrócić także uwagę na inny podział ze względu na charakter zagrożeń tj. umyślne oraz losowe (wewnętrzne i zewnętrzne)

1. Zagrożenia umyślne mające charakter incydentów w postaci kradzieży danych i sprzętu, czy też ujawnianiem danych osobom nieupoważnionym oraz świadomym niszczeniem danych i włamaniem do systemu;

[221] Statut Rady Europy, przyjęty w Londynie w dniu 5 maja 1949 r. (Dz.U. z 1994 r., Nr 118, poz. 565).
[222] Zob. V. Boehme-Nebler, *Privacy: a matter of democracy. Why democracy needs privacy and data protection,* “International Data Privacy Law”, Vol. 6, s. 222-229.
[223] Zob. A. Walther, *Protection Privacy also Means Preserving Democracy,* źródło: www.phys.org/news/2014-09-privacy-democracy.html, data dostępu: 18.07.2018.
[224] Por. A. Tabrez, *Technology Convergence and Protection of Data Privacy: Human Rights, Democracy Issues and Judical Responses in USA, European Union and India,* “University of Petroleum and Energy Studies (UPES) – College of Legal Studies” 2009, źródło: www.papers.ssrn.com/sol3/papers.cfm?abstract_id=1480718, data dostępu: 18.07.2018.
[225] A. Borowska, *Czym jest incydent w ochronie danych osobowych?,* źródło: www.poradnikprzedsiębiorcy.pl/-incydent-w-ochronie-danych-osobowych, data dostępu: 18.07.2018.

2. Zagrożenia losowe o charakterze wewnętrznym będące wynikiem awarii komputera bądź serwera a także skutkiem zwykłem pomyłki;
3. Zagrożenia losowe o charakterze zewnętrznym powstające w wyniku pożaru, zalania wodą, utratą zasilania czy też utratą łączności[226].

W Polsce wdrożenie standardów dotyczących bezpieczeństwa danych osobowych jest równoznaczne ze spełnieniem wymogów RODO. W związku z tym, Generalny Inspektor Danych Osobowych (GIODO) w celu ochrony przed możliwymi zagrożeniami opracował wskazówki do przeprowadzenia oceny ryzyka obejmujące następujące etapy:
1. Kontekst dla oceny ryzyka – charakter, zakres i cele przetwarzania danych osobowych;
2. Opis i identyfikacja wymagań prawnych i technicznych organizacji – jakie środki są niezbędne do przetwarzania danych; czy dane są przetwarzane zgodnie z prawem; czy stosowane są środki ochronne;
3. Szacowanie oraz ocena ryzyka – analiza prawdopodobieństwa wystąpienia zdarzenia naruszającego ochronę danych osobowych;
4. Postępowanie z ryzykiem[227].

Obawy związane z możliwością wystąpienia określonego zagrożenia są w pełni uzasadnione. Bowiem wzrost działań przestępczych ukierunkowanych na kradzież oraz nielegalne wykorzystanie danych osobowych systematycznie wzrasta, podobnie jak tendencję wzrostową odnotowuje się w przypadku liczby dostępnych usług i wielkości zgromadzonych w sieci baz danych. Jako najpoważniejsze z zagrożeń od wielu lat wymienia się ataki hakerskie, jak również ataki przestępców komputerowych, zwanych crakerami, którzy wykorzystują wiedzę i/lub procedury opublikowane przez hakerów, a także nieświadomość oraz naiwność użytkowników[228]. Bardzo istotny obszar zagrożeń stanowi tez posługiwanie się kartami kredytowymi i debetowymi, gdzie przestępcy dążą

[226] Tamże.
[227] Zob. J. Greser, *Nowe zasady ochrony danych osobowych. Analiza ryzyka,* źródło: www.poradnik.ngo.pl/wiadomości/2158375.html, data dostępu: 18.07.2018.
[228] Zob. *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych,* Biuro Generalnego Inspektora Danych Osobowych, Warszawa 2009, s. 7.

do dotarcia do istotnych danych identyfikacyjnych, umożliwiających dostęp do kont i rachunków posiadaczy tych instrumentów finansowych[229].

1.5. Ogólne zasady związane z zapewnieniem bezpieczeństwa danych osobowych

W Rekomendacji Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z 23 września 1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajam i wymieniono 7 zasad zgodnie z którymi należy postępować przetwarzając dane osobowe:

1. zasada ograniczonego pozyskiwania – pozyskiwanie danych musi się odbywać zgodnie z prawem i być adekwatne w stosunku do celu w jakim są zbierane;
2. zasada adekwatności danych – dane powinny być kompletne, a także aktualne;
3. zasada celowości – wykorzystanie danych (w przyszłości) winno ograniczać się do wypełniania jedynie tych celów, które nie stoją z nimi w sprzeczności;
4. zasada ograniczonego użytkowania – późniejsze wykorzystanie danych nie powinno polegać na ich ujawnieniu bądź też wykorzystaniu bez zgody ich właściciela;
5. zasada otwartości – polityka dot. postępowania z danym powinna być jawna;
6. zasada indywidualnego udziału – każdy powinien mieć zapewniony dostęp do jego prywatnych danych będących w posiadaniu administratora;
7. zasada odpowiedzialności – administrator ponosi odpowiedzialność za przetwarzanie danych osobowych w oparciu o sformułowane zasady[230].

Rok później w art. 5 Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[231], wskazano, iż wszelkie dane będące przedmiotem automatycznego przetwarzania powinny być pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem, gromadzone dla określonych i usprawiedliwionych celów oraz niewykorzystywane w sposób niezgodny z tymi celami.

---

[229] Zob. A. Chuvakin, B.R. Williams, W. Spangerberg, *PCI compliance understand and implement effective PCI data security standard compliance.Payment Card Industry compliance*, Syngress, Amsterdam 2010, s. 34.

[230] Recommendation of the Council concerning guidelines governing the Protection of privacy and transborder flows of personal data, OECD 23 September 1980.

[231] 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. 2003 nr 3 poz. 25).

Powinny one być również odpowiednie, rzeczowe, niewykraczające poza potrzeby, wynikające z celów, dla których są gromadzone. Dane te powinny być dokładne i w razie potrzeby uaktualniane, a ponadto przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczącą, przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego dane te zgromadzono[232].

W nawiązaniu do powyższego warto zaznaczyć, iż zasadę rzetelności i legalności zarówno akty prawa międzynarodowego jak i europejskiego podejmujące tematykę ochrony danych osobowych wymieniają zazwyczaj na pierwszym miejscu[233]. Podobnie rzecz się ma w przypadku ustaw krajowych[234]. Należy także zauważyć, iż zasada ta składa się z dwóch elementów: rzetelności oraz zgodności z prawem. Pierwszy z nich, najogólniej rzecz biorąc, nakłada na administratora danych obowiązek zadbania w trakcie ich przetwarzania o interesy osoby, której dane dotyczą. Oznacza to, że administrator nie może wykorzystywać danych przeciwko ich podmiotowi, a w ramach podejmowania dowolnych czynności przetwarzania powinien za każdym razem dokładać staranności, by wybrać opcję, która – pozwalając mu osiągnąć cel przetwarzania – w najmniejszym stopniu będzie narażała na szwank interesy podmiotu danych. Innymi słowy przetwarzanie ma być jak najmniej dla podmiotu danych uciążliwe, a między celami administratora i prawami osoby, której dane dotyczą, musi zostać zachowana odpowiednia proporcja[235].

W art. 5 Konwencji 108 Rady Europy wskazano także, iż dane powinny być „odpowiednie, rzeczowe, niewykraczające poza potrzeby, wynikające z celów, dla których są gromadzone". Zatem mamy tu odniesienie do zasady minimalizmu w której zachodzi zależność między celem przetwarzania a jego zakresem. Formułowana jest ona poprzez określenie dwóch wymogów:

1) administrator posiada uprawnienia do zbierania jedynie takich danych, które są niezbędne do osiągnięcia celu, dla jakiego dane te są zbierane;

2) gdy dane te staną się do osiągnięcia celu zbędne, powinny być usunięte lub poddane anonimizacji.

[232] Tamże.
[233] Zob. wytyczne ONZ z 1990 r., pkt. 1; dyrektywa 95/46, art. 6 ust. 1 lit. a; wytyczne OECD z 1990 r. *expressis verbis* wymieniają ją jedynie w kontekście zbierania danych (pkt. 7).
[234] M. Jagielski, *Prawo do ochrony danych…,* s. 78.
[235] Zob. art. 6 RODO.

Zasada ta w przeciwieństwie do zasady rzetelności i legalności nie jest tak mocno wyeksponowana w aktach prawnych na poziomie międzynarodowym, natomiast jej sformułowanie wymaga pewnych zabiegów interpretacyjnych. Aczkolwiek formułuje ją wyraźnie doktryna, a jej elementy można odnaleźć w orzecznictwie Europejskiego Trybunału Praw Człowieka[236], jak również w niemal wszystkich ustawach krajowych poświęconych ochronie danych osobowych[237].

Wśród zasad związanych z zapewnieniem bezpieczeństwa danych osobowych nie należy także pomijać zasady określoności celu, która wyraźnie wskazuje iż cel przetwarzania musi być wyraźnie określony; usprawiedliwiony (zgodny z prawem) a także że dane którymi dysponuje administrator nie mogą być wykorzystywane do realizacji innego celu niż ten, dla którego zostały one zebrane[238].

1.6. Standardy międzynarodowe w obszarze bezpieczeństwa danych osobowych

1.6.1. Standardy uniwersalne

Analizując standardy międzynarodowe w obszarze bezpieczeństwa danych osobowych wypracowane w systemie uniwersalnym warto zaznaczyć, iż w ramach ONZ nie odniesiono się szeroko do tego zagadnienia. Źródeł ochrony danych osobowych można poszukiwać w treści art. 12 Powszechnej Deklaracji Praw Człowieka z 10 grudnia 1948 r., w którym zagwarantowano, iż nikt nie może być poddany arbitralnemu ingerowaniu w jego życie prywatne, rodzinne, domowe lub korespondencję, ani też obiektem ataków, godzących w jego honor i dobre imię[239]. Jak zauważa J. Sobczak[240], zdaje się je także wyrażać art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych z 16 grudnia 1966 r. (dalej. MPPOiP), w którym stwierdzono, że nikt nie może być „narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję, ani też na bezprawne

[236] Zob. Wyrok ETPC w sprawie 27798/95 Amann v. Switzerland, 16.02.2000, par. 61 i 75; wyrok ETPC w sprawie 62332/00 Segerstedt-Wiberg and others v. Sweden, 06.06.2006, par. 79.
[237] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz,* 5. wyd., LEX a Wolters Kluwer business, Warszawa 2011, s. 537.
[238] M. Jagielski, *Prawo do ochrony danych…,* s. 89.
[239] Powszechna Deklaracja Praw Człowieka przyjęta 10 grudnia 1948 r. źródło: libr.sejm.gov.pl/tek01/txt/ONZ/1948.html, data dostępu: 19.07.2018.
[240] J. Sobczak, *Ochrona danych osobowych…,* s. 482.

zamachy na jego część i dobre imię”[241]. Komitet Praw Człowieka na gruncie treści art. 17 MPPOiP, sformułował uwagi ogólne, w których stwierdzono, że prawa gwarantowane w art. 17 powinny być chronione przed wszelkimi zamachami, zarówno ze strony funkcjonariuszy państwowych, jak też osób fizycznych lub prawnych. Zaznaczono, że zakaz „bezprawnej” ingerencji wiąże się z niedopuszczalną jakąkolwiek ingerencją z wyjątkiem sytuacji przewidzianych w ustawie. Zakaz arbitralnej ingerencji Komitet odniósł do tych działań organów państwowych, które podejmowane są na podstawie norm prawnych. Określenie to gwarantuje, że jakakolwiek ingerencja ze strony organów władzy publicznej odbywać się będzie zgodnie ze wszystkimi przepisami prawa wewnętrznego oraz w myśl postanowień MPPOiP. We wspomnianych uwagach ogólnych stwierdzono także, iż wszyscy ludzie żyją w pewnych więzach społecznych, więc ochrona ich życia prywatnego, z konieczności, jest sprawą relatywną. Kompetentne organy państwowe mogą, a nawet powinny, dysponować wiedzą, wchodzącą w zakres sfery prywatności jednostek. Zbierając te informacje, nie mogą jednak naruszać norm prawnych, w tym również postanowień MPPOiP. Wskazano także, iż gromadzenie i przechowywanie danych osobowych za pośrednictwem komputerów, banków danych bądź w inny sposób, bez względu na to czy czynią to organy państwowe, pojedyncze osoby lub grupy osób, musi stanowić przedmiot uregulowania prawnego. Zauważono, że państwa powinny podejmować skuteczne środki gwarantujące, że informacje dotyczące życia prywatnego nie dostaną się w ręce osób nieupoważnionych przez przepisy prawne do otrzymywania, przetwarzania oraz wykorzystywania takich danych oraz że dane nigdy nie zostaną użyte do celów niedających się pogodzić z Paktem. Komitet Praw Człowieka stwierdził także, że każda jednostka powinna dysponować możliwością ustalenia, jakie organy państwowe albo osoby prawne czy grupy osób, sprawują bądź mogą sprawować kontrolę nad jej danymi osobowymi. Każda osoba powinna również dysponować prawem do ustalenia, jakie dane jej dotyczące podlegają gromadzeniu oraz w jakich celach. Powinna także mieć możność wprowadzenia odpowiednich sprostowań bądź usunięcia takich danych[242].

[241] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. 1977 nr 38 poz. 167).
[242] Uwagi ogólne Komitetu Praw Człowieka z 23.03.1988 r., [w:] *Wspólny standard do osiągnięcia. Stan urzeczywistnienia. W pięćdziesięciolecie Powszechnej Deklaracji Praw Człowieka z 10 grudnia 1948 roku,* red. T. Jasudowicz, Toruń 1998, s. 262.

W uniwersalnym systemie prawa międzynarodowego kwestii ochrony danych osobowych dotyczą przed wszystkim rezolucja 34/169 oraz rezolucja 45/95, a także akty normatywne wypracowane przez UNESCO, w tym Powszechna Deklaracja UNESCO w sprawie genomu ludzkiego i praw człowieka z 11 listopada 1967 r. W rezolucji 34/169 przyjętej przez Zgromadzenie Ogólne ONZ 17 grudnia 1979 r. – Kodeks postępowania funkcjonariuszy porządku prawnego sformułowano w art. IV zalecenia dla funkcjonariuszy, którzy z racji pełnionych zadań mają dostęp do danych osobowych innych osób. W treści rezolucji zawarto zasady postępowania z tymi danymi, wskazując, że mogą być one udostępniane wyłącznie w celu wypełniania obowiązków służbowych oraz dla potrzeb wymiaru sprawiedliwości. Podkreślono przy tej okazji konieczność zachowania wszystkich zasad bezpieczeństwa w zakresie wykorzystywania takowych danych i ogólne wskazanie, że „wszelkie ujawnianie tych informacji dla innych celów jest całkowicie niestosowne”[243]. O wiele szerszy zakres ma rezolucja z 14 grudnia 1990 r. wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych[244]. Rezolucja ma charakter generalny i formułuje minimalny standard ochrony danych osobowych, jaki powinien być zapewniony w ustawodawstwach krajowych. Nie ma jednak charakteru wiążącego, a stanowi jedynie zalecenia, które powinny zostać spełnione przez ustawodawstwa krajowe. W ramach wytycznych, sformułowano następujące zasady: legalności i uczciwości, jakości danych, celowości, niedyskryminacji, dostępu zainteresowanego do swoich danych, bezpieczeństwa danych[245]. W myśl rezolucji, dane wrażliwe czyli takie, które mogą prowadzić do niezgodnej z prawem bądź arbitralnej dyskryminacji, nie mogą być zbierane. W przepisie tym wymieniono przykłady takich danych, wśród których nie znalazły się jednak dane medyczne, aczkolwiek niewątpliwie mają one charakter danych wrażliwych. Zakaz przetwarzania danych wrażliwych może być uchylony, jeżeli przetwarzanie takich danych jest przewidziane przez prawo i konieczne dla ochrony bezpieczeństwa narodowego, porządku publicznego, zdrowia, moralności publicznej oraz ochrony praw i wolności innych osób, zwłaszcza osób prześladowanych[246].

[243] The General Assembly Resolution 34/169, Code of Conduct for Law Enforcement Officials, 17 December 1979, A/RES/34/169.
[244] The General Assembly Resolution 45/95, Guidelines for the Regulation of computerized personal data files, adopted on 14 December 1990, A/RES/45/95.
[245] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz…,* s. 114-119.
[246] J. Sobczak, *Ochrona danych osobowych…,* s. 483.

Intensywne prace w kierunku stworzenia wspólnych międzynarodowych zasad zapewniających poszanowanie praw i wolności jednostek w warunkach automatycznego przetwarzania danych osobowych doprowadziły do osiągnięcia wspólnego zestawu zasad, które znalazły swe odzwierciedlenie w wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z 1980 r. dotyczących ochrony prywatności i transgranicznego przepływu danych osobowych[247]. Co prawda nie był to dokument prawnie wiążący, jednakże odegrał zasadniczą rolę w tym obszarze.

Warto wskazać także na rolę standardów wynikających z dokumentów UNESCO. Bowiem w Powszechnej Deklaracji UNESCO w sprawie genomu ludzkiego i praw człowieka z 11 listopada 1997 r., wskazano, iż danym genetycznym dającym się zidentyfikować osobie należy zapewnić poufność, przy czym ochrona dotyczy danych bez względu na cel, w jakim są one zbierane. Zauważono, że należy szanować prawo każdej jednostki do decydowania o tym, czy chce być informowana o wynikach badań genetycznych i wynikających stąd konsekwencjach (art. 5 lit c). W treści art. 7 Deklaracji wskazano, że poufność danych genetycznych dotyczących osoby podlegającej identyfikacji i przechowywania lub przetwarzanych dla celów badawczych lub jakichkolwiek innych powinna być chroniona prawem. Stwierdzono poza tym, że ograniczenia zasad i poufności mogą być jedynie przewidziane przez prawo z powodów naglących, wynikających z międzynarodowego prawa publicznego oraz z międzynarodowego prawa praw człowieka[248].

Z kolei w Międzynarodowej deklaracji w sprawie danych genetycznych człowieka z dnia 16 października 2003 r. wskazano, że każdy zbiór danych, przetwarzanie i wykorzystywanie danych genetycznych człowieka, danych i próbek biologicznych ma następować zgodnie z zasadami międzynarodowych praw człowieka (art. 1 lit. b). Wskazano przy tym, że dane genetyczne człowieka to informacje o dziedziczonych cechach fizycznych uzyskanych przez analizę kwasów nukleinowych lub w drodze innych analiz naukowych. Natomiast ludzkie dane protemiczne to informacje odnoszące się do indywidualnych białek, ich modyfikacji i współdziałania. Dane dotyczące każdej osoby to takie, które zawierają takie informacje jak: imię,

[247] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23.9.1980.
[248] The Universal Declaration on the Human Genome and Human Rights was adopted by the General Conference of UNESCO at its 29th session on 11 November 1997.

nazwisko, datę urodzenia i adres, dzięki którym można zidentyfikować określoną osobę (art. 2 pkt IX)[249].

1.6.2. Standardy regionalne

Analizując standardy regionalne w obszarze bezpieczeństwa danych osobowych nie sposób nie wspomnieć o tych wypracowanych w systemach aksjologicznych Rady Europy oraz Unii Europejskiej (szersze odniesienie w kolejnych rozdziałach).

W systemie aksjologicznym Rady Europy dość długo podstawowymi aktami normatywnymi regulującymi ochronę danych osobowych były: rezolucja Komitetu Ministrów nr 73/22 z 26 września 1973 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym[250] oraz rezolucja Komitetu Ministrów 74/29 z 20 września 1974 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze publicznym[251], w której zawarto zasady gromadzenia informacji, przechowywania oraz dostępu do nich.

Zasadniczą rolę w systemie regionalnym zaczęła odgrywać Konwencja nr 108 Rady Europy z 28 stycznia 1981 r.[252], której celem było zapewnienie na obszarze państw członkowskich każdemu, niezależnie od obywatelstwa i zamieszkania, ochronę jego praw i wolności, a w szczególności prawa do poszanowania sfery osobistej w związku z automatycznym przetwarzaniem danych osobowych[253].

W systemie aksjologicznym Unii Europejskiej zagadnienie ochrony danych osobowych długi czas wydawało się być niezauważalne[254]. Komisja Europejska zleciła jedynie państwom członkowskim Wspólnoty ratyfikację Konwencji 108 Rady Europy[255]. Stopniowo od początku lat 90. problematyka ochrony danych zaczęła

[249] J. Sobczak, *Ochrona danych osobowych…,* s. 484.
[250] Committee of Ministers The Council of Europe Resolution 73/22 on the Protection of the privacy of Individuals vis-a-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th Meeting of the Ministers' Deputies.
[251] Committee of Ministers of The Council of Europe Resolution 74/29, On the Protection of the Privacy of Individuals Vis-A Electronic Data Banks in the Public Sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.
[252] Dz.U. 2003 nr 3 poz. 25.
[253] Tamże.
[254] J. Sobczak, *Ochrona danych osobowych… ,*s. 492.
[255] Zob. G.F. Gonzalez, *Security and the Future of Personal Data Protection in the European Union,* "Security and Human Rights" 2013, Vol. 23, s. 331-342.

pojawiać się w dokumentach Wspólnoty, potem Rady[256]. Kwestii tej poświeciła uwagę m.in. dyrektywa 95/46/WE/ Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[257], dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej[258], dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnieniem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE[259], dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów[260].

Obecnie zasadnicze znaczenie w systemie aksjologicznym Unii Europejskiej odgrywa 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 osobowych)[261].

[256] Zob. P. Graham, N. Platten, *Achieving Personal Data Protecting in the European Union,* "Journal of Common Market Studies" 1998, Vol. 26, s. 529-547.
[257] Directive No. 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with regard to the processing of personal data and on the Free Movements of such data, October 24, 1995.
[258] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the Protection of privacy in the electronic communication sector, Official Journal L 201, 31/07/2002 P. 0037-0047.
[259] Dz.Urz. UE L 105/54 z 13.04.2006.
[260] Dz.Urz. UE L 337/11 z 18.12.2009, s. 11-36.
[261] Rozporządzenie dostępne na: www.giodo.gov.pl/569/9276.

Rozdział 2: Bezpieczeństwo danych osobowych w systemie aksjologicznym Rady Europy i mechanizmy jego realizacji w państwach członkowskich

2.1. Ogólna charakterystyka Rady Europy

W literaturze dość często przytaczany jest art. 1 lit a Statutu Rady Europy z dnia 5 maja 1949 r.[262], zgodnie z którym u podstaw jej utworzenia leżała idea „ściślejszej jedności państw" nawiązująca do „wspólnego dziedzictwa narodów", opartego na „swobodach osobistych, wolnościach politycznych i praworządności"[263]. Za datę jej powstania uznaje się 5 maja 1949 r. (Londyn)[264]. Utworzona została za sprawą 10 państw tj.: Belgii, Danii, Francji, Irlandii, Włoch, Luksemburga, Holandii, Norwegii, Szwecji, Wielkiej Brytanii[265].

Bez wątpienia, szeroko ujęte zadania państw przystępujących do Rady Europy wskazują na potrzebę istnienia wspólnej płaszczyzny rozumienia zasad praworządności oraz wolności i praw człowieka[266]. Takimi właśnie założeniami kierowano się tworząc koncepcję Rady Europy w Hadze w maju 1948 r., podczas Kongresu Europy[267]. Wskazywano wówczas o konieczności powstania zgromadzenia europejskiego, karty praw człowieka, jak również sądu stojącego na straży jej przestrzegania[268]. Dało to impuls dla państw zachodnioeuropejskich do pobudzenia negocjacji multilateralnych w celu powołania nowej organizacji o charakterze międzynarodowym[269].

W świetle art. 3 Statutu RE „Każdy członek Rady Europy uznaje zasadę praworządności oraz zasadę, iż wszystkie osoby pozostające pod jego jurysdykcją korzystają z praw człowieka i podstawowych wolności; musi też szczerze i wydatnie

[262] Zob. S.A. Paruch, *Czynniki wpływające na skuteczność systemu instytucjonalnego ochrony praw człowieka w Radzie Europy,* [w:] *Ochrona praw człowieka w Europie. Aksjologia – instytucje – nowe wyzwania – praktyka,* red. J. Jaskiernia, K. Spryszak, tom III, Wydawnictwo Adam Marszałek, Toruń 2017, s. 56.
[263] Statut Rady Europy z dnia 5 maja 1949 r., (Dz.U. 1994, nr 118, poz. 565).
[264] Zob. J. Robel, *Wpływ Rady Europy na realizację koncepcji bezpieczeństwa demokratycznego w państwach członkowskich,* Wydawnictwo Adam Marszałek, Toruń 2016, s. 11.
[265] Aktualna lista państw członkowskich dostępna na: www.coe.int.
[266] Zob. D. Bach-Golecka, *Demokracja w prawie międzynarodowym,* Wydawnictwo DANTE, Kraków 2007, s. 229.

współpracować dla urzeczywistnienia celu Rady określonego w rozdziale I”[270]. Tym samym państwa członkowskie zobowiązały się do otwartej oraz efektywnej współpracy na rzecz osiągnięcia większej jedności i torowania drogi rozwoju gospodarczego oraz społecznego[271].

Warto zauważyć, iż z punktu widzenia typologii kształtowania organizacji międzynarodowych Rada Europy stanowi organizację prekursorską, jeżeli chodzi o fundament członkostwa, którym stały się wspólne wartości. Zasadniczym osiągnięciem tej organizacji jest bogaty i wszechstronny system norm i standardów ochrony praw człowieka[272].

Kluczowym dokumentem dotyczącym ochrony praw człowieka, w tym praw społecznych jest Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności (dalej: Europejska Konwencja Praw Człowieka)[273]. Zasadniczą rolę odgrywa także jej mechanizm kontrolny w postaci Europejskiego Trybunału Praw Człowieka (ETPCz)[274].

O dokumencie tym mówi się jako o wspólnej wartości europejskich demokracji, tworzącym zespół kryteriów, którym powinny odpowiadać systemy polityczne, aby można było je uznać za rzeczywiście demokratyczne[275].

EKPCz, poprzez skuteczną implementację gwarancji materialnych oraz formalnych, przyczynia się stale do poprawy standardu poszanowania praw człowieka. Zachowanie odpowiednio wysokiego poziomu ochrony praw człowieka i podstawowych wolności wymaga stanowczości w ocenie naruszeń fundamentalnych wartości demokratycznych społeczeństw[276].

---

[267] Zob. *Congress of Europe,* The Hague, 7-11 May 1948, Council of Europe Publishing, Strasbourg 1999.
[268] Zob. B. Podgórski, *Rada Europy w procesie integracji europejskiej,* [w:] *Efektywność europejskiego systemu ochrony praw człowieka. Efektywność mechanizmów ochrony praw człowieka Rady Europy, Unii Europejskiej i OBWE,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2012, s. 13.
[269] Zob. B. Wassenberg, *History of the Council…,* s. 4.
[270] Dz.U. 1994, nr 118, poz. 565.
[271] Zob. K. Łasak, *Prawa społeczne w orzecznictwie Europejskiego Trybunału Praw Człowieka,* Instytut Wydawniczy EuroPrawo, Warszawa 2013, s. 14.
[272] Por. M. Papucki, *Grupa Państw przeciwko Korupcji (GRECO) jako instrument oddziaływania Rady Europy na zwalczanie korupcji,* [w:] *Europejski system ochrony praw człowieka. Inspiracja uniwersalna – uwarunkowania kulturowe – bariery realizacyjne,* red. J. Jaskiernia, K. Spryszak, tom III, Wydawnictwo Adam Marszałek, Toruń 2016, s. 272.
[273] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., (Dz.U. 1993 nr 61 poz. 284).
[274] Zob. J.A. Sweeney, *The European Court of Human Rights in the Post-Cold War Era: Universality in Transition,* Routledge, Abington 2012, s. 48.
[275] A.I. Jackiewicz, *Prawo do dobrej administracji…,* s. 73.
[276] Zob. I. Ganfalean, M. Tudorascu, M. Cojan, *Human Rights Protection in Europe,* “Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy” 2014, nr 11, s. 21-27.

R. Arnold wskazuje, iż „staje się coraz bardziej oczywiste, iż orzecznictwo organów ze Strasburga stwarza swego rodzaju konstytucję europejską, która oddziałuje bądź bądź bezpośrednio na porządek państw – sygnatariuszy, bądź pośrednio wpływa na porządek prawny w każdym z tych państw, dając jednostce coraz więcej możliwości zwrócenia się do „instancji" strasburskich po wyczerpaniu krajowej drogi prawnej"[277].

Ewolucja Rady Europy od „ekskluzywnego klubu państw demokratycznych Europy Zachodniej" do otworzenia się na państwa Europy Środkowej i Wschodniej świadczy o zwiększeniu roli tejże organizacji międzynarodowej. Co prawda wpływ na tą pozycję miały przemiany zachodzące w Europie, to jednak dzięki skutecznym działaniom stała się ona cennym a także trwałym elementem europejskiej architektury instytucjonalnej[278]. Dziś do RE należy 47 państw (stan na dzień: 07.09.2018).

Największą rolę w systemie instytucjonalnym RE odgrywają dwa organy statutowe: Komitet Ministrów i Zgromadzenie Parlamentarne. Celem Komitetu jest – jak stwierdza wspólne oświadczenie państw członkowskich, złożone podczas pospisywania statutu – „utrzymanie rozwoju współpracy między rządami", zadaniem Zgromadzenia jest „dostarczanie środków, za pomocą których Europejczycy mogliby formułować i wyrażać swoje pragnienia, aby w ten sposób rządy mogły mieć ciągły kontakt z europejską opinią publiczną"[279].

Warto zauważyć, iż możliwość podejmowania przez organy Rady spraw z różnych dziedzin nie oznacza możliwości podejmowania takich aktów, które wiązałyby państwa członkowskie[280]. Przy bardzo obszernym przedmiocie działania Rada została wyposażona, poza jednak sferą ochrony praw człowieka[281], w środki typowe dla klasycznej organizacji międzynarodowej[282]. Środki te nie mają nic wspólnego z

[277] R. Arnold, *Znaczenie prawa europejskiego dla polskiego porządku prawnego,* „Monitor Prawniczy" 1996, nr 7, s. 237.
[278] Zob. P.A. Świtalski, *Rola Rady Europy w systemie organizacji międzynarodowych,* [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2010, s. 14.
[279] Zob. J. Sieńczyło-Chlabicz, *Wkład Rady Europy w tworzenie i kodyfikację norm prawa międzynarodowego,* „Białostockie Studia Prawnicze" 1994, Nr 2, s. 140 – 141.
[280] Zob. K. Spryszak, *Wpływ Rady Europy na transformację prawnokonstytucyjną na Węgrzech,* [w:] *Ochrona praw człowieka w Europie. Aksjologia – instytucje – nowe wyzwania – praktyka,* red. J. Jaskiernia, K. Spryszak, t. III, Wydawnictwo Adam Marszałek, Toruń 2017, s. 244-254.
[281] Zob. H. Winkler, *Democracy and human Rights – a Survey of the Admission Practice of the Council of Europe,* "Austrian Journal of Public and International Law" 1995, t. 47, s. 21.
[282] A. Koller, *The Legal Heritage of the Council of Europe,* "Human Rights Law Journal" 1990, nr 1-2, s. 214.

ponadpaństwowością, która stała się cechą charakterystyczną Wspólnot i Unii Europejskiej.

Środki, którymi dysponuje Rada Europy, wymienia w sposób ogólny art. 1 lit. a jej Statutu: omawianie wspólnych problemów, zawieranie porozumień i podejmowanie wspólnych działań.

Rozpatrywanie wspólnych problemów – spraw budzących wspólne zainteresowanie odpowiada roli Rady jako klubu dyskusyjnego. Forum dyskusji jest przede wszystkim Zgromadzenie Parlamentarne[283], choć w swoim zakresie działania – forum dyskusyjnym jest również Kongres Władz Lokalnych i Regionalnych[284].

Sprawy o wspólnym znaczeniu podejmować muszą także, z natury rzeczy, Komitet Ministrów, oraz komitety.

Domeną Komitetu Ministrów jest jednak przede wszystkim podejmowanie wspólnych działań. Jak wykazuje praktyka, działania te mają z reguły szczegółowy i raczej techniczny charakter[285].

Formą najbardziej klasyczną jest „zawieranie porozumień" – co oznacza przygotowywanie projektów umów międzynarodowych. Projekty te uchwalane są przez Komitet Ministrów, czasem jednak, na zalecenie Zgromadzenia, aby mogły stać się aktami prawa międzynarodowego i w efekcie oddziaływać na treść wewnętrznego porządku prawnego państw, wymagają podpisania przez rząd oraz ratyfikacji, w której z reguły uczestniczy parlament danego państwa (w takim trybie powstała Europejska Konwencja Praw Człowieka)[286].

2.2. Bezpieczeństwo danych osobowych w systemie aksjologicznym RE

W systemie aksjologicznym Rady Europy na szczególną uwagę zasługują dwa rodzaje standardów: standardy prawnie wiążące (tzw. twarde prawo), obejmujące

[283] Zob. T.E. Kleinsorge, *The Parliamentary Assembly: Europe's Motor and Conscience,* [w:] *Council of Europe,* red. T. Kleinsorge, Kluwer Law International, Alhen aan den Rijn 2010, s. 129.
[284] Zob. J. Robel, *Kongres Władz Lokalnych i Regionalnych Europy na straży europejskiej samorządności terytorialnej,* „Zeszyty Naukowe Instytutu Administracji AJD w Częstochowie, Gubernaculum et Administration" 2016, nr 2, s. 25-27.
[285] Zob. M. Balcerzak, *Zalecenia Komitetu Ministrów Rady Europy jako forma pozatraktatowej działalności normatywnej i harmonizującej w dziedzinie praw człowieka,* [w:] *Rada Europy – 60 lat na rzecz jedności europejskiej,* red. I. Głuszczyńska, K. Lankosz, Bielsko – Biała 2009, s. 6-25.
[286] Zob. J. Jaskiernia, *Zgromadzenie Parlamentarne Rady Europy,* Biuro Rady Europy, Warszawa 2000, s. 58.

umowy międzynarodowe mające charakter aktów prawnie wiążących, które przybierają z reguły formę konwencji[287], oraz standardy o charakterze „miękkiego prawa" (uchwałodawcze), nie posiadające mocy wiążącej, ale mające znaczenie o charakterze politycznym[288], np. zalecenia Komitetu Ministrów Rady Europy[289].

2.2.1. Standardy prawnie wiążące

Standardy o charakterze prawnie wiążącym wypracowane w systemie aksjologicznym Rady Europy mają fundamentalne znaczenie. Ta kwalifikacja wynika stąd, że zostały one usytuowane w dokumentach, które mają charakter umów (traktatów) międzynarodowych, a więc źródeł prawa międzynarodowego wiążących dla państw, które są ich stronami[290]. Takim traktatem międzynarodowym jest niewątpliwie Statut Rady Europy. Do grupy tej należy też Europejska Konwencja Praw Człowieka, której przyjęcie wiąże się z istotnymi ograniczeniami suwerenności państwa, ale następuje to zgodnie z logiką rozszerzania międzynarodowej ochrony praw człowieka[291].

Standardy prawnie wiążące niosą również pozostałe konwencje wypracowane w systemie Rady Europy. Zasadnicze znaczenie dla wzmocnienia bezpieczeństwa danych osobowych ma Konwencja nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych[292]. Polska podpisała konwencję 21 kwietnia 1999 r. zaś ratyfikowała 23 marca 2002 r. [293].

Konwencja 108 Rady Europy ma charakter normy określającej minimalne standardy ochrony danych, które muszą zostać wprowadzone do prawa wewnętrznego państwa członkowskiego[294]. Jej celem, jak zauważa E. Kulesza, jest osiągnięcie

[287] Zob. K. Abbott, D. Sindal, *Hard and Soft Law in International Governance,* [w:] *International Law: Classic and Contemporary Readings,* red. C. KU. P.F. Dietl, Lynne Rienner, Boulder 2009, s. 18.
[288] Zob. J. Robel, *Wpływ Rady Europy…,* s. 48.
[289] Szerzej: M. Balcerzak, *Zalecenia Komitetu Ministrów Rady Europy jako forma pozatraktatowej działalności normatywnej i harmonizującej w dziedzinie praw człowieka,* [w:] *Rada Europy – 60 lat na rzecz jedności europejskiej,* Bielsko – Biała 2009, s. 6-25.
[290] Zob. M.A. Fitzmaurice, *The Identification and Character of Treaties and Treaty Obligations between States in International Law,* "British Year Book of International Law" 2002, vol. 73, s. 149.
[291] Por. S.J. Barkin, *The Revolution of the Constitutions of Sovereignty and the Emergencje of Human Rights Norms,* "Millenium – Journal of International Studies" 1998, No. 2, s. 239.
[292] Dz.U. 2003 nr 3 poz. 25.
[293] Dz.U.03.3.25.
[294] Zob. P. de Hert, V. Papakonstantinou, *The Council of Europe Data Protection Convention reform: Analysis of the new text and Critical Comments on its global ambition,* "Computer Law & Security Review: The International Journal of Technology Law and Practice" 2014, Vol. 30, s. 663-642.

większej jednolitości ustawodawstw państw członkowskich w zakresie praworządności oraz praw człowieka i podstawowych wolności, w szczególności prawa do prywatności, z jednoczesnym uwzględnieniem możliwości swobodnego przepływu informacji, bez względu na istniejące granice[295].

Intencją Konwencji nie było, jak wynika z jej art. 4, bezpośrednie zagwarantowanie prawa dla osób fizycznych, lecz zobowiązanie państw do wprowadzenia w prawie wewnętrznym podstawowych zasad ochrony danych, w celu ujednolicenia standardów ochrony[296].

We wstępie raportu wyjaśniającego stwierdzono, iż celem Konwencji jest wzmocnienie prawnej ochrony jednostek wobec automatycznego przetwarzania danych osobowych. Wzmocnienie ochrony było – zdaniem autorów – niezbędne ze względu na stale rosnące wykorzystanie informatyki do celów administracyjnych i zarządzania. Wskazano przy tym, iż „Kartoteki zautomatyzowane mają dużo większe możliwości rejestracyjne niż kartoteki ręczne i pozwalają na szybsze dokonywanie bardziej różnorodnych operacji"[297]. Zwrócono, też uwagę na fakt, że w nowoczesnym społeczeństwie część decyzji dotyczących jednostek podejmuje się na podstawie informacji zawartych w różnego rodzaju kartotekach (np. w dokumentacji medycznej, w kartotekach ubezpieczeń społecznych, itp.). Większe możliwości rejestracji i kojarzenia danych z różnych źródeł oznaczają, że w procesie decyzyjnym mniejszą wagę będą odgrywały bezpośrednie kontakty z zainteresowanymi.

Podstawowe zasady ochrony danych określone w rozdziale II Konwencji nr 108 obejmują: wymóg posiadania danych osobowych uzyskanych i przetwarzanych rzetelnie i zgodnie z prawem, przechowywania ich dla określonych i legalnych celów oraz nie wykorzystywania w sposób niezgodny z tymi celami. Za bardziej rygorystyczny reżim prawny zawarty w Konwencji uznać należy natomiast automatyczne przetwarzanie danych poufnych („specjalne kategorie danych")[298].

---

[295] E. Kulesza, *Wpływ regulacji Rady Europy…*s. 238.

[296] Por. G. Greenleaf, *'Modernising' data Protection Convention 108: A safe Basic for a global,* "Computer Law and Security Review: The International Journal of Technology and Practice" 2013, vol 29, s. 430.

[297] Rapport explicatif concernant la Convention pour la protectiondes personnes a l'egard du traitement automatise des donnees a caractere personel, Strasbourg 1981, s. 5.

[298] Dane osobowe dotyczące zdrowia lub życia seksualnego, dane osobowe ujawniające pochodzenie rasowe, opinie polityczne lub przekonania religijne lub inne, jak również dane osobowe dotyczące wyroków skazujących za przestępstwa.

Na mocy Konwencji nr 108 ustanowiono także Komitet Konsultacyjny złożony z przedstawicieli stron konwencji, którego rola polegać miała na interpretowaniu jej postanowień i dążeniu do ułatwienia oraz usprawnienia jej stosowania[299]. Jedną z inicjatyw Komitetu było zbadanie, w jakim stopniu stosowanie klauzul umownych może usprawnić transgraniczny przepływ danych między stronami konwencji i państwami niebędącymi stroną, a także współpracy z Komisją Europejską i Międzynarodową Izbą Handlową.[300]

Celem Rady Europy było, zatem osiągnięcie większej jedności między jej członkami w oparciu o poszanowanie praworządności, praw człowieka i podstawowych wolności oraz uznanie za pożądane rozszerzenie gwarancji dla wszystkich praw, a w szczególności prawa do poszanowania prywatności każdego człowieka, zwłaszcza biorąc pod uwagę rosnący przepływ danych osobowych przez granice, podlegających automatycznemu przetwarzaniu[301]. Co więcej Konwencja została opracowana w sposób neutralny technologicznie, co pozwala na jej pełne stosowanie po dziś dzień, niezależnie od rozwoju technologicznego[302]. Aby jednak zapewnić, że zasady ochrony danych są nadal dostosowane do nowych narzędzi i praktyk, jej tekst jest poddawany aktualizacji[303]. Dla przykładu w dniu 15 czerwca 1999 r. przyjęto poprawki do Konwencji nr 108 w związku z przystąpieniem Wspólnot Europejskich[304]. Stanowiło to niewątpliwie efekt dążenia Unii do rozwijania współpracy z Radą Europy i przyczynienia się do stworzenia silniejszego międzynarodowego forum na temat ochrony danych osobowych, w szczególności w odniesieniu do krajów trzecich[305].

---

[299] Szerzej: *Consultative Committee,* źródło: www.coe.int/web/data-protection/consultative-committee-tpd, data dostępu: 13.09.2018.

[300] Explanatory Memorandum to Recommendation No. R (2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes, Adopted by the Committee of Ministers on 18 September 2002 at the 808 th meeting of the Minister's Deputies.

[301] Zob. S. Kierkegaard, N. Waters, G. Greenleaf, L.A. Bygrave, L. Lloyd, S. Saxby, *30 Years on – The review of the Council of Europe Data Protection Convention 108,* "Computer & Security Review" 2011, Vol. 27, s. 223.

[302] Zob. A. Mantelero, *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework,* "Computer Law & Security Review: The International Journal of Technology Law and Practice" 2017, vol. 33, s. 600.

[303] Zob. *Protection of Personal Data and Privacy,* źródło: www.coe.int/en/web/portal/personal-data-protection-and-privacy?deskopt, data dostępu: 13.09.2018.

[304] Zob. *Amendments to Convention 108,* źródło: www.coe.int/en/web/data-protection/convention108/amendments, data dostępu: 13.09.2018.

[305] Zob. *Council of Europe Discusses Amendments to Convention 108,* źródło: www.personaldata.ge/en/strasburgshi-108-e-konventsiashi-shesat-tsvlilbebze-msdjelebon/610, data dostępu: 13.09.2018.

W Protokole Dodatkowym do Konwencji z dnia 8 listopada 2001 r. umieszczono wymóg ustanowienia niezależnego organu w celu zapewnienia zgodności z zasadami ochrony danych osobowych („*Każda Strona ustanowi jeden lub większą liczbę organów odpowiedzialnych za zapewnienie zgodnej ze środkami swego prawa krajowego realizacji zasad określonych w rozdziałach II i III konwencji w niniejszym protokole")*, jak również ustanowiono zasady dotyczące transgranicznego przepływu danych[306]. Protokół ten jest ważny również w odniesieniu do zasad dotyczących przekazywania danych osobowych państwom lub organizacjom, które nie są stronami Konwencji nr 108. Jest to zasadniczo dozwolone, pod warunkiem zapewnienia odpowiedniego poziomu ochrony danych (z pewnymi wyjątkami)[307].

Zgodnie z raportem wyjaśniającym do Protokołu, art. 1 ma podwójny cel: egzekwowanie skutecznej ochrony jednostki, oraz poprawę harmonizacji przepisów regulujących organy nadzoru ustanowione już przez strony Konwencji[308]. W jego treści zaznaczono także, iż uprawnienia wymienione w przywołanym artykule nie są wyczerpujące, a organy nadzoru mogą także być uprawnione do wykonywania dodatkowych obowiązków, takich jak wcześniejsze kontrole operacji przetwarzania, utrzymanie publicznego rejestru podmiotów przetwarzających dane, czy też komentarz do proponowanych środków legislacyjnych, regulacyjnych lub administracyjnych związanych z przetwarzaniem danych[309].

Każda ze stron protokołu zobowiązuje się, że przekazanie danych podmiotowi podlegającemu jurysdykcji państwa lub organizacji nie będących stronami konwencji nastąpi tylko wtedy, jeżeli zachowany zostanie wystarczający poziom ochrony danych, które mają zostać przekazane. Wyjątki dopuszczalne są w szczególności z uwagi na określone interesy podmiotu danych, uzasadniony prawnie interes powszechny lub szczególnie ważny interes publiczny, pod warunkiem, że przewiduje to prawo krajowe.

Do dnia dzisiejszego Konwencja nr 108 nadal pozostaje jedynym wiążącym międzynarodowym instrumentem prawnym o światowym zasięgu stosowania w dziedzinie prywatności danych, otwartym na wszystkie kraje, w tym te niebędące

[306] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory Authorities and transborder data flows, ETS nr 181.
[307] Zob. G. Greenleaf, N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick, *A World Data Privacy Treaty?, 'Globalisation' and 'Modernisation' of Council of Europe Convention 108,* Cambridge University Press, Cambridge 2014, s. 92-98.
[308] Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS nr 181.
[309] Tamże, par. 16.

członkami Rady Europy[310]. Ponadto Konwencja ta przetrwała próbę czasu, ponieważ jest dostosowana i dość rygorystyczna. Od pewnego czasu zasady w niej zawarte są badane pod kątem ich przydatności do gromadzenia i przetwarzania danych biometrycznych[311].

Aby dostosować się do nowych realiów coraz bardziej połączonego świata i wzmocnić skuteczne wdrażanie Konwencji nr 108, konieczna okazała się modernizacja tego przełomowego instrumentu.

W dniu 18 maja 2018 r. przyjęto protokół zmieniający Konwencję (CETS nr 223), który potwierdza podstawowe zasady zapisane w 1981 r. i integruje nowe zabezpieczenia. Został on otwarty do podpisu dniu 10 października 2018 r.[312]

Modernizacja Konwencji nr 108, jedynego istniejącego prawnie wiążącego traktatu międzynarodowego o globalnym znaczeniu w tej dziedzinie, stanowi odpowiedź na wyzwania związane z prywatnością, wynikające z zastosowania nowych technologii informacyjnych i komunikacyjnych oraz wzmacnia mechanizm konwencji, aby zapewnić jego skuteczne wdrożenie.

Protokół zapewnia solidne i elastyczne wielostronne ramy prawne w celu ułatwienia przepływu danych przez granice, zapewniając jednocześnie skuteczne zabezpieczenia, gdy wykorzystywane są dane osobowe. Stanowi pomost między różnymi regionami świata i różnymi ramami normatywnymi, w tym nowym ustawodawstwem Unii Europejskiej, które zaczęło w pełni obowiązywać w dniu 25 maja 2018 r. I które odnosi się do konwencji 108 w kontekście transgranicznego przepływu danych.

Niektóre innowacje zawarte w protokole są następujące:

- Bardziej surowe wymogi dotyczące proporcjonalności i minimalizacji danych oraz zgodności z prawem przetwarzania;
- Rozszerzenie rodzajów wrażliwych danych, które będą teraz obejmować dane genetyczne i biometryczne, członkostwo w związkach zawodowych i pochodzenie etniczne;

[310] Zob. N. Gumzej, *The Council of Europe and the Right to Personal Data Protection: Embracing Postmodernity,* "Journal of Arts & Sciences" 2013, No 6, s. 14.
[311] Zob. The Council of Europe Progress Report on The Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data, Tilburg Institute for Law, Technology and Society, Tilburg University, April 2013.
[312] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Pressing of Personal Data, Strasbourg, 10/10/2018 – Treaty open for signature by the Contracting States to Treaty ETS 108.

- Obowiązek zgłoszenia naruszenia danych;
- Większa przejrzystość przetwarzania danych;
- Nowe prawa dla osób w kontekście algorytmicznego podejmowania decyzji, które są szczególnie istotne w związku z rozwojem sztucznej inteligencji;
- Większa odpowiedzialność administratorów danych;
- Wymóg stosowania zasady „poszanowania prywatności od samego początku";
- Stosowanie zasad ochrony danych do wszystkich działań związanych z przetwarzaniem, w tym ze względów bezpieczeństwa narodowego, z możliwymi wyjątkami i ograniczeniami z zastrzeżeniem warunków określonych w konwencji, a w każdym przypadku z niezależnym i skutecznym przeglądem i nadzorem;
- Jasny reżim transgranicznych przepływów danych;
- Wzmocnione uprawnienia niezależności organów ochrony danych oraz wzmocnienie podstawy prawnej dla współpracy międzynarodowej[313].

Działalność Rady Europy w zakresie ochrony danych nie ogranicza się jednak wyłącznie do Konwencji nr 108 i protokołu dodatkowego. Wśród standardów konwencyjnych uwzględnić należy także postanowienia Europejskiej Konwencji Praw Człowieka, która w art. 8 gwarantuje prawo do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji oraz określa warunki, pod jakimi dopuszczalne są te ograniczenia[314]. Przepis ten stał się postawą działalności orzeczniczej Europejskiego Trybunału Praw Człowieka[315].

Warto zwrócić uwagę także na art. 10 Konwencji potwierdzający podstawowe prawo do wolności słowa. Prawo to wyraźnie obejmuje wolność „przyjmowania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice".

Zgodnie z logiką EKPC art. 8 i 10 mają charakter komplementarny, a nie sprzeczny. W praktyce jednak każde z tych praw ogranicza czasem korzystanie z drugiego. Organy EKPC wykorzystały zatem swoje orzecznictwo do określenia

[313] Tamże.
[314] Dz.U. 1993 nr 61 poz. 284.
[315] Zob. J. Raman, *European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland, no. 20511/03, 17 July 2008*, "The Computer Law and Security Report", 2008, nr 6, s. 562.

ograniczeń w korzystaniu z każdego z tych praw. W szczególności określają one zakres, w jakim władze publiczne mają prawo ingerować w prawa uznane przez Konwencję lub są zachęcane do towarzyszenia niektórym sektorom w zakresie gwarancji prawnych[316]. ETPCz, na przykład, orzekł, że ochrona danych stanowi podstawowy element ochrony przyznanej prawu do poszanowania prywatności[317]. Decyzje te mają, zatem duże znaczenie dla działań Rady Europy w dziedzinie ochrony danych. Co więcej, były one i nadal są głównym źródłem kryteriów, na których rządy mogą oprzeć swoje krajowe regulacje. Niemniej jednak od wielu lat od przyjęcia EKPC stało się jasne, że aby zapewnić skuteczność ochrony prawnej, należy rozwijać bardziej szczegółowe standardy[318].

Nie należy również pomijać najnowszego orzecznictwa strasburskiego w zakresie przekazywania danych medycznych[319]. Kluczowe są również postanowienia Europejskiej Konwencji Bioetycznej z 4 kwietnia 1997 r.[320] w części odnoszącej się do ochrony danych osobowych, wraz z odpowiednimi fragmentami Sprawozdania Wyjaśniającego do niej[321].

2.2.2. Standardy o charakterze tzw. „miękkiego prawa"

Zagadnienie bezpieczeństwa danych osobowych, uregulowane zostało ponadto w wielu innych dokumentach RE o charakterze tzw. miękkiego prawa. Tematyki tej dotyczą rezolucje wydane przez Komitet Ministrów Rady Europy, np. rezolucja w

[316] Zob. Explanatory Memorandum to Recommendation No. R (2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes, Adopted by the Committee of Ministers on 18 September 2002 at the 808 th meeting of the Minister's Deputies.
[317] Zob. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 25 lutego 1997 r. w sprawie *Z przeciwko Finlandii*. Orzecznictwo to zostało potwierdzone w *wyrokach MS przeciwko Szwecji* z dnia 27 sierpnia 1997 r., Rec. 1997, *Amman przeciwko Szwajcarii* z 16 lutego 2000 r., Rec. 2000, oraz *Rotaru przeciwko Rumunii* z 4 maja 2000, Rec. 2000.
[318] Por. N. Purtova, *Private Law Solutions in European Data Protection,* "Netherlands Quarterly of Human Rights" 2010, No. 28, s. 185.
[319] Zob. Case Law of the European Court of Human Rights Concerning the Protection of Personal Data, Council of Europe, Strasbourg, 15 November 2017, T-PD(2017)23.
[320] Convention for the Protection of Human Rights and Dignity of The Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4.IV.1997, ETS – No. 164.
[321] Explanatory Report to the Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine, Convention on Human Rights and Biomedicine, ETS- No. 164, źródło: www.rm.coe.int/16800cde5, data dostępu: 13.09.2018.

zakresie ochrony sfery prywatności osób fizycznych w aspekcie wykorzystywania elektronicznych banków danych w sektorze prywatnym (Rezolucja nr 22)[322] oraz w sektorze publicznym (Rezolucja nr 29)[323].

Warto zwrócić uwagę na zasady zawarte w treści tych rezolucji. Według rezolucji nr 22 państwa członkowskie powinny kierować się następującymi zasadami: „a) gromadzone informacje powinny być dokładne i aktualne, przy czym w zasadzie nie powinny to być informacje dotyczące „ścisłego" życia prywatnego lub takie, które mogłyby łatwo prowadzić do dyskryminacji, a gdy tego rodzaju informacje już są zbierane – nie powinny być rozpowszechniane;

b) gromadzone informacje powinny ograniczać się do takich, jakie odpowiadają celowi, dla którego są zbierane, oraz jakie są w tej mierze niezbędne;

c) informacje nie powinny być uzyskiwane sposobami podstępnymi lub nieuczciwymi;

d) postanowienia powinny oznaczać, do jakiego momentu określone rodzaje informacji mogą być gromadzone lub wykorzystywane;

e) bez odpowiedniego upoważnienia informacje nie powinny być ani używane do innych celów niż te, dla których były zbierane, ani też udostępniane innym osobom;

f) zainteresowanym osobom powinno zasadniczo przysługiwać uprawnienie do uzyskania informacji o zbieranych na ich temat informacjach, o celu ich zbierania i szczegółach dotyczących ich wydawania;

g) powinno się bezwarunkowo zadbać o poprawianie informacji nieścisłych i usuwanie informacji przestarzałych lub uzyskanych w sposób bezprawny;

h) należy zastosować środki ostrożności zapobiegające niewłaściwemu lub podstępnemu wykorzystywaniu informacji; elektroniczne banki danych powinny być wyposażone w systemy zabezpieczające uniemożliwiające dostęp do nich osobom nieuprawnionym i służące wykryciu informacji utraconych oraz zniekształconych w sposób zamierzony lub niezamierzony;

i) zebrane dane powinny być dostępne tylko dla osób mających uzasadniony powód, by się z nimi zapoznać; personel obsługujący elektroniczny bank danych powinien podlegać regulaminowi zakładowemu, który zapobiegałby wszelkim przypadkom

[322] Resolution (73)22 on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in The Private Sector, Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Minister's Deputies.

[323] Resolution (74)29 on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Public Sector ,Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

nadużycia danych, a w szczególności postanowieniom o zachowaniu tajemnicy zawodowej;
j) dane statystyczne powinny być udostępniane tylko w formie zbiorczej i w sposób, który uniemożliwia łączenie tych informacji z określonymi osobami”[324].

Co prawda analiza Rezolucji nr 29 wskazuje na to, iż w wielu aspektach powtarza ona główne założenia wynikające z zasad sformułowanych w przedstawionej wyżej rezolucji, jednakże wprowadza również pewne uściślenia dotyczące zarówno granic czasowych obejmujących zbierania czy też wykorzystywania określonych kategorii danych, jak również zastrzega kto może zarządzać udostępnianymi informacjami tj. „osoby posiadające odpowiednią wiedzę w związku z wykonywaniem określonych funkcji zawodowych”[325].

Na szczególną uwagę zasługują także rezolucje wskazujące na nowe zagrożenia dla bezpieczeństwa danych osobowych związane z rozwojem technologicznym, tj. Rezolucja nr 3 w sprawie ochrony danych i prywatności w trzecim tysiącleciu (2010 r.)[326]; Rezolucja 1843 dotycząca ochrony prywatności i danych osobowych w Internecie i mediach internetowych (2011 r.)[327]; czy też Rezolucja 1986 dotycząca poprawy ochrony i bezpieczeństwa użytkowników w cyberprzestrzeni (2014 r.)[328].

Nie sposób pominąć znaczenia także tych rezolucji, które jedynie częściowo odnoszą się do bezpieczeństwa danych osobowych, jednak ze względu na szczególną kategorię spraw i kategorię danych, których dotyczą, zawierają istotne wskazówki, co do reguł postępowania. Przykładem może być Rezolucja 29(78), wskazująca na konieczność poufności indywidualnych zabiegów i nieujawnianie wzajemnie tożsamości biorcy i dawcy w związku z pobieraniem i przeszczepianiem tkanek i organów[329], czy też Rezolucja 3(95) dotycząca oceny zawodowej osób niepełnosprawnych, wskazująca m.in. iż dane zbierane dla oceny przydatności

[324] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz. 5. Wydanie,* Lex a Wolters Kluwer business, Warszawa 2011, s. 54-55.
[325] Tamże, s. 55.
[326] Resolution No. 3 on data protection and privacy in the third millennium, 30th Council of Europe Conference of Ministers of Justice, Istanbul, Turkey, 24-26 November 2010), MJU-30(2010) RESOL. 3E.
[327] Resolution 1843 (2011), The protection of privacy and personal data on the internet and online media, Parliamentary Assembly debate on 7 October 2011 (36th Sitting), Doc. 12695.
[328] Resolution 1986 (2014), Improving user protection and security in cyberspace, Parliamentary Assembly debate on 9 April 2014 (14th Sitting(, Doc. 13451).
[329] Resolution (78)29 on Harmonisation of Legislations of Member States Relating to Removal, Grafting and Transplantation of Human Substances, Adopted by the Committee of Ministers on 11 May 1978 at the 287th meeting of the Ministers' Deputies.

zawodowej niepełnosprawnych powinny podlegać tajemnicy zawodowej i medycznej oraz, że mogą być wykorzystywane wyłącznie w interesie niepełnosprawnych, za ich zgodą oraz do celów rehabilitacji zawodowej[330].

Brak mocy wiążącej standardów o charakterze tzw. „miękkiego prawa" wiąże się z tym, iż nie istnieją w tym przypadku żadne nakazy, których brak wykonania wiązałby się z nałożeniem na dane państwo członkowskie RE, określonych sankcji. Chodzi tu bardziej o wypracowanie, czy też dostosowanie określonych obszarów do standardów RE na zasadzie kompromisu oraz współpracy. Jednakże realizacja określonych zaleceń nieposiadających mocy wiążącej może także wynikać z samego członkostwa w tejże organizacji międzynarodowej i wynikających z tego względu zobowiązań przyjętych w momencie uzyskania członkostwa[331].

Standardy o charakterze „miękkiego prawa" mogą jednak zarówno inspirować powstanie standardów traktatowych (wtedy ich znaczenie jest przejściowe), jak też je uzupełniać (wtedy ich znaczenie jest trwałe, pod jednak warunkiem, że materia przez nie regulowana nie nadaje się do ujęcia w standardy traktatowe)[332].

Warto zaznaczyć, iż zalecenia Zgromadzenia Parlamentarnego często inspirują aktywność Komitetu Ministrów RE w zakresie kreowania standardów w dziedzinie ochrony danych osobowych. Jednak istnieją też przypadki gdy standardy o charakterze „miękkiego prawa" tworzone są bezpośrednio przez Zgromadzenie Parlamentarne, bowiem jego rola nie ogranicza się wyłącznie do inspirowania działań Komitetu Ministrów w formie zalecenia.

Komitet Ministrów Rady Europy do dziś przyjął szereg zaleceń w zakresie bezpieczeństwa danych osobowych. Ich celem jest interpretacja i wyjaśnienie zastosowania zasad ogólnych ochrony danych wynikających z Konwencji nr 108 w konkretnych przypadkach tj. w odniesieniu do danych szczegółowych dotyczących różnych sektorów i obszarów, w których odbywa się przetwarzanie danych wymagających szczególnej ochrony. W przeciwieństwie do Konwencji zalecenia te nie są wiążące dla państw członkowskich RE, jednak Komitet Ministrów może zażądać od nich poinformowania go o działaniach podjętych w odniesieniu do danego zalecenia[333].

[330] Resolution AP (95) 3 on a Charter on the Vocational Assessment of People with Disabilities, Adopted by the Committee of Ministers on 12 October 1995 at the 545th meeting of the Minister's Deputies.
[331] Por. W. Bańczyk, *„Miękkie prawo, ale prawo", czyli o obowiązku przestrzegania soft law,* „Internetowy Przegląd Prawniczy TB ŚP UJ" 2016, nr 1, s. 63.
[332] Zob. C. Mik, *Standardy Rady Europy dotyczące prasy,* „Palestra" 1993, nr 9-10, s. 97.
[333] Zob. artykuł 15 lit. b) Statutu Rady Europy, Londyn, 5.5.1949.

Na szczególną uwagę zasługują tu szczegółowe zalecenia przyjęte przez Komitet Ministrów w latach 80. i 90. XXI w., np. Zalecenie nr (81)1 dotyczące zautomatyzowanych medycznych banków danych[334], Zalecenie nr 10 (84) w sprawie rejestrów karnych[335], Zalecenie nr 20 (85) w sprawie ochrony danych wykorzystywanych dla celów marketingu bezpośredniego[336], Zalecenie nr 15(87) o ochronie danych osobowych wykorzystywanych w sektorze policji[337], czy Zalecenie nr 4 (95) w sprawie ochrony danych osobowych przetwarzanych w sektorze telekomunikacji[338].

Ostatnie z wymienionych zaleceń dotyczyło wyzwań wynikających z szerokiego wzrostu ilości danych osobowych generowanych z wykorzystaniem usług telekomunikacyjnych oraz danych przechowywanych przez operatorów w związku z rozwojem technologicznym, a zwłaszcza digitalizacją sieci. Zawarto w nim zasady ochrony danych oparte na Konwencji nr 108, a także te wynikające z gwarancji poszanowania życia prywatnego i tajemnicy łączności zgodnie z art. 8 Europejskiej Konwencji Praw Człowieka. Od momentu, kiedy zalecenie to zostało przyjęte nastąpiło wiele zmian związanych z rozwojem technologicznym i przetwarzaniem danych z wykorzystaniem Internetu. Dlatego działania na poziomie Rady Europy oparto na rozwiązywaniu powstających wyzwań wszechobecnego człowieka a zwłaszcza w kwestii przetwarzania jego danych osobowych w środowisku online a w szczególności dla ochrony jego prawa do prywatności. W związku z tym kolejne zalecenia przyjęte przez Komitet Ministrów Rady Europy dotyczyły konkretnych obszarów profilowania, wyszukiwarek online i serwisów społecznościowych[339].

[334] Recommendation No. R (81)1 of the Committee of Ministers to Member States on regulations for automated medical data banks (Adopted by the Committee of Ministers on 23 January 1981, at the 328th meeting of the Minister's Deputies).
[335] Recommendation No. R (84)10 of the Committee of Ministers to Member States on the Criminal Record and Rehabilitation of Convicted Persons, Adopted by the Committee of Ministers on 21 June 1984 at the 374th meeting of the Minister's Deputies.
[336] Recommendation No. R (85)20 of the Committee of Ministers to Member States on the Protection of Personal Data Used for the Purposes of Direct Marketing, Adopted by the Committee of Ministers on 25 October 1985 at the 389th meeting of the Minister's Deputies.
[337] Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Minister's Deputies.
[338] Recommendation No. R (95) 4 of the Committee of Ministers to Member States on the Protection of Personal Data in the Area of Telecommunication Service with Particular Reference to Telephone Service, Adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the Minister's Deputies.
[339] Zob. Recommendation No. R (97)5 on the Protection of Medical , 13 February 1997; Recommendation No. R (97)18 on the Protection of Personal Data Collected and Processed for Statistical Purposes, 30

W 2013 r. Komitet Ministrów przyjął Deklarację w sprawie zagrożeń dla praw podstawowych, wynikających ze śledzenia cyfrowego i innych technologii nadzoru[340]. Z kolei w 2015 r. wydał kompleksowe zalecenie, które zawiera zasady dotyczące przetwarzania danych osobowych w kontekście zatrudnienia[341].W zaleceniu tym Komitet dokonał przeglądu swojego poprzedniego zalecenia (89)2, biorąc pod uwagę nowe wyzwania przed którymi często stoją państwa członkowskie formułując swoje ustawodawstwo ze względu na nowe technologie informacyjne i komunikacyjne. Celem tego zalecenia było zapewnienie pracownikom przysługujących im praw do ochrony danych przy korzystaniu z nowych technologii informacyjnych i komunikacyjnych.

W dniu 28 marca 2019 r. Rada Europy wydała nowe zalecenie w sprawie ochrony danych związanych ze zdrowiem. W zaleceniu wzywa się wszystkie państwa członkowskie Rady Europy do podjęcia kroków w celu zapewnienia, aby zasady przetwarzania danych związanych ze zdrowiem (zarówno w sektorze publicznym, jak i prywatnym) określone w załączniku do zalecenia znalazły odzwierciedlenie w ich prawie i praktyce[342].

Większość zasad przetwarzania danych dotyczących zdrowia określonych w zaleceniu przypomina stanowisko zawarte w ogólnym rozporządzeniu UE o ochronie danych (RODO) oraz odpowiednie wytyczne wydane przez europejskie organy ochrony danych i Europejską Radę Ochrony Danych. W zaleceniu podano jednak pewne szczegółowe wytyczne dotyczące przetwarzania danych związanych ze zdrowiem, które są bardziej szczegółowe niż w niektórych aspektach i wykraczają poza wymogi RODO, jak opisano poniżej:

September 1997; Recommendation No. R (99) 5 for the Protection of Privacy on the Internet, 23 February 1999, Recommendation No. R (2002)9 on the Protection of ersonal Data Collected and Processed for Insurance Purposes, 18 September 2002; Recommendation CM/Rec (2010)13 of the Committee of Ministers to member states on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, 23 November 2010; Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines; Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services; Recommendation CM/Rec (2012)

[340] Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers Deputies).

[341] Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.

[342] Zob. *Council of Europe issues recommendation on health – related data,* źródło: www.insideprivacy.com/uncategorized/council-of-europe-issues-resommendation-on-health-related-data, data dostępu: 03.01.2020.

- **Dane genetyczne**. W zaleceniu przewidziano, że dane genetyczne powinny być gromadzone wyłącznie z zastrzeżeniem odpowiednich zabezpieczeń, jeżeli jest to określone przez prawo lub na podstawie zgody (z wyjątkiem przypadków, gdy taka zgoda jest prawnie wykluczona). Dane genetyczne wykorzystywane do profilaktycznej opieki zdrowotnej, diagnozy lub leczenia pacjentów lub badań naukowych powinny być wykorzystywane wyłącznie do tych celów lub w celu umożliwienia osobom zainteresowanym wynikami testów genetycznych podjęcia świadomej decyzji w tych sprawach. Dane genetyczne wykorzystywane w kontekście zatrudnienia, do celów ubezpieczenia oraz do postępowań sądowych lub dochodzeń są szczególnie przywoływane jako obszary wymagające dalszego rozważenia przez państwa członkowskie przepisów prawnych w celu zapewnienia odpowiednich zabezpieczeń.
- **Udostępnianie danych związanych ze zdrowiem do celów dodatkowych.** W odniesieniu do udostępniania danych związanych ze zdrowiem do celów innych niż świadczenie opieki zdrowotnej i administrowanie nią, zalecenie stanowi, że tylko odbiorcy upoważnieni przez prawo powinni mieć dostęp do danych związanych ze zdrowiem, bez wzmianki o zgodzie pacjenta jako sposobu legitymizacji takiego dostępu. Ta pozycja jest potencjalnie bardziej restrykcyjna niż obecne podejście na mocy RODO, w którym osoby trzecie nieuczestniczące w zapewnieniu opieki zdrowotnej pacjentom (takim jak instytucje badawcze lub akademickie lub formy komercyjne) mogą otrzymywać dane dotyczące zdrowia, o ile robią to zgodnie z RODO. W zaleceniu stwierdzono także, że odbiorcy danych związanych ze zdrowiem muszą podlegać zasadom poufności obowiązującym pracownika służby zdrowia (lub równoważnego), chyba że prawo zapewnia inne zabezpieczenia.
- **Badania naukowe.** W zaleceniu zastosowano kontekstowe podejście do badań naukowych, przewidując, że potrzebę przetwarzania danych związanych ze zdrowiem do celów badań naukowych należy porównać z ryzykiem dla osoby, której dane dotyczą i dla ich rodziny biologicznej, jeśli w grę wchodzą dane genetyczne). W przeciwieństwie do RODO zalecenie nie kwalifikuje automatycznie badań naukowych jako zgodnych z pierwotnymi celami dla których dane zostały zgromadzone. Zgodnie z ogólną zasadą dane związane ze zdrowiem powinny być przetwarzane wyłącznie do celów badawczych, jeżeli osoba, której dane dotyczą, wyraziła zgodę, chyba że prawo stanowi, że dane dotyczące zdrowia mogą być przetwarzane bez zgody. Osobom należy

również zapewnić przejrzyste i zrozumiałe informacje na temat projektu badawczego. W zaleceniu dodano, że warunki, w których dane dotyczące zdrowia są przetwarzane na potrzeby badań naukowych, muszą zostać ocenione, w razie potrzeby, przez właściwy niezależny organ, tai jak komisja etyczna, a takie projekty badawcze powinny podlegać zabezpieczeniom określonym w prawie.

- **Cyfrowe zdrowie.** Szereg zasad zawartych w zaleceniu ma wyraźne znaczenie dla cyfrowych aplikacji zdrowotnych, w szczególności dotyczących sztucznej inteligencji, uczenia maszynowego i urządzeń mobilnych. W zaleceniu przewidziano, że systemy przechowujące dane dotyczące zdrowia powinny być „audytowalne" co oznacza, że powinna istnieć możliwość śledzenia dostępu, modyfikacji i działań przeprowadzonych w systemie informatycznym, aby można było zidentyfikować autora. Zalecenie zachęca także do przyjęcia „ram odniesienia" które są skoordynowanym zbiorem zasad i najnowocześniejszych procesów dostosowanych do praktyki i mających zastosowanie do systemów informacji zdrowotnych, obejmujących obszary interoperacyjności i bezpieczeństwa, które powinny mieć zastosowanie do systemów informatycznych lub przetwarzania danych związanych ze zdrowiem. Zalecenia wyraźnie wspominają także specjalistów, którzy nie są bezpośrednio zaangażowani w zapewnienie indywidualnej opieki zdrowotnej nad pacjentem, ale mogą mieć dostęp do danych związanych ze zdrowiem, aby zapewnić „sprawne działanie systemów informatycznych". Tacy specjaliści muszą w pełni przestrzegać tajemnicy zawodowej i wymogów bezpieczeństwa danych.

- **Prawa osób fizycznych.** Zalecenie stanowi, że osoby powinny mieć prawo do informacji i sprawowania kontroli nad sowimi danymi dotyczącymi zdrowia i danymi genetycznymi, zgodnie z RODO. Istnieją jednak trzy obszary odchyleń:

1) osoby powinny mieć prawo *nie* być informowanym o diagnozach medycznych lub wynikach badań genetycznych, ponieważ mogą mieć własne powody, dla których nie chcą wiedzieć, z zastrzeżeniem ograniczonych wyjątków, w których muszą być informowani przez prawo;

2) gdy osoby wycofują się z projektu badań naukowych, należy poinformować że ich dane dotyczące zdrowia przetwarzane w kontekście tych badań zostaną zniszczone lub zanonimizowane w sposób, który nie zagraża naukowej ważności badań;

3) osoby powinny mieć prawo do otrzymania informacji na temat uzasadnionego przetwarzania danych obejmującego dane związane ze zdrowiem, w przypadku gdy stosuje się do nich wyniki takiego przetwarzania, szczególnie jeśli dotyczy to profilowania.

Przedstawione zalecenia stanowią grupę o charakterze niekonwencyjnym, nie mającym, zatem mocy prawnej konwencji, jako aktu prawa międzynarodowego. Stanowią wiec instrumenty w przypadku, których do ich obowiązywania nie jest konieczny żaden akt przystąpienia. Z chwilą, bowiem przyjęcia ich przez odpowiedni organ RE, rozpoczyna się ich „życie" prawne. Wiążą one więc państwo członkowskie już od momentu ich przyjęcia, ale jest to związanie słabsze, właśnie o charakterze „miękkiego prawa".

Nie ulega wątpliwości, iż Rada Europy znacząco przyczynia się do aktywnej globalnej harmonizacji w obszarze ochrony danych osobowych. *Dzień ochrony danych* jest obchodzony w Europie od 2007 r.[343], ale także poza nią tj. w USA i Kanadzie[344]. Uwidacznia się tu zasadniczo proaktywana rola Rady Europy, która zaprasza państwa nie członkowskie do przystąpienia do Konwencji nr 108 i jej protokołu dodatkowego. Kraje na całym świecie są proszone o ratyfikowanie tego dokumentu[345]. Rada Europy szczególnie w ostatnich latach promowała także korzyści wynikające z globalnego przystąpienia UE do Konwencji[346], z kolei Urugwaj był pierwszym krajem pozaeuropejskim, który przystąpił do Konwencji w 2013 r.[347]

3.3. Mechanizmy egzekwowania standardów dotyczących bezpieczeństwa danych osobowych w państwach członkowskich

Za najbardziej skuteczne mechanizmy egzekwowania standardów dotyczących bezpieczeństwa danych osobowych w państwach członkowskich Rady Europy uznaje

[343] Ministers' Deputies Decisions, CM/Del/Dec(2006)962, Decisions adopted 2.5.2006.
[344] Zob. *Council of Europe, Data Protection Day,* źródło: www.coe.int/t/dghl/standardsetting/dataprotection/Data, data dostępu: 12.09.2018.
[345] Zob. np. Resolution calling for the Organisation of an intergovernmental Conference with a view to developing a binding International instrument on privacy and the protection of personal data, International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 27-29.10.2010.
[346] Zob. N. Gumzej, *The Council of Europe…,* s. 18.
[347] Tamże.

się procedurę akcesyjną, w ramach której państwa przygotowują się do realizacji standardów umożliwiających członkostwo w RE[348], a także procedurę monitoringową stwarzającą możliwość oceny w jakim stopniu państwa wywiązują się z przyjętych zobowiązań w momencie przystąpienia[349]. Lista tych zobowiązań formułowana jest przez Komitet Ministrów, natomiast podstawę do ich stworzenia stanowi uchwała Zgromadzenia Parlamentarnego zalecająca członkostwo. Jednym z nich jest zapewnienie prawa do prywatności obejmującego ochronę danych osobowych. Warto przy tym zauważyć, iż obecnymi stronami Konwencji nr 108 jest 47 państw członkowskich Rady Europy oraz Mauritius, Senegal, Tunezja i Urugwaj, natomiast Argentyna, Burkina Faso, Cap Verde, Meksyk i Maroko zostały zaproszone do przystąpienia do traktatu. Wiele innych krajów wykorzystało go jako wzór dla nowych przepisów dotyczących ochrony danych osobowych[350].

2.3.1. Procedura akcesyjna

Transformacja polityczna w Europie Środkowej i Wschodniej zapoczątkowana ruchem „Solidarności" w Polsce i upadkiem muru berlińskiego przyniosła dla Rady Europy nową sytuację, na którą Organizacja w istocie nie była przygotowana. Państwa Europy Środkowej i Wschodniej pragnęły jak najszybciej włączyć się w nurt integracji europejskiej[351]. Przede wszystkim zależało im na integracji gospodarczej ze Wspólnotami Europejskimi, w nich upatrując możliwości rozwoju gospodarczego i podniesienia stopy życiowej dla mieszkańców. Z uwagi na stan ich gospodarki oraz prawa ją regulującego, Wspólnoty – a później Unia Europejska – nie były skore do szybkiego rozszerzenia członkostwa. W zamian proponowano państwom umowy stowarzyszeniowe ze Wspólnotami oraz możliwość szybszej integracji politycznej w

[348] Zob. B. Bowring, *Russia's Accession to the Council of Europe and human rights. Four years on,* "Helsinki Monitor" 2000, vol. 11, s. 53-72.
[349] Por. Ch. Altenhoener, *Review of the Monitoring Process of the Council of Europe Framework Convention for the Protection of National Minorities,* "European Yearbook of Minority Issues" 2012, Vol. 9, s. 549-564.
[350] Zob. *Council of Europe modernises Convention 108,* źródło: www.privacylaws.com/Publications/enews/International=E-news-Dates/2018/5/Council-of-Europe-modernises-Convention-108/, data dostępu: 14.09.2018.
[351] Por. I. Miedzińska, *Polska w systemie ochrony praw człowieka Rady Europy,* [w:] *Konstytucja w dobie europejskich wyzwań,* red. M. Zubik, A. Paprocka, R. Puchta, „Legislator", Warszawa 2010, s. 101 – 118.

ramach Rady Europy[352]. RE właściwie entuzjastycznie podchodziła do możliwości rozszerzenia członkostwa upatrując w tym nadzieję na realizację pierwotnych zamierzeń – stworzenia organizacji obejmującej cały kontynent europejski[353], a także podniesienia własnej rangi w społeczności międzynarodowej i europejskiej[354]. Ambicje Rady Europy, pierwszej dużej organizacji europejskiej, sięgały dalej aniżeli pozostawianie w cieniu Wspólnot Europejskich, organizacji o węższym członkostwie, ale bardziej dynamicznych i dysonujących dalej idącymi kompetencjami, w które wyposażyły je państwa członkowskie[355].

Przystąpienie do Rady Europy wymagało przejścia procedury akcesyjnej, w trakcie której dokonywano oceny spełnienia przez kandydatów warunków członkostwa[356]. W ramach starań o przyjęcie do organizacji, państwa Europy Środkowej i Wschodniej skłonne były przyjmować na siebie dodatkowe zobowiązania związane z akcesją[357]. Przyjęcie zobowiązania międzynarodowego nie jest równoznaczne z jego późniejszym faktycznym wykonaniem, dlatego powstała wkrótce kwestia, w jaki sposób można kontrolować wypełnianie przez nowe państwa członkowskie zobowiązań akcesyjnych[358]. Zaczęto więc w latach 90- tych tworzyć nowe procedury kontrolne w ramach organizacji, niektóre początkowe nastawione wyłącznie na kontrolowanie nowych państw członkowskich, a niektóre – bardziej demokratyczne – od razu na

[352] Zob. B. Podgórski, *Rola Rady Europy w procesie integracji europejskiej,* [w:] *Efektywność europejskiego systemu ochrony praw człowieka. Efektywność mechanizmów ochrony praw człowieka Rady Europy, Unii Europejskiej i OBWE,* red. J. Jaskiernia, t. 2, Wydawnictwo Adam Marszałek, Toruń 2012, s. 11- 44.

[353] Zob. M. Indan-Pykno, *Współpraca Rady Europy oraz Unii Europejskiej w zakresie ochrony praw człowieka,* [w:] *Prawa człowieka wczoraj i dziś. W 60. rocznicę powstania Rady Europy oraz 20 – lecia przyjęcia Konwencji Praw Dziecka,* UAM, Toruń 2010, s. 27 – 38.

[354] Zob. M. Nowotka, *Współpraca między Unią Europejską a Radą Europy w kontekście ochrony praw człowieka w Europie,* [w:] *Państwo i prawo wobec współczesnych wyzwań. Integracja Europejska i stosunki międzynarodowe. Księga jubileuszowa Profesora Jerzego Jaskierni,* red. R.M. Czarny, K. Spryszak, t. V, Wydawnictwo Adam Marszałek, Toruń 2012, s. 213 – 226.

[355] Zob. P. Filipek, *Geneza i ewolucja monitoringu Zgromadzenia…,* s. 67.

[356] Zob. E. Denkiewicz, *Płaszczyzny oddziaływania Rady Europy na przemiany systemowe w Federacji Rosyjskiej – wpływ Europejskiej Konwencji Praw Człowieka oraz Europejskiego Trybunału Praw Człowieka na zmiany systemu prawnego w Rosji,* [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989 – 2009,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2010, s. 718 – 734.

[357] Zob. K. Gawkowski, *Wpływ Rady Europy na rozwój samorządności terytorialnej,* [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989 – 2009,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2010, s. 542 – 552.

[358] Zob. P.A. Świtalski, *Miejsce Rady Europy w Europejskiej architekturze instytucjonalnej,* [w:] *Sześćdziesiąt lat Rady Europy. Tworzenie i stosowanie standardów prawnych,* red. H. Machińska, Oficyna Prawa Polskiego, Warszawa 2009, s. 29.

wszystkie państwa członkowskie[359]. W takich okolicznościach powstały procedury monitoringowe Zgromadzenia Parlamentarnego oraz Komitetu Ministrów RE[360]. Jako pewne ich uzupełnienie można traktować powołaną do życia w 1999 r. instytucję Komisarza Praw Człowieka Rady Europy[361].

Procedura akcesyjna Rady Europy zaczęła wiązać się z wymogami związanymi z uzyskaniem członkostwa zawartymi w jej Statucie. Co prawda zapisy te w początkowej fazie uznawano za zbyt generalne, jednakże do ich konkretyzacji doszło za sprawą Deklaracji Wiedeńskiej Szefów Państw i Rządów z 1993 r.[362] Ustalono wówczas kryteria progowe, jakie państwa ubiegające się o członkostwo muszą spełniać aby mogły uzyskać miano pełnoprawnego członka RE[363].

W świetle Deklaracji Wiedeńskiej z 1993 r. przystąpienie do RE zakłada, że „państwo aplikujące dostosowało swoje instytucje i system prawny do podstawowych zasad demokracji, rządów prawa i poszanowania praw człowieka. Przedstawiciele społeczeństwa muszą być wybierani w drodze wolnych i uczciwych wyborów, opartych na powszechnym prawie do głosowania. Zagwarantowana swoboda wypowiedzi, przestrzeganie zasad prawa międzynarodowego muszą pozostać, w naszej opinii, decydującym kryterium oceny każdego wniosku o członkostwo. Równie fundamentalnym jest podpisanie Europejskiej Konwencji Praw Człowieka i przyjęcie w całości, w krótkim okresie, mechanizmów nadzoru, określanych w Konwencji. Jesteśmy zdecydowani zapewnić pełne poszanowanie zobowiązań przyjętych przez wszystkie państwa członkowskie Rady Europy”[364].

W praktyce obowiązuje następująca procedura przyjmowania nowych członków. Wniosek o przyjęcie składa się sekretarzowi generalnemu Rady, który przekazuje go Komitetowi Ministrów. Po przeprowadzeniu dyskusji w tym organie wniosek trafia do

[359] Zob. J. Jaskiernia, *Wpływ Rady Europy na jedność aksjologiczną systemu prawa w rozwijających się państwach demokratycznych Europy,* [w:] *Jedność aksjologiczna systemu prawa w rozwijających się państwach demokratycznych Europy,* red. L. Stadniczeńko, Uniwersytet Opolski, Opole 2011, s. 85 - 109.
[360] Zob. M. Lewoc, *Ocena stanu realizacji przez Polskę Zaleceń Komitetu Ministrów Rady Europy,* „Probacja” 2009, nr 2, s. 59 – 71.
[361] Zob. M. Heinze, *Poszukiwanie nowych instrumentów ochrony praw człowieka przez Radę Europy, Organizację Bezpieczeństwa i Współpracy w Europie i Unię Europejską,* [w:] *Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania,* red. J. Jaskiernia, t. 1, Wydawnictwo Sejmowe, Warszawa 2014, s. 458.
[362] Declaration of the Council of Europe’s First Summit (Vienna, 9 October 1993), źródło: www.cvce.eu/en/obj/declaration, data dostępu: 14.09.2018.
[363] Zob. J.G. Stegen, *The Parliamentary Assembly of the Council of Europe and its Relations with Central and Eastern Europe,* [w:] *Working Paper on Comparative Legislative Studies,* red. L.D. Longley, Appleton 1994, s. 408.
[364] Declaration on the Council…, jw.

Zgromadzenia Parlamentarnego. Wyznacza ono sprawozdawców, którzy wizytują dane państwo i przeprowadzają rozmowy z przedstawicielami rządu, parlamentu, partii politycznych, grup społecznych, wymiaru sprawiedliwości oraz badają obowiązujące prawo. Przedstawione przez nich wnioski są omawiane przez odpowiednie komisje Zgromadzenia. Cała ta procedura służy ustaleniu, czy dane państwo odpowiada kryteriom demokracji. Jeśli ocena jest pozytywna, Zgromadzenie uchwala rekomendacje w sprawie przyjęcia danego państwa. Ostateczną decyzję o przyjęciu podejmuje Komitet Ministrów. 2 lutego 1995 r. Zgromadzenie postanowiło zawiesić procedurę rozpatrywania wniosku o przyjęcie Rosji do Rady, ze względu na pogwałcenie przez ten kraj w czasie konfliktu w Czeczenii podstawowych praw człowieka i zasad humanitarnych. W czerwcu 1995 r. w Moskwie i w Czeczenii przebywała podkomisja praw człowieka Zgromadzenia. W sierpniu tegoż roku, w tych samych miejscach, przebywał sprawozdawca Zgromadzenia w sprawie wniosku o przyjęcie Rosji. Na podstawie tych sprawozdań, wskazujących na złagodzenie wcześniejszych rygorów i naruszeń praw człowieka, Komisja spraw politycznych zaproponowała Zgromadzeniu podjęcie na nowo postępowania. Inne stanowisko zajęła Komisja spraw prawnych i praw człowieka. We wrześniu 1995 r. po dość burzliwej dyskusji, Zgromadzenie podjęło postępowanie, a następnie na sesji, w styczniu 1996 r., wyraziło pozytywną opinię w sprawie wniosku Rosji, co mogło stać się podstawą do skierowania przez Komitet Ministrów formalnego zaproszenia Rosji. Opinia Zgromadzenia, trzeba zaznaczyć, nie była bezkrytyczna, skoro jej merytoryczna część zaczynała się od sów: „Zgromadzenie stwierdza, że podtrzymywane są reformy polityczne, prawne i gospodarcze. System prawny nadal wykazuje niedociągnięcia…”[365].

System aksjologiczny Rady Europy w obszarze bezpieczeństwa danych osobowych wynika zarówno z Konwencji nr 108 jak i z innych dokumentów tj. EKPC. Dlatego działanie obejmujące przystąpienie do EKPC, wiążące się z uzyskaniem członkostwa w RE a następnie podjęcie decyzji o przystąpieniu do Konwencji nr 108 przybliżyło wiele państw do jednego z celów organizacji jakim stała się ochrona prywatności obejmująca w późniejszym czasie ochronę danych osobowych. Nastąpiło wówczas upowszechnienie konwencji, które wprowadziły w państwach członkowskich

[365] Zob. H. Ognik, *Rada Europy,* [w:] *Europejskie struktury współpracy. Informator,* red. S. Parzymies, Polski Instytut Spraw Międzynarodowych, Warszawa 1995, s. 58.

nowy porządek międzynarodowy w dziedzinie ochrony praw człowieka, w tym ochrony danych. Umożliwiło to początkowo sięganie po standardy zawarte w art. 8 EKPC a następnie po te zawarte w Konwencji nr 108 jako po źródło obowiązujących standardów międzynarodowych, tak bardzo istotnych dla ochrony prawa do prywatności jednostki w tak różnych dziedzinach życia społecznego[366].

Zagwarantowanie prawa do prywatności znalazło się zatem wśród kryteriów otrzymania członkostwa w Radzie Europy, co otworzyło możliwość Zgromadzeniu Parlamentarnemu monitorowania stanu ochrony tego prawa w państwach zabiegających o członkostwo w RE.

2.3.2. Procedura monitoringowa

Kolejnym ważnym mechanizmem egzekwowania standardów dotyczących bezpieczeństwa danych osobowych w państwach członkowskich jest procedura monitoringowa. Stanowi ona konsekwencję zobowiązań podjętych przez państwo z chwilą uzyskania członkostwa w Radzie Europy i ma miejsce pomimo tego, że państwa te posiadają konstytucyjną autonomię, będącą konsekwencją ich suwerenności[367].

Pośród mechanizmów monitorowania bezpieczeństwa danych osobowych w systemie Rady Europy należy dostrzec instrumenty znajdujące się w dyspozycji Komitetu Ministrów, będącego organem kierowniczym tej organizacji międzynarodowej, a także podległych mu organów współpracy międzyrządowej[368].

Instrumenty kontrolne Komitetu Ministrów, w aktualnym ich kształcie, zostały zainicjowane wraz z deklaracją tego organu „w sprawie przestrzegania zobowiązań przyjętych przez państwa członkowskie Rady Europy", przyjętą przez Komitet Ministrów podczas 95. posiedzenia w dniu 10 listopada 1994 r. Na mocy art. 1 deklaracji „sprawy dotyczące poszanowania zobowiązań odnoszących się do warunków demokracji, praw człowieka i rządów prawa w państwach członkowskich" mogą być przedkładane Komitetowi Ministrów przez jedno lub kilka państw członkowskich,

[366] Zob. K. Czarnecki, *Ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych,* [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X – lecie polskiej ustawy i ochronie danych osobowych,* red. G. Góździewicz, M. Szabłowska, TNOiK, Toruń 2008, s. 189 – 196.
[367] Zob. A. Drzemczewski, *Monitoring by the Committee of Ministers of the Council of Europe: A Useful 'Human Rights' Mechanisms?,* "Baltic Yearbook of International Law Online" 2002, Vol. 2, s. 83-103.
[368] Tamże, s. 86.

Sekretarza Generalnego lub na podstawie zalecenia Zgromadzenia Parlamentarnego Rady Europy". W ramach takiego rozpatrywania Komitet Ministrów uwzględniać będzie „wszelkie odnośne informacje pochodzące z różnych źródeł, takich jak Zgromadzenie Parlamentarne i KBWE (obecnie – OBWE). W świetle art. 4 deklaracji Komitet Ministrów może „w sprawach wymagających konkretnych działań": zwrócić się do Sekretarza Generalnego o nawiązanie kontaktów, zbieranie informacji i formułowanie rad; wydać opinię lub zalecenie; przedłożyć komunikat Zgromadzeniu Parlamentarnemu; podjąć inne decyzje w ramach statutowych uprawnień[369]. Postanowienie to kryje w sobie szereg możliwości, skoro podjęcie „konkretnych działań może oznaczać zarówno zbieranie informacji, jak również zawieszenie członkostwa danego państwa w Radzie Europy. Początkowo Komitet Ministrów niechętnie korzystał z tego uprawnienia. Postanowienie to zostało zastosowane dopiero w listopadzie 1999 r. i czerwcu 2000 r. w kwestiach dotyczących „funkcjonowania i ochrony instytucji demokratycznych", oraz „wolności słowa i informacji". W dniu 26 czerwca 2000 r. sekretarz generalny RE, Walter Schwimmer zwrócił się do Komitetu Ministrów w sprawie sytuacji w Czeczenii (Federacja Rosyjska). Natomiast w 2001 r. użyto po raz pierwszy procedury, na mocy której – przed udzieleniem odpowiedzi Zgromadzeniu Parlamentarnemu – wysłana została misja Sekretariatu w celu zebrania informacji o sytuacji politycznej w danym państwie. Miało to miejsce w odniesieniu do dwóch państw członkowskich – Ukrainy i Gruzji[370].

Warto zaznaczyć, iż ustanowienie procedury monitoringowej Komitetu Ministrów nastąpiło już po wprowadzeniu tej procedury w Zgromadzeniu Parlamentarnym. To, że wymieniam ją w pierwszej kolejności wynika z najważniejszej pozycji Komitetu Ministrów w RE, a w konsekwencji z wag decyzji podejmowanych przez ten organ. Należy wszakże już w tym miejscu zaznaczyć, że monitoring prowadzony przez Zgromadzenie Parlamentarne ma niewątpliwie ważniejsze znaczenie, a – co jest szczególnie ważne – ma charakter otwarty, gdyż raporty Zgromadzenia są publicznie ogłaszane. Natomiast monitoring podejmowany przez Komitet Ministrów ma

[369] Council of Europe Committee of Ministers Declaration on Compliance with Commitments (Adopted by the Committee of Ministers on 10 November 1994 at its 95th Session).
[370] A. Drzemczewski, *Procedura monitoringowa Komitetu Ministrów a Rada Europy. Użyteczny mechanizm „praw człowieka",* [w:] *Polska w Radzie Europy. 10 lat członkostwa – wybrane zagadnienia,* red. H. Machińska, Ośrodek Informacji Rady Europy, Centrum Europejskiego Uniwersytetu Warszawskiego, Warszawa 2002, s. 59.

charakter procedury poufnej, co w istotny sposób ogranicza jego oddziaływanie na europejską opinię publiczną.

A. Drzemczewski wskazuje na walory tej procedury tj.:

„1) komplementarność z pracami podejmowanymi przez Zgromadzenie Parlamentarne;
2) zbieranie informacji przez Sekretariat, jeśli tylko ma charakter profesjonalny, może zapewnić Komitetowi Ministrów o wiele lepszy i bardziej dokładny obraz sytuacji w danym kraju, co nie jest możliwe w tym samym stopniu w przypadku podejmowania decyzji w oparciu o informacje zbierane w Strasburgu oraz na podstawie informacji zwrotnych o postępach we współpracy miedzynarodowej;
3) misje Sekretariatu umożliwiają danemu państwu podjęcie środków naprawczych na podstawie aktualnych informacji pozyskanych z różnych źródeł – w powiązaniu ze wsparciem, na przykład, w postaci tworzenia lub dostosowywania programów współpracy Rady Europy z ewentualnym dodatkowym „wkładem", jakim może być obecność RE w danym państwie"[371].

Jedną z cech procedury monitoringowej Komitetu Ministrów jest jej przedmiotowy charakter[372]. Badaniu poddawane są bowiem określone grupy zagadnień[373], a nie państwa jako takie. Podejmowany przez Komitet Ministrów monitoring dotyczy więc wszystkich państw członkowskich, zarówno „starych" przyjętych przed 1989 r., jak i „nowych", przyjętych po tym terminie. Natomiast monitoring realizowany przez Zgromadzenie Parlamentarne podejmowany jest w zasadzie jedynie w stosunku do państw nowoprzyjętych, choć od tej zasady mogą być wyjątki.

Monitoring realizowany przez Komitet Ministrów odgrywa niewątpliwie istotną rolę w procesie kontroli wdrażania standardów demokratycznych RE w dziedzinie bezpieczeństwa danych osobowych. Problematyka ta wielokrotnie poddawana była kontroli z zastosowaniem tej procedury. Podniosło to jej rangę pośród zagadnień rozwoju europejskiego, które podejmuje Komitet Ministrów. Ważną cechą tej procedury jest to, że nie jest ona zawężona jedynie do „nowych członków", a więc

[371] Tamże, s. 65-66.
[372] Zob. J. Jaskiernia, *Funkcje Konstytucji RP w dobie integracji europejskiej i radykalnych przemian politycznych*, Wydawnictwo Adam Marszałek, Toruń 2020, s. 275.
[373] Zob. J. Chrzanowska, *Problematyka tymczasowego aresztowania w praktyce Komitetu Ministrów Rady Europy (art. 46 EKPC),* [w:] *Przewlekłość tymczasowego aresztowania w Polsce w świetle europejskich standardów ochrony praw człowieka,* red. P. Turek, Prokuratura Generalna, Warszawa 2013, s. 36.

państw, które stały się członkami RE po 1989 r.[374], a ma charakter obejmujący wszystkich członków RE. Jest to istotna przesłanka dla stwierdzenia, że system aksjologiczny RE, zmaterializowany w kreowanych przez nią międzynarodowych standardach prawnych, podlega implementacji w sposób ciągły i na całym obszarze oddziaływania RE, a nie może być zawężony tylko do procesu akcesyjnego i fazy uzyskania członkostwa.

Jednym z poważnych mankamentów tej procedury jest z kolei to, iż posiada ona charakter poufny. Choć nie należy lekceważyć tej formy współpracy międzyrządowej i pozytywnych konsekwencji, jakie niesie ona dla przekształcania rzeczywistości ustrojowej w państwach członkowskich, m.in. w dziedzinie ochrony danych osobowych, to jednak taka poufność ogranicza, a nieraz nawet uniemożliwia dostęp europejskiej opinii publicznej do wyników tej procedury. Tymczasem efektywność oddziaływania RE jest wprostproporcjonalna do tego, na ile europejska opinia dostrzega tę działalność i przywiązuje do niej wagę. Obok bowiem sankcji natury wewnątrzorganizacyjnej, stosowanych zresztą bardzo ostrożnie w działalności Komitetu Ministrów, najistotniejsze może być napiętnowanie ze strony europeskiej opinii publicznej w oparciu o ustalenia wynikające z procedur kontroli wdrażania standardów demokratycznych wykreowanych przez RE.

Obok procedury monitoringowej podejmowanej przez Komitet Ministrów RE, istotną rolę w monitorowaniu bezpieczeństwa danych osobowych odgrywa ustanowiony przez Konwencję nr 108, Komitet Konsultacyjny składający się z przedstawicieli Stron Konwencji uzupełnionych przez obserwatorów z innych państw (członków lub osób niebędących członkami) i organizacji międzynarodowych. Jest on odpowiedzialny za interpretację przepisów oraz poprawę implementacji Konwencji. Jego rola polega także na sporządzaniu sprawozdań, wytycznych i zasad przewodnich w obszarze ochrony danych osobowych[375].

Generalnie można stwierdzić, że działania Rady Europy w zakresie ochrony danych osobowych miały charakter pionierski w skali europejskiej. Wynikało to stąd, że ochrona danych osobowych ma istotne znaczenie w systemie aksjologicznym tej organizacji międzynarodowej. Charakterystyczne jest to, że RE zaoferowała w tej

[374] Zob. *Vade-mecum on the Committee of Ministers monitoring Procedure,* Document prepared by the Secretary General's Monitoring Unit, Strasbourg – 1 March 1999, s. 3.
[375] Zob. *Consultative Committee,* źródło: www.coe.int/en/web/data-protection/consultative-committee-tpd, data dostępu: 14.09.2018.

dziedzinie nie tylko instrumenty o charakterze prawnie wiążący cym (na szczególne wyeksponowanie zasługuje tu konwencja nr 108 o o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych), ale też o charakterze tzw. miękkiego prawa (zwłaszcza zalecenia Komitetu Ministrów). Mogła w tej sytuacji elastycznie reagować na nowe typy zagrożeń, jakie pojawiały się w obszarze ochrony praw człowieka wraz z rozwojem cywilizacyjnym.

Rozdział 3: Bezpieczeństwo danych osobowych w systemie Unii Europejskiej i mechanizmy jego realizacji w państwach członkowskich

3.1. Ogólna charakterystyka Unii Europejskiej

Utworzenie Unii Europejskiej nastąpiło w dniu 1 listopada 1993 r. na mocy traktatu o Unii Europejskiej (Traktat z Maastricht)[376]. UE stanowi dalszy etap w rozwoju wcześniej powstałych struktur tj. Europejskiej Wspólnoty Węgla i Stali (EWWiS), jak również Europejskiej Wspólnoty Energii Atomowej (EURATOM) i Europejskiej Wspólnoty Gospodarczej (EWG)[377].

Na mocy traktatu z Maastricht Unię utworzyło 12 państw: Belgia, Dania, Francja, Grecja, Hiszpania, Holandia, Irlandia, Luksemburg, Niemcy, Portugalia, Wielka Brytania, Włochy[378]. Dało to zasadniczy impuls do tego by w kolejnych latach do Unii przystąpiły kolejne państwa, tj. w 1995 r. Austria, Finlandia i Szwecja; w 2004 r. Cypr, Czechy, Estonia, Litwa, Łotwa, Malta, Polska, Słowacja, Słowenia i Węgry[379]; w 2007 r. Bułgaria i Rumunia[380], oraz w 2013 r. Chorwacja[381].

Za podstawę prawną polityki rozszerzenia UE uznaje się art. art. 49 Traktatu o Unii Europejskiej, stanowiący, iż: „*Każde państwo europejskie, które szanuje wartości, o których mowa w artykule 2, i zobowiązuje się je wspierać, może złożyć wniosek o członkostwo w Unii. O wniosku tym informuje się Parlament Europejski i parlamenty narodowe. Państwo ubiegające się o członkostwo kieruje swój wniosek do Rady, która stanowi jednomyślnie po zasięgnięciu opinii Komisji oraz po otrzymaniu zgody Parlamentu Europejskiego, udzielonej większością głosów jego członków. Brane są pod*

[376] Traktat o Unii Europejskiej podpisany 7 lutego 1992 r. w Maastricht, wszedł w życie 1 listopada 1993 r. (Dz.U. z 2004 r. Nr 90, poz. 864/30.
[377] Por. J. Szymańska, *Reformy na jubileusz: Unia Europejska w 50. i 60. rocznicę podpisania traktatów rzymskich,* „Sprawy Międzynarodowe" 2017, nr 4, s. 112.
[378] Zob. S. Parzymies, *Unia Europejska od Maastricht do Lizbony. Polityczne aspekty aktywności,* Wydawnictwo Dialog, Warszawa 2012, s. 4.
[379] Zob. Ch. Hillion, *Rozszerzenie Unii Europejskiej – analiza prawna,* [w:] *Odpowiedzialność i legitymizacja Unii Europejskiej,* red. A. Arnull, D. D. Wincott, Wydawnictwo Sejmowe, Warszawa 2007, s. 367.
[380]Zob. M. Błaszczuk, *Rozszerzenie Unii Europejskiej – Bułgaria i Rumunia nowymi państwami członkowskimi,* „Wspólnoty Europejskie" 2006, nr 10, s. 3-11.
[381] Szerzej: P. Maldini, *Croatian Accession to the European Union: UE Democratization Potential and Issues of Democratic Consolidation,* [w:] *Croatia and the European Union. Changes and Development,* red. P. Maldini, D. Pauković, Routledge, London-New York 2016, s. 11.

uwagę kryteria kwalifikacji uzgodnione przez Radę Europejską. Warunki przyjęcia i wynikające z tego przyjęcia dostosowania w Traktatach stanowiących podstawę Unii są przedmiotem umowy między Państwami Członkowskimi a państwem ubiegającym się o członkostwo. Umowa ta podlega ratyfikacji przez wszystkie umawiające się państwa, zgodnie z ich odpowiednimi wymogami konstytucyjnymi"[382]..

W Traktacie amsterdamskim (TA) z 1997 r. starano się dokonać odpowiedzi na różnego rodzaju niedomagania instytucjonalne, jak również proceduralne Wspólnoty, które rozpoznano w momencie stosowania Traktatu z Maastricht[383]. Pewne ustalenia dotyczące systemu instytucjonalnego UE zostały zawarte w Protokole w sprawie instytucji w perspektywie poszerzenia UE[384], a także Deklaracji w sprawie organizacji i funkcjonowania Komisji Europejskiej. Przełożono jednak dokonanie kluczowej reformy instytucjonalnej na czas rozszerzenia UE[385].

W coraz wyższym stopniu państwa członkowskie Wspólnot stawały w obliczy konieczności rozpoczęcia prac nad skodyfikowanym katalogiem praw. Pewnym przełomem był rok 1999, gdy podczas szczytu Rady Europejskiej w Kolonii przywódcy państw członkowskich Unii oficjalnie zainicjowali proces przygotowanie skodyfikowanego katalogu praw podstawowych Unii Europejskiej. W celu sporządzenia projektu takiego katalogu powołano do życia specjalny Europejski Konwent składający się z przedstawicieli zarówno instytucji unijnych (Parlamentu oraz Komisji), jak i rządów państw członkowskich Unii.

Kolejnym krokiem w kierunku pogłębiania integracji europejskiej był szczyt Rady Europejskiej w Nicei (7-10 grudnia 2000 r.). Jego następstwem stało się opracowanie traktatu wprowadzającego zasadnicze zmiany w przepisach o charakterze instytucjonalnym[386]. Traktat Nicejski, bo o nim tu mowa, został podpisany w dniu 26 lutego 2001 r.[387]

---

[382] Treść Traktatu dostępna na: www.arslege.pl/wniosek-o-czlonkostwo-w-unii/k78/a11057, data dostępu: 17.10.2018.

[383] Szerzej: Ł. Szymczyk, *Wszedł w życie Traktat Amsterdamski,* „Wspólnoty Europejskie" 1999, nr 5, s. 4-10.

[384] Zob. G. Bernatowicz, *Traktat Amsterdamski a kwestia rozszerzenia Unii Europejskiej,* „Zeszyty Naukowe Wyższej Szkoły Zarządzania i Marketingu w Warszawie" 1998, nr 4, s. 8.

[385] Por. A. Przyborowska-Klimczak, *Prawne aspekty integracji europejskiej – rys historyczny,* [w:] *Prawo Unii Europejskiej. Zagadnienia systemowe,* red. J. Barcz, Wydawnictwo Prawio i Praktyka Gospodarcza, Warszawa 2002, s. 42.

[386] Por. J. Mokrosiński, *Reformy instytucji w Unii Europejskiej po „szczytach" w Nicei i Goteborgu,* 'Studia Europejskie Centrum Europejskie Uniwersytetu Warszawskiego" 2001, nr 2, s. 48.

[387] Traktat z Nicei zmieniający Traktat o Unii Europejskiej. Traktat ustanawiający Wspólnotę Europejską oraz niektóre związane z nim akty prawne, Nicea, 26.02.2001.

To właśnie podczas szczytu w Nicei został zatwierdzony a także podpisany tekst Karty Praw Podstawowych (KPP). Nie nadano jednak wówczas Karcie mocy prawnej, choć rzecz jasna jej znaczenie polityczne i tak było olbrzymie, a Europejski Trybunał Sprawiedliwości regularnie są na nią powoływał. Karta miała stać się częścią składową Traktatu ustanawiającego Konstytucję dla Europy, ale w związku z brakiem jego ratyfikacji na uzyskanie mocy prawnej musiała czekać jeszcze przez kilka kolejnych lat. 13 grudnia 2007 r. KPP – po drobnych modyfikacjach – dołączono do podpisanego wówczas Traktatu Lizbońskiego. Stanowi ona nie tyle jego część składowa, co odrębny dokument. Mocy prawnej KPP ostatecznie nabrała 1 grudnia 2009 r. gdy Traktat Lizboński – po dość długim procesie ratyfikacyjnym – wreszcie wszedł w życie[388].

Wraz z wejściem w życie Traktatu z Lizbony podstawę prawną Unii tworzą dwa traktaty (art. 1 akapit trzeci TUE i art. 1 ust. 2 TFUE)[389]. Podział materii między oba te traktaty nie jest całkowicie jednoznaczny, choć TUE zawiera głównie postanowienia dotyczące zasad ustrojowych Unii[390], natomiast TFUE postanowienia dotyczące działania dziedzin objętych jej kompetencją. Prawo UE obejmuje Unię Europejską i powiązane z nią organizacje. Czyli jest to całokształt norm prawnych ustanowionych przez sygnatariuszy traktatów założycielskich, konwencji międzynarodowych, orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE), oraz ogólnych zasad prawa[391].

W TUE zawarto przepisy odnoszące się do takich zagadnień jak „ustanowienie Unii, katalogu jej wartości, określenia jej celów oraz głównych zasad podziału kompetencji między Unię a jej państwa członkowskie, ochrony praw podstawowych, zasad demokratycznych przestrzeganych w Unii”[392]. Znalazły również w nim miejsce postanowienia obejmujące „zasady działania instytucji unijnych, wzmocnionej współpracy, rewizji traktatów stanowiących podstawę Unii, akcesji do Unii i dobrowolnego z niej wystąpienia”[393].

---

[388] Zob. M. Brkan, *The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core,* “European Constitutional Law Review” 2018, nr 2, s. 334.
[389] Zob. M.M. Brzezińska, *Skutki zmian systemowych Unii Europejskiej po ratyfikacji Traktatu Lizbońskiego,* [w:] *Traktat Lizboński, Co po Irlandii?,* red. M.M. Brzezińska, R. Zenderowski, UKSW, Warszawa 2009, s. 9-35.
[390] Por. M. Adamowicz, *Traktat o Unii Europejskiej,* „Problemy Integracji Rolnictwa” 1997, nr 3, s. 7.
[391] Szerzej: J. Sozański, *Prawo Unii Europejskiej po Traktacie Lizbońskim,* Polskie Wydawnictwo Prawnicze „IURIS”, Warszawa – Poznań 2010.
[392] J. Barcz, *Struktura Unii Europejskiej,* [w:] *Zasady ustrojowe Unii Europejskiej,* red. J. Barcz, t. 2, Instytut Wydawniczy EuroPrawo, Warszawa 2010, s. II-6.
[393] Tamże.

Od momentu wejścia w życie KPP, zarówno w Polsce jak i w Wielkiej Brytanii toczyły się spory o charakterze polityczno-prawnym odnośnie statusu prawnego Protokołu 30 i zakresu obowiązywania Karty w tych dwóch krajach[394]. W Wielkiej Brytanii, spory te dotyczyły – zgodnie z przewidywaniami – roli Trybunału Sprawiedliwości Unii Europejskiej w interpretowaniu wynikających z przepisów Karty środków, które miały mieć zastosowanie tylko w niektórych państwach członkowskich Unii Europejskiej. Gdyby Trybunał miał uznać, że w części państw członkowskich określone przepisy dotyczące praw człowieka nie są prawnie wiążące, oznaczałoby to podważenie podstawowej zasady, zgodnie z którą już od lat 70-tych XX wieku prawa podstawowe, nawet jako prawa niepisane, były traktowane jako część dorobku prawnego Wspólnot i z tego tytułu wiążące dla instytucji unijnych i państw członkowskich. Sugerowano więc, że Karta Praw Podstawowych będzie mogła mieć pośredni wpływ na prawo brytyjskie, szczególnie w sprawach, w których Trybunał będzie rozsądzał status praw przewidzianych Kartą w innych państwach członkowskich UE. Ale pytań pojawiało się dużo więcej – choćby o to, czy obywatele innych państw członkowskich Unii mieszkający i pracujący na terytorium Wielkiej Brytanii będą mogli domagać się ochrony prawnej na mocy Karty. Wiele wątpliwości sprowadzało się zatem do tego w jaki sposób można połączyć prawnie wiążący charakter Karty (wraz z Protokołem 30) z obowiązkiem jednolitego stosowania prawa europejskiego we wszystkich państwach członkowskich Unii[395].

Odpowiadając na pytanie czy mimo podpisania Protokołu 30 Karta Praw Podstawowych obowiązuje w Polsce (oraz Wielkiej Brytanii) wybitny polski prawnik i były wiceprezes Trybunału Konstytucyjnego prof. Stanisław Biernat podkreślił, iż orzecznictwo Trybunału Sprawiedliwości, a także praktyka prawna w sposób jednoznaczny potwierdziły, że Karta obowiązuje realnie[396].

---

[394] Zob. A. Wyrozumska, *Protokół w sprawie stosowania Karty Praw Podstawowych Unii Europejskiej w stosunku do Polski i Zjednoczonego Królestwa,* [w:] *Ochrona Praw Podstawowych w Unii Europejskiej,* red. J. Barcz, Wydawnictwo C.H. Beck, Warszawa 2008, s. 80-112; M. Księżniakiewicz, *Stosowanie Karty Praw Podstawowych Unii Europejskiej: Protokół brytyjski i Sprawozdania ze stosowania KPP UE,* „Rocznik Integracji Europejskiej" 2012, nr 6, s. 333-348.

[395] Zob. V. Miller, *Effects of the EU Charter of Rights in the UK,* Standard Note SN/IA/6765, 17 March 2014, House of Commons Library, s. 4-5.

[396] Zob. S. Biernat, *Czy Karta Prawo Podstawowych Unii Europejskiej obowiązuje w Polsce?,* [w:] *Państwo prawa i prawo karne: księga jubileuszowa profesora Andrzeja Zolla,* Wydawnictwo Lex a Wolters Kluwer business, Warszawa 2012, s. 59-77.

3.2. Bezpieczeństwo danych osobowych w systemie aksjologicznym Unii Europejskiej

Obywatele państw należących do Unii Europejskiej są nie tylko obywatelami tych państw, ale również obywatelami Unii[397]. Z tego powodu istotne znaczenie ma informowanie ich o obowiązującym porządku prawnym, tj. nie tylko o krajowych przepisach prawa, ale również o przepisach unijnych prawnie wiążących, jak i tych o charakterze „miękkiego prawa", które stanowią integralną część europejskiej rzeczywistości i mają wpływ na nasze życie[398]. Częścią prawa UE, która ma istotne znaczenie dla jej obywateli są prawa podstawowe[399]. Wprawdzie w prawodawstwie unijnym nie wypracowano definicji tego pojęcia[400], ale została ona sformułowana w doktrynie prawa unijnego. Przyjmuje się, że „prawa podstawowe są ogólnymi zasadami prawa UE, które czerpią swoje źródło z tradycji konstytucyjnych wspólnych dla państw członkowskich oraz z umów międzynarodowych, których państwa te są stronami lub przy których opracowaniu uczestniczyły, ze szczególnym uwzględnieniem umów i porozumień z zakresu międzynarodowego prawa ochrony praw człowieka w tym praw socjalnych gospodarczych i kulturalnych oraz doświadczeń państw członkowskich w tym zakresie"[401]. Jednym z praw podstawowych jest prawo do ochrony danych osobowych, powiązane z prawem do poszanowania życia prywatnego i rodzinnego, jednak rozróżnione jako odrębne prawo podstawowe[402].

Ochrona danych osobowych na poziomie prawodawstwa unijnego jest szczególnie unormowana zarówno w aktach prawnie wiążących (traktaty, rozporządzenia, dyrektywy), jak i w aktach o charakterze tzw. „miękkiego prawa"

[397] Szerzej: J. Wojnowska-Radzińska, *Obywatelstwo Unii Europejskiej,* „Studia BAS" 2015, nr 4, s. 39-56.
[398] Zob. M. Poboży, *Obywatelstwo i obywatelskość w Unii Europejskiej,* „Przegląd Europejski" 2014, nr 1, s. 48.
[399] Zob. R. Grzeszczak, *Zupełny i efektywny system ochrony praw podstawowych w Unii Europejskiej,* [w:] *Unia Europejska w roli gwaranta i promotora praw podstawowych,* red. D. Kornobis-Romanowska, Currenda, Sopot 2016, s. 77-102.
[400] Zob. *Sprawozdanie na temat praw podstawowych 2017. Opinie FRA,* European Union Agency, źródło: www.fra.europa.eu/sites/.../fra-2017-fundamental-rights-report-2017-opinions_pl, data dostępu: 07.01.2019.
[401] F. Jasiński, *Karta Praw Podstawowych Unii Europejskiej,* Dom Wydawniczy ABC, Warszawa 2003, s. 28.
[402] Zob. K. Majchrzak, *Wzmacnianie świadomości obywateli Unii Europejskiej na temat gromadzenia i przetwarzania danych osobowych oraz ich ochrony,* [w:] *Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania,* red. J. Jaskiernia, t. 2, Wydawnictwo Sejmowe, Warszawa 2014, s. 214.

(opiniach i zaleceniach)[403]. Co więcej, obywatele UE, którzy uważają, że ich prawo do ochrony danych osobowych zostało naruszone, mogą w tej sprawie zwracać się o pomoc prawną nie tylko do kompetentnych w tej dziedzinie organów krajowych, ale również przysługuje im ochrona na poziomie unijnym[404]. Aby w pełni mogli oni korzystać z przysługujących im praw, niezbędne jest wzmacnianie ich świadomości na temat przysługującej ochrony prawnej w zakresie danych osobowych[405]. W celu zapewnienia skutecznej ochrony danych osobowych obywateli UE, konieczne jest również dostosowanie prawodawstwa unijnego do zmian zachodzących w otaczającej na rzeczywistości[406]. Służą temu instrumenty prawne UE, zarówno prawnie wiążące (*hard law*), jak i o charakterze tzw. miękkiego prawa (*soft law*)[407].

3.2.1. Standardy prawnie wiążące

Przez długi czas w systemie prawnym Unii Europejskiej problem ochrony danych osobowych wydawał się niezauważalny[408]. Nastąpiła tu jednak bardzo charakterystyczna ewolucja[409]. Wiązała się ona ze wzrostem znaczenia bezpieczeństwa danych osobowych pośród ogólnych uwarunkowań bezpieczeństwa Unii Europejskiej[410]. Nałożyło to na UE zadanie poszukiwania zwiększenia bezpieczeństwa danych osobowych w sytuacji, gdy w skali masowej dochodziło w tym zakresie do istotnych naruszeń[411].

---

[403] Por. *General principles of EU law and the EU digital order*, red. U. Bernitz, X. Groussot, S.A. de Vries, J. Paju, Wolters Kluwer, Aplphen aan den Rijn 2020.
[404] Por. D. Fleszer, *Zabezpieczenie danych osobowych – zakres, obowiązki i sankcje za jego naruszenie,* [w:] *Bezpieczeństwo informacji w administracji publicznej,* red. D. Fleszer, Wyższa Szkoła Humanitas, Sosnowiec 2017, s. 83-96.
[405] Zob. A. Gonschior, *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej,* [w:] *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego. Aspekty teoretyczne i praktyczne,* red. D. Kornobis – Romanowska, Uniwersytet Wrocławski, Wrocław 2017, s. 239-287.
[406] Zob. D. Adamski, *Unijne modele regulacji jawności i jej ograniczeń oraz ich wpływ na systemy krajowe,* [w:] *Jawność i jej ograniczenia,* red. G. Szpor, C. Mik, C.H. Beck, Warszawa 2016, s. 39-65.
[407] Zob. U. Bernitz, X. Groussot, S.A. de Vries, J. Paju, *General principles of EU law and the EU digital order*, Wolters Kluwer, Aplphen aan den Rijn 2020, s. 36.
[408] J. Sobczak, *Ochrona danych osobowych…,* s. 492.
[409] Zob. G. González Fuster, *Security and the future of personal data protection in the European Union*, "Security and Human Rights", 2013, nr 4, s. 331-342.
[410] Por. *The European Union: facing the challenge of multiple security threats*, red. A. Bakardijeva Engelbrekt, A. Michalski, N. Nillson, L. Oxelheim, Edward Elgar Publishing, Cheltenham – Portsmouth 2018.
[411] Zob. C. Magnusson Sjőberg, *Threats to personal data security: how does the EU protect its citizens?*, "The European Union", 27 April 2018, s. 163.

Pierwszymi krokami w tym zakresie była ratyfikacja przez kraje Wspólnoty Konwencji nr 108 Rady Europy zgodnie z zaleceniami Komisji Europejskiej[412], a następnie postępujące poszerzanie tejże ochrony szczególnie widoczne w latach 90[413]. W szczególności, kwestę tę podjęto w dyrektywie 95/46/WE Parlamentu Wspólnoty i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[414].W jej preambule podkreślono, że celem krajowych przepisów prawa dotyczących przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności[415], którego wagę w obrębie prawa wspólnotowego podkreślono odwołując się do art. 8 Europejskiej Konwencji Praw Człowieka[416] oraz zasad ogólnych prawa wspólnotowego[417]. Przy czym wskazano, iż zasady ochrony muszą odnosić się do całokształtu przetwarzania danych osobowych, przez każdą osobę, której działania podlegają przepisom prawa wspólnotowego[418].

Ponadto dla zapewnienia należytej ochrony interesów osób fizycznych w zakresie przetwarzania danych osobowych zalecono utworzenie w państwach członkowskich organów nadzorczych wykonujących swoje funkcje w sposób całkowicie niezależny. Jednocześnie na poziomie wspólnotowym uznano za konieczne powołanie zespołu roboczego do spraw ochrony osób fizycznych co do przetwarzania danych osobowych, który ma służyć radą Komisji oraz, w szczególności, przyczyniać się do jednolitego stosowania przepisów krajowych przyjętych na mocy przedmiotowej dyrektywy[419]. W przepisach ogólnych dyrektywy zdefiniowano pojęcia „danych osobowych", „przetwarzania danych osobowych", „zbioru danych", 'przetwarzającego danych", „osoby trzeciej", „odbierających danych", „zgody osoby" - o czym była mowa wcześniej.

---

[412] Por. M. Ciechomska, *Zmiana Konwencji nr 108 Rady Europy o ochronie danych osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych,* „Monitor Prawniczy" 2017, nr 16, s. 871-877.

[413] Zob. A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej,* „Państwo i Prawo" 1997, nr 6, s. 29-41.

[414] Dz.Urz. L 281/31, s. 355-374.

[415] Motyw (10) Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.

[416] Dz.U. 1993 nr 61, poz. 284.

[417] Konkretyzacja zasad ogólnych prawa wspólnotowego m.in. w zakresie ochrony prawa do prywatności znalazła wyraz w art. 7 i w szczególności w art. 8 Karty Praw Podstawowych Unii Europejskiej (Dz.Urz. UE C 303 z 14.12.2007 r., s. 1).

[418] Motyw (12) Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.

[419] Motyw (65) Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.

W treści dyrektywy zobowiązano państwa członkowskie do zapewnienia, aby dane osobowe były przetwarzanie rzetelnie i legalnie. Powinny być gromadzone do określonych, jednoznacznych i legalnych celów oraz niepoddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych w celach naukowych nie jest uważanie za niezgodne z przepisami pod warunkiem ustanowienia przez państwa członkowskie odpowiednich środków zabezpieczających, ponadto adekwatne, stosowne oraz nadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone. Dane te powinny być także prawidłowe, oraz w razie konieczności, aktualizowane. Wskazano, że należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Dane osobowe powinny być w końcu przechowywane w formie umożliwiającej identyfikację osób, których dotyczą, przez czas nie dłuższy niż jest to konieczne dl celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane. Państwa członkowskie ustanowią odpowiednie środki zabezpieczające dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych. Obowiązek przestrzegania tych zasad dyrektywa nakłada na administratora danych[420].

Stosownie do dyspozycji przepisu art. 7 przedmiotowej Dyrektywy państwa członkowskie zapewniają, że dane osobowe mogą być przetwarzane tylko wówczas gdy: osoba której dane dotyczą jednoznacznie wyraziła na to zgodę; lub przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy; lub przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega; lub przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą; lub przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z

[420] Art. 6 ust. 1 i 2 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.

podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1 Dyrektywy.

Państwa członkowskie, co do zasady, zabraniają przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego (art. 8 ust. 1 Dyrektywy). Jednak powyższa reguła nie ma zastosowania w przypadku gdy (art. 8 ust. 2 Dyrektywy: osoba, której dane dotyczą, udzieliła wyraźnej zgody na ich przetwarzanie, chyba że ustawodawstwo państwa członkowskiego przewiduje, że zakaz określony w ust. 1 nie może być uchylony mimo udzielonej zgody przez osobę, której dane dotyczą; lub przetwarzanie jest konieczne do wypełniania obowiązków i szczególnych uprawnień administratora danych w dziedzinie prawa pracy, o ile jest to dozwolone przez prawo krajowe przewidujące odpowiednie środki i zabezpieczające; lub przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, w przypadku gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody; lub przetwarzanie danych jest dokonywane w ramach legalnej działalności wspartej odpowiednimi gwarancjami przez fundację, stowarzyszenie lub inną instytucję nienastawioną na osiąganie zysku, której cele mają charakter polityczny, filozoficzny, religijny lub związkowy, pod warunkiem, że przetwarzanie danych odnosi się wyłącznie do członków tej instytucji lub osób mających z nią regularny kontakt w związku z jej celami oraz, że dane nie zostaną ujawnione osobie trzeciej bez zgody osób, których dane dotyczą; lub jest konieczne do ustalenia, wykonania lub ochrony roszczeń prawnych.

W treści dyrektywy ustalono zasady przekazywania informacji w przypadku gromadzenia danych od osoby, której dane dotyczą (art. 10) oraz innych źródeł (art. 11); prawa dostępu do danych (art. 12); prawa sprzeciwu przysługującego osobie, której dane dotyczą (art. 14 i 15). Uregulowano również kwestie poufności i bezpieczeństwa przetwarzania danych (art. 16 i 17); obowiązki administratora (art. 18 – 21); odpowiedzialność za wyrządzenie szkody (art. 22-24); przekazywanie danych osobowych do państw trzecich (art. 25 – 26); problem kodeksów postępowania w zakresie przetwarzania danych (art. 27) oraz uprawnienia organu nadzorczego i grupy

roboczej do spraw ochrony osób fizycznych w zakresie przetwarzania danych (art. 28 – 30), sprawę wspólnotowych środków wykonawczych (art. 31)[421].

Zagadnienie ochrony danych osobowych zostało także podjęte w dyrektywie Parlamentu i Rady WE z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku („dyrektywa dotycząca handlu elektronicznego") 2000/31/WE[422]. W treści tej dyrektywy zawarto regulacje dotyczące praw i obowiązków usługodawców społeczeństwa informacyjnego. Wskazano, że świadczenie usług drogą internetową powinno podlegać zasadzie transparentności usługodawcy i poszanowania prywatności usługobiorcy. Zawarto specjalne zasady ochrony danych osobowych usługobiorcy wskazując, że ochrona ta powinna polegać na przetwarzaniu danych wyłącznie za zgodą usługobiorcy. Istniejące dane muszą być przy tym ograniczone do niezbędnego minimum, koniecznego do wywiązania się z umowy o świadczeniu usługi. Użytkownik powinien mieć także prawo do korzystania z usług anonimowo lub przy użyciu pseudonimu[423].

W dyrektywie 2002/58/WE Parlamentu Europejskiego i Radu z 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (dyrektywa o ochronie prywatności i komunikacji elektronicznej)[424] zobowiązano państwa członkowskie do zapewnienia ekwiwalentnego stopnia ochrony podstawowych praw i wolności osobom fizycznym, a w szczególności prawa do prywatności w odniesieniu do przetwarzania danych osobowych w sektorze komunikacji elektronicznej oraz swobodnego przepływu tych danych osobowych w państwach Wspólnoty. Dyrektywa ta rozwija i uzupełnia postanowienia dyrektywy 95/46/WE, zapewniając także ochronę uzasadnionych interesów osobom prawnym. Przepisy tej dyrektywy uchyliły z dniem 31 października 2003 r. dyrektywę 97/66/WE z 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności

[421] Szerzej: M. Gołda-Sobczak, *Unia Europejska wobec potrzeby ochrony danych osobowych,* [w:] *Europejski system ochrony praw człowieka. Aksjologia-instytucje-efektywność,* red. J. Jaskiernia, t. III, Wydawnictwo Adam Marszałek, Toruń 2015, s. 161-168.
[422] Dz.Urz. UE L 178/1 z 17.7.2000.
[423] Por. M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym,* „Państwo i Prawo" 2002, nr 6, s. 3-12.
[424] Dz.Urz. UE L 337/11 z 18.12.2009.

w sektorze telekomunikacyjnym. Dyrektywa ta uwzględniała propozycję Komisji[425] oraz opinię Komitetu Ekonomiczno Społecznego[426].

Zagadnienie ochrony danych osobowych ujęto również w dyrektywie 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnieniem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE[427]. Celem wspomnianej dyrektywy było zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez niegenerowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych w celu dochodzenia wykrywania i ścigania poważnych przestępstw określonych w ustawodawstwie każdego państwa członkowskiego. W 2014 r. Dyrektywa ta została uznana przez Trybunał Sprawiedliwości Unii Europejskiej za nieważną z powodu zbytniej ingerencji w poszanowanie życia prywatnego oraz w ochronę danych[428].

Kwestii ochrony danych osobowych dotyczy także dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów[429].

Komisja Europejska 4 listopada 2010, opublikowała komunikat pod tytułem "*Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*". Zapowiedział on kompleksową nowelizację prawa europejskiego w zakresie ochrony danych osobowych. Tak jak poprzednio, tak i teraz, u podstaw najnowszych przepisów stał przede wszystkim rozwój nowych technologii przetwarzania informacji oraz

[425] Dz.Urz. UE C 365 E, z 19.12.200, s. 223.
[426] Dz.Urz. UE C 123, z 25.04.2001, s. 53.
[427] Dz.Urz.UE L 105/54 z 13.04.2006.
[428] *Ochrona danych osobowych,* źródło: www.europarl.eu/factsheet/pl/sheet/157/ochrona-danych-osobowych, data dostępu: 08.02.2019.
[429] Dz.Urz.UE L 337/11 z 18.12.2009, s. 11-36.

globalizacja. W szczególności chodziło o automatyczne „narzędzia obróbki danych", za sprawą których informacja o osobie uzyskała rangę wartościowego ekonomicznie produktu. 25 stycznia 2012 roku Komisja Europejska przedstawiła kolejny, bardzo ważny, komunikat – *Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku*. Czytamy w nim między innymi:

„*Unijna dyrektywa z 1995 r., będąca głównym instrumentem prawnym w zakresie ochrony danych osobowych w Europie, była przełomowym dokumentem w historii ochrony danych. Nadal aktualne są jej cele polegające na zapewnieniu funkcjonowania jednolitego rynku i skutecznej ochrony praw podstawowych i swobód osób fizycznych. Została ona jednak przyjęta 17 lat temu, kiedy internet dopiero raczkował. W dzisiejszym nowym, wymagającym środowisku cyfrowym istniejące przepisy nie zapewniają wymaganego stopnia harmonizacji ani niezbędnej skuteczności gwarantującej prawo do ochrony danych osobowych. Z tego względu Komisja Europejska proponuje gruntowną reformę unijnych ram ochrony danych"***.**

W komunikacie tym zaproponowano, by nowe ramy prawne obejmowały:

- rozporządzenie (zastępujące dyrektywę 95/46/WE) ustanawiające ogólne unijne ramy ochrony danych oraz

- dyrektywę (zastępującą decyzję ramową 2008/977/WSiSW) określającą przepisy o ochronie danych osobowych przetwarzanych do celów zapobiegania przestępstwom, wykrywania ich, prowadzenia dochodzeń w ich sprawie i ścigania ich oraz powiązanych działań sądowych[430].

Istotne znaczenie ma też to, ochrona danych osobowych została zagwarantowana w art. 8 **Karty Praw Podstawowych Unii Europejskiej**: „1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą. 2. 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 zabranych danych, które

[430] Zob. *Droga do RODO – rys historyczny*, https://a1k.pl/droga-do-rodo-rys-historyczny/, data dostępu: 26.12.2020.

go dotyczą, i prawo do dokonania ich sprostowania. 3. Przestrzeganie tych zasad podlega kontroli niezależnego organu”[431].

Należy zwrócić uwagę, że ochrona danych osobowych została potraktowana jako odrębne prawo od przewidzianego w przepisie art. 7 Karty prawa do prywatności – Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania.

Tak decyzja prawodawcy unijnego pozwala na przyjęcie, że doszło do emancypacji prawa do ochrony danych osobowych, które historycznie było traktowane jako element składowy prawa do prywatności[432]. Powoduje to konieczność odpowiedzi na fundamentalne pytanie, które z tych praw ma pierwszeństwo w sytuacji kolizji prawa do ochrony danych osobowych i prawa do prywatności. Punktem wyjścia jest przepis art. 52 ust. 1 Karty, który stanowi, że „Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób”.

Warto zaznaczyć, iż nadanie Karcie mocy prawnej równiej traktatom unijnym wpłynęło na zwiększenie skuteczności ochrony praw podstawowych w Unii Europejskiej, w tym ochrony danych osobowych jako jednego z tych praw. Karta wzmacnia aksjologię Unii Europejskiej przez nadanie jej obywatelom prawnie wiążącego katalogu praw podstawowych, które przysługują w przypadku korzystania przez obywatela z prawa unijnego lub prawa krajowego implementującego prawo UE. Ze względu na to, że porządek prawny jest rzeczywistym fundamentem Unii, który nadaje charakter wspólnoty prawa, dostosowanie regulacji prawnych dotyczących ochrony danych osobowych do zmian zachodzących w otaczającej nas rzeczywistości pozwala Unii na osiąganie jednego z jej celów jakim jest ochrona obywateli i ich praw podstawowych.

Poza Kartą, ochrona danych osobowych w prawie unijnym została unormowana na poziomie pierwotnego prawa traktatowego – w art. 16 Traktatu o funkcjonowaniu

[431] Dz.Urz. UE C 303 z 14.12.2007.
[432] Szerzej: P. Sobczyk, *Ochrona danych osobowych jako element prawa do prywatności,* „Zeszyty prawnicze UKSW z 2009”, nr 9, s. 299 i n.

Unii Europejskiej (TFUE)[433]: „Każda osoba ma prawo do ochrony danych osobowych jej dotyczących. 2. Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą prawodawczą, określają zasady dotyczące 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. Przestrzeganie tych zasad podlega kontroli niezależnych organów"[434].

W odniesieniu do wskazanych regulacji dotyczących ochrony danych osobowych w prawodawstwie unijnym, należy zauważyć, że treść art. 16 TFUE wyraźnie koresponduje z treścią art. 8 Karty. W ust. 1 art. 16 TFUE została ustanowiona zasada, zgodnie z którą każda osoba ma prawo do ochrony jej danych osobowych, a w ust. 2 art. 16 została wprowadzona podstawa prawna dla przyjmowania przepisów dotyczących ochrony danych osobowych. Natomiast art. 8 Karty nadaje prawu do ochrony danych osobowych rangę prawa podstawowego[435].

Poza Kartą i TFUE w systemie unijnego prawa pierwotnego kwestię ochrony danych osobowych uregulowane zostały także w układzie Schengen[436] oraz w Konwencji wykonawczej do układu z Schengen z 14 czerwca 1985 r.[437] Na podstawie Konwencji stworzono System Informacyjny Schengen (SIS), stanowiący bazę danych, której cel oparto na wymianie informacji między organami państw członkowskich Schengen w zakresie kategorii osób lub przedmiotów[438]. W Konwencji uregulowano zasady dotyczące przetwarzania danych osób przekraczających granice państw należących do porozumienia[439].

---

[433] Dz. Urz. UE 2016, C 202, s. 1.
[434] Tamże.
[435] Zob. D. Adamski, *Unijne modele regulacji jawności i jej ograniczeń oraz ich wpływ na systemy krajowe,* [w:] *Jawność i jej ograniczenia,* red. G. Szpor, C. Mik, t. 11, Wydawnictwo C.H. Beck, Warszawa 2016, s. 39-65.
[436] Układ pomiędzy Rządami Państw Unii Gospodarczej Beneluksu oraz Republiki Federalnej Niemiec i Republiki Francuskiej dotyczący stopniowego znoszenia kontroli na wspólnych granicach zawarty w Schengen 14 czerwca 1985 r. (Opublikowany w języku polskim przez Departament ds. Migracji i Uchodźstwa MSWiA, seria: „Dokumenty", zeszyt 2, Warszawa 1998.
[437] Konwencja Wykonawcza do Układu z Schengen z dnia 14 czerwca 985 roku między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, Dz.Urz. nr L 239 22/09/2000, s. 19.
[438] Zob. S. Kaniewski, *Geneza i znaczenie Systemu Informacyjnego Schengen,* „Edukacja Humanistyczna" 2015, nr 2, s. 89-96.
[439] Por. J. Wącior, *Zniesienie kontroli granicznych a bezpieczeństwo: System Informacyjny Schengen,* „Zeszyty Naukowe AON" 2010, nr 3, s. 51.

W systemie unijnego prawa wtórnego prócz wymienionych wcześniej dyrektyw i decyzji należy zwrócić szczególną uwagę na dokumenty opublikowane w dniu 4 maja 2016 r. w związku z reformą ochrony danych tj. 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 (ogólne rozporządzenie o ochronie danych)[440], a także Dyrektywę 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[441].

Ze względu na fakt, że unijne dyrektywy wymagają wdrożenia do krajowych systemów prawnych[442], zdecydowano, iż standardy zawarte w powyższych dokumentach będą stosowane bezpośrednio[443].

Istotne jest to, że – jak wynika z badań socjologicznych prowadzonych w krajach członkowskich Unii Europejskiej – wdrożenie nowych instrumentów przyczyniło się do zwiększenia świadomości społecznej w kwestii ochrony danych osobowych i zagrożeń, jakie tu występują. Choć wdrażanie ich postanowień mogło się wydawać uciążliwe, to jednak narastało przekonanie, że chodzi o instrument istotny dla ochrony praw obywatelskich[444].

W maju 2015 r. Komisja Europejska ogłosiła strategię Jednolitego Rynku Cyfrowego dla Europy (Digital Single Market Strategy for Europe), uwzględniającą 16

[440] OJ L 119, 4.5.2016, s. 1-88.
[441] OJ L 119, 4.5.2016, p. 89-131.
[442] Zob. J. Goerick, *Współpraca międzynarodowa organów ochrony danych osobowych państw członkowskich Unii Europejskiej przed i po wejściu w życie ogólnego rozporządzenia o ochronie danych,* „Przegląd Naukowy Disputatio" 2017, nr 2, s. 19-28. Por. *RODO w e-commerce*, red. D. Lubasz, Wolters Kluwer Polaska, Warszawa 2018.
[443] B. Mendyk, *Nowe Rozporządzenie Unii Europejskiej w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych,* [w:] *Współczesne wyzwania państwa i prawa. Księga jubileuszowa prof. Jerzego Jaskierni z okazji 45 lecia pracy naukowej,* red. Ł. Baratyński, P. Ramiączek, K. Spryszak, Wydawnictwo Adam Marszałek, Toruń 2017, s. 795.
[444] Zob. M. Lang, J. Devitt, S. Kelly, A. Kinneen, J. O'Malley, D. Prunty, *Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland*, [w:] 2009 International Conference on Management of e-Commerce and e-Government, 2009, s. 486.

legislacyjnych i nielegislacyjnych inicjatyw, których realizacja ma sprzyjać utworzeniu takiego rynku. Celem tych działań jest zwiększenie dostępu do rynku cyfrowego, wzmocnienie cyfrowych platform i pobudzenie transformacji cyfrowej małych i średnich przedsiębiorstw, które stanowią 99% ogółu przedsiębiorstw w UE. Chodziło także o ujednolicenie przepisów prawnych, wobec ich dotychczasowej fragmentaryczności[445].

Serwisy społecznościowe, usługi mobilne, chmury obliczeniowe - to jedne z tych usług internetowych, które powodują, że dane osobowe są przetwarzane i wykorzystywane na coraz więcej sposobów. Tym samym prywatność jest coraz słabiej chroniona, a my często tracimy kontrolę nad informacjami na swój temat. Z badania przeprowadzonego przez Komisję Europejską wynikało, że ponad 75% Europejczyków nie ufa portalom społecznościowym i wyszukiwarkom internetowym, połowa obawia się, że stanie się ofiarą oszustwa polegającego na niewłaściwym wykorzystaniu danych na ich temat, a zaledwie 15% przyznało, że ma poczucie pełnej kontroli nad swoimi danymi. Między innymi te liczby przemawiały za koniecznością znowelizowania obowiązującego od 1995 roku unijnego prawa w zakresie danych osobowych. Parlament Europejski i Rada Unii Europejskiej pracowała nad zmianami przez cztery lata[446].

Kluczowe znaczenie w zakresie regulacji przetwarzania danych osobowych w Unii Europejskiej ma **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**[447], w skrócie angielskim znane jako GDPR (General Data Protection Regulation)[448], a w skrócie w języku polskim jako RODO (Rozporządzenie o ochronie danych osobowych)[449]. Dokument ten ma istotne znaczenie porządkujące. Do czasu jego uchwalenia w dziedzinie działalności

[445] Zob. *Guidelines for SMEs on the security of personal data processing*, ENISA, Heraklion 2016, s. 12.
[446] Zob. *Po co nam RODO, czyli jak będą chronione nasze dane osobowe i co nam dają unijne regulacje*, https://portal.librus.pl/artykuly/po-co-nam-rodo-czyli-jak-beda-chronione-nasze-dane-osobowe-i-co-nam-daja-unijne-regulacje, data dostępu: 26.12.2020.
[447] General Data Protection Regulation (GDPR), Dz.Urz. UE L z 2016 nr 119, s. 1.
[448] Zob. D. Kościuk, *General Data Protection Regulation (GDPR) - The EU Law Strengthening the Information Society in Poland*, "Białostockie Stud.Prawnicze" 2018, nr 2, s. 139.
[449] Por. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, C.H. Beck, Warszawa 2018.

gospodarczej obowiązywało w tym zakresie na terenie Unii Europejskiej 28 aktów prawnych, co nie sprzyjało ich realizacji. Bardzo utrudniało to działalność biznesu w zakresie zapewnienia ochrony danych osobowych, a także ekspansję firm europejskich na rynki zewnętrzne.

RODO reguluje przetwarzanie przez osoby fizyczne, przedsiębiorstwa lub organizacje danych osobowych dotyczących osób fizycznych w UE. Nie obejmuje ono swoim zakresem przetwarzania danych osobowych dotyczących osób zmarłych ani osób prawnych. Przepisy te nie mają zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, pod warunkiem że nie ma ona związku z działalnością zawodową lub komercyjną. Jeśli jednak osoba fizyczna wykorzystuje dane osobowe w celach wykraczających poza „sferę osobistą" — na przykład w związku z działalnością społeczną, kulturową lub finansową — wówczas musi przestrzegać przepisów o ochronie danych[450].

RODO wprowadza nowe definicje:

- profilowanie — czyli przewidywanie tego, co klient sklepu internetowego kupi następnym razem, bazując na zebranych danych na temat jego preferencji zakupowych, ale także sytuacji zdrowotnej, finansowej, bieżącej lokalizacji i innych;
- pseudonimizacja — proces (spseudonimizowane), po którym można przypisać konkretne dane do określonej osoby; forma zabezpieczenia danych osobowych;
- wyodrębnienie osobnych definicji dotyczących danych na temat zdrowia i danych genetycznych;
- wprowadzenie nowej definicji danych biometrycznych — wraz z generalnym zakazem przetwarzania takich danych;
- nowa definicja jednostki organizacyjnej;

[450] Zob. *Czego dotyczy ogólne rozporządzenie o ochronie danych (RODO)?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pl, data dpstpu: 26.12.2020.

- definicja zgody na przetwarzanie danych osobowych — rozporządzenie określa, że wyrażenie zgody musi mieć formę okazania woli w formie oświadczenia lub wyraźnego działania potwierdzającego[451].

RODO obejmuje 7 zasad:

1. Zasada zgodności z prawem, rzetelności i przejrzystości – z danymi osobowymi należy postępować w sposób zgodny z prawem, w sposób uczciwy wobec osoby której dotyczą i dla niej przejrzysty.
2. Zasada ograniczenia celu przetwarzania – dane osobowe można gromadzić wyłącznie w konkretnym, wyraźnie określonym i zgodnym z prawem celu.
3. Zasada minimalizowania danych – przetwarzane dane osobowe muszą adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
4. Zasada prawidłowości danych – osoby, których dane dotyczą muszą mieć prawo żądania usunięcia lub skorygowania swoich danych, jeśli są one nieprawidłowe lub niekompletne.
5. Zasada ograniczenia przechowywania danych – dane osobowe należy usuwać z chwilą realizacji celu, w którym były przetwarzane.
6. Zasada integralności i poufności (bezpieczeństwa) – dane osobowe należy chronić przed niedozwolonym, niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem.

7. Zasada rozliczności – w celu spełnienia obowiązujących wymagań przedsiębiorstwa muszą być zdolne do wykazania prawidłowości przechowywania danych[452].

Ocena sytuacji powinna być przeprowadzana za każdym razem, gdy istnieje ryzyko, że podczas przetwarzania danych osobowych naruszone zostanie prawo lub wolność osób fizycznych. RODO dokładnie określa, w jakich sytuacjach konieczne jest

[451] Zob. *Czym jest RODO i jakie zmiany wprowadza nowa ustawa Parlamentu Europejskiego*, https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-rodo-i-jakie-zmiany-wprowadza-nowa-ustawa-parlamentu-europejskiego, data dostępu: 26.12.2020.
[452] Zob. *RODO i przepisy danych osobowych na świecie, https://www.dnvgl.pl/article/rodo-i-przepisy-o-ochronie-danych-osobowych-na-swiecie-161457*, data dostępu: 26.12.2020.

przeprowadzenie takiej procedury, a kiedy Administrator Danych Osobowych może ją pominąć. Administratorzy Danych Osobowych, wraz z wejściem w życie nowego rozporządzenia, będą musieli także zgłaszać wszelkie incydenty związane z naruszeniem bezpieczeństwa danych osobowych, określanych przez RODO jako takie, które "prowadzą do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych". Administrator ma 72 godziny na zgłoszenie GIODO faktu zaistnienia takiego incydentu. Dodatkowo RODO wprowadza obowiązek prowadzenia rejestru naruszeń, w którym powinny się znajdować wszystkie informacje na temat naruszeń. W przedsiębiorstwach, które zarówno przetwarzają, jak i kontrolują dane osobowe wymagane będzie wyznaczenie osoby na stanowisko Inspektora Ochrony Danych (IOD) – zastąpi ona Administratora Bezpieczeństwa Informacji. RODO wprowadza także nowe procedury, wśród których są między innymi *privacy by design* i *privacy by default.* Zmiany te wymuszają na Administratorach konieczność wdrożenia zasad prywatności na etapie projektowania oraz to, że zasady prywatności powinny stanowić „domyślny" element składowy każdego projektu zakładającego przetwarzanie danych osobowych. Administratorzy mają także obowiązek prowadzenia rejestru czynności przetwarzania. Zawierać on powinien informacje na temat administratorów i innych osób zajmujących się przetwarzaniem danych osobowych, cel ich przetwarzania, listę osób, którym dane te zostały udostępnione i sposoby ich zabezpieczenia[453].

Organizacje przetwarzające dane osobowe pochodzące z innych firm, w trakcie świadczenia usług na ich rzecz (jak na przykład firmy dostarczające rozwiązania w chmurze czy firmy hostingowe), będą ponosić bezpośrednią odpowiedzialność za złamanie zapisów RODO, włączając w to ryzyko otrzymania kary finansowej. Są również wymagane bardziej restrykcyjne niż dotychczas obowiązki w zakresie tworzenia umów o przetwarzaniu, natomiast odszkodowania i ograniczenia odpowiedzialności będą podlegać renegocjacji. Wprowadzone zostały ograniczenia w zakresie profilowania włączając w to obowiązek otrzymania zgody na profilowanie przed rozpoczęciem zbierania danych, surowy obowiązek informowania o profilowaniu oraz konieczność akceptacji braku zgody na profilowanie Kontrolujący i przetwarzający są zobowiązani od przygotowania i utrzymania wszechstronnych rejestrów dotyczących

[453] Tamże.

przetwarzanych danych, uwzględniających m.in.: powody przetwarzania danych, kategorie podmiotów danych i danych osobowych, adresatów danych, rejestry międzynarodowych transferów danych, rejestry naruszeń i incydentów, rozwój i utrzymanie zasad ochrony prywatności dla każdej linii produktowej, przechowywanie potwierdzonych zgód na przetwarzanie danych itd.[454].

Rozporządzenie RODO wprowadza też kilka nowych praw dla obywateli, a wśród nich:

- Możliwość żądania przeniesienia danych;
- Wzmocnione prawo do wglądu i dostępu do swoich danych;
- Możliwość usunięcia danych osobowych obywatela („Prawo do bycia zapomnianym")[455].

W myśl RODO bezpieczeństwo danych osobowych powinno w równym stopniu uwzględniać poufność, integralność i dostępność, przy czy powinna być uwzględniona zasada, że im większe występuje ryzyko, tym ostrzejsze powinny być środki zapobiegawcze (risk-based approach). Zasadę tę wyeksponowała Europejska Agencja Bezpieczeństwa Sieci i Informacji (The European Union Agency for Cybersecurity - ENISA w zaleceniach dotyczących realizacji RODO przez państwa członkowskie. Są one pomocne zwłaszcza przy dokonywaniu oceny ryzyka dla bezpieczeństwa danych osobowych[456]. Zalecenia te oparte są na najnowszej wiedzy dotyczącej rozwoju technik cyfrowych i uwzględniają nowoczesne technologie związane z przetwarzaniem danych osobowych w różnych dziedzinach życia społecznego i gospodarczego[457]. Stąd formułowana była teza, że chodzi tu o rewolucję w ochronie danych osobowych[458].

Standardy wynikające z nowych przepisów oparto w szczególności na czterech zasadach:

[454] Zob. *Co to jest RODO i jakie zmiany wprowadza ustawa*, https://www.pwc.pl/pl/artykuly/co-to-jest-rodo-i-jakie-zmiany-wprowadza-ustawa.html, data dostępu: 26.12.2020.
[455] Tamże.
[456] Zob. *Handbook on security of personal data processing,* ENISA, Heraklion 2017, s. 12.
[457] Zob. *Reinforcing trust and security in the area of electronic communications and online services: sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*, ENISA, Heraklion 2018, s. 14.
[458] Zob. E. Bielak-Jomaa, *Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?*, „Monitor Prawniczy" 2017, dodatek specjalny do nr. 20, s. 3.

1) jeden kontynent – jedno prawo ze skutecznymi sankcjami dla przedsiębiorców ze wszystkich 28 państw UE, niezależnie od kraju pochodzenia przedsiębiorców;
2) punkt kompleksowej usługi – ustalono, iż przedsiębiorstwa, które prowadzą działalność w kilku państwach UE oraz ich klienci będą mieli do czynienia z jednym krajowym organem nadzorczym; jest to szczególnie przydatne np. dla polskich przedsiębiorców działających w Niemczech, bowiem w tym państwie w każdym landzie funkcjonuje oddzielny system ochrony danych osobowych, które wykazują różne praktyki; najważniejsze znaczenie dla przedsiębiorstwa ma jego główna siedziba[459].
3) te same zasady dla wszystkich przedsiębiorstw, niezależnie od miejsca ich siedziby – przedsiębiorstwa spoza Unii Europejskiej będą musiały przestrzegać europejskiego prawa ochrony danych, jeżeli będą prowadzić działalność gospodarczą na rynku europejskim;
4) prawo do bycia zapomnianym (prawo żądania usunięcia danych)[460].

Regulacja ta rozstrzygnęła szereg kwestii szczegółowych. Uregulowała bowiem kwestię prywatności pacjenta postrzeganą w charakterze dobra osobistego[461]. Podjęła kwestię odpowiedzialności cywilnej administratora danych osobowych[462].

W motywie 4 tego rozporządzenia zwrócono uwagę, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym, należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności[463]. W szczególności – w myśl RODO - dotyczy to prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania, ale także ochrony danych osobowych innych osób, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do

[459] Zob. A. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej,* dodatek „MoP" 2012, nr 7.
[460] B. Mendyk, *Nowe Rozporządzenie…,* j.w., s. 795. Por. *Post-reform personal data protection in the European Union: general data protection regulation (EU) 2016/679*
Subjects, Wolter Kluwer, Alphen aan den Rijn 2017, s. 14.
[461] Zob. I. Wrześniewska-Wal, L. Janiszewska, *Prywatność pacjenta jako dobro osobiste. Nowe wyzwania w świetle regulacji RODO*, „Studia Prawnoustrojowe" 2019, nr 43, s. 361.
[462] Zob. F. Morawski, *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według Ogólnego Rozporządzenia o Ochronie Danych Osobowych*., „Acta Iuris Stetinensis" 2019, nr 2, s. 81.
[463] Zob. A. Denley, M. Foulsham, B. Hitchen, *GDPR: how to achieve and maintain compliance*, Routledge, London-New York 2019, s. 46.

skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej[464].

W sytuacji, gdy – w myśl art. 32 RODO - ochrona danych osobowych jest kluczowym zobowiązaniem kontrolerów i zarządzających danymi osobowymi, Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji zaproponowała system zapewnienia bezpieczeństwa w dziedzinie ochrony danych osobowych. Podkreśla się jednak, że zaproponowana platforma jest tylko jednym z instrumentów, które mogą służyć ochronie bezpieczeństwa informacji w sieci i musi być postrzegana w ramach kompleksowego systemu rozwiązań, jakie w tym zakresie mają zastosowanie[465].

Rozporządzenie unijne dotyczące ochrony danych osobowych wprowadziło znaczne zmiany w pracy poszczególnych działów w dużych firmach – w szczególności tych zajmujących się rekrutacją pracowników. Działy HR, w świetle nowych obowiązków, muszą informować kandydatów o tym, w jakim celu oraz jak długo będą przetwarzane podane przez nich dane, oraz kto będzie miał do nich dostęp. Mniejsze firmy – te, które zatrudniają mniej niż 250 pracowników – mają też pewne przywileje, których nie mają firmy duże. Jest to między innymi brak obowiązku prowadzenia rejestru czynności przetwarzania (o ile przetwarzane nie są dane wrażliwe). Mniejsze przedsiębiorstwa mają też więcej czasu na wdrożenie wszelkich wymagań i jest on dostosowany do ich możliwości. RODO wprowadziło więc szereg obowiązków, które mogą być kłopotliwe do wdrożenia dla przedsiębiorców. Jednakże rozporządzenie nakłada też na organy nadzorcze obowiązek edukacyjny, stąd osoby, których dane są przetwarzane będą bardziej świadome tego faktu i będą znać dokładne procedury[466].

Wprowadzenie RODO zakłada, że dzięki niemu konsumenci będą bardziej świadomi tego, jak przetwarzane są ich dane osobowe i jakie mają w tym zakresie prawa. Dlatego też sklepy internetowe mają obowiązek wprowadzenia do swoich regulaminów nowych zapisów, informujących klientów o tym, w jakim celu i w jaki sposób ich dane są przetwarzane. Oprócz tego, sklep internetowy musi zapewnić w swoim regulaminie, że nie udostępni danych osobowych konsumenta innym firmom, a

[464] Por. D. Adamski, *Unijne modele regulacji jawności i jej ograniczeń oraz ich wpływ na systemy krajowe*, [w:] *Jawność i jej ograniczenia*, red. G. Szpor, C. Mik, t. 11, *Standardy europejskie*, C.H. Beck, Warszawa 2016, s. 39.

[465] Zob. A. Bourka, P. Drogkaris, *Online platform for security of personal data processing: reinforcing trust and security in the area of electronic communications and online services*, Publications Office, Luxembourg 2019, s. 16.

[466] Zob. *Czym jest RODO…*, s. 1.

klient ma prawo zgłosić administratorowi chęć zaprzestania ich przetwarzania. Dodatkowo konsumenci muszą mieć świadomość tego, że w razie zauważenia wszelkich nieprawidłowości mogą złożyć skargę do GIODO[467].

RODO wprowadza szereg zmian oraz rozszerza zakres obowiązków administratorów oraz podmiotów przetwarzających dane. Celem przepisów jest również wyposażenie osób fizycznych oraz organów nadzorujących w skuteczne narzędzia reagowania na naruszenia Rozporządzenia. Bardzo istotną dla przedsiębiorców kwestią jest też określenie maksymalnego poziomu kar za naruszenia przepisów, które to kary mogą sięgnąć nawet 20 000 000 euro lub 4% całkowitego rocznego światowego obrotu przedsiębiorcy z roku obrotowego poprzedzającego naruszenie[468].

Ochrona danych osobowych nie będzie zatem sprowadzała się do wykonania kilku jasno określonych czynności, a raczej do zaprojektowania całego systemu tej ochrony – i ustawiania procedur osobno pod wszystkie procesy, jakie dzieją się w firmie i uwzględniają wykorzystanie danych osobowych. *Każdy przedsiębiorca działa inaczej. Inaczej zabezpiecza się dane w sektorze ubezpieczeniowym, inaczej w bankowym, a jeszcze inaczej w handlu internetowym. W związku z tym nie ma jednego szablonu, tylko każdy dostanie obowiązek stworzenia go sobie samemu. Przechodzimy z zamkniętego do otwartego modelu ochrony danych. Można powiedzieć, że to taka ochrona danych 2.0. Resort dostrzega to zagrożenie i w związku z tym będzie pomagał przedsiębiorcom odnaleźć kierunek, w jakim mają wprowadzać nowe rozwiązania dotyczące ochrony danych osobowych. Zaprojektowaliśmy przepis, w myśl którego urzędnik będzie upoważniony do wydawania tzw. dobrych praktyk, wskazujących rekomendowane sposoby zabezpieczania danych w każdym sektorze. To nie będą konkretne wytyczne, tylko raczej garść wskazówek i idei, którymi można się kierować – mówi pracownik ministerstwa cyfryzacji* – stwierdził dr Maciej Kawecki, doradca ministra w Ministerstwie Cyfryzacji[469].

Podejście do nowej ustawy na ternie innych państwo członkowskich Unii Europejskiej było zdecydowanie spokojniejsze w Polsce. Przedsiębiorcy nie reagowali

---

[467] Tamże.
[468] Zob. *RODO – rozporządzenie o ochronie danych osobowych*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/topics/RODO-ochrona-danych-osobowych.html, data dostępu: 26.12.2020.
[469] Zob. W. Maroszek, *RODO czyli ochrona danych 2.0. Nowe unijne przepisy oznaczają trudności dla przedsiębiorców*, https://businessinsider.com.pl/firmy/przepisy/rodo-gdpr-regulacje-o-ochronie-danych-osobowych-zmiany-w-firmach/21p6svs, data dostępu: 26.12.2020.

lękiem i strachem na zaproponowane zmiany. Tym, co odróżnia Polskę od innych krajów jest odwlekanie wprowadzania zmian. W większości państw członkowskich UE zmiany wprowadzano w firmach stopniowo. W efekcie z dniem wejścia w życie RODO firmy były gotowe na zmiany. Wszystko przebiegło płynnie i bez niepotrzebnego stresu. Co ważne, firmy zagraniczne wykazywały się również ogromną kreatywnością, jeśli chodzi o wypracowywanie własnego modelu ochrony danych osobowych. RODO oznacza bowiem przejście od modelu zamkniętego, który stosowany był dotychczas, do modelu o charakterze otwartym. W trosce o swoich obywateli władze Unii Europejskiej zdecydowały się na opublikowanie wskazówek mających pomóc we wdrożeniu RODO. Skierowane były one do małych oraz średnich przedsiębiorstw. Wszystkie wątpliwości zostały wyjaśnione w jasny, przystępny sposób. Udzielono odpowiedzi na najbardziej nurtujące pytania, które najczęściej pojawiały się w kontekście nowych przepisów. Wszystko po to, aby wprowadzanie zmian było jak najmniej dotkliwe[470].

RODO ma szeroki zakres zastosowania, co istotne, wykraczający poza terytorium UE. Zgodnie z art. 3 ust. 2 RODO organizacje, które nie posiadają jednostek organizacyjnych na terenie UE, podlegają jego przepisom, jeśli przetwarzają dane osobowe mieszkańców UE w związku z monitorowaniem ich zachowania na terenie UE lub oferowaniem im towarów lub usług, bez znaczenia, czy następuje to odpłatnie czy nie. Emanacja przepisów RODO poza terytorium UE, oprócz zwiększenia ochrony danych osobowych jej mieszkańców, jest wyrazem roli, jaką Unia wyznaczyła sobie w zakresie propagowania reprezentowanych przez nią wartości w dziedzinie ochrony danych. RODO ma ułatwić transgraniczne transfery danych poprzez wspieranie ujednolicenia systemów prawnych w skali globalnej.

RODO wprowadziło tzw. zasadę swobodnego przepływu danych osobowych, która obowiązuje na terytorium krajów należących do Europejskiego Obszaru Gospodarczego (kraje Unii Europejskiej oraz Islandia, Norwegia i Liechtenstein). Pozostałe kraje traktowane są jako tzw. państwa trzecie. Od 30 marca 2019 r. Wielka Brytania również jest traktowana jako państwo trzecie. Zgodnie z zasadą swobodnego transferu, przekazywanie danych pomiędzy administratorami danych osobowych i podmiotami przetwarzającymi mającymi siedzibę na wskazanym powyżej obszarze nie

[470] Zob. M. Zygmunt-Jakuć, *RODO w Polsce i w innych krajach członkowskich. Różnice w podejściu do wdrożenia*, https://bezowijania.com/rodo-w-polsce-i-innych-krajach-czlonkowskich-roznice-w-podejsciu-do-wdrozenia, data dostępu: 26.12.2020.

wymaga uzyskiwania żadnych dodatkowych zgód czy pozwoleń. Administratorzy danych mający siedzibę na terenie EOG mają obowiązek stosowania przepisów RODO, a zatem dane osobowe powinny być bezpieczne w równym stopniu. Jeśli administrator danych zamierza je przekazać poza terytorium Unii Europejskiej, musi zadbać o bezpieczeństwo transferu. Zgodnie z przepisami RODO procedura postępowania jest zależna od kraju, do którego dane mają zostać przekazane. Jeśli Komisja Europejska stwierdzi, że dane państwo spełnia odpowiedni stopień ochrony, przekazanie nie wymaga uzyskania odrębnego zezwolenia; w pozostałych przypadkach administrator danych jest – co do zasady – zobowiązany do uzyskania zezwolenia na przekazanie danych, chyba że zachodzą wyjątki wymienione w treści rozporządzenia[471].

Poziom ochrony danych wprowadzony przez poszczególne państwa wciąż jest mocno zróżnicowany, zaś niewiele z nich zdecydowało się zastosować standard porównywalny z unijnym, uznawanym za jeden z najwyższych na świecie. Natomiast podstawowym założeniem unijnego modelu ochrony danych osobowych jest zasada, że transfer danych osobowych z UE do państwa trzeciego może się odbyć tylko wtedy, gdy państwo trzecie zapewnia adekwatny stopień ochrony. Ochrona danych osobowych zapewniana przez RODO „przemieszcza się" wraz tymi danymi. Komisja Europejska wydała decyzje (o różnym charakterze i zakresie stosowania) uznające odpowiedni stopień ochrony danych osobowych wobec takich państw jak Andora, Argentyna, Australia, Izrael, Japonia, Kanada Szwajcaria, Urugwaj, Nowa Zelandia. Wśród nich zabrakło USA. W świetle danych statystycznych Komisji Europejskiej z 2016 r. to właśnie Stany Zjednoczone pozostają głównym partnerem gospodarczym UE, na którego przypada niemal 23% udziału w unijnym eksporcie towarów i usług. Dla porównania na drugim miejscu plasuje się Szwajcaria z prawie 10% udziału, zaś na trzecim Chiny, do których z UE trafia 8% eksportowanych dóbr i usług[472].

Gromadzenie danych, utrata prywatności oraz zagrożenia bezpieczeństwa są obecnie kwestiami o zasięgu globalnym, a RODO uważany jest za najbardziej rygorystyczny systemem ochrony danych na świecie. Wyznacza on „złotą regułę", będącą standardem dla innych jurysdykcji. Podobne ustawy przyjęto na przykład w Brazylii, Australii, Japonii, Korei Południowej czy Tajlandii. Obowiązująca w stanie

[471] Zob. *Transfer danych osobowych poza terytorium Unii Europejskiej*, https://poradnikprzedsiebiorcy.pl/-rodo-transfer-danych-osobowych-poza-terytorium-unii-europejskiej, data dostępu: 26.12.2020.
[472] Zob. E. Roguska, *Systemy ochrony danych*…, s. 2.

Kalifornia ustawa o ochronie danych osobowych konsumentów (The California Consumer Privacy Act – CCPA) jest najsurowszym prawem ochrony prywatności w całych Stanach Zjednoczonych, jednakże na terenie USA nie wprowadzono dotąd żadnych federalnych przepisów w zakresie ochrony danych osobowych, które obowiązywałyby we wszystkich branżach i obszarach działalności[473].

We wrześniu 2016 r. Komisja Europejska zaprezentowała projekt nowej regulacji, która przewiduje swobodny przepływ informacji niemających charakteru danych osobowych. Chodzi o budowanie Systemu Europejskich Danych Ekonomicznych („Building a European Data Economy"), który ma być częścią Cyfrowej Strategii Jednolitego Rynku (Digital Single Market Strategy - DSM Strategy)[474].

Najważniejszą korzyścią związaną z reformą ochrony danych osobowych jest pobudzenie wzrostu gospodarczego poprzez redukcję kosztów i biurokracji dla europejskich przedsiębiorstw, w szczególności dla małych i średnich przedsiębiorstw (MŚP). Wynika to z tego, że Komisja Europejska zaproponowała zwolnienie MŚP z szeregu postanowień rozporządzenia o ochronie danych, podczas gdy uchylona tym rozporządzeniem dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 1995 r. miała zastosowanie do wszystkich europejskich przedsiębiorstw niezależnie od ich wielkości. Jednakże zgodnie z nowymi przepisami MŚP korzystają z czterech ograniczeń biurokracji:

1) zwolnienie z obowiązku powoływania osoby odpowiedzialnej za ochronę danych osobowych (np. Administrator bezpieczeństwa informacji – w rozporządzeniu zwany jako Inspektor danych) jako osobnej funkcji: W Polsce powyższy obowiązek już został zniesiony: rozporządzenie ujednoliciło ten stan prawny w całej Unii Europejskiej;
2) brak konieczności dokonywania zgłoszeń zbiorów danych do instytucji odpowiedzialnej za nadzór nad prawidłowym przetwarzaniem danych osobowych (GIODO);

[473] Zob. *RODO i przepisy o ochronie danych*…, s. 1.
[474] Zob. K. Irion, *Digital Single Market Strategy (DSM Strategy),* European Parliament, Brussels 2018, s. 34.

3) możliwość pobierania przez przedsiębiorców opłat za zapewnienie dostępu do danych osobowych, ich poprawiania itd. w przypadku, gdy wnioski w tych sprawach będą powtarzały się zbyt często;
4) MŚP nie mają obowiązku przeprowadzenia oceny wpływu na ochronę prywatności.

Zasadniczą rolę odgrywają mechanizmy kontrolne bezpieczeństwa danych osobowych. Zgodnie z rozporządzeniem w podmiotach publicznych (np. urząd gminy, ministerstwo czy inny organ centralny), w przedsiębiorstwach zatrudniających więcej niż 25 stałych pracowników oraz w sektorze małych i średnich przedsiębiorstw, których przetwarzanie danych osobowych jest podstawową działalnością gospodarczą[475] zaleca się powołanie osoby odpowiedzialnej za ochronę danych osobowych[476].

W obowiązującej dyrektywie jest mowa o „usunięciu danych". Z kolei w rozporządzeniu jest mowa o „prawie bycia zapomnianym". Elementem odróżniającym je od siebie, jest fakt, że przedmiotem tego drugiego są w szczególności dane osobowe udostępnione przez osobę zainteresowaną, gdy była ona dzieckiem, czyli w okresie kiedy nie dysponowała doświadczeniem umożliwiającym świadome przewidywanie konsekwencji swoich działań. Prawo do bycia zapomnianym nie odnosi się jednak wyłącznie do danych osobowych udostępnionych przez dzieci i młodzież, a dotyczy również osób dorosłych[477].

W założeniu prawo do bycia zapomnianym daj możliwość całkowitego usunięcia informacji, które już zostały rozpowszechnione czy też przez nich samych, czy też bez ich zgody[478]. Zwiera w sobie kilka aspektów.

Pierwszy aspekt wiąże się np. z lekkomyślnym udostępnianiem fotografii na portalach społecznościowych, które mogą mieć nieodpowiednią treść. Powyższe dotyczy zarówno młodzieży, jak i rodziców, którzy upubliczniają zdjęcia swoich potomków.

Drugi aspekt dotyczy niekorzystnych informacji, które psują reputację.

[475] Por. A. Dmochowska, *Współadministratorzy danych – ułatwienie dla grup przedsiębiorców,* „Jurysta" 2017, nr 3, s. 42-43.
[476] Zob. M. Barański, M. Giernak, *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego (uwagi na tle ferenda),* „Państwo i Prawo" 2017, nr 10, s. 90-99.
[477] Por. J. Buchalska, *Prawo do bycia zapomnianym – w orzecznictwie polskim,* [w:] *{Rawo prywatności jako reguła społeczeństwa informacyjnego,* red. K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak, Wydawnictwo C.H. Beck, Warszawa 2017, s. 147.
[478] Por. T. Banyś, A.J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Prescom, Wrocław 2017, s. 26.

Rozwiązanie to nie jest jednak w pełni rewolucyjne, potwierdził to Trybunał Sprawiedliwości Unii Europejskiej w sprawie przeciwko wyszukiwarce Google[479]. Na podstawie wskazanego orzeczenia również w Polsce przeglądarka Google na żądanie rocznie usuwa odpowiednie wyniki wyszukiwania.

Nowe przepisy rozporządzenia implementowanie do krajowych systemów prawnych regulują także kwestia tworzenia profili[480]. Rozporządzenia znosi również generalny obowiązek rejestracji zbioru danych[481]. Zgodnie z przepisami rozporządzenia to Administrator danych osobowych oraz procesor danych ma obowiązek przechowywać dokumentację dotyczącą zbioru, która musi być ujawniona organowi ochrony danych na jego żądanie[482].

Rozporządzenie wprowadza kluczowe zmiany dotyczące:

- uprzedniej zgody – która może być udzielona przez organ ochrony danych i jest wymagana w dwóch przypadkach: przekazania danych za granicę, gdy są stosowne tzw. klauzule umowne; jeżeli nie ma odpowiednich środków ochronnych zagwarantowanych przez prawo państwa przekazującego;
- uprzedniej konsultacji przetwarzania danych – z wyników oceny administratora danych może wynikać, że przetwarzanie danych wiąże się z wysokim stopniem ryzyka złamania prawa z uwagi na charakter danych, ich zakres lub cele przetwarzania.

Ważnym elementem jest także udostępnianie danych do państwa trzeciego[483]. Zgodnie z dyrektywą o przetwarzaniu danych osobowych, przekazywanie danych osobowych do państwa trzeciego zapewnia odpowiedni stopień ochrony danych. Chodzi tu głównie o to, iż to Komisja może stwierdzić, że państwo trzecie poprzez

[479] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r. w sprawie Google Spain SL i Google Inc. Przeciwko Agencia Espanola de Protection de Datos (AEPD) i Mario Sosteja Gonzale, sygn. akt. C-131/12.

[480] Zob. M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych,* „Europejski Przegląd Prawa" 2017, nr 5, s. 37-42.

[481] Por. M. Cwener, *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych,* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia,* red. M. Kawecki, T. Osiej, Wydawnictwo C.H. Beck, Warszawa 2017, s. 97.

[482] Por. M. Chodorowski, *Nowe prawa i obowiązki administratorów bezpieczeństwa informacji (inspektorów ochrony danych osobowych w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29,* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia,* red. M. Kawecki, T. Osiej, Wydawnictwo C.H. Beck, Warszawa 2017, s. 141-158.

[483] Zob. J. Byrski, *Nowe zasady przekazywania danych osobowych do państwa trzeciego, jako instrument prawny oddziaływania na gospodarkę,* [w:] *Prawne instrumenty oddziaływania na gospodarkę,* red. A. Powałowski, Wydawnictwo C.H. Beck, Warszawa 2016, s. 570-582; Por. B. Baran, K. Południak-Gierz, *Aspekt podmiotowy udostępniania informacji publicznej na przykładzie regulacji polskich i szwedzkich,* „Przegląd Prawa Publicznego" 2017, nr 10, s. 34.

swoje ustawodawstwo krajowe lub zobowiązania międzynarodowe, zapewnia odpowiedni stopień ochrony[484].

Dotychczasowe doświadczenia ustawodawców unijnych wskazały, że sankcje karne (np. kara pozbawienia wolności) nie przyniosły spodziewanych efektów[485]. Znacznie większą skutecznością cechowały się natomiast kary o charakterze finansowym. Rozporządzenie Unii Europejskiej zawiera dość rozbudowany system tych kar. Zaczynają się one od ostrzeżeń do kar w wysokości 20 mln EUR lub do 4 % rocznego światowego dorobku[486].

Nie ulega wątpliwości, iż rozporządzenie jest doniosłym aktem prawnym i długo oczekiwanym przez społeczność europejską[487]. Długie doświadczenie w poszczególnych krajach, zebrane za pomocą Zespołu roboczego ds. ochrony osób fizycznych pozwoliło zebrać doświadczenia państw UE oraz wypracować nowe rozwiązania, w związku z postępującym rozwojem techniki. Dlatego od momentu wejścia w życie ogólnego rozporządzenia o ochronie danych tj. 25 maja 2018 r. można już mówić o jednym zbiorze przepisów dotyczących ochrony danych w systemie Unii Europejskiej[488]. Oznacza to, że w dniu 25 maja 2018 r. upłynął dwuletni okres przygotowania jaki Unia dała państwom oraz przedsiębiorcom by dostosowały przepisy wewnętrzne do regulacji europejskich. Choć w Polsce od 20 lat obowiązywała ustawa o ochronie danych osobowych, której rozwiązania wielokrotnie były bardziej rygorystyczne niż Rozporządzenia, w krajach europejskich problematyka ochrony danych osobowych często była pomijana. Pod wpływem UE wprowadzono zatem kluczowe zmiany, które były wymagane ze względu na gwałtowny rozwój technologiczny za którym do tej pory nie nadążały działania ustawodawców europejskich.

---

[484] Zob. Trybunał Sprawiedliwości Unii Europejskiej, Komunikat Prasowy nr 117/15, Luksemburg, 6 października 2015 r.

[485] Por. A. Romkowski, *Przepisy karne ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. w kontekście standardów ochrony danych osobowych w rozporządzeniu GOPR (RODO) z dnia 27 kwietnia 2016 r.,* "Przegląd Prawno-Ekonomiczny" 2018, nr 1, s. 268.

[486] Zob. A. Gonschior, *Ochrona danych …,* s. 240.

[487] Zob. D. Fleszer, *Zabezpieczenie danych osobowych – zakres, obowiązki i sankcje za jego naruszenie,* [w:] *Bezpieczeństwo informacji publicznej,* red. D. Fleszer, Wyższa Szkoła Humanitas, Sosnowiec 2017, s. 83.

[488] Zob. *Reforma unijnych przepisów o ochronie danych w 2018 roku,* źródło: www.ec.europa.eu/commission/priorites/justice-and-fundamental-rights/data -protection/2018-reform-eu-data-protection-rules_pl, data dostępu: 06.03.2019.

3.2.2. Standardy o charakterze „miękkiego prawa”

Prawo unijne (tak jak międzynarodowe) posługuje się aktami niewiążącymi prawa pochodnego. W literaturze przedmiotu wskazywany jest podział na dwie kategorie pojęciowe: akty nazwane i akty nienazwane[489]. Do nazwanych należą wymienione w art. 288 TFUE zalecenia i opinie[490]. W drugiej kategorii zawierają się różnorodne instrumenty uchwalane w praktyce przez instytucje unijne, takie jak: komunikaty, rezolucje, noty informacyjne i opinie. Ponadto mogą występować również inne instrumenty,, np. deklaracje, konkluzje Rady, noty i wytyczne Komisji, uchwały, wspólne stanowiska i zalecenia, porozumienia, programy i strategie, białe i zielone księgi[491]. Już w 2007 r. Komisja Prawna PE w dokumencie roboczym w sprawie instytucjonalnych i prawnych skutków stosowania instrumentów „miękkiego prawa” zwracała uwagę na rozszerzanie się zasięgu soft law i przestrzegała przed działaniami stojącymi w sprzeczności z jasnością i pewnością prawną[492].

Analizując standardy dotyczące ochrony danych osobowych w systemie aksjologicznym Unii Europejskiej, należy także zwrócić uwagę na te, które pomimo tego, iż nie posiadają mocy prawnie wiążącej, odgrywają zasadniczą rolę w tym zakresie. Ochronie danych osobowych poświęcono, bowiem wiele tego typu dokumentów, jak np. poruszono tę kwestię w decyzji ramowej Rady 2008/9777/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[493], czy też w decyzji Rady 2009/936/WSiSW z 30 listopada 2009. r. w sprawie przyjęcia przepisów wykonawczych dotyczących plików roboczych do celów analizy stosowanych przez Europol[494], w której wskazano m.in. iż, „dane osobowe” oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a „osoba możliwa do zidentyfikowania” to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio w szczególności na podstawie numeru

[489] Zob. S. Biernat, *Źródła prawa Unii Europejskiej,* [w:] *Prawo Unii Europejskiej,* red. J. Barcz, Warszawa 2006, s. 193.
[490] W celu wykonywania swych zadań oraz na warunkach przewidzianych w niniejszym Traktacie, Parlament Europejski wspólnie z Radą i Komisja uchwalają rozporządzenia i dyrektywy, podejmują decyzje, wydają zalecenia i opinie […] Zalecenia i opinie nie mają mocy wiążącej; dawny art. 249 TWE.
[491] S. Biernat, *Źródła prawa…,* jw., s. 227 – 228.
[492] Zob. (2007/2028(INI) przyjęty 15 marca 2007 r.
[493] Dz.Urz. UE L 350 z 30.12.2008 r. s. 60.
[494] Dz.Urz. UE L 325 z 11.12.2009, s. 14.

identyfikacyjnego lub co najmniej jednego znaku szczególnego związanego z jej tożsamością fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną. Warto przy tej okazji zwrócić uwagę na fakt, że w decyzji powołano się na Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych, przyjętą przez Radę Europy 28 stycznia 1981 r. oraz zalecenie nr R (87) 15 Komitetu Ministrów regulujące wykorzystywanie danych osobowych przez policję, przyjęte przez Radę Europy 17 września 1987 r.

W systemie prawa wspólnotowego kwestii ochrony danych osobowych dotyczy także Układ między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach[495].

W Opinii Europejskiego Inspektora Ochrony Danych Osobowych z 2006 r. podkreślono, iż „skuteczna ochrona danych osobowych jest ważna nie tylko dla osób, których dane dotyczą, ale także przyczynia się do powodzenia samej współpracy policyjnej i sądowej”[496]. Jak bowiem wskazano, w wielu aspektach oba interesy publiczne idą w parze.

Na szczególną uwagę zasługuje również Komunikat Komisji i Rady skierowany do Parlamentu Europejskiego z 2017 r. na temat wymiany i ochrony danych osobowych w zglobalizowanym świecie, w którym wskazuje się, iż większa kompatybilność między różnymi systemami ochrony danych osobowych ułatwiłaby międzynarodowy przepływ danych osobowych, zarówno w celach komercyjnych, jak i współpracy między organami publicznymi (np. Organami ścigania). Stwierdzono ponadto, iż „Unia powinna wykorzystać tę okazję do promowania swoich wartości ochrony danych i ułatwienia przepływu danych poprzez zachęcanie do konwergencji systemów prawnych”[497].

Za kluczowy uznaje się także Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 24 stycznia 2018 r. – Wzmocniona ochrona, nowe możliwości[498]. Zawarto w nim bowiem wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego

[495] Dz.Urz. UE L 00 nr 239, z 22.09.2000, s. 13.

[496] Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych, COM(2005) 475 wersja ostateczna, źródło: www.eur-lex.europa.eu/legal-content/ENTXT/?uri=CELEX:52006XX0225(01), data dostępu: 23.04.2019.

[497] Komunikat Komisji do Parlamentu Europejskiego i Rady: Wymiana i ochrona danych osobowych w zglobalizowanym świecie, COM/2017/07/ final, źródło: www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:7:FIN, data dostępu: 23.04.2019.

rozporządzenia o ochronie danych od dnia 25 maja 2018 r.[499] Komunikat ten w szczególności:

- przypomina główne innowacje i możliwości, jakie wiążą się z nowym prawodawstwem UE w zakresie ochrony danych;
- podsumowuje dotychczasowe prace przygotowawcze na szczeblu UE;
- nakreśla, co Komisja Europejska, krajowe organy ochrony danych i administracje powinny nadal robić aby wdrożenie nowych przepisów okazało się sukcesem;
- ustanawia środki, które Komisja zamierza podjąć w najbliższych miesiącach.

Ponadto równolegle z przyjęciem niniejszego komunikatu Komisja uruchomiła internetowy zestaw narzędzi, aby pomóc zainteresowanym stronom przygotować się do stosowania rozporządzenia oraz, przy wsparciu biur przedstawicielskich, przeprowadzić kampanię informacyjną we wszystkich państwach członkowskich.

Biorąc pod uwagę najnowsze osiągnięcia w zakresie ochrony danych osobowych z zakresu „miękkiego prawa", należy brać także pod uwagę: orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej[500], wytyczne tematyczne wydane przez Europejskiego Inspektora Ochrony Danych (EOID)[501] czy też dokumenty tematyczne grupy roboczej 29[502] (od 25 maja 2018 r. zastąpionej przez Europejską Radę Ochrony Danych (EDPB))[503].

Są to przydatne przewodniki, które mogą pomóc w określonych kwestiach lub odpowiedzieć na konkretne pytania z obszaru ochrony danych osobowych.

---

[498] Zob. Communication from the Commission to the European Parliament and the Council-Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation as 25 May 2018, COM/2018/043 final, Doc. 52018DC0043.

[499] Zob. M. Romanowicz, *Ochrona danych osobowych – ważny komunikat Komisji Europejskiej,* źródło: www.portalmorski.pl/prawo-polityka/38479-ochrona-danych-osobowych-wazny-komunikat-komisji-europejskiej-, data dostępu: 23.04.2019.

[500] Zob. *Case – law overview,* źródło: www.eds.europa.eu/data -protection/eu-institutions-dpo/case-law-guidance_en, data dostępu: 23.04.2019.

[501] Zob. *European Data Protection Supervisor,* źródło: www.eds.europa.eu/data -protection/eu-institutions-dpo/case-law-guidance_en, data dostępu: 23.04.2019

[502] Zob. *Opinions and Recommendations,* źródło: *European Data Protection Supervisor,* źródło: www.eds.europa.eu/data -protection/eu-institutions-dpo/case-law-guidance_en, data dostępu: 23.04.2019

[503] Europejska Rada Ochrony Danych ma status organu UE posiadającego osobowość prawną i niezależny secretariat. EDPB ma szerokie Zob. *European Data Protection Board,* źródło: www.ec.europa.eu/info/law-topic/data-protection/, data dostępu: 24.04.2019.

3.3. Mechanizmy egzekwowania standardów dotyczących bezpieczeństwa danych osobowych w państwach członkowskich

3.3.1. Faza procedury akcesyjnej

Procedura akcesyjna do Unii Europejskiej dotyczy tego państwa, które staje się oficjalnym kandydatem do członkostwa. Przechodzi ono wówczas formalne negocjacje. Jest to proces obejmujący przyjęcie ustanowionego prawa UE, przygotowanie do właściwego stosowania i egzekwowania go oraz implementacji reform sądowniczych., administracyjnych, gospodarczych, jak również innych niezbędnych temu państwu do spełnienia warunków akcesji[504].

Kiedy negocjacje i towarzyszące im reformy zostaną zakończone w sposób zadawalający obie strony, kraj może przystąpić do UE. Należy jednak zaznaczyć, iż negocjacje członkowskie nie mogą rozpocząć się, dopóki wszystkie rządy UE nie uzgodnią, w formie jednomyślnej decyzji Rady UE, ram lub mandatu do negocjacji z krajem kandydującym.

Negocjacje w ramach każdego etapu opierają się na następujących elementach:

1. Przegląd - Komisja przeprowadza szczegółową analizę, wraz z krajem kandydującym, każdej dziedziny polityki, aby określić, w jakim stopniu dany kraj jest przygotowany. Ustalenia według poszczególnych dziedzin są przedstawiane państwom członkowskim przez Komisję w formie sprawozdania z przeglądu. Wniosek z tego sprawozdania jest zaleceniem Komisji, aby albo otworzyć negocjacje bezpośrednio, albo wymagać spełnienia pewnych warunków – kryteriów akcesji – w pierwszej kolejności.
2. Stanowisko negocjacyjne – przed rozpoczęciem negocjacji kraj kandydujący musi przedstawić swoje stanowisko, a UE musi przyjąć wspólne stanowisko. W przypadku większości dziedzin UE ustali kryteria odniesienia na tym stanowisku, które muszą zostać spełnione przez kraj kandydujący przed zamknięciem negocjacji w danej dziedzinie polityki[505].

[504] Etapy akcesji szerzej opisane na: www.ec.europa.eu/neighbourhood-enlargement/policy/steps-towards-joining_en, data dostępu: 16.05,2019.
[505] Tamże.

Tempo negocjacji jest zatem uzależnione od szybkości reform i dostosowania do przepisów UE w każdym kraju. Czas trwania negocjacji może być różny – rozpoczęcie w tym samym czasie, co inny kraj, nie gwarantuje równoczesnego zakończenia.

Traktat akcesyjny jest dokumentem, który cementuje członkostwo danego kraju w UE. Zawiera szczegółowe warunki członkostwa, wszystkie ustalenia przejściowe i terminy, a także szczegóły ustaleń finansowych i wszelkich klauzul ochronnych. Jednak po podpisaniu traktatu kandydat staje się krajem przystępującym Oznacza to, że oczekuje się, że stanie się pełnoprawnym członkiem UE w dniu określonym w traktacie, pod warunkiem jego ratyfikacji. W międzyczasie korzysta się ze specjalnych ustaleń, takich jak możliwość komentowania projektów wniosków UE, komunikatów, zaleceń lub inicjatyw oraz „statusu aktywnego obserwatora" w organach i agencjach UE (ma prawo zabierać głos ale nie głosować)[506].

Europejski model ochrony prywatności odzwierciedla pewną koncepcję ludzkości i społeczeństwa. Celem Unii Europejskiej jest wspieranie polityki danych, która stawia na pierwszym miejscu interesy obywateli. Dlatego stale próbuje poszukiwać równowagi między dążeniem do innowacji a ochroną swoich obywateli.

Wiele z obecnych państw członkowskich UE nie było związanych na etapie akcesji regulacjami związanymi z ochroną danych osobowych. W systemie Wspólnot Europejskich, a następnie Unii Europejskiej brakowało bowiem przez dłuższy czas konkretnych przepisów w tym zakresie. Jedynym wymogiem stawianym w chwili starania się o członkostwo w Unii, było ratyfikowanie Konwencji nr 108. Jak wskazuje F. Jasiński, „dopiero na początku lat. 90. rozpoczęły się prace nad właściwym *acquis* w tym zakresie"[507].

Dopiero potrzeba ochrony danych osobowych w Unii Europejskiej odzwierciedlona w formułowaniu nowych dyrektyw i umieszczaniu w nich tego zagadnienia sprawiła, że musiało nastąpić wzmocnienie tejże ochrony w państwach starających się o członkostwo[508]. Tworzone przepisy zaczęły mieć znaczenie zarówno w sektorze publicznym, jak i prywatnym, zapewniając tym samym szeroki zakres ochrony.

[506] Zob. *Accession to the EU,* źródło: www.ec.europa.eu/neighbourhood-enlargement/policy/glossary/terms/accessior, data dostępu: 16.05.2019.
[507] F. Jasiński, *Ochrona danych osobowych w porządku prawnym Unii Europejskiej,* „Kwartalnik Prawa Publicznego" 2003, nr 3, s. 208.
[508] Zob. M. Gołda-Sobczak, *Unia Europejska…,* s. 151.

Należy także przypomnieć, iż dopiero w 2001 r. Komisja Europejska w wyniku przeprowadzonych konsultacji społecznych, wskazała na ten problem w swym komunikacie zatytułowanym „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”[509], który zdaniem Europejskiego Inspektora Ochrony Danych stanowił „istotny krok w kierunku zmiany ustawodawczej”, która z kolei stanowić miała „najważniejszą reformę w dziedzinie ochrony danych osobowych w UE od czasu przyjęcia dyrektywy 95/46/WE”[510].

Celem europejskiego ustawodawcy było zwiększenie świadomości osób zarówno w tych państwach, które starały się o członkostwo w Unii, jak i tych, które taki status już posiadały, co tak naprawdę dzieje się z ich danymi, oraz jakie te osoby posiadają prawa[511].

Wpływ na kształt procedury akcesyjnej UE miała także potrzeba dostosowania przepisów o ochronie danych osobowych do stale rozwijających się nowych technologii. Kluczowa była także chęć rozszerzenia praw osób, których dane dotyczą. Co więcej, europejski ustawodawca dostrzegł, że wdrażając dyrektywę 95/46/WE, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami podejmowanymi w Internecie[512].

Dziś można powiedzieć, iż ogólne rozporządzenie o ochronie danych nadaje daleko idące uprawnienia osobom, których dane dotyczą. Prawa te dają osobie, której dane dotyczą, większą kontrolę nad dotyczącymi jej informacjami. Rozporządzenie dostrzega przede wszystkim, iż osoby fizyczne powinny mieć kontrole nad własnymi danymi osobowymi. Ponadto osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe poczucie pewności prawa i jego stosowania w praktyce[513].

---

[509] European Commission Communication from the Commission to the European Parliament, the Council, The Economic and Social Committee and The Committee of the Regions”, *A comprehensive approach on personal data protection in the European Union,* Brussels, 4.11.2010, COM(2010)609 final.

[510] Zob. Opinia Europejskiego Inspektora Ochrony Danych dotycząca komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów – “Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”, (2011/C 181/01), źródło: www.eds.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_pl.pdf, data dostępu: 20.05.2019.

[511] Zob. A. Dmochowska, *Obowiązek informacyjny,* [w:] *Unijna ochrona danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, Ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, 2. wyd. Wydawnictwo C.H. Beck, Warszawa 2018, s. 25.

[512] Zob. A. Dmochowska, *Prawa osoby, której dane dotyczą,* [w:] *Unijna ochrona danych…,* j.w., s. 41.

[513] Tamże.

Istotne jest też to, jak europejska opinia publiczna podchodzi do ochrony danych osobowych. W kwestii tej przeprowadzone były badania obejmujące wszystkie państwa członkowskie Unii Europejskiej. Z badań tych wynika, że 62% obywateli UE przywiązuje dużą wagę do ochrony danych osobowych i oczekuje skutecznego zabezpieczenia danych drogą odpowiednich regulacji prawnych[514].

3.3.2. Faza członkostwa

Od 2009 r. ochrona danych osobowych jest jednym z podstawowych praw Unii Europejskiej[515]. Jest to szczególnie istotne z punktu widzenia procedury monitoringowej państw członkowskich, bowiem pojawił się wówczas zarys nowych ram prawnych, które zaczęły obowiązywać od 25 maja 2018 r. Negocjacje dotyczące nowego rozporządzenia trwające ponad cztery lata, od stycznia 2012 r. do kwietnia 2016 r. doprowadziły do ogólnej reformy systemu ram prawnych ochrony danych osobowych[516]. Dwuletni okres przejściowy pod względem jego wdrożenia był okazją do podniesienia świadomości i wzmocnienia pozycji europejskich obywateli, a także osób odpowiedzialnych za przetwarzanie ich danych wraz z podwykonawcami. Stanowiło to także doskonały moment do monitoringu państw pod względem dostosowawczym do nowych wyzwań stawianych w tym obszarze.

Wkrótce po wejściu w życie rozporządzenia, w połowie 2016 r., Komisja nawiązała współpracę z władzami państw członkowskich, organami ochrony danych i zainteresowanymi stronami w celu przygotowania stosowania rozporządzenia i zapewnienia wsparcia oraz doradztwa[517]. Współpraca ta podjęta został także w celu wsparcia państw w okresie przejściowym, aby zapewnić najwyższy możliwy poziom spójności[518]. W tym celu Komisja powołała grupę ekspertów, która miała towarzyszyć państwom w ich wysiłkach na rzecz przygotowania rozporządzenia. Grupa, ta działała jako forum, na którym państwa członkowskie mogły dzielić się doświadczeniami i

[514] Zob. D. Patoglou, F. Dunkerley, S. Patil, N. Robinson, *Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study*, "Computers in Human Behavior", 2017, vol. 75, p. 811.
[515] Por. F. Pizzetti, *Europejska ochrona danych osobowych,* „Zeszyty Naukowe USz Praw." 2010, nr 22, s. 5-15.
[516] Zob. A. Adamski, *Unijne modele regulacji jawności …,* s. 43.
[517] Por. A. Gonschior, *Ochrona danych osobowych a prawo …,* s. 239-242.
[518] Zob. M. Kawecki, *Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych*, Wolters Kluwer, Warszawa 2017, s. 24.

wiedzą. Komisja uczestniczyła wówczas także w dwustronnych spotkaniach z władzami państw członkowskich w celu omówienia kwestii pojawiających się na szczeblu krajowym[519].

Twierdzono wówczas, iż nowe regulacje jeszcze bardziej wzmocnią zdolność UE do aktywnego promowania ochrony danych i ułatwią ich transgraniczny przepływ, zachęcając do konwergencji systemów prawnych na całym świecie[520]. Co więcej unijne przepisy dotyczące ochrony danych były coraz częściej uznawane na szczeblu międzynarodowym za ustanawiające niektóre z najwyższych standardów ochrony danych na świecie. Modernizacji uległa również konwencja 108 Radu Europy, jedynie prawnie wiążący wielostronny instrument w dziedzinie ochrony danych osobowych. Komisja podjęła starania, aby odzwierciedlała te same zasady, które były zawarte w unijnych przepisach o ochronie danych. Ponadto Komisja postanowiła aktywnie wspierać szybkie przyjęcie zmodernizowanego testu konwencji, tak aby UE stała się jej stroną. Komisja podjęła starania w celu zachęcenia państw poza UE do ratyfikowania Konwencji 108 RE i jej protokołu dodatkowego.

Kluczowe znaczenie miało przyjęcie w UE regulacji określającej ogólne zasady ochrony danych osobowych[521]. Rozporządzenie General Data Protection Regulation (EU) 2016/679 (GDPR) ma bezpośrednie zastosowanie do wszystkich państw członkowskich[522]. Oznacza to, że wchodzi ono w życie i ma zastosowanie niezależnie od wszelkich środków prawa krajowego. Niemniej jednak, zgodnie z rozporządzeniem, państwa członkowskie muszą podjąć niezbędne kroki w celu dostosowania swojego ustawodawstwa poprzez uchylenie i zmianę obowiązujących przepisów oraz ustanowienie krajowych organów ochrony danych, wybór jednostki akredytującej i określenie zasad pojednania wolności słowa i ochrony danych[523].

Preambułą RODO (motyw 11) stanowi, że aby ochrona danych osobowych w Unii była skuteczna należy zapewnić równorzędne uprawnienia w zakresie

[519] Zob. M. Zadrożny, *Reorganizacja systemu ochrony danych,* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018, s. 1-2.
[520] Zob. Reflections Paper on Harnessing Globalisation, COM(2017)240.
[521] Zob. M. Krzysztofek, *GDPR, General Data Protection Regulation (EU) 2016/679 : post-reform personal data protection in the European Union*, Kluwer Law International, Alphen aan den Rijn 2019, s. 23.
[522] Art. 288 TFUE.
[523] Zob. M. Gawronski, *Guide to the GDPR*, Kluwer Law International, Alpena aan den Rijn 2019, s. 34.

monitorowania i egzekwowania przepisów o ochroni danych osobowych oraz równorzędne kary za naruszenia tych przepisów w państwach członkowskich[524].

Warto także przypomnieć, iż rozporządzenie daje państwom członkowskim możliwość dalszego sprecyzowania stosowania zasad ochrony danych w określonych dziedzinach tj.: sektor publiczny[525], zatrudnienie i zabezpieczenie społeczne[526], medycyna prewencyjna i zawodowa[527], zdrowie publiczne, cele archiwizacji w interesie publicznym, nauka lub do celów badań historycznych lub celów statystycznych[528], krajowy numer identyfikacyjny[529], publiczny dostęp do oficjalnych dokumentów[530] i obowiązek zachowania tajemnicy[531]. Ponadto w odniesieniu do danych genetycznych, danych biometrycznych i danych dotyczących zdrowia rozporządzenie upoważnia państwa członkowskie do utrzymania lub wprowadzenia dalszych warunków, w tym ograniczeń[532].

Dostosowując swoje ustawodawstwo krajowe, państwa członkowskie muszą wziąć pod uwagę fakt, że wszelkie środki krajowe, które spowodowałyby przeszkodę w bezpośrednim stosowaniu rozporządzenia i zagroziłyby jego jednoczesnemu i jednolitemu stosowaniu w całej UE są sprzeczne z Traktatami[533].

Ponadto założono, iż w przypadku, gdy państwa członkowskie nie podejmą niezbędnych działań wymaganych na mocy rozporządzenia, spóźnią się z ich przyjęciem lub skorzystają z klauzul specyfikacji określonych w rozporządzeniu w sposób sprzeczny z rozporządzeniem, Komisja wykorzysta wszystkie dostępne do dyspozycji narzędzia, w tym odwołanie się do postępowania w sprawie naruszenia.

Zasadnicze znaczenie dla zapewnienie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w UE ma ustanowienie w pełni niezależnych organów nadzoru w każdym państwie członkowskim. Organy te muszą działać zgodnie

[524] Zob. M. Zadrożny, *Środki ochrony prawnej* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018, s. 191.
[525] Art. 6 ust. 2 rozporządzenia.
[526] Artykuły 88 i 9 ust. 2 lit. b.
[527] Art. 9 ust. 2 lit. h) i (i) rozporządzenia.
[528] Art. 9 ust. 2 lit. J) rozporządzenia.
[529] Art. 87 rozporządzenia.
[530] Art. 86 rozporządzenia.
[531] Art. 90 rozporządzenia.
[532] Art. 9 ust. 4 rozporządzenia.
[533] Por. Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 31 stycznia 1978 r. w sprawie Fratelli Zerbone SNc przeciwko Amministrazione delle finanse dello Stato, sprawa 94/77, ECLI:EU:C:1978:17.

z przepisami rozporządzenia niezależnie[534], dzięki czemu są one odpowiednio przygotowane do skutecznego rozpatrywania skarg, prowadzenia skutecznych dochodzeń, podejmowania wiążących decyzji oraz nakładania skutecznych i odstraszających sankcji. Dyspozycję tę zastosowano np. w ustawodawstwie Rumunii[535].

Organy ochrony danych są naturalnymi rozmówcami i pierwszym punktem kontaktowym dla ogółu społeczeństwa, przedsiębiorstw i administracji publicznej w kwestiach dotyczących rozporządzenia. Rola organów ochrony danych obejmuje informowanie administratorów danych i podmiotów przetwarzających o ich obowiązkach oraz podnoszenie świadomości i zrozumienia opinii publicznej w zakresie zagrożeń, zasad, zabezpieczeń i praw związanych z przetwarzaniem danych[536].

Krajowe organy ochrony danych odgrywają zatem centralną rolę, ale względny brak równowagi między zasobami ludzkimi i finansowymi przydzielonymi im w różnych państwach członkowskich może zagrozić ich skuteczności, a ostatecznie całkowitej niezależności wymaganej na mocy rozporządzenia. Może to również negatywnie wpłynąć na sposób, w jaki organy danych są w stanie wykonywać uprawnienia, takie jak uprawnienia dochodzeniowe. Zachęca się przy tym państwa do wypełnienia ich prawnego obowiązku zapewnienia swoim krajowym organom ochrony danych zasobów ludzkich, technicznych i finansowych, pomieszczeń i infrastruktury niezbędnych do skutecznego wykonywania swoich zadań i wykonywania ich uprawnień.

W Komunikacie Komisji Europejskiej i Rady z 2017 r. wskazano, iż reforma w obszarze ochrony danych osobowych upoważniła Komisję do rozwijania mechanizmów współpracy międzynarodowej w celu ułatwienia egzekwowania przepisów o ochronie danych, w tym za pomocą porozumień o wzajemnej pomocy. Uznaje to wkład, jaki ściślejsze formy współpracy między organami nadzoru na szczeblu międzynarodowym mogłyby wnieść, aby zapewnić zarówno skuteczniejszą ochronę praw indywidualnych, jak i większą pewność prawną dla przedsiębiorstw[537].

---

[534] Art. 52 ust. 4 rozporządzenia.

[535] Zob. D.C. Mâță, *The protection of personal data in the context of national security protection measures*, Universul Juridic, 2018 (Suplement), s. 144.

[536] M. Zadrożny, *Uprawnienia organu nadzorczego,* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018, s. 180.

[537] Komunikat Komisji do Parlamentu Europejskiego i Rady: Wymiana i ochrona danych osobowych w zglobalizowanym świecie, COM/2017/07/ final.

Przedsiębiorcy przetwarzający dane mogą korzystać z nowych narzędzi przewidzianych w rozporządzeniu jako elementu wykazującego zgodność, takich jak kodeksy postępowania, czy też mechanizmy certyfikacji. Są to podejścia oddolne, które pochodzą od społeczności biznesowej, stowarzyszeń lub innych organizacji reprezentujących kategorie kontrolerów lub przetwórców i odzwierciedlają najlepsze praktyki, ważne wydarzenia w danym sektorze lub mogą informować o poziomie ochrony danych wymaganych przez niektóre produkty i usługi. Rozporządzenie przewiduje uproszczony zestaw zasad dla takich mechanizmów, uwzględniając realia rynkowe (np. certyfikacja przez jednostkę certyfikującą lub organ ochrony danych).

Organem odpowiedzialnym za stosowanie RODO jest Europejska Rada Ochrony Danych (EROD)[538], która powinna w określonym terminie wydawać opinie, jeżeli tak postanowią większością głosów jej członkowie lub jeżeli zwróci się do niej z takim wnioskiem organ nadzorczy, którego sprawa dotyczy, lub Komisja. EROD powinna być także umocowana do przyjmowania prawnie wiążących decyzji w razie sporów między organami nadzorczymi[539].

EROD powinna przyczyniać się do spójnego stosowania RODO w całej Unii, m.in. poprzez doradzanie Komisji – w szczególności w sprawie stopnia ochrony w państwach trzecich lub organizacjach międzynarodowych – i propagowanie współpracy organów nadzorczych w całej Unii. Wypełniając swoje zadania[540].

Zasadniczą rolę w obszarze unijnej ochrony danych osobowych, przypisuje się także Europejskiemu Inspektorowi Ochrony Danych (EOID). Jest to niezależny organ nadzoru Unii Europejskiej, który został powołany na mocy rozporządzenia nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[541]. Jego głównym zadaniem jest gwarantowanie, że instytucje i organy europejskie respektują prawo do ochrony danych osobowych, gdy przetwarzają dane osobowe osób fizycznych.

---

[538] Zob. A. Dmochowska, *Europejska Rada ochrony Danych,* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018, s. 187.

[539] Tamże.

[540] Tamże, s. 188.

[541] Rozporządzenie dostępne na: www.eds.europa.eu/sites/edp/files/publication/regf_45-2001_pl.pdf, data dostępu: 23.04.2019.

W odniesieniu do procedury monitoringowej istotne jest to, że EOID monitoruje stosowanie przez instytucje i organy UE przepisów prawa unijnego, regulującego ochronę osób fizycznych w odniesieniu do przetwarzana ich danych osobowych. Dodatkowo EOID doradza instytucjom i organom unijnym oraz podmiotom danych we wszystkich kwestiach dotyczących przetwarzania danych osobowych. W tym celu EOID wykonuje obowiązki określone w art. 46 rozporządzenia, (wzmocnione następnie rozporządzeniem 2018/1725[542]) wśród których najważniejszą rolę w gwarantowaniu jednostkom ich prawa do ochrony danych osobowych jest przeprowadzanie dochodzeń (zarówno z własnej inicjatywy, jak i na podstawie skarg) oraz informowanie podmiotów danych o ich wyniku. Ponadto EOID korzysta z uprawnień nadanych mu na mocy art. 47 rozporządzenia, wśród których w odniesieniu do prowadzonych przez niego dochodzeń ważną rolę odgrywa uprawnienie do uzyskania od instytucji lub organu UE dostępu do wszystkich danych osobowych i informacji koniecznych dla prowadzenia dochodzenia. EOID może również przekazać sprawę Trybunałowi Sprawiedliwości UE oraz interweniować w sprawach wniesionych przed Trybunał. Do zakresu kompetencji EOID należy także monitorowanie rozwoju technologii informatycznych i telekomunikacyjnych, jeśli mają one wpływ na ochronę danych osobowych. EOID bierze również udział w pracach grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych.

Ponadto EOID współpracuje z krajowymi organami ds. ochrony danych w poszczególnych państwach członkowskich UE. Celem tej współpracy jest przede wszystkim upowszechnianie spójnej ochrony danych w całej UE. Należy jednak podkreślić, że EOID nie pełni funkcji nadrzędnej ani odwoławczej wobec krajowych organów ds. ochrony danych. Ze względu na to, że EOID posiada kompetencje nadzorcze jedynie wobec instytucji i organów unijnych w związku z przetwarzaniem przez nie danych osobowych, nie jest on kompetentny w odniesieniu do spraw związanych z przetwarzaniem danych osobowych na szczeblu krajowym (czyli przez instytucje poszczególnych państw członkowskich UE) oraz nie posiada uprawnień

[542] W szczególności art. 42 ust. 1 wyraźnie zobowiązuje Komisję Europejską do zasięgania opinii Europejskiego Inspektora Ochrony Danych po przyjęciu wniosków dotyczących aktu ustawodawczego, zaleceń i wniosków do Rady zgodnie z art. 218 TFUE (tj. umów międzynarodowych) lub podczas przygotowywania aktów delegowanych; Zob. 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, PE/31/2018/REV/1, Doc. 32018R1725.

nadzorczych wobec podmiotów prywatnych przetwarzających dane (czyli przedsiębiorstw).

Natomiast w odniesieniu do kwestii organizacyjnych dotyczących funkcjonowania EOID, należy wskazać, że za wykonywanie zadań tego organu odpowiadają dwie jednostki: Dział Nadzoru i Egzekwowania Prawa (który dokonuje oceny przestrzegania przepisów o ochronie danych osobowych przez instytucje i organy UE) oraz Dział Polityki i Konsultacji (który doradza instytucjom UE w kwestiach związanych z projektami nowych aktów prawnych dotyczących przetwarzania danych osobowych).

Generalnie można stwierdzić, że aczkolwiek pierwszeństwo w zakresie inicjowania rozwiązań prawnych w zakresie ochrony danych osobowych na kontynencie europejskim należy się Radzie Europy, to jednak to właśnie Unia Europejska doprowadziła do rozwinięcia i uszczegółowienia systemu ochrony do poziomu nienotowanego w skali światowej. Postanowienia RODO i zawarte w nim mechanizmy egzekwowania ochrony danych osobowych stawiane są dziś za wzór regulacji w skali międzynarodowej. Istotne znaczenie ma to, że mechanizmy ochrony danych osobowych w UE są stale aktualizowane, by w ten sposób reagować na nowe zagrożenia, które niesie rozwój cywilizacyjny. Taka elastyczna reakcja jest możliwa dzięki sięganiu również po instrumenty o charakterze tzw. „miękkiego prawa", a w szczególności po Komunikaty Komisji Europejskiej.

Rozdział 4: Realizacja standardów bezpieczeństwa danych osobowych w państwach członkowskich Rady Europy i Unii Europejskiej

4.1. Przekształcenia w obszarze ustawodawstwa

Początkowo to Rada Europy, starała się dawać przewagę krajowym ustawodawcom w dziedzinie ochrony danych osobowych, poprzez opracowanie i otwarcie do podpisu Konwencji nr 108[543]. Stanowiło to jednocześnie dobry bodziec do rozważań na temat wpływu technologii informatycznej na normy zawarte w Konwencji i ich przełożenia na ustawodawstwo krajowe Państw – Stron. W tym kontekście Komitet Ekspertów ds. Ochrony Danych (CJ-PD) dostał upoważnienie Komitetu Ministrów RE do zbadania konsekwencji dla ochrony danych nowych technologii oraz przygotowania wszelkich niezbędnych instrumentów prawnych dot. telemetrii, mediów interaktywnych czy też elektronicznych systemów handlowych[544].

Grupa robocza, której powierzono zbadanie tej kwestii, odbyła swoje pierwsze spotkanie w dniach 16-18 grudnia 1985 r., podczas którego udało się dokonać przeglądu problemów, na jakie natknął się system ochrony danych według trzech w.w. rodzajów technologii. CJ-PD zdecydowanie podjął dalsze działania, które miały posłużyć poszukiwaniu dodatkowych informacji w państwach członkowskich RE na temat ich doświadczeń w tej kwestii. Dla przykładu Republika Federalna Niemiec, była wówczas praktycznie jedynym krajem gdzie system telemetryczny był stosowany na dużą skalę (system Temex). Został on uwzględniony w przepisach telekomunikacyjnych, gdzie art. 9 stanowił, iż uzyskane informacje przez telemetrię, która zawierała dane osobowe, mogły być tymczasowo przechowywane przez Federalną Agencję Sieci na żądanie użyteczności publicznej i tylko w celu identyfikacji ilości konsumpcji ich klientów[545]. We Francji z kolei wprowadzenie i wykorzystanie systemów telemetrycznych zostało

[543] Dz.U. 2003 nr 3 poz. 25.
[544] Zob. *New Technologies: a challenge to Privacy Protection?*, Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1989, źródło: www.coe.int/en/web/data-protection/reports-studies-and-opinions, data dostępu: 26.07.2019.
[545] Tamże, s. 9.

objęte ustawą z 1978 r. o przetwarzaniu danych[546]. Co się tyczy mediów interaktywnych, to badanie CJ-PD wykazało, iż w Norwegii pojęcie to zostało wprowadzone do ustawodawstwa co oznaczało dużą aktywność w tej dziedzinie[547].

Badanie CJ-PD z 1991 r. wykazało natomiast, iż w wielu państwach tj. Belgia, Cypr, Dania, Finlandia czy też Niemcy i Holandia wprowadzono do ustawodawstwa przepisy dotyczące używania i rejestrowania numerów identyfikacyjnych. Tylko wymagane dane osobowe mogły być rejestrowane[548].

Zasadniczą kwestią były też postanowienia konwencji dot. obowiązku stosowania jej postanowień do kartotek. Z tej możliwości skorzystało wiele państw. Kartoteki zwykłe (ręczne) objęły zakresem swego ustawodawstwa: Austria, Belgia, Węgry, Islandia, Liechtenstein, Holandia, Norwegia, Słowenia i Szwajcaria, a także w pewnym zakresie Francja i Niemcy[549].

W sumie należy podkreślić, że Konwencji nr 108 zaczęła mieć zastosowanie w przypadku każdej informacji osobowej przetwarzanej automatycznie, niezależnie od tego, czy występowała ona pojedynczo, czy w zbiorze danych oraz do danych osobowych przetwarzanych ręcznie, jeśli występowały w zbiorze i o ile dane państwo rozciągnęło ochronę na zbiory ręczne. Podobny wniosek można wysunąć w przypadku art. 3 Dyrektywy Unii Europejskiej, przy czym przepis ten jest precyzyjniejszy od postanowień Konwencji. Stwierdza on, że Dyrektywa ma zastosowanie do przetwarzania danych osobowych, zautomatyzowanego w całości lub w części, jak również do przetwarzania danych osobowych zawartych lub mających być zawartymi w zbiorze. Należy zatem podkreślić, że postanowienia Dyrektywy miały zastosowanie również do danych nie przetwarzanych automatycznie, a występujących w zbiorze. Dyrektywa nie pozostawiała, więc państwom, w przeciwieństwie do Konwencji, swobody decydowania o tym, czy zbiory ręczne mają być objęte ochroną czy też nie. Zarówno według postanowień Konwencji, jak i Dyrektywy nie podlega więc ochronie informacja osobowa nie będąca elementem zbioru ani przedmiotem przetwarzania automatycznego. Jest to o tyle zrozumiałe, że w przeciwnym wypadku ochronie

[546] Zob. Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, źródło: www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf, data dostępu: 26.07.2019.
[547] *New Technologies: a challenge…,* s. 16.
[548] Zob. *The introduction and use of personal identification numbers: the data Protection Issues (1991),* Study prepeared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1991, źródło: www.rm.coe.int/16806845b3, data dostępu: 26.07.2019.
[549] Zob. A. Mednis, *Ochrona danych…,* s. 34.

musiałyby podlegać dane osobowe występujące pojedynczo, np. w książkach, czasopismach, itp.

Ustawodawstwo o ochronie danych osobowych pojawiło się jako reakcja na zinformatyzowanie procesów przetwarzania, przechowywania i transmisji danych. Dlatego też Konwencji nr 108 Rady Europy reguluje przede wszystkim kwestie ochrony danych przetwarzanych przy pomocy środków informatycznych lub, szerzej automatycznych.

W latach 90-tych najważniejsze problemy związane z ochroną danych osobowych klasyfikowano w następujący sposób: a) wymogi co do jakości przetwarzanych informacji osobowych; b) dopuszczalność przetwarzania danych osobowych; c) dopuszczalność przetwarzania szczególnych kategorii danych; d) prawa osób, których dane dotyczą; e) problemy bezpieczeństwa danych[550].

Konwencja nr 108 i Dyrektywa nr 95/46/CE potwierdziły, iż zawarte w nich regulacje co do wyżej wymienionych zagadnień stanowiły jedynie ramy dla prawodawstwa wewnętrznego poszczególnych państw. Uważano bowiem, iż przepisy krajowe powinny określać szczegółowo, kiedy i w jakich warunkach dopuszczalne jest gromadzenie i przetwarzanie informacji osobowych[551].

Oba omawiane akty prawne nie miały charakteru norm tzw. *self – executing,* ponieważ skierowane były do państw i były sformułowane w postaci obowiązków dla ustawodawcy z postanowieniami Konwencji nr 108, były jedna niewątpliwie bardziej od nich szczegółowe. Większość przepisów Konwencji została w Dyrektywie rozwinięta lub doprecyzowana. W Dyrektywie pojawiły się także nowe postanowienia, których w Konwencji nie było (np. warunki dopuszczalności przetwarzania danych osobowych lub zawodowych wykorzystujących dane osobowe, a więc lekarzy, statystyków, bankowców, itd.). Dlatego wydało się niezbędne dopasowanie polskiej ustawy do unormowań Dyrektywy, zakładając nawet, iż pierwszym etapem po jej uchwaleniu mogłoby być podjęcie starań w celu podpisania Konwencji nr 108.

Warto przy tym zauważyć, iż Polska funkcjonująca w systemie Rady Europy od 1991 r. stosunkowo późno podpisała i ratyfikowała konwencję nr 108. Zasadniczą przyczyną tej sytuacji stały się przepisy art. 4 ust. 1 i 2. Obligowały one bowiem stronę do podjęcia niezbędnych kroków dla osiągnięcia zgodności przepisów prawa

[550] Zob. A. Mednis, *Ochrona danych …,* s. 37.
[551] Tamże.

wewnętrznego z normami konwencyjnymi, przy czym harmonia ta powinna zostać osiągnięta nie później niż w dniu wejścia w życie konwencji dla strony. I tu znów należy przypomnieć, iż normy konwencji 108 nie miały charakteru samowykonalnego. Tymczasem aż do 29 sierpnia 1997 r. problematyka ochrony danych osobowych nie była w polskim porządku prawnym w ogóle uregulowana[552].

Konstytucyjne zobowiązanie do ustawowego uregulowania zasad i trybu gromadzenia i udostępniania informacji zrealizowane zostało bowiem poprzez uchwalenie ustawy o ochronie danych osobowych[553].

Ustawa o ochronie danych osobowych ukształtowana została niewątpliwie w ścisłej korelacji z treścią Konwencji nr 108. Na wyraźny wpływ Konwencji na opracowanie projektów ustawy o ochronie danych osobowych oraz na niektóre z przyjętych przepisów wskazuje również wystąpienie posła sprawozdawcy, przedstawiającego projekt ustawy o ochronie danych osobowych w Sejmie[554]. Przede wszystkim jednak zestawienie poszczególnych przepisów Konwencji nr 108 i polskiej ustawy w pełni odpowiadają wymaganiom stawianym przez Konwencję, a przepisy Konwencji wprost stanowiły wzorzec dla polskiego ustawodawcy.

Zgodnie z art. 1 Konwencji, jej celem jest zagwarantowanie na terytorium każdej ze Stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowania jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem jej danych osobowych. Jak wskazano wcześniej, polskie ustawodawstwo wewnętrzne realizuje cele określone w Konwencji poprzez norm konstytucyjne, gwarantujące każdemu prawo do prywatności (art. 47) oraz prawo do ochrony danych osobowych (art. 51), a realizację konstytucyjnego prawa do ochrony danych dotyczących każdej osoby stanowi w ustawodawstwie zwykłym ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

---

[552] Zob. K. Czarnecki, *Ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych,* [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X – lecie polskiej ustawy o ochronie danych osobowych,* red. G. Goździewicz, M. Szabłowska, Wydawnictwo TNOiK, Toruń 2008, s. 189 – 196.

[553] Dz.U. nr 133, poz. 883 z późn. zm.

[554] Wystąpienie posła M. Lewandowskiego na 112. posiedzeniu Sejmu w dniu 30 lipca 1997 r., przedstawiającego sprawozdanie Komisji Administracji i Spraw Wewnętrznych, Komisji Sprawiedliwości i Praw Człowieka oraz Komisji Ustawodawczej o poselskim oraz rządowym projektach ustaw o ochronie danych osobowych (*Sprawozdanie Stenograficzne,* s. 117 i nast.).

Ustawa zawiera zasady i przesłanki przetwarzania danych osobowych, ze szczególnym uwzględnieniem zasad przetwarzania danych sensytywnych, określa prawa osób, których dane dotyczą, wymogi dotyczące zabezpieczenia zbiorów danych osobowych oraz kontrolę zgodności przetwarzania danych z regułami przyjętymi w ustawie, w tym zakres działania niezależnego organu ochrony danych, jakim jest Generalny Inspektor Ochrony Danych Osobowych.

Wyraźna zbieżność rozwiązań prawnych zawartych w Konwencji nr 108 i w polskiej ustawie widoczna jest przy zestawieniu podstawowych definicji, np. definicji danych osobowych będących przedmiotem ochrony. Przypomnieć należy, iż w art. 2 Konwencji znajduje się definicja danych osobowych, zgodnie z którą dane te „*oznaczają każdą informację dotyczącą osoby fizycznej o ustalonej tożsamości albo dającej się zidentyfikować*".

Formule tej odpowiada definicja danych osobowych przyjęta w ustawie o ochronie danych osobowych, w której zgodnie z art. 6 ust. 1, w rozumieniu ustawy za dane osobowe, uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Wprawdzie definicja danych osobowych zawarta w polskiej ustawie, jest bardziej rozbudowana, określa ona bowiem w dalszych częściach art. 6, jak można zidentyfikować osobę: „*Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań"* – jednakże to uszczegółowienie nie zmienia sensu definicji danych osobowych, pozwalającej na objęcie ochroną zarówno danych umożliwiających określenie tożsamości, jak i dotyczących osoby zidentyfikowanej.

Podobna refleksja nasuwa się przy zestawienie przepisu Konwencji i ustawy o ochronie danych w odniesieniu do ochrony danych sensytywnych. Zgodnie z art. 6 Konwencji, danych o charakterze osobistym, ujawniających pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne, oraz danych osobowych dotyczących zdrowia lub życia seksualnego nie można przetwarzać automatycznie,

chyba że prawo wewnętrzne przewiduje odpowiednie zabezpieczenia. Przepis niniejszy stosuje stosowano również do danych osobowych dotyczących wyroków skazujących.

Odpowiednikiem przepisu art. 6 Konwencji jest art. 27 ustawy o ochronie danych osobowych, przy czym zakres danych określonych w polskich przepisach jest szerszy niż w regulacjach Konwencji. Zgodnie z art. 27 ustawy zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym a także danych dotyczących skazań, orzeczeń o ukaraniu, mandatów karnych, innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Przetwarzanie takich danych było dopuszczalne wyłącznie w oparciu o przesłanki szczegółowo wyliczone w art. 27 ust. 2 ustawy.

Precyzyjne i wyczerpujące określenie przesłanek dopuszczalności przetwarzania danych sensytywnych, a także wysoki standard warunków przetwarzania oraz surowa odpowiedzialność za naruszenie przepisów o dopuszczalności przetwarzania danych szczególnie chronionych[555] stanowią prawdziwe gwarancje praw osób, których dane dotyczą.

Przepisy ustawy o ochronie danych są odwzorowaniem norm Konwencji również w odniesieniu do zakresu przedmiotowego ochrony. Konwencja zobowiązuje Strony do stosowania ochrony danych przetwarzanych w zautomatyzowanych zbiorach danych, prowadzonych w sektorze publicznym i prywatnym. Konwencja dopuszcza stosowanie jej zasad także w odniesieniu do zbiorów danych osobowych nieobjętych automatycznym przetwarzaniem (ust. 2 pkt. c), jak też niestosowanie do niektórych kategorii zautomatyzowanych zbiorów danych.

Ponadto stworzono możliwość stosowania Konwencji także do innych informacji dotyczących ugrupowań, stowarzyszeń, fundacji, spółek, korporacji i wszelkich innych organizacji gromadzących bezpośrednio lub pośrednio osoby fizyczne, niezależnie od posiadania przez nie osobowości prawnej, stawiając wymóg powiadomienia Sekretarza Generalnego Rady Europy o zakresie ochrony.

[555] Art. 49 ust. 2 ustawy o ochronie danych osobowych przewiduje karę grzywny, ograniczenia wolności albo pozbawienia wolności do lat 3 w przypadku przetwarzania w zbiorze danych osobowych szczególnie chronionych w sytuacji, gdy przetwarzanie jest dopuszczalne albo gdy przetwarzanie prowadzone było przez osobę nieupoważnioną.

Polska ustawa o ochronie danych osobowych objęła ochroną dane osobowe osób fizycznych, przetwarzane w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych (art. 2 ust. 2), co oznaczało, iż ustawa objęła ochroną zarówno dane przetwarzane automatycznie, jak i dane nieprzetwarzane w systemie automatycznym.

Wszelkie obowiązki nałożone polską ustawą w równym zakresie odniesiono do podmiotów należących do sektora publicznego, jak i sektora prywatnego. Zgodnie z art. 3, ustawę stosuje się do organów państwowych oraz organów samorządu terytorialnego, a także do innych niepaństwowych i komunalnych jednostek organizacyjnych realizujących zadania publiczne (art. 3 ust. 1), a także do osób fizycznych i prawnych oraz jednostek organizacyjnych nie mających osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych (art. 3 ust. 2).

Podstawową zasadą przetwarzania danych akcentowaną w normach Konwencji, jest „jakość" danych. Zgodnie z treścią art. 5 Konwencji dane o charakterze osobistym będące przedmiotem automatycznego przetwarzania muszą być zbierane oraz przetwarzane rzetelnie i zgodnie z prawem, rejestrowane dla określonych i legalnych celów i nie mogą być wykorzystywane niezgodnie z tymi celami. Muszą być odpowiednie, rzeczowe, nie wykraczające poza cel dla którego są rejestrowane, dokładne i w razie potrzeby uaktualniane, przechowywane w formie umożliwiającej identyfikację osób zainteresowanych przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego są rejestrowane.

Przepisowi temu odpowiada art. 26 ust. 1 polskiej ustawy o ochronie danych osobowych, zgodnie z którym administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem okoliczności wyraźnie wskazanych w ust. 2 przepisu, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Jedynie w przypadkach określonych ustawą (jeżeli nie naruszało to praw i wolności osób, których dane dotyczą, oraz następowało: w celu badań naukowych, dydaktycznych, historycznych lub statystycznych oraz z zachowaniem przepisów art. 23 i 25) dopuszczono przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane.

Wreszcie, polska ustawa spełnia również wymogi stawiane przez Konwencję w zakresie odpowiedniego zabezpieczenia danych.

W ustawie o ochronie danych osobowych zagadnienie zapewnienia danym odpowiedniego poziomu bezpieczeństwa zostało uregulowane w przepisach art. 36 – 39. Administrator przetwarzający dane jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.

Ustawodawca polski uregulował ponadto problem dotyczący dopuszczenia do przetwarzania wyłącznie osób posiadających upoważnienie (art. 37), zobowiązał administratora danych do zapewnienia kontroli nad tym, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane (art. 38), oraz nałożył ustawowy obowiązek prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych oraz po ustaniu ich zatrudnienia (art. 39).

Dodatkowe wymogi mające na celu zagwarantowanie odpowiedniego poziomu ochrony danych osobowych przetwarzanych w systemach informatycznych, zawarte zostały w przepisach wykonawczych do ustawy o ochronie danych osobowych – rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych[556].

Nie omawiając szczegółowo wszystkich przepisów rozporządzenia, warto wskazać, choćby na te, które nakazują administratorowi danych opracowanie instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczonej dla osób zatrudnionych przy przetwarzaniu danych (§ 6), opracowanie instrukcji

[556] Dz.U. nr 80, poz. 521.

określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji (§ 11), czy też przechowywanie kopii awaryjnych w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco (§ 12).

Należy nadto podkreślić, iż przepisy karne, które zawarto w ustawie o ochronie danych osobowych z 1997 r. przewidują odpowiedzialność karną każdego, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionych (art. 51). Ponadto, za naruszenie, choćby nieumyślnie, obowiązku zabezpieczenia danych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, osobie administrującej danymi grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do jednego roku (art. 52).

Przyjęte w polskim ustawodawstwie rozwiązania stanowią spełnienie wymogów określonych w art. 7 Konwencji, który nakazuje wprowadzenie odpowiednich sposobów ochrony danych osobowych zarejestrowanych w zautomatyzowanych kartotekach, w celu ich zabezpieczenia przed zniszczeniem przypadkowym lub bez upoważnienia, lub przypadkowym zagubieniem, jak też przed dostępem do nich, zmianami lub rozpowszechnieniem bez upoważnienia.

Przy analizie wpływu Konwencji nr 108 Rady Europy w zakresie ochrony danych osobowych na ustawodawstwo polskie, nasuwa się pytanie, czy w ogóle można byłoby mówić o ustawodawstwie polskim w zakresie ochrony danych osobowych, gdyby nie Konwencja i regulacje Rady Europy. Ustawodawstwo polskie w zakresie ochrony danych osobowych jest jednym z przykładów kształtowania ustawodawstwa krajowego pod wpływem i według wzorców stanowionych aktami Rady Europy.

Kluczowe znaczenie w erze cyfrowej ma wejście w życie konwencji nr 108 +. Dlatego oczekuje się wiele ratyfikacji w 2020 r. co umożliwić szybkie wejście w życie tego zmodernizowanego przełomowego instrumentu. W dniu 18 grudnia 2019 r. dokument ratyfikacyjny został złożony przez ambasadora Tomę Galli, stałego przedstawiciela Chorwacji w Radzie Europy[557]. Była to druga ratyfikacja. Pierwsza

[557] *Croatia is the Second country to ratify Convention 108+,* źródło: www.coe.int/en/web/data-protection/-/croatia-is-the -second-country-to-ratify-convention-108, data dostępu: 03.01.2020.

nastąpiła 10 grudnia 2019 r. i została ona dokonana przez Bułgarię[558]. W pierwszym roku otwarcia podpisów zarejestrowano ich 38[559], w tym podpisy w Argentynie, Tunezji i Urugwaju.

Warto zaznaczyć, iż poprawki do konwencji stanowią zachętę dla państw trzecich, które przystąpiły do konwencji i nie są objęte RODO, do stosowania podstawowych zasad przetwarzania danych osobowych. W ten sposób wymogi dotyczące przekazywania i ochrony danych osobowych zostały ujednolicone na szczeblu międzynarodowym.

Odnowiona konwencja ma na celu zagwarantowanie, że trzecie państwa członkowskie zastosują najwyższe możliwe standardy ochrony danych osobowych, dlatego jest to szczególnie istotne dla Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, które stara się opuścić Unię Europejską. Zjednoczone Królestwo jest jednym z sygnatariuszy protokołu, dlatego ocena przystąpienia do konwencji jako odpowiedniego zabezpieczenia dla przekazywania danych do państw trzecich mogłaby uprościć wymianę danych osobowych między Wielką Brytanią a UE.

Interesujące jest to, że rząd Wielkiej Brytanii przedstawia swoje propozycje dotyczące ochrony danych osobowych lokalnym firmom, aby uzyskać lepszy wgląd w poprawki do Konwencji. W związku z tym odnowiona konwencja prawdopodobnie będzie zbiorem przepisów dotyczących ochrony danych osobowych, których Wielka Brytania będzie używać w celu zachowania zgodności z międzynarodowymi standardami ochrony danych osobowych po opuszczeniu Unii Europejskiej.

W dniu 9 kwietnia 2019 r. Rada Europejska przyjęła decyzję upoważniającą państwa członkowskie UE do „ratyfikowania, w interesie Unii, protokołu zmieniającego Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem

[558] *First ratification of Convention 108+ Congratulations Bulgaria,* źródło: www.coe.int/en/web/data-protection/-/first-ratification-of-convention-108-congratulations-bulgaria, data dostępu: 03.01.2020.

[559] Andora (28.01.2019); Armenia (02.10.2019); Austria (10.10.2018); Belgia (10.10.2018); Bułgaria (10.12.2019); Chorwacja (18.12.2019); Cypr (09.01.2019); Republika Czeska (10.10.2018); Estonia (10.10.2018); Finlandia (10.10.2018); Francja (10.10.2018); Niemcy (10.10.2018); Grecja (06.09.2019); Węgry (09.01.2019); Islandia (21.11.2018); Irlandia (10.10.2018); Włochy (05.03.2019); Łotwa (10.10.2018); Litwa (10.10.2018); Luksemburg (10.10.2018); Monako (10.10.2018); Holandia (10.10.2018); Macedonia Północna (05.12.2019); Norwegia (10.10.2018); Polska (16.05.2019); Portugalia (10.10.2018); Federacja Rosyjska (10.10.2018); San Marino (16.07.2019); Serbia (22.11.2019); Republika Słowacka (17.12.2019); Słowenia (16.05.2019); Hiszpania (10.10.2019); Szwecja (10.10.2018); Szwajcaria (21.11.2019); Zjednoczone Królestwo (10.10.208); Argentyna (19.09.2019); Tunezja (24.05.2019); Urugwaj (10.10.2018).

danych osobowych (nr ETS 108) w zakresie, w jakim jego postanowienia wchodzą w zakres wyłącznych kompetencji Unii”[560].

W przypadku całej UE zasady ochrony danych są określone w tak zwanym ogólnym rozporządzeniu o ochronie danych (RODO). Posłużenie się formą rozporządzenia, a zatem aktu prawnego obowiązującego na obszarze całej Unii Europejskiej, bez potrzeby transpozycji do porządku krajowego niewątpliwie przyczyniłoby 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. Niestety, Komisja przygotowując projekt rozporządzenia nie była konsekwentna. W rezultacie RODO odsyła w ponad 40 przepisach do możliwości odmiennego uregulowania w prawie krajowym[561]. Z jednej strony, prawodawca słusznie założył, że należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Z drugiej strony, uznano, że jeżeli chodzi o przetwarzanie danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące stosowanie przepisów rozporządzenia. Co więcej, nie wykluczono możliwości określenia w prawie państwa członkowskiego okoliczności dotyczących konkretnych sytuacji związanych z przetwarzaniem danych wrażliwych, w tym dookreślenia warunków, które decydują o zgodności przetwarzania z prawem.

Jak zauważa dr Maciej Kawecki, doradca w Gabinecie Politycznym Ministra Cyfryzacji, założeniem reformy ochrony danych osobowych jest „*odejście od równego tratowania wszystkich podmiotów przetwarzających dane osobowe. W tym zakresie rozporządzenie ogólne o ochronie danych osobowych wprowadza więc podejście oparte na ryzyku. To każdy przetwarzający dane osobowe musi ocenić, czy w danym stanie*

[560] Zob. *EU Member States to ratify Convention 108+,* źródło: www.coe.int/en/web/data-protection/-/eu-member-states-to-ratify-convention-108-, data dostępu: 03.01.2020.

[561] Jak stanowi motyw 8 RODO: „W zakresie, w jakim niniejsze rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do swego prawa krajowego”.

faktycznym zastosował dostępne i uznane w chwili przetwarzania za stabilne technologiczne środki zapewniające najwyższą ochronę danych osobowych"[562].

Warto wskazać na zasadnicze różnice w podejściu do wdrożenia RODO w Polsce i innych krajach członkowskich. Bowiem w polskim podejściu zaobserwować było można odwlekanie od wprowadzania zmian[563]. Szereg przedsiębiorców czekało z tym do ostatniej chwili. Inaczej sytuacja przedstawiała się w innych państwach, gdzie zmiany wprowadzane były płynnie[564].

W Polsce istotnym wydarzeniem w tym obszarze było uchwalenie ustawy 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 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanej ustawą wprowadzającą, czy też wdrażającą[565]. Stanowiła on drugą po ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych[566], ustawę związaną bezpośrednio ze stosowaniem RODO w polskim systemie prawnym, które była niezbędna dla możliwości zapewnienia stosowania RODO w Polsce[567]. Dokonała ona nowelizacji ponad 150 ustaw odnoszących się do różnych obszarów tj. sport, turystyka, ubezpieczeniowa, obszary prawa pracy, prawa karnego i administracyjnego. Ta jedna z większych oraz znaczących nowelizacji polskiego porządku prawnego rozpoczęła swoje obowiązywanie w dniu 4 maja 2019 r.[568] Wiązało się to z potrzebą dostosowania się do wymogów ustawowych przez wszystkie organy władzy publicznej,

[562] M. Kawecki, *Wdrażanie ogólnego rozporządzenia unijnego do polskiego porządku prawnego a techniczne aspect zabezpieczenia danych osobowych – wystąpienie Macieja Kaweckiego,* źródło: www.gov.pl/web/cyfryzacja/wdrazanie-ogolnego-rozporzadzenia-unijnego-do-polskiego-porzadku-prawnego-a-techniczne-aspekty-bezieczenstwa-danych-osobowych, data dostępu: 21.12.2019.
[563] Zob. K. Sobczak, *KE ponagla państwa ws wdrożenia RODO,* źródło: www.prawo.pl/prawnicy-sady/ke-ponagla-panstwa-ws-wdrazania-rodo,73668.html, data dostępu: 21.12.2019.
[564] M. Zygmunt, *RODO w Polsce i innych krajach członkowskich. Różnice w podejściu do wdrożenia,* źródło: www.bezowijania.com/rodo-w-polsce-i-innych-krajach-czlonkowskcih-roznice-w -podejsciu-do-wdrozenia, data dostępu: 21.12.2019.
[565] Dz.U.2019 poz. 730.
[566] Dz.U.2018 poz. 1000.
[567] Por. *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Wolters Kluwer Warszawa 2018.
[568] Zob. K. Majczak, *RODO rok od stosowania nowych przepisów,* źródło: www.rp.pl/Firma.306039975-RODO-rok-od-stosowania-nowych-przepisow-html, data dostępu: 21.12.2019.

m.in. przez Zakład Ubezpieczeń Społecznych[569] cz urzędy stanu cywilnego[570]. Dotyczyło to m.in. gromadzenia dokumentacji ochrony danych osobowych[571].

Wdrażanie RODO objęło różne obszary regulacyjne[572], uwzględniające organy administracji państwowej, organy administracji samorządowej[573], jak też inne podmioty. Zagrożenie dla bezpieczeństwa informacji może bowiem występować np. Straży Miejskiej jako organizacji publicznej[574]. Należy tu odnotować konsekwencje ograniczenia stosowania rozporządzenia o ochronie danych osobowych w sferze publiczno-prawnej[575]. Wartym uwzględnienia jest także problem ochrony danych osobowych w kontekście niezależności organów nadzorczych[576].

Rozporządzenie RODO oddziałuje również na działalność kościołów i związków wyznaniowych, m.in. Kościoła katolickiego[577] i Świadków Jehowy[578].

Kluczowe znaczenie ma identyfikacja urzędnika odpowiedzialnego za ochronę danych osobowych[579].

---

[569] Zob. T. Błoński, *Wyzwania stojące przed Zakładem Ubezpieczeń Społecznych w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych (2016/679),* „Ubezpieczenia Społeczne" 2016, nr 3, s. 141.

[570] Zob. P. Fajgielski, *Unijna reforma ochrony danych osobowych a działalność urzędów stanu cywilnego*, „Metryka" 2017, nr 2, s. 99.

[571] Zob. K. Gałaj-Emiliańczyk, *Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku*, Difin, Warszawa 2016, s. 23.

[572] Zob. K. Gałaj-Emiliańczyk, *Dokumentacja wdrożenia RODO (z suplementem elektronicznym),* ODDK Gdańsk 2018, s. 8.

[573] Zob. M. Ganczar, A. Sytek, *Jednostki samorządu terytorialnego wobec ogólnego rozporządzenia o ochronie danych (RODO)*, [w:] *Źródła prawa w samorządzie terytorialnym*, red. B.Dolnicki, Wolters Kluwer Polska, Warszawa 2018, s. 259; K. Gawkowski, *Informacja i jej bezpieczeństwo w jednostkach administracji samorządowej*, [w:] *Koncepcje i instrumenty zarządzania w administracji publicznej*, red. A. Gołębiowska, P. B. Zientarski, Kancelaria Senatu, Warszawa 2017, s. 273.

[574] Zob. G. Grondys, *Zagrożenia bezpieczeństwa informacji w Straży Miejskiej jako organizacji publicznej*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Warszawa-Siedlce 2018, s. 155.

[575] Zob. M. Jabłoński, K. Wygoda, *Reforma ochrony danych osobowych - konsekwencje ograniczonego stosowania ogólnego rozporządzenia o ochronie danych w sferze publiczno-prawnej (zagadnienia wybrane),* [w:] *Dookoła Wojtek... Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Presinerowi*, red. R. Balicki, M. Jabłoński, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2018, s. 231.

[576] Zob. 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, nr 4, s. 70.

[577] Zob. P. Zając, *RODO a Kościół Katolicki w Polsce. Określenie zakresu działalności Unii Europejskiej*, „Biuletyn - Stowarzyszenie Kanonistów Polskich" 2018, nr 31, s. 61.

[578] Zob. M. Bielecki, *Przetwarzanie danych osobowych przez Świadków Jehowy*, „Przegląd Prawno-Ekonomiczny" 2017, nr 3, s. 267

[579] Zob. R. Szałowski, *Data protection officer in the light of the provisions of the general data protection regulation (GDPR)*, "Ius Novum "2018, nr 4, s. 115.

Istotne znaczenie miała regulacja dokumentacji danych osobowych[580] oraz zasad ich czasowego przechowywania[581]. W obszarze regulacji znalazły się: powierzenie danych[582], powierzanie przetwarzania danych[583], przetwarzanie danych[584], przetwarzanie danych a prawo do bycia zapomnianym[585] i przenoszenie danych[586]. Z punktu widzenia ochrony bezpieczeństwa danych istotne znaczenie ma ich pseudonimizacja[587] i szyfrowanie[588]. Ważnym obszarem jest ochrona danych osobowych w procesie głosowania[589].

Obszarem szczególnych zagrożeń, gdzie ochrona danych osobowych odgrywa istotne znaczenie, jest ochrona zdrowia[590].

Istotnym obszarem regulacyjnym ochrony danych osobowych, charakteryzującym się swą specyfiką, jest e-commerce[591].

---

[580] Por. K. Andrzejak, P. Glen, P. Janiszewski, Ł. Onysyk, A. Kręcisz-Sarna, M. Sarna, A. Stępień, W. Szczygielska, J. Tyski, *Dokumentacja ochrony danych osobowych według RODO*, Wiedza i Praktyka, Warszawa 2018; M. Cwener, Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, C.H. Beck, Warszawa 2017, s. 97.

[581] Zob. M. Bienias, *Zasada czasowego ograniczenia przechowywania danych osobowych na gruncie RODO*, „ Prawo Mediów Elektronicznych" 2017, nr 4, s. 13.

[582] Zob. A. Czarnowski, M. Gawroński, P. Naklicka, *Powierzenie danych oraz elementy nowej umowy powierzenia danych*, [w:] *RODO. Przewodnik ze wzorami*, jw., *Przewodnik ze wzorami*, red. M. Gawroński, Wolters Kluwer Polska, Warszawa 2018 s. 329.

[583] Zob. P. Glen, Umowa powierzenia przetwarzania danych osobowych, [w:] K. Andrzejak, P. Glen, P. Janiszewski, Ł. Onysyk, A. Kręcisz-Sarna, M. Sarna, A. Stępień, W. Szczygielska, J. Tyski, *Dokumentacja ochrony danych osobowych według RODO*, Wiedza i Praktyka, Warszawa 2018, s. 46.

[584] Zob. M. Barański , M. Giermak, *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego (uwagi na tle ferenda)*, „Państwo i Prawo" 2017, nr 10, s. 90.

[585] Zob. D. Skoczylas, *Przetwarzanie danych osobowych a prawo do bycia zapomnianym i prawo do przenoszenia danych na gruncie RODO*, „Acta Iuris Stetinensis" 2018, nr 4, s. 87. Por. J. Buchalska, *Prawo do bycia zapomnianym - w orzecznictwie polskim*, [w:] *Prawo prywatności jako reguła społeczeństwa informacyjnego*, red. K. Chałubińska-Jentkiewicz, K. Kakareko, J, Sobczak, C.H. Beck, Warszawa 2017, s. 147.

[586] Zob. A. Czarnowski, M. Gawroński, P. Punda, Prawo do przenoszenia danych, czyli jak przenieść dane od jednego administratora danych do drugiego (art. 20 RODO), [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, jw., s. 225.

[587] Zob. M. Kujawa, *Pseudonimizacja danych - co to właściwie jest?*, „Jurysta" 2018, nr 5, s. 41; M. Niedźwiecki, *Pseudonimizacja jako nowy środek zabezpieczenia danych osobowych w świetle zmian prawnych w UE - wybrane aspekty*, „Studia Erasmiana Wratislaviensis" 2018, nr 12, s. 621.

[588] Zob. A. Czarnowski, M. Gawroński, P. Punda, *Pseudonimizacja i szyfrowanie - preferowane środki zabezpieczania danych osobowych*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, jw., s. 225.

[589] Zob. K. Gałaj-Emiljańczyk, *Ochrona danych osobowych podczas głosowania*, „Jurysta" 2018, nr 4, s. 42.

[590] Zob. J. Rzucidło, J. Węgrzyn, *Wybrane problemy ochrony danych dotyczących zdrowia pacjenta w kontekście ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz RODO*, [w:] *Dookoła Wojtek...*, s. 313.

[591] Por. *RODO w e-commerce*, red. D. Lubasz, Wolters Kluwer Polska, Warszawa 2018.

Ochrona danych osobowych nabiera istotnego znaczenia w działalności osób wykonujących prawnicze zawody zaufania publicznego[592]. Ma to znaczenie w procedurach doradztwa prawnego realizowanego m.in. przez adwokatów[593] i radców prawnych, jak też doradców podatkowych[594]. Obejmuje to nie tylko osoby świadczące usługi prawnicze, ale też osoby z nimi współpracujące[595].

Nowe regulacje objęły potrzebę prawidłowego usytuowania administratora danych osobowych[596]. Podjęły też rejestry publiczne o charakterze personalnym prowadzone przez systemy teleinformatyczne[597]. Przedmiotem regulacji stało się dysponowanie danymi z rachunku bankowego[598]. Podjęto też problem ochrony danych osobowych w rejestrach prowadzonych przez przedsiębiorców[599]. Odpowiednie zmiany wprowadzono m.in. w ustawie o działalności ubezpieczeniowej i reasekuracyjnej[600]. Podjęto też problem ochrony danych osobowych w działalności posła[601].

Na tle rozporządzenia RODO powstało szereg kwestii szczegółowych, do których należy rejestr sprawców przestępstw o charakterze seksualnym w kontekście prawa do prywatności i prawa do bycia zapomnianym[602].

---

[592] Zob. M. Jabłoński, J. Węgrzyn, *Ochrona tajemnic osób wykonujących prawnicze zawody zaufania publicznego*, wyd. 2., Wrocławskie Wydawnictwo Naukowe Atla 2, Wrocław 2018, s. 34.

[593] Zob. M. Jackowski, M. Ciesielska, *Adwokat według RODO - administrator czy procesor*, „Palestra" 2018, nr 10, s. 74. Por. M. Zejda, K. Zaleska-Korziuk, *Problematyka przetwarzania danych osobowych przez adwokatów w charakterze współadministratorów i podmiotów przetwarzających w świetle RODO*, „Palestra" 2018, nr 10, s. 52.

[594] Zob. M. Gumularz, M. Kawecki, *RODO a doradcy podatkowi*, „Przegląd Podatkowy" 2018, nr 5, s. 19.

[595] Zob. J. Borowicz, *Obowiązki poufności pracowników współpracujących z wykonawcami wolnych zawodów*, „Praca i Zabezpieczenie Społeczne" 2017, nr 12, s. 22.

[596] Zob. D. Dörre-Kolasa, *Administrator danych osobowych w zbiorowym prawie zatrudnienia*, Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019, nr 4, s. 367; M. Gawroński, K. Kloc, M. Wojtas, Magdalena, *Administrator i podmiot przetwarzający*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*... s. 114.

[597] Zob. J. Dobkowski, *Rejestry publiczne o charakterze personalnym prowadzone w systemie teleinformatycznym i administracyjne prawo dowodowe*, „Casus" 2018, nr 91, s. 63.

[598] Zob. Z. Długosz, M. Mostowik, *Dysponowanie danymi z rachunku w świetle przepisów PSD2 oraz RODO*, „Monitor Prawa Bankowego" 2018, nr 5, s. 60.

[599] Zob. J. Ciesielski, *Rejestry przedsiębiorców a ochrona danych osobowych*, „Acta Universitatis Wroclaviensis. Przegląd Prawa i Administracji" 2018, nr 112, s. 13.

[600] Zob. J. Byrski, H. Hoser, *Zakres zmian w ustawie o działalności ubezpieczeniowej i reasekuracyjnej w związku z dostosowaniem do unijnych regulacji dotyczących ochrony danych osobowych*, „Prawo Asekuracyjne" 2019, nr 2, s. 73.

[601] Zob. B. Bińkowska-Artowicz, *W sprawie obowiązków posła jako administratora w kontekście ogólnego rozporządzenia o ochronie danych (RODO*), „Przegląd Sejmowy" 2018, nr 5, s. 129.

[602] Zob. J. Ryter, E. Ryter, *Rejestr sprawców przestępstw na tle seksualnym a prawo do prywatności i prawo do bycia zapomnianym w świetle ogólnego rozporządzenia o ochronie danych osobowych (RODO), dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27.04.2016 r. oraz innych ustaw*, „Probacja" 2018, nr 4, s. 177.

Istotny kontekst dla implementacji rozporządzenia RODO stanowi dostęp do informacji publicznej[603], m.in. dotyczącej ochrony środowiska[604]. Ważne znaczenie dla omawianych tu zagadnień miała też ustawowa regulacja dostępu do informacji publicznej[605]. Jej postanowienia dotyczyły całokształtu administracji publicznej: zarówno administracji państwowej, jak i administracji samorządowej[606]. Uregulowane zostały m.in. zasady dostępu do informacji publicznej przez podmioty prowadzące działalność gospodarczą[607]. Obejmują one ochronę danych osobowych przedsiębiorcy będącego osobą fizyczną[608]. Szczególne znaczenie ma tu ochrona danych związanych z zatrudnieniem[609]. Dotyczy to również zatrudnienia przez kościoły i związki wyznaniowe[610]. Ochrona danych osobowych znajduje też zastosowanie w sferze sportu[611].

Należy uwzględnić, że ochrona danych osobowych może być przesłanką odmowy udostępnienia informacji publicznej[612]. Na zagadnienie to można spojrzeć z szerszej perspektywy realizacji zasady jawności działania administracji publicznej[613].

---

[603] Zob. I. Szczepańska-Kulik , *W sprawie problematyki prawa do informacji publicznej w kontekście przepisów rozporządzenia o ochronie danych osobowych*, „Przegląd Sejmowy" 2018, nr 5, s. 145.

[604] Zob. A. Trela-Smalarz, *Dostęp do informacji o ochronie środowiska*, „Przegląd Prawa Publicznego" 2018, nr 1, s. 21

[605] Por. M. Bidziński, M. Chmaj, P. Szustakiewicz, *Ustawa o dostępie do informacji publicznej. Komentarz*, wyd. 3. C. H. Beck, Warszawa 2018.

[606] Zob. G. Cern, *Realizacja zasady jawności i dostępu do informacji publicznej w "spółkach gminnych",* [w:] *Źródła prawa w samorządzie terytorialnym*, red. B. Dolnicki, Wolters Kluwer Polska, Warszawa 2018, s. 53.

[607] Zob. A. Bochentyn , K. Ważny, *Udostępnianie informacji publicznej przez podmioty prowadzące działalność gospodarczą*, [w:] *Administracja publiczna a gospodarka*, red. B. Jaworska-Dębska, A. Dobaczewska, Wydawnictwo Ius Publicum, Warszawa 2018, s. 13.

[608] Zob. P. Fajgielski, *Ochrona danych osobowych przedsiębiorcy będącego osobą fizyczną*, [w:] *Dysfunkcje publicznego prawa gospodarczego*, red. M. Zdyb, E. Kruk, G. Lubeńczuk, C. H. Beck, Warszawa 2018, s. 65.

[609] Zob. A. Kamińska-Pietnoczko, *Wpływ RODO na zasady przetwarzania danych osobowych związanych z zatrudnieniem - w oczekiwaniu na nowelizację Kodeksu pracy*, „Monitor Prawa Pracy" 2018, nr 6, s. 15.

[610] Zob. O. Kucharski, P. Wolnicki, *Przetwarzanie danych osobowych dotyczących zatrudnienia w Kościołach i innych związkach wyznaniowych*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2018, nr 4, s. 355.

[611] Zob. M. Biliński, *Ochrona danych osobowych w sferze sportu w świetle aktualnych zmian legislacyjnych*, „Przegląd Naukowy Disputatio" 2017, t. 24, nr 2, s. 9

[612] Zob. M. Pieńczykowski, *Ochrona danych osobowych jako negatywna przesłanka udostępniania informacji publicznej*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2018, nr 2, s. 64.

[613] Zob. Ł. Regner, *Aktualne problemy i wyzwania w obszarze jawności działania administracji publicznej oraz kierunki dalszego kształtowania modelu*, [w:] *Stulecie polskiej administracji. Doświadczenia i perspektywy*, red. W. Federczyk, Krajowa Szkoła Administracji Publicznej, Warszawa 2018, s. 155.

Istotne znaczenie mają przepisy regulujące odpowiedzialność za naruszenie danych osobowych[614]. Znajdują tu zastosowanie przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[615]. Ważnym instrumentem jest sądowa kontrola pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych[616]. Ochrona danych osobowych rozważana jest również w kategoriach celu procesu karnego[617].

W Niemczech do ustawodawstwa wprowadzono rozbudowane regulacje dotyczące technicznych aspektów bezpieczeństwa danych osobowych. Ustawodawca niemiecki zwrócił uwagę na kryteria mające służyć ocenie ryzyka przetwarzania danych osobowych tj. możliwość kontroli dostępu do danych w tym kontroli nośników na których dane są przechowywane. Podkreślono także rolę pseudonimizacji danych[618] oraz ich szyfrowania.

Rok po wprowadzeniu RODO Komisja Europejska wskazywała, iż wszystkie państwa członkowskie z wyjątkiem Grecji, Portugalii i Słowenii, dokonały aktualizacji swoich krajowych przepisów w dziedzinie bezpieczeństwa danych osobowych w celu zapewnienia ich zgodności ze standardami Unii Europejskiej. Jako potwierdzenie tego traktować można także słowa Very Jourovej, komisarz do spraw sprawiedliwości, konsumentów i równouprawnienia płci, według której „*Ogólne rozporządzenie o ochronie danych przynosi efekty. Daje ono Europejczykom skuteczne narzędzia, które pomagają im podjąć wyzwania związane z cyfryzacją, i zapewnia im kontrolę nad własnymi danymi osobowymi. Przedsiębiorstwom umożliwia pełne wykorzystanie cyfrowej rewolucji, a jednocześnie gwarantuje społeczne zaufanie do niej. Poza Europą otwiera możliwości dyplomacji cyfrowej mającej na celu wspieranie przepływu danych w oparciu o wysokie standardy, między państwami, które podzielają wartości UE.*

[614] Zob. A. Kaczmarek, *Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych*, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Wolters Kluwer, Warszawa 2018, s. 331.
[615] Zob. A. Romkowski, *Przepisy karne ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. w kontekście standardów ochrony danych osobowych w rozporządzeniu GDPR (RODO) z dnia 27 kwietnia 2016 r.*, „Przegląd Prawno-Ekonomiczny" 2018, nr 1, s. 268.
[616] Zob. M. Tomkiewicz, *Sądowa kontrola pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych*, „Państwo i Prawo" 2018, nr 4, s. 67.
[617] Zob. A. Wolska-Bagińska, *Ochrona danych osobowych a cele procesu karnego*, „Palestra" 2018, nr 7-8, s. 91.
[618] Przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której one dotyczą, bez użycia dodatkowego "klucza", Zob. *Pseudonimizacji danych,* źródło: www.odo24.pl/blog-post.pseudonimizacja-anonimizacja-danych-wyjasniamy-pojecie, data dostępu: 21.12.2019.

Należy jednak kontynuować działania, aby nowy system ochrony danych był w pełni funkcjonalny i skuteczny"[619].

W Estonii podjął działania Inspektorat Ochrony Danych Osobowych[620].

Poniższa tabela przedstawia stan wdrażania RODO na szczeblu krajowych.

Tabela 1. Wdrożenie RODO na szczeblu krajowym

Państwo:	**Czy spełniono wymagania RODO ?**	**Obowiązujące prawodawstwo:**
Austria	Stare przepisy zostały zaktualizowane	Data Protection Act, Federal Law Gazette I Nr. 165/1999 (the "Data Protection Act") amended to reflect GDPR requirements by two Data Protection Amendmend Acts in 2018. (Date in force: 1 January 2000, amended on 25 May 2018). - Data Protection Act 1 § 2 on the Amendment of Material Laws (Federal Law Gazette I Nr. 32/2018 & Nr. 37/2018).
Belgia	Zostało przyjęte nowe ustawodawstwo	- Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (the "Law of 30 July 2018"), Date in force: 5 September 2018. - Law of 5 September 2018 establishing the information security committee and modifying various laws regarding the implementation of 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 procession

[619] *RODO jednak chroni,* źródło: www.ec.europa.eu/poland/news/190724_RODO_pl, data dostępu: 21.12.2019.
[620] Zob. K. Szwed, *Inspektorat Ochrony Danych Osobowych*, [w:] *Ustrój państwowy Republiki Estonii*, red. S. Sagan, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2018, s. 87.

		of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Date in force: 10 September 2018. - Law of 3 December 2017 establishing in DPA, Date in force: 25 May 2018. - Law of 21 March 2018 amending the existing Act of 21 March 2007 on camera surveillance, Date in force: 25 May 2018.
Bułgaria	Stare przepisy zostały zaktualizowane	- Law on Amendment and Supplement to the Personal Data Protection Act, Date in force: 29 February 2019.
Chorwacja	Zostało przyjęte nowe ustawodawstwo	- Act on the Implementation of the General Data Protection Regulation (in Cratian: Zakon o provedbi Opce uredbe o zasiti podataka) (the "Implementation Act"), Date in force: 25 May 2018.
Cypr	Zostało przyjęte nowe ustawodawstwo	- Law providing for the protection of natural persons with regard to the processing of personal data and for free movement of such data (Law 125 (I) of 2018 (the "Data Protection Act"), Date in force: 31 July 2018.
Republika Czeska	Zostało przyjęte nowe ustawodawstwo	- Act on processing of personal data (the "Data Protection Act"), Date in force: 24 April 2019. - Act amending certain legislations due the adoption of the act on processing of personal data (the "Amending Act") , Date in force: 24 April 2019.
Dania	Nowe ustawodawstwo zostało przyjęte a stare ustawodawstwo zostało zmienione	- Databeskyttelsesloven (the „Data Protection Act"), Date in Force: 25 May 2018. - Videosurveillance Monitoring Act (the "CCTV Act"), Date in force: 25 May 2018.
Estonia	Nowe ustawodawstwo	- Personal Data Protection Act (the „PDPA"),

	zostało przyjęte a stare ustawodawstwo zostało zmienione.	Date in force: 15 January 2019. - Personal Data Protection Act Implementation Act, Date in force: 15 March 2019.
Finlandia	Zostało przyjęte nowe ustawodawstwo	- Finnish Data Protection Act (1050/2018) (the "Data Protection Act"), Date in force: 1 January 2019. - Act on Protection of privacy in Working Life (759/2004) (the "Workplace Privacy Act"), Date in force: 1 April 2019.
Francja	Stare przepisy zostały zaktualizowane	- French Data Protection Act (as amendment by the Law No. 2018-493 of 20 June 2018 on the protection of personal data and by the Decree No. 2018-687 of 1 August 2018), (The "FDPA", Date in force: 21 June 2018. - Order No. 2018 – 1125 of 12 December 2018 reorganising the FDPA and various provisions concerning the protection of personal data, Date in force: 1 June 2019.
Grecja	Wprowadzono nowe ustawodawstwo	- Law 4624/2019 („Data Protection Law"), which entered into force on 29 August 2019.
Hiszpania	Zostało wprowadzone nowe ustawodawstwo	- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights ("Ley Organica 3/2018, de 5 de diciembre de Protecction de Datos Personales y garantia de los derechos digitales"), (the "Data Protection Act"), Date in force: 7 December 2018.
Holandia	Zostało przyjęte nowe ustawodawstwo	- Uitvoeringswet Algemene Veordening Gegevenscherming (General Data Protection Regulation Implementation Act), Date in force; 25 May 2018.
Islandia	Zostało przyjęte nowe ustawodawstwo	- Act No. 90/2018 on Data Protection and the Processing of Personal Data (in Icelangic Log

		nr. 90/2018 um personuvernd og vinnslu personuupplysinga).
Irlandia	Zostało przyjęte nowe ustawodawstwo	- Data Sharing and Governance Act 2019, Date in force: part commenced 18 April 2019.
Liechtenstein	Zostało przyjęte nowe ustawodawstwo	- Datenschultzgesetz (the "Data Protection Act"), Date in force: 1 January 2019.
Litwa	Stare przepisy zostały zaktualizowane	- The Law on Legal Protection of Personal Data ("Data Protection Law"), Date in force: 16 July 2018.
Luksemburg	Zostało przyjęte nowe ustawodawstwo	- Law of 1 August 2018 organising the National Commission on Data Protection and implementing the GDPR (the "Data Protection Law"), Date in force: 20 August 2018.
Łotwa	Zostało przyjęte nowe ustawodawstwo	- Personal Data Processing Law ("PDPL"), Date in force: 5 July 2018.
Malta	Zostało przyjęte nowe ustawodawstwo	- Data Protection Act, CAP 586, Date in force: 28 May 2018.
Niemcy	Stare przepisy zostały zaktualizowane	- Bundesdatenschultzgesetz, Neufassung 2018 ("BDSG"), Date in force: 25 May 2018.
Norwegia	Zostało przyjęte nowe ustawodawstwo	- The Norwegian Data Protection Act, Date in force: 20 July 2018.
Polska	Nowe ustawodawstwo zostało przyjęte a stare ustawodawstwo zostało zmienione.	- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018 poz. 1000. - 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. 2019 poz. 730.
Portugalia	Zostało przyjęte nowe	- Act 58/2019 of 8 August (the „Data

	ustawodawstwo	Protection Act"), Date in Force: 9 August 2019.
Rumunia	Stare przepisy zostały zaktualizowane	- Law No. 190 of 18 July 2018 regarding the Measures for the Application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 re the Protection of Natural Persons With regard to the Processing Personal Data and on the Free Movements of Such Data, and Repeal of the Directive 95/46/EC (General Data Protection Regulation), (the „Data Protection Act"), Date in force: - Law No. 129 of 15 June 2018 re the Amendment and Supplementation of Law No. 102 of 2005 regarding the Organisation and Functioning of the National Supervisory Authority for Personal Data Processing and for repealing Law No. 677/2001 regarding the Protection of the Individuals re the Processing of Personal Data and Free Movement of Such Data, Date in force: 24 June 2018.
Słowacja	Zostało przyjęte nowe ustawodawstwo	- Act. No. 18/2018 Coll., on the Protection of Personal Data and Changing and Amending of Other Acta (the „Data Protection Act"), Date in force: 25 May 2018.
Słowenia	Jest w trakcie przyjmowania nowego ustawodawstwa (projektu ustawy).	
Szwecja	Główna krajowa ustawa o ochronie danych przed RODO została uchylona,	- The Swedish Data Protection Act (2018;218), (Swe. Lag(2018;218) med kompletterande bestammesler till EU: s dataskyddsforording, (the "Data Protection

	podczas gdy inne rodzaje ustawodawstwa obejmującego również ochronę danych, tj. ustawa o danych pacjentów, zostały zmienione zgodnie z RODO.	Act"), Date in force: 25 May 2018.
Węgry	Stare przepisy zostały zaktualizowane	- Act CXII of 2011 on the Right of Informational Self – Determination and on Freedom od Information (the "Data Protection Act"), Date in force: 26 April 2019. - Act XLVII of 1997 on the processing and protection of personal data concerning health (the "Health Data Processing Act"), Date in force: 26 April 2019.
Włochy	Stare przepisy zostały zaktualizowane	- Legislative Decree No. 101/2018 setting out rules adapting Italia law to the GOPR, chich amendment Legislative Decree No. 196/2003 setting out Italian privacy code (the "Italian Privacy Code", Date in force: 19 September 2018.
Wielka Brytania	Zostało przyjęte nowe ustawodawstwo	- UK Data Protection Act 2018, Date in force: 25 May 2018.

Źródło: Opracowanie własne na podstawie danych internetowych

RODO uważane jest za przełomowe ustawodawstwo i odpowiedni środek wymagany w celu pomocy rządom i obywatelom w odzyskaniu kontroli nad bezpieczeństwem danych. Na podstawie przedstawionej listy warto odnieść się do kwestii Wielkiej Brytanii. Obowiązująca tam ustawa o ochronie danych z 2018 r. jest niemal identyczną kopią RODO. Dlatego w momencie gdy Wielka Brytania opuści UE, nie nastąpi znacząca zmiana w prawie. Po opuszczeniu Wielkiej Brytanii RODO nadal

będzie chronić prawa obywateli UE, dzięki czemu firmy i organizacje nie będą musiały zmieniać swoich polityk.

Mogą jednak nastąpić zmiany w organizacjach przenoszących dane między Europejskim Obszarem Gospodarczym a Wielką Brytanią. Zależy to od tego, z czym wychodzi Wielka Brytania. Ponieważ Wielka Brytania nie będzie technicznie częścią RODO, nie ma żadnych gwarancji, że dane będą chronione. W związku z tym adekwatność danych staje się ważna.

Obecnie rząd Wielkiej Brytanii zapowiedział, że będzie starał się zawrzeć umowy o odpowiedniej ochronie z UE, aby wyjaśnić, że jej system ochrony danych jest zasadniczo taki sam jak RODO. Po uzgodnieniu oznaczałoby to, że dane mogą z łatwością przepływać między EOG i Wielką Brytanią[621].

4.2. Przekształcenia w obszarze kreowania polityki bezpieczeństwa danych osobowych

Początkowo to Rada Europy przyczyniała się do przekształceń w obszarze kreowania polityki bezpieczeństwa danych osobowych. Komitet Konsultacyjny Konwencji nr 108 zaczął w 1989 r. zastanawiać się nad możliwością stosowania technik umownych w celu zapewnienia ochrony prywatności jednostki w sieci w kontekście transgranicznego przepływu danych. O tej umownej technice mówiono już w kilku zaleceniach sektorowych dotyczących ochrony danych przez Komitet Ministrów (np. Zalecenie nr R(86)2 w sprawie wykorzystywanych danych osobowych w celu zabezpieczenia społecznego; Zalecenie nr R (89)2 w sprawie ochrony wykorzystywanych danych osobowych do celów zatrudnienia).

Biorąc pod uwagę powyższe rozważania, Rada Europy wspólnie z Komisją Wspólnot Europejskich i Międzynarodową Izbą Handlu, przygotowała w 1992 r. badanie zawierające „modelową umowę w celu zapewnienia równoważnej ochrony w kontekście transgranicznych przepływów danych", w której obowiązki licencjonodawcy

[621] Zob. M. Burgess, *What is GDPR? The summary guide to GDPR compliance in the UK,* źródło: www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary, data dostępu: 10.01.2020.

i licencjonobiorcy oparte zostały na gwarancjach ustanowionych przez Konwencję nr 108 Rady Europy[622].

Klauzule modelowej umowy miały na celu umożliwienie przekazywania danych osobowych między niezależnymi podmiotami gospodarczymi. Z kolei Strony miały opcjonalne prawo decydowania czy skorzystać z klauzul, czy też nie.

Ten „wzór umowy" stanowił pierwszy krok do przygotowania podobnych modelowych klauzul umownych o zasięgu międzynarodowym[623]. Dla przykładu kolejny ruch należał do Grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, która na mocy dyrektywy 95/46/WE wydała wytyczne w celu pomocy w ocenie odpowiedniego poziomu ochrony wymaganej przy przekazywaniu danych osobowych do krajów trzecich[624]. Po nich Komisja Europejska przyjęła decyzję 2001/497/WE z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do krajów trzecich. Mówiąc w skrócie, zawarto w niej standardowe klauzule umowne zapewniające odpowiednie zabezpieczenie danych osobowych przesyłanych z Unii Europejskiej do krajów spoza niej.

Biorąc pod uwagę zmiany legislacyjne i technologiczne, które nastąpiły w obszarze ochrony danych od czasu przygotowania „modelowej umowy" w 1992 r. Rada Europejskiego Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy postanowiła ponownie przeanalizować problem klauzul umownych, które należy stosować przy przekazywaniu danych osobowych do państw trzecich, w których nie było odpowiedniego poziomu ochrony.

Na podstawie przeprowadzonego badania, a także nowych instrumentów międzynarodowych w szczególności Protokółu dodatkowego do Konwencji 108 i decyzji Komisji wymienionej powyżej, Rada postanowiła przygotować przewodnik, którego celem miało być niesienie pomocy stronom w sporządzaniu klauzul umownych zgodnie z wymogami ochrony wynikającej z Konwencji 108 i przekazywania danych[625].

---

[622] Zob. *Guide to the reparation of contractual clauses governing data protection the transfer of personal data to third not bound by an adequate level of data protection (2002),* Prepared by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) in 2002, źródło: www.rm.coe.int/168068416c, data dostępu: 26.07.2019.

[623] Tamże.

[624] Zob. WP 4(5020/97), "First orientations on transfer of personal data to third countries working document – possible forward in assessing adequacy, a discussion document adopted by the Working Party on 26 June 1997.

[625] *Guide to the reparation…,* jw.

Rządy na całym świecie reagują na zwiększone zapotrzebowanie na ochronę danych poprzez różne przepisy. W ciągu ostatnich kilku lat obserwujemy rozpowszechnianie się przepisów o ochronie danych, które wprowadziły nowe wymogi zgodności dla organizacji. W przypadku nowych przepisów zasadnicze znaczenie ma osiągnięcie równowagi między ochroną a swobodnym przepływem wrażliwych danych. Globalna zgodność obejmuje ochronę danych wrażliwych, takich jak dane dotyczące płatności i dane osobowe.

Chociaż Internet jest z natury bezgraniczny, lokalizacja danych osobowych między państwami ma charakter geograficzny, co może prowadzić do pytań dotyczących suwerenności cyfrowej. Norma europejskie w zakresie prywatności i swobodnego przepływu danych poddawana jest testowi pod tym względem. Przykładem tego może być unieważnienie umowy Safe Harbor miedzy Unią Europejską a USA przez Trybunał Sprawiedliwości w 2015 r.[626] Została ona zastąpiona przez Tarczę Prywatności w październiku 2017 r.[627]

RODO jest prawem dotyczącym prywatności i kamieniem milowym w erze cyfrowej. Zaczęło ono odgrywać zasadniczą rolę w politykach państw na całym świecie.

Polityka bezpieczeństwa danych to wewnętrzny dokument, który służy jako podstawa praktyk zgodności z RODO. Wyjaśnia wymagania RODO wobec pracowników i określa zobowiązanie organizacji do przestrzegania przepisów.

Polityka bezpieczeństwa danych nie musi zawierać szczegółowych informacji na temat tego, w jaki sposób organizacja spełnia wymagania rozporządzenia, ponieważ zostaną one uwzględnione w procedurach organizacji. Zamiast tego polityka musi jedynie nakreślić, w jaki sposób RODO odnosi się do organizacji.

Polityka bezpieczeństwa danych służy trzem celom. Po pierwsze, stanowi podstawę dzięki której organizacja może osiągnąć zgodność z RODO. Po drugie, daje możliwość uczynienia RODO zrozumiałym dla obywateli. Po trzecie, zasady ochrony danych dowodzą, że organizacje są zobowiązane do przestrzegania RODO.

Polityka bezpieczeństwa danych osobowych powinna zawierać:

[626] Zob. Court of Justice of the European Union, Press Release No 117/15, The Court of justice declares that the Commission's US Safe Harbour Decision is invalid, Luxembourg, 6 October 2015, Judgment in Case C-362/14.

[627] Zob. *A New Swiss – U.S. Privacy Shield Replaces the U.S. – Swiss Safe Harbor,* źródło: www.jonesday.com/en/insights/2017/01/a-new-swissus-privacy-shield-replaces-the-usswiss-safe-harbor, data dostępu: 07.01.2020.

1) Cel polityki – może to służyć jako wprowadzenie, wyjaśniające związek polityki z RODO, znaczenie zgodności i dlaczego polityka jest konieczna.
2) Definicja kluczowych terminów – RODO jest pełne terminologii związanej z ochroną danych, którą należy wyjaśnić. Ta sekcja powinna zawierać bardzo trudne terminy, takie jak „administrator" i „procesor". Ale może także wyjaśniać takie kwestie jak „osoba, której dane dotyczą", które nie są tak jednoznaczne, jak mogłyby się wydawać.
3) Zakres – Wymagania RODO dotyczą danych osobowych rezydentów UE i wszystkich osób w organizacji, które przetwarzają te informacje. ‘
4) Zasady – należy kierować się sześcioma zasadami RODO dotyczącymi przetwarzania danych.
5) Prawa podmiotów danych – RODO przyznaje osobom fizycznym osiem praw podmiotów danych. Należy je zdefiniować i stwierdzić, że zapewnią ich spełnienie.
6) Inspektor danych osobowych – należy wskazać dane organu kontrolnego[628].

Wpływ RODO na politykę bezpieczeństwa danych osobowych jest zasadniczy. Sposób, w jaki największe światowe firmy internetowe wykorzystywały dane swoich klientów stał się wyraźnym sygnałem, że potrzebne są regulacje takie jak RODO. Wiele platform cyfrowych, takich jak Google i Facebook oferuje usługi bezpłatnie – ale często polegają one na gromadzeniu danych z pasywnej bazy użytkowników, na których mogą następnie zarabiać. Użytkownicy, kolektywnie nie płacą konwencjonalnymi środkami, na przykład, gdy korzystają z wyszukiwarki Google, ale każde działanie jest rejestrowane i pakowane w punkty danych, które są uważane za bardzo cenne przez strony trzecie.

W przeszłości tego rodzaju gromadzenie danych było często maskowane przez niejasne pola wyboru lub przyciski zgody. Dlatego kształtowanie polityk na podstawie

[628] Zob. L. Irwin, *How to write a GDPR data protection policy – with template examples,* źródło: www.itgovernance.co.uk, data dostępu: 07.01.2020.

przyjętych standardów wzmocniło system ochronny poprzez zobowiązanie użytkowników danych do ich przestrzegania, podczas przetwarzania danych w naszym imieniu. Co więcej, zgodnie z RODO każde naruszenie tych standardów może skutkować działaniami dyscyplinarnymi[629].

Warto zaznaczyć, iż już pierwsze uchwalane akty prawne poświęcone ochronie danych osobowych powoływały do życia specjalne organy wyspecjalizowane w tej dziedzinie[630]. Jak zauważa M. Jagielski: „Jeszcze zanim zostały wydane akty z lat 90,. ukształtowały się w Europie dwa modele działania organów nadzorujących przetwarzanie danych osobowych na poziomie krajowym. Cechą charakterystyczną modelu pierwszego jest nakierowanie działalności organu na ochronę praw konkretnej jednostki. Organ taki działa z zasady na wniosek podmiotu danych i koncentruje się na tych działaniach, które bezpośrednio zmierzają do realizacji jej żądań: zapewnienia ochrony jej danych lub – ewentualnie – zapewnienia jej odszkodowania za doznaną szkodę. W związku z nakierowaniem działalności na ochronę praw jednostki określa się ten model mianem orzecznikowego (od pojęcia „ombudsman"). Jest on charakterystyczny dla państw skandynawskich, zwłaszcza Szwecji i Finlandii. Model drugi polega na nastawieniu działalności organu na zapewnienie realizacji prawa. Podejmowane przez organ działania mają w pierwszym rzędzie zapewnić wdrożenie i realizację postanowień prawa ochrony danych osobowych. Zagwarantowanie uprawnień konkretnej jednostki ma charakter wtórny wobec tego działania. Ze względu na podobieństwo działania organu nadzorczego do działalności organów regulacyjnych w innych dziedzinach prawa określa się go mianem modelu regulacyjnego"[631].

W Polsce organem odpowiedzialnym za kształtowanie polityki państwa w zakresie bezpieczeństwa danych osobowych jest Ministerstwo Cyfryzacji[632]. Jego rolą jest podejmowanie działań mających na celu tworzenie przepisów zapewniających pełne oraz skuteczne wdrażanie RODO w polskim porządku prawnym. Ministerstwo implementując RODO udostępniło projekt nowej ustawy o ochronie danych osobowych a także projekt zmian przepisów sektorowych. (obejmujący ponad 130 ustaw). Jak zauważa M. Dziembaja „pod względem ilości zmienianych aktów prawnych projekt ten

[629] Zob. A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, wyd. 2., Wolters Kluwer Polska Warszawa 2018, s. 48.
[630] Zob. M. Jagielski, *Prawo do ochrony…,* s. 164.
[631] Tamże, s. 167 – 168.
[632] Zob. *Baza wiedzy RODO,* źródło: www.gov.pl/web/cyfryzacja/baza-wiedzy-rodo, data dostępu: 08.01.2020.

jest jednym z największych w ciągu ostatnich lat"[633]. Polska stała się jednym z pierwszych państw zmieniających cały krajowy system prawny w tym obszarze[634].

Istotne znaczenie w tym obszarze odgrywa również Urząd Ochrony Danych Osobowych[635].

4.3. Przekształcenia w obszarze mechanizmów kontrolnych bezpieczeństwa danych osobowych

W 2003 r. Komitet Rady Europy zajmujący się ochroną danych dokonał analizy pewnych szczególnych aspektów nadzoru. CJ-PD zwrócił się w tym celu do konsultanta, dr Giovanniego Buttarelliego (sekretarza generalnego włoskiego urzędu ochrony danych) w celu sporządzenia raportu na temat ochrony danych w związku z działaniami nadzorczymi. Raport ten potwierdził, że wszelkie badania nadzoru są związane z rozwojem technologicznym w Europie i należy je analizować w aspekcie historycznym. W efekcie zgodzono się uzgodnić listę zasad przewodnich, które należało uwzględnić w odniesieniu do gromadzenia i przetwarzania danych za pomocą nadzoru wideo[636].

Spowodowane to było tym, iż wiele podmiotów w coraz większym stopniu zaczęło korzystać z systemów nadzoru do różnych celów, w szczególności działania te dotyczyły kontroli przepływu osób i towarów, jak również dostępu do nieruchomości co łączyło się z gromadzeniem określonych danych osobowych. Znaczna część tych czynności odbywała się za pomocą urządzeń do nadzoru wideo, co rodziło konkretne problemy dotyczące danych. Informacje zebrane podczas działań związanych z nadzorem wideo często obejmowały dane (w postaci obrazów i dźwięki), które bezpośrednio lub pośrednio pozwalały na identyfikację osób i monitorowanie ich postępowania. Ponadto systemy monitoringu zaczęły coraz bardziej zbliżać się do

[633] M. Dziembała, *Koncepcja polityki bezpieczeństwa w świetle zmian w ochronie danych osobowych w placówce medycznej,* „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 355, s. 22.
[634] Tamże.
[635]Zob. P. Szustakiewicz, *Pozycja prawna Prezesa Urzędu Ochrony Danych Osobowych - ustrój i kompetencje polskiego organu nadzoru*, „Kontrola Państwowa" 2018, nr 6, s. 8.

[636] Zob. Report containing guiding principles for the Protection of Individuals with regard to collection and processing of data by means of video surveillance, as adopted by the European Committee on Legal Co-operation (CDCJ) at its 78th meeting (20-23 May 2003), źródło: www.rm.coe.int/1680684b, data dostępu: 26.07.2019.

innych technologii, które budziły obawy dotyczące prywatności i ochrony danych. Należały do nich: nagrywanie dźwięku, bezprzewodowe i szybkie sieci komputerowe wykorzystywane do przesyłania obrazów, rozpoznawanie twarzy itp.[637]

Działania w zakresie nadzoru wideo związane z przetwarzaniem danych osobowych weszły tym samym w zakres zastosowania Konwencji nr 108 Rady Europy. Dodatkowe prawa i zabezpieczenia zostały określone w zaleceniach Rady Europy, a w szczególności w;

- zaleceniu nr R (87)15 w sprawie wykorzystania danych osobowych w sektorze policji;
- zaleceniu nr R(89)2 w sprawie ochrony danych osobowych wykorzystywanych do celów zatrudnienia;
- zaleceniu nr R(95)4 w sprawie ochrony danych osobowych w sektorze telekomunikacyjnym.

W różnych zaleceniach, które choć nie odnosiły się wyraźnie do nadzoru wideo to objęto nimi zabezpieczenia i zasady, które stały się istotne z punktu widzenia ochrony danych osobowych, jak również związanej z nimi komunikacji danych i przepływu danych transgranicznych.

W Unii Europejskiej organy ochrony danych są niezależnymi organami publicznymi, które nadzorują poprzez uprawnienia dochodzeniowe i naprawcze, stosowanie prawa o ochronie danych. Zapewniają porady ekspertów w kwestiach związanych z ochroną danych i zajmują się skargami na naruszenie ogólnego rozporządzenia o ochronie danych i odpowiednich przepisów krajowych. W każdym państwie członkowskim UE jest jeden[638].

Aby egzekwowanie przepisów o ochronie danych było skuteczne, organy ochrony danych mają uprawnienia do badania, wykrywania i karania naruszeń, a także do odpowiedzialności za podnoszenie świadomości na temat praw i obowiązków w zakresie ochrony danych w ogóle[639].

W UE dodatkowo skuteczność tę wzmacnia wymóg niezależności organów ochrony danych od jakichkolwiek wpływów politycznych, rządowych lub innych. Wymóg ten został określony w art. 16 Traktatu o funkcjonowaniu UE[640] i art. 8 Karty

[637] Tamże.
[638] Zob. *What are Data Protection Authorities (DPAs)?,* źródło: www.europa.eu/info/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en&prev=search, data dostępu: 08.01.2020.
[639] Zob. *Data Protection,* źródło: www.edps.europa.eu/data-protection_en, data dostępu: 08.01.2020.
[640] Dz.U. C 202 z 7.6.2016.

Praw Podstawowych UE[641]. Trybunał Sprawiedliwości UE konsekwentnie podkreśla, że kontrola przez niezależny organ jest zasadniczym elementem prawa do ochrony danych i ustanawia kryteria takiej niezależności. W szczególności organ nadzorczy musi działać w sposób całkowicie niezależny, co oznacza uprawnienia decyzyjne niezależne od jakiegokolwiek bezpośredniego lub pośredniego wpływu zewnętrznego[642].

RODO również podkreśla znaczenie niezależności; Rozdział VI zawiera szczegółowe zasady dotyczące ustanawiania i funkcjonowania niezależnych organów nadzorczych, w tym przepisy dotyczące zasobów niezbędnych do skutecznego wykonywania ich zadań i uprawnień.

Europejski Inspektor Ochrony Danych jest niezależnym organem nadzorczym odpowiedzialnym za dopilnowanie, by instytucje i organy UE przestrzegały przepisów o ochronie danych podczas przetwarzania danych osobowych[643]. EIOD czyni to we współpracy z inspektorami ochrony danych obecnymi w każdej instytucji i organie europejskim.

Inspektor ochrony danych musi powiadomić EIOD o wszelkich operacjach przetwarzania dotyczących wrażliwych danych osobowych lub mogących stanowić inne szczególne ryzyko. Następnie EIOD analizuje to przetwarzanie w związku z rozporządzeniem o ochronie danych i wydaje opinię o „kontroli wstępnej". W większości przypadków działanie to prowadzi do sformułowania zestawu zaleceń, które instytucja lub organ musi wdrożyć, aby zapewnić zgodność z przepisami o ochronie danych[644].

Nadzorcza rola EIOD obejmuje także badanie skarg wniesionych przez pracowników UE lub każdą inną osobę, która uważa, że ich dane osobowe zostały niewłaściwie potraktowane przez instytucje lub organ europejski. Przykłady skarg obejmują rzekome naruszenie poufności, dostęp do danych, prawo do sprostowania, usunięcia danych oraz nadmiernego gromadzenia lub nielegalnego wykorzystywania danych przez administratora[645].

[641] Dz.Urz. UE C 303 z 14.12.2007.
[642] *Data Protection…,* j.w.
[643] Zob. *Europejski Inspektor Ochrony Danych (EIOD),* źródło: www.europa.eu>european-data-protection-supervisor.pl, data dostępu: 08.01.2020.
[644] Zob. V. Pozzato, *2014 Opinion of the European Data Protection Supervisor: Interplay Between Data Protection and Competition Law,* "Journal of European Competition Law & Practice" 2014, Vol. 5, s. 468 – 470.
[645] Por. *Annual report 2012,* European Data Protection Supervisor, Publications Office, Luxemburg 2013.

Europejskim Inspektorem Ochrony Danych Osobowych jest mianowany w dniu 6 grudnia 2019 r. Wojciech Wiewiórowski[646].

19 grudnia 2019 r. EIOD opublikował nowe wytyczne dotyczące oceny proporcjonalności. Mają one na celu zapewnienie decydentom praktycznych narzędzi pomagających w ocenie zgodności proponowanych środków UE, które miałyby wpływ na podstawowe prawa do prywatności i ochrony danych osobowych z Kartą Praw Podstawowych. Biorąc pod uwagę, iż RODO opiera się na art. 8 KPP i art. 16 Traktatu o funkcjonowaniu UE[647].

Także w 2019 r. EIOD wszczął dochodzenie w sprawie ustaleń umownych między instytucjami UE a gigantem technologicznym Microsoft, po zmianach regulujących outsourcing UE. Wstępne wyniki ujawniły poważne obawy dotyczące zgodności odpowiednich warunków umownych z przepisami dotyczącymi ochrony danych oraz roli Microsoft jako podmiotu przetwarzającego instytucje UE korzystające z jego produktów i usług. Komentując oświadczenie Microsoft, Wojciech Wiewiórowski, powiedział" Oczekujemy, że utworzenie Forum w Hadze i wyniki naszego dochodzenia pomogą poprawić zgodność wszystkich instytucji UE w zakresie ochrony danych, ale dążymy również do pozytywnego działania zmiany poza instytucjami UE, aby zapewnić maksymalne korzyści jak największej liczbie osób. Osiągnięte porozumienie między holenderskim Ministerstwem Sprawiedliwości i Bezpieczeństwa a Microsoftem w sprawie odpowiednich zabezpieczeń umownych i technicznych oraz środków ograniczających ryzyko dla osób fizycznych stanowi pozytywny krok na przód, Poprzez forum haskie i poprzez wzmocnienie współpracy regulacyjnej dążymy do tego, aby te zabezpieczenia i środki obowiązywały wszystkich konsumentów i władze publiczne mieszkające i działające w EOG"[648].

Europejska Rada Ochrony Danych Osobowych (EROD) jest niezależnym organem europejskim, który ma zapewnić spójne stosowanie przepisów o ochronie danych w całej Unii Europejskiej. EROD ustanowiono na mocy ogólnego

[646] Zob. *New EDPS mandate 2019 – 2024,* źródło: www.edps.europa.eu, data dostępu: 09.01.2019; *Wojciech Wiewiórowski mianowany Europejskim Inspektorem Ochrony Danych Osobowych*, https://www.consilium.europa.eu/pl/press/press-releases/2019/12/05/wojciech-wiewiorowski-appointed-european-data-protection-supervisor/#, data dostępu: 26.12.2020.
[647] Zob. Guidelines The European Data Protection Supervisor, *Assessing the proportionality of measures limit the fundamental rights to privacy and to the protection of personal data,* 19 December 2019, źródło: www.eds.europa.eu, data dostępu: 09.01.2020.
[648] Zob. *EU contracts with Microsoft raising 'serious' data concerns, says watchdog,* źródło: www.techcrunch.com/2019/10/21/eu-contracts-with-microsoft-raising-serious, data dostępu: 09.01.2019.

rozporządzenia o ochronie danych (RODO). W skład EROD wchodzą przedstawiciele krajowych organów ochrony danych w krajach UE/EOG i urzędu Europejskiego Inspektora Ochrony Danych (EIOD). Komisja Europejska uczestniczy w działaniach i posiedzeniach Rady, ale bez prawa głosu. Obsługa sekretariatu EROD jest zapewniana przez EIOD. Sekretariat wykonuje swoje zadania pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych. Zadania EROD polegają przede wszystkim na wydawaniu ogólnych wytycznych dotyczących kluczowych pojęć zawartych w RODO i dyrektywie o ochronie danych w sprawach karnych, doradzaniu Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych i nowymi proponowanymi przepisami w Unii Europejskiej oraz wydawaniu wiążących decyzji w sporach między krajowymi organami nadzorczymi[649].

W Polsce w latach 1997 – 2018 działał Generalny Inspektor Ochrony Danych Osobowych (GIODO)[650], którego rolą była „kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych"[651]. 10 maja 2018 r. na podstawie nowej ustawy o ochronie danych osobowych ustanowiono nowy organ w postaci Prezesa Urzędu Ochrony Danych Osobowych[652]. Istotne jest takie usytuowanie ustrojowe tego organu, które umożliwia mu realizację zadań, m.in. związanych z implementacją RODO[653].

W Belgii kontrolą bezpieczeństwa danych osobowych zajmuje się Komisja ochrony prywatności[654]. Posiada ona uprawnienia do prowadzenia dochodzeń w sprawach (w tym wnioskowania o dokumenty i prowadzenia dochodzeń na miejscu), rozpatrywania skarg i przeprowadzania procedur mediacyjnych, wydawania niewiążących porad i przekazywania spraw cywilnych do Sądu Pierwszej Instancji oraz spraw karnych do prokuratora[655].

---

[649] Zob. *Ochrona danych w UE,* https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pl, data dostępu: 26.12.2020.

[650] Szerzej: E. Kuczma, P. Kuczma, *Generalny Inspektor Ochrony Danych Osobowych i ochrony prawa,* „Zeszyty Naukowe Dolnośląskiej Wyższej Szkoły Przedsiębiorczości i Techniki w Polkowicach. Studia z nauk społecznych" 2013, nr 6, s. 209 – 230.

[651] *ABC zasad kontroli przetwarzania danych osobowych,* Generalny Inspektor Ochrony Danych (GIODO), Wydawnictwo Sejmowe, Warszawa 2011, s. 6.

[652] Zob. *Prezes Urzędu Ochrony Danych Osobowych,* źródło: www.uodo.gov.pl/pl/preses-i-urzad, data dostępu: 08.01.2020.

[653] Zob. M. Abu Gholeh, *Pozycja ustrojowa organu nadzorczego ochrony danych osobowych na przykładzie Polski*, „Przegląd Prawa Konstytucyjnego" 2019, nr 4, s. 163.

[654] Stron internetowa Komisji Ochrony Prywatności: www.privacycommission.be.

[655] Zob. *Data Protection Enforcement in Belgium,* źródło: www.globalcompliancenews.com/data-privacy/data-protection-enforcement-in-belgium/&prev=search, data dostępu: 08.01.2020.

Belgijski organ ochrony danych, jak również niemiecki organ, zostali powiadomieni przez firmę Mastercard o naruszeniu danych wykrytych w dniu 19 sierpnia 2019 r., które dotknęłoby dużą liczbę osób, których dane dotyczą, a z których znaczna część to Niemieccy klienci. Ponieważ główny zakład Mastercard znajduje się w Waterloo, belgijski organ ochrony danych ściśle współpracuje ze swoim niemieckim odpowiednikiem i innymi właściwymi organami w celu obrony interesów osób dotkniętych tym incydentem[656].

Szeroki zakres uprawnień dochodzeniowo, naprawczych i doradczych ma bułgarska Komisja Ochrony Danych Osobowych (CPDP). Stanowi ona organ kolegialny, w skład którego wchodzą przewodniczący i czterech członków wybieranych przez Parlament. CPDP jest jedynym bułgarskim organem publicznym, który oferuje wszystkie swoje usługi online, bezpłatnie i jest w pełni zintegrowany z krajowym portalem e-administracji. Dokonuje nadzoru ochrony danych osobowych na podstawie RODO zarówno w sektorze publicznym jak i prywatnym[657].

W Chorwacji zasadniczą rolę w zapewnieniu bezpieczeństwa danych osobowych odgrywa Agencja Ochrony Danych Osobowych. Jej najważniejszą rolą jest zapewnienie zgodności organizacji prywatnych i organów publicznych z przepisami dotyczącymi ochrony danych. Prócz tego Agencja ma także obowiązek informowania i edukowania administratorów danych, inspektorów ochrony danych, przedstawicieli administracji państwowej i lokalnej oraz wszystkich obywateli o ich prawach i obowiązkach wynikających z RODO[658].

Chorwacka Agencja Ochrony Danych Osobowych zarządza szeregiem działań, takich jak sesje edukacyjne i wydarzenia, których celem jest podniesienie i zwiększenie świadomości społecznej na temat znaczenia ochrony danych osobowych i prywatności. W związku z tym w okresie od stycznia do czerwca 2016 r. Agencja przeprowadziła dziesięć kampanii edukacyjnych dla administratorów danych i urzędników zajmujących się ochroną danych osobowych, a także 59 sesji edukacyjnych dla uczniów szkół podstawowych[659].

[656] Zob. *Belgian and German data protection authorities cooperate on Mastercard's data,* źródło: www.data protectionauthority.be/news, data dostępu: 08.01.2020.
[657] Zob. *The Bulgarian Commission for Personal Data Protection,* źródło: www.privacyconference2018.org/en/about/bulgarian-commission-personal-data-protection.html&prev, data dostępu: 08.01.2020.
[658] Zob. *Raising Awareness Activities 2017 – 2019,* źródło: www.azop.hr/data-protection-agency, data dostępu: 08.01.2020.
[659] Tamże.

Na Węgrzech funkcjonuje krajowy organ ds. ochrony danych i wolności informacji (Namzeti Adatvedelmi es Informacioszabadsag Hatosag, NAIH). Jest on odpowiedzialny za monitorowanie i promowanie egzekwowania dwóch podstawowych praw: prawa do ochrony danych osobowych i prawa do wolności informacji, jak również za promowanie swobodnego przepływu danych osobowych w Unii Europejskiej. Został on ustanowiony na mocy ustawy CXII z 2011 r. aby zapewnić nieskrępowane stosowanie RODO[660].

W Irlandii utworzono urząd Komisję ds. Ochrony danych. Stanowi ona organ nadzorczy w zakresie ogólnego rozporządzenia o ochronie danych (RODO), a także ma funkcje i uprawnienia związane z ważnymi ramami regulacyjnymi, w tym irlandzkimi rozporządzeniami o prywatności i łączności elektronicznej (2011 r.), oraz dyrektywą UE znaną jako dyrektywa w sprawie egzekwowania prawa[661].

Zarówno na Litwie jak i Łotwie organami nadzorującymi implementację RODO są Inspektoraty Ochrony Danych. Z kolei na Malcie rolę tę pełni Komisarz ds. Informacji i ochrony Danych. Podobnie w Słowenii i Wielkiej Brytanii funkcjonuje Komisarz ds. Informacji[662].

Każdy z przedstawionych krajowych organów ochrony danych odgrywa zasadniczą rolę nadzorczą. Został powołany w celu wdrażania i egzekwowania przepisów o ochronie danych oraz w celu udzielania wskazówek.

Warto przy tym wskazać, iż od momentu wprowadzenia nowych przepisów podstawowe role i obowiązki organów ochrony danych nie zmieniły się znacząco. Organizacje mogą w dużej mierze polegać na doświadczeniach w zakresie interakcji z organami ochrony danych.

Każdy organ ochrony danych jest powoływany na szczeblu krajowym na podstawie ustawodawstwa krajowego. Jego jurysdykcja i uprawnienia wykonawcze są w dużej mierze ograniczone do terytorium własnego państwa członkowskiego. Niektóre państwa członkowskie (np. Niemcy) wyznaczają wiele organów ochrony danych w strukturze federalnej. Inni (np. Dania) wyznaczają oddzielne organy publiczne odpowiedzialne za egzekwowanie różnych aspektów prawa o ochronie danych.

[660] Zob. *Hungarian to the National Authority for Data Protection and Freedom of Information,* źródło: www.naih.hu/general-information.html, data dostępu: 08.01.2020.
[661] Zob. *The Data Protection Commission,* źródło: www.dataprotection.ie, data dostępu: 08.01.2020.
[662] Zob. *Data Protection Authorities,* źródło: www.ec.europa.eu/justice/article-29/structure/data-protection-authorities, data dostępu: 08.01.2020.

Pozostając przy przykładzie Niemiec, warto zaznaczyć, iż w art. 51 RODO pozwala na ustanowienie regionalnych organów nadzoru. Spośród wszystkich państw członkowskich to właśnie Niemcy jako jedyne go wdrożyły.

Art. 51 ust. 3 stanowi, że gdy państwo członkowskie UE ustanawia wiele organów nadzoru, powinien istnieć jeden główny organ, który reprezentuje wszystkie pozostałe organy w radzie i zapewnia, aby jego poddani przestrzegali zasad współpracy określonych w sekcji II RODO. W przypadku Niemiec organem tym jest BFDI, który nadzoruje również wszystkie federalne władze i organizacje, firmy telekomunikacyjne i pocztowe.

Administracyjno – prawne mechanizmy nadzorcze nad procesami przetwarzania stanowią najbardziej praktyczny instrument wymuszania zgodności przetwarzania z obowiązującymi wymogami. Ich konstrukcja umożliwia bowiem najszybszy tryb reagowania na wszelkie nieprawidłowości. Przez wiele lat nie wypracowano jednak jednolitego ogólnoeuropejskiego modelu nadzoru. W efekcie przyjmowane rozwiązania w poszczególnych krajach zaczęły wahać się między modelem rzeczniowskim (zbliżonym do ombudsmana), a regulacyjnym (dysponującym szerokimi uprawnieniami administracyjnymi). I jak już zostało wspomniane, objęty jednolitym standardem stał się wymóg, by organ taki był niezależny w zakresie podejmowania działań oraz dysponował uprawnieniami monitorującymi, dochodzeniowymi i interwencyjnymi. Wybór konkretnych instrumentów został zasadniczo pozostawiony do rozstrzygnięcia na poziomie krajowym. Podkreśla się, że jako kryterium oceny zastosowanych w tym względzie środków nie służy ich charakter czy sposób oddziaływania, lecz skuteczność[663].

Warto odnotować szczególną sytuację, która dla stosowania RODO przyniósł brexit. 31 stycznia 2020 r. Wielka Brytania zawarła z Unią Europejską umowę o wystąpieniu Zjednoczonego Królestwa ze struktur europejskich (dalej jako „Porozumienie wyjściowe"). Zgodnie z art. 185 tego porozumienia postanowienia umowy wchodzą w życie 1 lutego 2020 r. i od tego momentu Wielka Brytania nie może być traktowana jako jeden z krajów Unii Europejskiej. Nie oznacza to jednak, że wszystkie europejskie przepisy przestały obowiązywać na terytorium Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej. Do końca 2020 r. trwał okres

[663] Zob. M. Jagielski, *Prawo do ochrony danych…,* s. 228.

przejściowy, podczas którego wszystkie dotychczasowe regulacje będą mieć zastosowanie. Odnosi się to również do przepisów z zakresu ochrony i przetwarzania danych osobowych, zatem Ogólne rozporządzenie o ochronie danych RODO obowiązywało na wyspach brytyjskich do końca tego okresu[664].

W dniu 24 grudnia 2020 r. osiągnięto porozumienie pomiędzy Unią Europejską a Wielką Brytanią w sprawie umowy handlowej, które zacznie obowiązywać po zakończeniu okresu przejściowego po brexicie[665].

4.4. Ocena efektywności wdrażania bezpieczeństwa danych osobowych w państwach członkowskich Rady Europy i Unii Europejskiej

Ochrona danych osobowych początkowo za sprawą Konwencji nr 108 Rady Europy, a następnie standardów wynikających z RODO[666] stała się prawdziwym globalnym zjawiskiem, ponieważ ludzie na całym świecie w coraz większym stopniu cenią ochronę i bezpieczeństwo swoich danych. Wiele krajów przyjęło lub jest w trakcie przyjmowania kompleksowych zasad ochrony danych na podstawie zasad określonych w RODO, co skutkuje globalną konwergencją zasady ochrony danych. Daje to również możliwość ułatwienia przepływu danych między celami komercyjnych operatorów lub władz publicznych, podnosząc jednocześnie poziom ochrony danych osobowych w UE i na całym świecie.

Wprowadzenie RODO spowodowało ogólny wzrost liczby skarg i powiadomień o naruszeniach, choć nie oznacza to, że zasady ochrony danych zostały złamane. Po prostu rosnąca świadomość spowodowała wzrost liczby raportów i odpowiedzialność organów regulacyjnych za ich przeglądanie i w razie potrzeby badanie.

Według Europejskiej Rady Ochrony Danych, w całej Unii Europejskiej w pierwszym roku stosowania RODO odnotowano 281088 przypadków. Spośród nich

---

[664] Zob. A. Polanowski, *Brixit a ochrona danych osobowych. Jak wystąpienie Wielkiej Brytanii z Unii Europejskiej wpłynie na polskich przedsiębiorców?*, https://www.parp.gov.pl/component/content/article/64651:brexit-a-ochrona-danych-osobowych-jak-wystapienie-wielkiej-brytanii-z-unii-europejskiej-wplynie-na-polskich-przedsiebiorcow, data dostępu: 26.12.2020.

[665] Zob. *Brexit. Wielka Brytania i UE osiagnęły porozumienie w sprawie umowy handlowej*, https://www.bankier.pl/wiadomosc/Brexit-Wielka-Brytania-i-UE-osiagnely-porozumienie-ws-umowy-handlowej-8026891.html, data dostępu: 27.1.2020.

[666] Zob. *EU General Data Protection Regulation (GDPR) : an implementation and compliance guide*, IT Governance Publishing, Ely 2017, s. 12.

144 376 dotyczyło skarg konsumentów, a 89 271 dotyczyło powiadomień o naruszeniu danych przez administratorów danych. Niderlandy, Niemcy i Zjednoczone Królestwo zgłosiły odpowiednio największą liczbę naruszeń. Najniższe odnotowano w Liechtensteinie, Islandii i na Cyprze[667].

Trzy obszary, które były przedmiotem największej liczby skarg konsumentów, to telemarketing, e-maile promocyjne oraz monitoring CCTV/wideo.

Jednak zgodnie z badaniem przeprowadzonym przez kancelarię DLA Piper, dotyczącym naruszeń danych osobowych od czasu wprowadzenia RODO, w ciągu pierwszych ośmiu miesięcy od wejścia w życie nowych przepisów nałożono zaledwie 91 grzywien na RODO w Europejskim Obszarze Gospodarczym. Liczba ta wzrosła w 2019 roku, ale niewiele[668]. W raporcie Europejskiej Rady Ochrony Danych dla Parlamentu Europejskiego z lutego 2019 r. wskazano, że 11 krajów nałożyło 56 mln. EUR – w ty, 50 mln EUR nałożonych na Google przez francuską Krajową Komisję Informatyki i Wolności (CNIL).

Większość krajów UE nałożyła grzywny na mocy RODO (tymi, które nie były to Belgia, Irlandia, Republika Czeska, Dania, Finlandia, Włochy, Słowacja, Słowenia, Hiszpania i Szwecja). W przeważającej części kwant był jak dotąd zgodny ze starym reżimem, co oznacza stosunkowo skromne kary[669].

Niektóre kraje, jak Austria, zdecydowały się na zwalczanie ogólnych nadużyć na niskim poziomie, które mogłyby dotyczyć szerszej gamy organizacji. Dla przykładu we wrześniu 2018 r. Austriacki organ nadzorczy, DSB nałożył karę pieniężną na zakład bukmacherski o wartości 5.280 EUR za instalacje kamery CCTV rejestrującej przechodniów, co uznano za sprzeczne z zakazem RODO dotyczącym monitorowania publicznego na dużą skalę[670].

Austria stosuje system, w którym pierwsze naruszenia RODO można zasadniczo ukarać ostrzeżeniem. Austriacki organ ochrony danych nakłada grzywny dopiero od drugiego naruszenia. Z kolei w Danii nawet 25 maja 2018 r. było jasne, że duński organ

[667] Zob. *2018 Annual Report – a new era in data protection,* źródło: www.edps.europa.eu/data-protection/our/publications/annual-reports/2018, data dostępu: 09.01.2020.
[668] Zob. DLA Piper GOPR Data Breach Survey, A report by DLA Piper's cybersecurity team, February 2019, źródło: www.dlapiper.com/-/media/files/data dostępu: 30.12.2019.
[669] Zob. N. Hodge, *GDPR enforcement varies widely by country,* źródło: www.complianceweek.com/gdpr-enforcement-varies-widely-by-country, data dostępu: 31.12.2019.
[670] Zob. *GDPR Guide to National Implementation: Austria. A practical guide to national GDPR compliance requirements across the EEA,* źródło: www.whitecase.com/publications/article/gdpr-guide-national-implementation, data dostępu: 09.01.2020.

nie będzie nakładał kar pieniężnych na mocy RODO, ponieważ duńskie prawo konstytucyjne oznacza, że organ regulacyjny nie może nakładać kar zgodnie z nowymi przepisami dotyczącymi danych, dopóki duńskie sądy nie ustalą odpowiedniego poziomu grzywny za różne rodzaje naruszenia RODO[671].

Duński organ ochrony danych przekazał jednak jedną konkretną sprawę duńskiej prokuraturze. Po wizycie kontrolnej w duńskiej firmie taksówkowej duński organ ochrony danych stwierdził, że przechowała ona dane osobowe (głównie numery telefonów) z około 9 milionów przejazdów taksówką bez uzasadnionego powodu. W związku z tym duński organ ochrony danych zasugerował nałożenie grzywny w wysokości 1,2 mln DKK[672].

Niektóre z bardziej surowych do tej pory kar koncentrowały się na niewłaściwym wykorzystaniu danych w technologii. Na przykład krajowa liga piłki nożnej w Hiszpanii, LaLiga, została ukarana grzywną w wysokości 250 000 EUR za oferowanie aplikacji, która bez ich wiedzy i zgody uzyskiwała dostęp do mikrofonów telefonów komórkowych użytkowników w celu wykrycia, czy puby, które oglądały mecze piłki nożnej faktycznie uiściły wymaganą w tym celu opłatę[673].

Tymczasem portugalski szpital został ukarany grzywną w wysokości 400 000 EUR, po tym jak dochodzenie ujawniło, że personel szpitala, psychologowie, dietetycy i inni specjaliści mieli nieograniczony dostęp do danych pacjentów poprzez fałszywe profile. Przeprowadzona później kontrola wykazała, że szpital ma 985 zarejestrowanych profili lekarzy, mimo że miał tylko 296 lekarzy[674].

W Niemczech organy ochrony danych są zorganizowane na poziomie państwowym, co oznacza, że istnieje 16 organów regulacyjnych ds. Danych. W sumie niemieckie organy ochrony danych wydały 75 grzywien od czasu wprowadzenia RODO. Pierwszy taki przypadek miał miejsce w listopadzie 2018 r., kiedy LfDI Baden-Württemberg nałożyła karę pieniężną w wysokości 20 000 EUR na platformę społecznościową Knuddels za przechowywanie haseł w postaci zwykłego tekstu, w

[671] Tamże.
[672] Zob. *Denmark: Data Protection 2019,* źródło: www.iclg.com/practice-areas/data-protection-laws-and-regulations/denmark, data dostępu: 09.01.2020.
[673] Zob. *LaLiga fined EUR 250, 000 for using smartphone microphones to detect illegal feeds,* źródło: www.telecompaper.com/news/la-liga-fined-eur-250000-for-using-smartphone-microphones-to-detect-illegal-feeds-1296384, data dostępu: 09.01.2020.
[674] Zob. *First GDPR fine in Portugal Issues against hospital for three violations,* źródło: www.iapp.org/news/a /first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations, data dostępu: 09.01.2020.

następstwie naruszenia bezpieczeństwa danych, w wyniku którego narażono około 330 000 użytkowników[675]. Najwyższą niemiecką grzywnę do tej pory wydał również organ Badenii-Wirtembergii: 80 000 EUR na rzecz organizacji opieki zdrowotnej, która ujawniła wrażliwe dane osobowe[676].

Tymczasem Węgierski Krajowy Urząd ds. Ochrony Danych i Wolności Informacji (NAIH) wydał grzywnę w wysokości 30 000 000 HUF organizatorom wielokulturowego festiwalu muzyki i sztuki w Sziget w związku z ich procedurami bezpieczeństwa, które obejmowały kopiowanie dokumentów tożsamości oraz robienie zdjęć przy bramce wejściowej uczestnikom festiwalu. Kara stanowiła 2,3 procent przychodów netto firmy[677].

Podczas gdy Holandia nałożyła bardzo niewiele grzywien, jedna odbiła się dość szerokim echem. W listopadzie 2018 r. holenderski Urząd Ochrony Danych uderzył w firmę taksówkarską Uber z karą pieniężną w wysokości 600 000 EUR za „naruszenie holenderskiego przepisu o naruszeniu danych", nie informując organu regulacyjnego w ciągu 72 godzin od wykrycia, że doszło do nieuprawnionego naruszenia. Dotknęło to 57 milionów użytkowników Uber na całym świecie (z czego 174 000 było obywatelami holenderskimi). Wyszło również na jaw, że Uber zapłacił atakującym 100 000 USD za zniszczenie danych, w tym nazwiska, adresy e-mail oraz numery telefonów pobranych klientów[678].

Łotewski organ ochrony danych nie nałożył wielu kar w pierwszym roku stosowania RODO. Najwieksza publicznie ogłoszona grzywna wyniosła zaledwie 2000 EUR, czyli nawet mniej niż kary nałożone przed rokiem, gdy RODO zaczęło obowiązywać. Istnieje jednak kilka powodów: po pierwsze, regulator powiedział, że chce skonsultować się z organizacjami i pomóc im w przestrzeganiu przepisów, a nie ich ukarać (podejście przyjęte przez kilka innych organów UE ds. Danych, takich jak Belgia, Bułgaria, Chorwacja, Cypr i Grecji), a po drugie jest on przeciążony sprawami[679].

[675] Zob. T. Foltyn, *German chat site faces fine under GDPR after data breach,* źródło: www.welivesecurity.com/2018/11/27, data dostępu: 09.01.2020.
[676] Zob. *What we can learn from the Biggest GDPR Fines So Far,* źródło: www.complianceweek.com, data dostępu: 09.01.2020.
[677] Zob. R. Woolen, *GDPR Compliance – The Fines Have Begun,* źródło: www.infogoto.com/gdpr-compliance-the-fines-have-begun, data dostępu: 09.01.2020.
[678] Zob. *Uber fines E600, 000 in the Netherlands,* źródło: www.cloudprivacycheck.eu, data dostępu: 09.01.2020.
[679] Zob. R. Woolen, *GDPR Compliance…,* j.w.

Szwedzki organ ochrony danych nie nałożył jeszcze żadnych grzywien, ale organ regulacyjny przekazał informacje o toczących się dochodzeniach. Interesujące przypadki obejmują dostęp Google do danych o lokalizacji użytkowników za pomocą ta zwanej „Historii lokalizacji" i „Aktywności w Internecie i aplikacjach" oraz w jaki sposób dostawca usług płatniczych Klarna wykorzystuje dane osobowe klientów[680].

Według danych PrivacyAffairs, opublikowanych w 2020 r., w całej Unii Europejskiej dotychczasowa, łączna liczba kar wynikających z nieprzestrzegania przepisów RODO wynosi 347, a łączna wartość tych kar to 176 mln euro. Kraje charakteryzujące się największą liczbą naruszeń to Hiszpania (100), Węgry (32) i Rumunia (30). Do tej pory największą grzywną (50 mln euro) została ukarana firma Google, która utrudniała dostęp do informacji o zasadach przetwarzania danych na terytorium Francji. Dlatego Francja znajduje się na pierwszym miejscu listy państw, płacących najwyższe kary za naruszenia przepisów RODO. Dla porównania, do tej pory w Polsce zgłoszono tylko 9 naruszeń przepisów RODO, za które podmioty zostały ukarane grzywną o łącznej wartości 1,2 mln euro. Liderem pod względem przyznanej kary jest Morele, które pod koniec 2019 r. zostało ukarane grzywną w wysokości 645 tys. euro za wyciek danych ponad 2 mln swoich klientów[681].

Państwa, gdzie nałożono najwyższe kary, to:

Francja: 51 100 000 euro

Włochy: 39 452 000 euro

Niemcy: 26 492 925 euro

Austria: 18 070 100 euro

Szwecja: 7 085 430 euro

Hiszpania: 3 306 771 euro

Bułgaria: 3 238 850 euro

Niderlandy: 3 490 000 euro

Polska: 1 162 648 euro

[680] Tamże.
[681] Zob. *Coraz więcej kar za RODO w Unii Europejskiej*, https://ictmarketexperts.com/aktualnosci/coraz-wiecej-kar-za-rodo-w-unii-europejskiej/, data dostępu: 26.12.2020.

Norwegia 985 400 euro[682].

Nie ulega wątpliwości, iż organy nadzorcze z zasady są upoważnione do nakładania kar, w szczególności stosowania grzywny. Jednak jak można zauważyć, z czasem ich uprawnienia ograniczają się jedynie do przeprowadzenia postępowania wyjaśniającego, po którym muszą wnieść sprawę przed sąd. W przypadku stwierdzenia popełnienia przestępstwa same rzadko mają uprawnienia dochodzeniowe, raczej powiadamiają odpowiednie organy ścigania, które przejmują sprawę. W zasadzie jednak stosowanie sankcji zwłaszcza o charakterze karno-prawnym, jest traktowane jako ostateczność na gruncie praktyki stosowania prawa ochrony danych osobowych. Ma miejsce jedynie w odniesieniu do wyjątkowo poważnych lub uporczywych przypadków naruszenia prawa. Jeszcze przed wejściem RODO, znacznie chętniej organy nadzorcze odwoływał się do środków z zakresu tzw. *soft law* – wytykania błędów, perswazji, potępienia złych praktyk poprzez kampanie medialne[683].

Oceniając efektywność wdrażania standardów dot. bezpieczeństwa danych osobowych w państwach członkowskich RE i UE, warto zwrócić uwagę na jeszcze jeden aspekt. Albowiem początkowo zagadnienie to nie odgrywało ważnej roli w działalności legislacyjnej Unii Europejskiej. Dlatego również w odniesieniu do Rady Europy uzasadnionym jest pytanie, jak powinny układać się relacje między działaniami legislacyjnymi Unii z jednej strony, zwłaszcza we wspomnianej dziedzinie, a działaniami Rady Europy – z drugiej. Niewątpliwie, jest rzeczą ważną, że UE ma na uwadze dotychczasowe osiągnięcia RE, jak również działania przez Radę Europy planowane. Ale jest jeszcze jeden argument. Działalność legislacyjna UE jest wiążąca dla 28 państw europejskich, podczas gdy konwencje RE adresowane są do 47 państw członkowskich. Dlatego też potencjalny obszar geograficzny stosowania Konwencji nr 108 Rady Europy jest znacznie szerszy niż ten, na którym działają instrumenty prawne Unii Europejskiej. A zatem współpraca między Unią Europejską a Radą Europy jest nie tylko pożądana dla uniknięcia dublowania pracy i kolizji działań obu instytucji, ale jest także godna polecenia z uwagi na to, że Rada Europy dociera do wielu krajów spoza Unii Europejskiej.

[682] Zob. W. Żółcińska, *RODO – ranking kar*, https://www.computerworld.pl/news/RODO-ranking-kar,422090.html, data dostępu: 26.12.2020.
[683] Zob. M. Jagielski, *Prawo do ochrony danych …,* s. 189.

Kompleksowe badania, przeprowadzone we Francji, Niemczech, Wielkiej Brytanii, Irlandii, Rumunii, we Włoszech, Szwecji i Holandii wykazały, według stanu na maj 2018 r., że aczkolwiek RODO przyczyniło się do znaczącego ujednolicenia regulacji dotyczących ochrony danych osobowych, to jednak faktycznie występują tu bardzo zróżnicowane rozwiązania, gdyż uwzględnienie zróżnicowanych kultur prawnych w tych krajach prowadzi do różnic w praktyce implementacyjnej, interpretacji norm, a konsekwencji do różnic w procesie egzekwowania standardów europejskich ochrony danych osobowych[684].

Ważne znaczenie dla omawianych w tej pracy zagadnień ma wyrok Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 16 lipca 2020 r. ws. C-311/18, znanym jako *Schrems II*. Wyrok TSUE stanowi pokłosie tzw. sprawy Schremsa. Maximillian Schrems, to zamieszkały w Austrii użytkownik Facebook, który swoje konto społecznościowe założył w tym portalu w 2008 r. Od wszystkich osób mieszkających na terytorium Unii Europejskiej, które chcą używać Facebooka wymagane jest zawarcie w chwili rejestracji umowy ze spółką Facebook Ireland, będącą spółką zależną spółki dominującej Facebook Inc. z siedzibę w Stanach Zjednoczonych. Dane osobowe użytkowników Facebooka mieszkających na terytorium Unii są, w całości lub częściowo, przekazywane na serwery spółki Facebook Inc., położone na terytorium Stanów Zjednoczonych, gdzie dane te są przetwarzane[685].

W wyroku *Schrems II* TSUE nie tylko usunął mechanizm legalizujący transfer danych osobowych do USA, czyli Tarczę Prywatności, lecz także zwrócił uwagę, że wykorzystywanie innych mechanizmów legalizujących transfer, np. Standardowych Klauzul Umownych, wymaga zagwarantowania, że dane osobowe przekazywane poza obszar Europejskiego Obszaru Gospodarczego będą chronione co najmniej w równym stopniu jak na terenie Europejskiego Obszaru Gospodarczego (EOG). Uwagi TSUE wywołały spore zaniepokojenie wśród podmiotów dokonujących transferu danych z uwagi na fakt, że wyrok nie precyzuje, z jakich dodatkowych środków można korzystać, aby transfer oparty na mechanizmach przewidzianych w RODO mógł zostać uznany za bezpieczny. Europejska Rada Ochrony Danych (EROD) wydała rekomendacje, w których został przedstawiony modelowy sposób dokonywania

[684] Zob. A. Sears, F. Dehesne, I. Georgieva, T. Tani, S. van der Hof, *EU personal data protection in policy and practice*, T.M.C. Asser Press, The Hague 2019, s. 238.
[685] Zob. K. Raczek, *Przetwarzanie danych w USA jest niezgodne z RODO*, https://itwiz.pl/tsue-przetwarzanie-danych-usa-jest-niezgodne-rodo/, data dostępu: 26.12.2020.

transferu danych oraz wskazano przykładowe środki, które mogą wspomóc przewidziane w RODO narzędzia legalizujące przesyłanie danych osobowych poza EOG, aby zapewnić odpowiedni poziom ochrony danych w kraju trzecim. EROD przypomniała, że do transferu danych nie jest konieczne, aby poziom ochrony danych w kraju trzecim był identyczny jak w EOG, lecz aby był istotnie równoważny poziomowi ochrony w EOG. W przypadku, gdy prawo lub praktyka działalności w kraju trzecim powoduje, że dane po transferze byłyby chronione w mniejszym stopniu, niż przewidują to mechanizmy legalizujące transfer („odpowiednie zabezpieczenia" wskazane w art. 46 ust. 2 oraz 3 RODO), potrzebne jest skorzystanie z dodatkowych środków, niwelujących lukę w ochronie danych w kraju trzecim. Wśród okoliczności, które mogą stanowić o niższym poziomie ochrony w kraju trzecim, EROD wymienia m.in. możliwość dostępu do danych przez organy publiczne czy niejasność lub brak upublicznienia regulacji dotyczących przetwarzania danych osobowych[686].

W rekomendacjach tych została określona mapa drogowa, która ma obrazować właściwą ścieżkę postępowania w przypadku transferu danych do państw trzecich. Podmiot eksportujący dane powinien dokładnie zidentyfikować wszystkie transfery, a także zweryfikować zakres transferowanych danych pod kątem zasady minimalizacji. Następnym krokiem jest wybór odpowiedniego mechanizmu legalizującego transfer, jednego z określonych w rozdziale V RODO. Trzecim krokiem jest ocena, czy wybrany do konkretnego transferu mechanizm legalizujący będzie mógł być w pełni przestrzegany. Taka ocena uzależniona jest m.in. od tego, czy przepisy kraju trzeciego:

- uniemożliwiają realizację praw podmiotów danych,
- nie przyznają organom publicznym zbyt szerokiego i dowolnego dostępu do danych (punktem odniesienia może być art. 47 oraz 52 Karty Praw Podstawowych),
- nie stoją na przeszkodzie zabezpieczeniom przewidzianym w wybranym mechanizmie legalizującym transfer.

Istotnym czynnikiem przy takiej ocenie jest okoliczność, czy dany kraj:

[686] Zob. M. Madecki, *Transfer danych osobowych – rekomendacje Europejskiej Rady Ochrony Danych po wyroku Schrems II*, https://rodoradar.pl/transfer-danych-osobowych-rekomendacje-europejskiej-rady-ochrony-danych-po-wyroku-schrems-ii/, data dostępu: 28.12.2020.

- posiada niezależne organy właściwe ds. ochrony danych,
- uchwalił przepisy dotyczące ochrony danych oraz
- czy przystąpił do międzynarodowych instrumentów czy porozumień związanych z danymi osobowymi (przykładem może być Konwencja nr 108 Rady Europy).

Jeśli w wyniku oceny eksporter dojdzie do wniosku, że w konkretnym kraju trzecim nie będzie zapewniony równoważny poziom ochrony jak w EOG, zgodnie z wybranym mechanizmem legalizującym transfer, w celu kontynuowania transferu konieczne będzie zapewnienie środków uzupełniających[687].

Do momentu wydania wyroku *Shrems II* i stwierdzenia przez Trybunał Sprawiedliwości Unii Europejskiej nieważności decyzji wykonawczej Komisji Europejskiej (UE) 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności, krajem, co do którego istniała decyzja Komisji Europejskiej potwierdzająca odpowiedni stopień ochrony, były także USA. Oznacza to w praktyce, że obecnie transfer danych do USA może odbywać się nadal, ale podstawą transferu nie może być już Tarcza Prywatności. W razie braku decyzji Komisji Europejskiej, a w tym także w związku z unieważnieniem Tarczy Prywatności, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią one odpowiednie zabezpieczenia i skuteczne środki ochrony prawnej. Owo odpowiednie zabezpieczenie można osiągnąć przede wszystkim przy pomocy:

1. prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,
2. wiążących reguł korporacyjnych (są stosowane relatywnie rzadko i głównie w dużych grupach międzynarodowych przedsiębiorstw),
3. standardowych klauzul ochrony danych (jest to najbardziej popularne zabezpieczenie transferu, jednak UWAGA – nie istnieją klauzule zakładające „podpowierzenie" danych osobowych),
4. zatwierdzonego kodeksu postępowania,
5. zatwierdzonego mechanizmu certyfikacji[688].

[687] Tamże.

Stosowanie powyższych zabezpieczeń nie wymaga dodatkowego zezwolenia organu nadzorczego. Wymaga go natomiast stosowanie następujących rodzajów zabezpieczeń:

1. klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej,

2. uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą[689].

Wyrok TSUE *Shrems II* wywołał istotne konsekwencje praktyczne w obszarze ochrony danych osobowych.

Facebook twierdzi, że może zostać zmuszony do zawieszenia swoich operacji w UE po tym, jak irlandzki organ nadzorujący prywatność dał gigantowi trzy tygodnie na wstrzymanie wszystkich transferów danych użytkowników do Stanów Zjednoczonych. Firma wyjaśnia, że "nie grozi wycofaniem się z Europy", ale wniosła sprawę do sądu, ponieważ uważa, że znalazła się niesłusznie na celowniku, za powszechną praktykę wielu amerykańskich organizacji działających w regionie. W sierpniu 2020 r. irlandzka Komisja Ochrony Danych (DPC) wysłała Facebookowi wstępny nakaz zaprzestania przesyłania danych europejskich użytkowników do Stanów Zjednoczonych, po tym jak Europejski Trybunał Sprawiedliwości orzekł, że amerykańskie przepisy dotyczące prywatności są nieadekwatne. Jeśli Facebook nie dostosuje się do nakazu, może zostać m.in. ukarany grzywną w wysokości do czterech procent rocznego obrotu, co stanowi około 2,8 miliarda dolarów (dane za 2019 rok). Gigant społecznościowy twierdzi jednak, że decyzja DPC uniemożliwi docieranie z usługami do 410 milionów ludzi na terenie UE, którzy stale korzystają z Facebooka i Instagrama. Ponadto firma pozwała DPC, twierdząc, że została namierzona w morzu ponad 5000 firm, które polegają na standardowych klauzulach umownych (SCC) i Tarczy Prywatności w zakresie obsługi

[688] Zob. K. Rączkowiak, *Przekazywanie danych osobowych do państw trzecich*, https://grantthornton.pl/publikacja/przekazywanie-danych-osobowych-do-panstw-trzecich/, data dostępu: 26.12.2020.
[689] Tamże.

transferów danych między UE a USA. Facebook uważa, że działania DPC są zbyt pospieszne i wpływ takiego postępowania na gospodarkę europejską jest bardzo dyskusyjny, ponieważ klauzule SCC są również wykorzystywane przez innych gigantów technologicznych, a także banki, linie lotnicze i wiele małych firm. Firma zaapelowała do organów regulacyjnych, aby zastanowili się nad bardziej pragmatycznym podejściem, zanim zostanie znalezione trwałe, długoterminowe rozwiązanie. DPC wydało wstępny nakaz, aby zapobiec przechowywaniu lub przetwarzaniu danych mieszkańców Europy w Stanach Zjednoczonych, gdzie mogą one zostać objęte programami masowego nadzoru. Ocenia się, że jest to działanie na pokaz, po niedawnych oskarżeniach, że nie podejmowane są wystarczające kroki w celu egzekwowania RODO u gigantów technologicznych[690].

Nowe wyzwania dla ochrony danych osobowych przyniosła pandemia COVID-19. Przeprowadzone w skali międzynarodowej badania wykazały, że w związku z tą pandemią wzrosła gotowość ludzi do udostępniania danych osobowych wszędzie tam, gdzie może to przyczynić się do ograniczenia skutków pandemii[691].

W świetle przytoczonych informacji i ocen, że system ochrony danych osobowych w Europie, zainicjowany przez Radę Europy (zwłaszcza Konwencja nr 108), a rozwijany przez Unię Europejską (zwłaszcza RODO) okazał się skutecznym sposobem na zapewnienie bezpieczeństwa danych osobowych. Chodzi tu przy tym zarówno o standardy o charakterze prawnie wiążącym, jak i standardy o charakterze tzw. miękkiego prawa. To zróżnicowanie standardów umożliwiło elastyczne reagowanie na zagrożenia w zakresie ochrony danych osobowych, jakie przynosi rozwój cywilizacyjny. Zarazem należy pamiętać, że nie oznacza to zakończenie procesu ochrony bezpieczeństwa danych osobowych. Stale pojawiają się bowiem nowe typy zagrożeń, które wymagają odpowiedniej reakcji regulacyjnej. Poważnym wyzwaniem staje się w szczególności zapewnienie należytej ochrony w odniesieniu do przepływu informacji o charakterze tran granicznym, z jakim mamy do czynienia w odniesieniu do takich gigantów informacyjnych, jak Facebook, Istagram czy Google. Istotnym

[690] Zob. P. Czajkowski, *Facebook wyrzucony z UE?To możliwe ze względu na RODO i zakaz przesyłania danych do USA*, https://ithardware.pl/aktualnosci/facebook_wyrzucony_z_ue_to_mozliwe_ze_wzgledu_na_rodo_i_zakaz_przesylania_danych_do_usa-13425.html, data dostępu: 26.12.2020.

[691] Zob. C. Degeling, G. Chen, G.L. Gilbert, W. Brookes, T. Thai, A. Wilson, J. Johnson, *Changes in public preferences for technologically enhanced surveillance following the COVID-19 pandemic: a discrete choice experiment*, "British Medical Journal" 2020, nr 11, s. e041592.

wsparciem dla działań ochronnych państw członkowskich UE staje się tu orzecznictwo sądowe, zwłaszcza Trybunału Sprawiedliwości Unii Europejskiej.

Zakończenie

Analiza podjęta w dysertacji dowiodła, że zasadniczą rolę w zapewnieniu bezpieczeństwa danych osobowych odgrywają standardy stworzone w systemach aksjologicznych Rady Europy oraz Unii Europejskiej. Wiele z państw członkowskich skorzystało z tych „wzorców postępowania", czego efektem stały się zmiany legislacyjne poprzedzone ratyfikacją określonych dokumentów, i implementacją przepisów w nich zawartych.

Zarówno Rada Europy jak i Unia Europejska przywiązały szczególną wagę do prawa prywatności, na które w zasadniczy sposób zaczęła wpływać dynamika zmian związana z postępem technologicznym, zwłaszcza w sferze komunikowania się.

Bezpieczeństwo danych osobowych stało się kluczowym celem obydwu organizacji. Pomimo różnić w szerokości oddziaływania (Rada Europy – 47 państw, UE – 27 państw), podjęto kroki mające na celu utworzenie formalnych podstaw dla ochrony danych osobowych.

Ściśle z tym powiązana była **hipoteza 1**, zgodnie z którą „Pod wpływem standardów Rady Europy i Unii Europejskiej dokonano podniesienia bezpieczeństwa danych osobowych do rangi konstytucyjnie chronionego prawa. Oddziaływanie tych standardów zaowocowało nie tylko stworzeniem odpowiedniego ustawodawstwa, ale i podjęciem prac legislacyjnych w celu jego skutecznego dostosowania do norm międzynarodowych".

Hipoteza ta została zweryfikowana pozytywie. Oceniając bowiem powstałe standardy, a także przyjęte na ich podstawie rozstrzygnięcia z punktu widzenia interesów osób, których dane dotyczą, należy cenić je jako zasadniczo pozytywne. Wprawdzie standardy Rady Europy nie zawsze gwarantują bezpieczeństwo danych na takim samym poziomie, jaki obowiązuje wewnątrz Unii, a przewidziane w ich ramach mechanizmy ochronne bywają trudne do wyegzekwowania, to jednak sam fakt ich wprowadzenia oznacza zazwyczaj podniesienie poziomu bezpieczeństwa w stosunku do stanu poprzedniego. Można także zaobserwować, że już samo istnienie europejskiej procedury uznawania odpowiedniości stopnia ochrony wpływa na przebieg dyskusji na temat standardów tej ochrony np. w państwach pozaeuropejskich, przystąpienie zaś do

negocjacji skutkuje zmianami w ustawodawstwie, które pozostają w mocy nawet wówczas, gdy ostatecznie do dojdzie do porozumienia. Nie ulega wątpliwości, że to RE torowała drogę dla uświadomienia przez europejską opinię publiczną znaczenia ochrony danych osobowych i szukania sposobów dla zapewnienia ich bezpieczeństwa, a działania UE są rozwinięciem tych działań i nadaniem im bardziej skutecznego charakteru, poprzez system sankcji, który wiążę się z naruszeniem bezpieczeństwa danych osobowych.

Hipoteza 2 brzmiała: **„**Nacisk, jaki na państwa członkowskie od wielu lat kładą Rada Europy i Unia Europejska w kontekście bezpieczeństwa danych osobowych, sprawił, iż w każdym z tych państw zagadnienie to stało się przedmiotem regulacji prawnych. Potwierdza to monitoring prowadzony zarówno w systemie RE, jak i UE, który daje możliwość uchwycenia stopnia realizacji standardów międzynarodowych w tym zakresie. Doświadczenia zgromadzone w państwach członkowskich RE i UE wskazują jednak, że istnieje potrzeba identyfikowania coraz to nowych zagrożeń powstających w systemie ochrony danych osobowych. Mogą one skłaniać do modyfikacji standardów międzynarodowych, a także do odpowiedniego dostosowania do nich ustawodawstwa krajowego".

Hipoteza ta została zweryfikowana pozytywnie. Początkowy nacisk widoczny był ze strony Rady Europy, która przyjęła Konwencję nr 108, stanowiącą akt wiążący państwa będące jej stronami. W Unii Europejskiej natomiast do momentu wprowadzenia nowych przepisów Dyrektywa 95/46/CE Unii Europejskiej nie pełniła wprawdzie roli aktu bezpośredniego i natychmiast wiążącego państwa Unii, stanowiła jednak instrument ujednolicenia przepisów krajowych. Należy przypomnieć bowiem, iż w art. 189 ust. 3 Traktatu Rzymskiego zawarto obowiązek przeniesienia postanowień dyrektyw na grunt prawa krajowego, pozostawiając państwom jedynie swobodę wyboru najwłaściwszej formy prawnej (np. rangi przepisu). W tym celu dyrektywy zawierały postanowienia określające czas pozostawiony państwom członkowskim na dostosowanie swego ustawodawstwa wewnętrznego. Co więcej uznano, iż nieprzestrzeganie powyższego obowiązku może powodować konieczność wypłacenia odszkodowania podmiotom, które poniosły szkodę w wyniku niewykonania obowiązku wprowadzenia przepisów dyrektywy do państwa wewnętrznego w określonym czasie.

Ze względu więc na zasięg i moc wiążącą postanowień Konwencji i Dyrektywy były one najważniejszymi aktami międzynarodowymi dotyczącymi ochrony danych osobowych.

Doświadczenia zgromadzone w państwach członkowskich, niejako wymusiły potrzebę zmian. Rada Europy uznała za niezbędną modernizację swojego przełomowego instrumentu jakim jest Konwencja nr 108 wprowadzając Konwencję nr 108+. Głównym celem tego działania było zbliżenie poziomu ochrony danych osobowych do przepisów europejskich w tej dziedzinie oraz zmniejszenie barier między innymi państwami, zapewniając odpowiedni poziom ochrony danych osobowych na świecie. W Unii Europejskiej do momentu wprowadzenia nowych przepisów świadomość dotycząca ochrony danych osobowych była bardzo ograniczona. Dopiero RODO w sposób najbardziej daleko idący określiło zasady ochrony danych osobowych w dokumencie bezpośrednio wiążącym, a przy tym zaoferowało sankcje o istotnym znaczeniu dla realizacji postanowień RODO. Powstał w wyniku tego komplementarny system, uwzględniający nieco słabsze mechanizmy ochronne w systemie RE, a silniejsze w systemie UE. Należy się jednak liczyć, że RODO – w zakresie przyjętych mechanizmów gwarancyjnych zastosowanych w UE – będzie coraz silnie oddziaływało na sytuację w państwach

W Polsce dało się zaobserwować bardzo silną, przepełnioną paniką i skrajnością reakcję na RODO, która nakazywała zmieniać całą prowadzoną do tej pory działalność. Należy jednak zaznaczyć, że taką reakcję można było zaobserwować tylko u osób, które zdały sobie sprawę z istnienia Rozporządzenia. Znaczna większość społeczeństwa nie miała pojęcia o tym, mimo że RODO miało wprowadzić nie tylko wymagania dotyczące ochrony danych osobowych, ale również kary za naruszenia przepisów. Stopniowo jednak narastała gotowość w szerokiej skali do realizacji postanowień RODO, gdy wiedza o jego postanowieniach objęło całe społeczeństwo. Z podobnymi procesami mieliśmy do czynienia w całej UE.

Hipoteza 3 brzmiała: „Współcześnie zasadniczy krok w kwestii bezpieczeństwa danych osobowych dokonała Unia Europejska. Tworząc RODO założyła, iż głównym celem będzie zapewnienie spójnego stopnia ochrony danych osób fizycznych w Unii oraz zapobiegnięcie rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym. Standardy te mają także gwarantować podmiotom

gospodarczym pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten dam poziom prawnie egzekwowalnych praw i obowiązków. Wdrażanie rozporządzenia RODO w państwach członkowskich UE przyniosło jednak szereg obserwacji i doświadczeń, które powinny zachęcać do ponownego przemyślenia niektórych zawartych w nim rozwiązań. Chodzi o to, by system ten był skuteczny, a jednocześnie nie rodził nadmiernej uciążliwości po stronie podmiotów, do których jest adresowany".

Hipoteza ta została zweryfikowana pozytywnie. RODO ujednoliciło bowiem europejskie prawo ochrony danych osobowych, obowiązujące w UE, ale także wymusiło na państwach spoza Unii Europejskiej, które prowadzą działalności na jej terenie, wprowadzenie szeregu realnych zmian mających na celu bezpieczeństwo danych osobowych. Za cel nadrzędny uznany został obowiązek chronienia danych osób fizycznych. Tym samym sposobem nawet giganci zza oceanu musieli dostosować się do przepisów Rozporządzenia.

Warto wskazać, iż celem który przyświecał Unii Europejskiej, poza ochroną praw i wolności osób, które dane są przetwarzane, było ujednolicenie przepisów obowiązujących na obszarze Wspólnoty. W UE panująca przed wejściem w życie RODO dowolność w regulowaniu tej kwestii doprowadziła do wielu naruszeń. W tym zakresie udało się osiągnąć zasadniczy postęp. Istotne jest przy tym to, żę RODO obowiązuje wszystkie podmioty, które przetwarzają dane na terenie UE, nawet jeśli siedziba tych podmiotów jest poza Wspólnotą.

Generalnie można więc stwierdzić, że RODO wprowadziło kluczowe zmiany, które były wymagane ze względu na gwałtowny rozwój technologiczny, za którym do tej pory nie nadążały działania ustawodawców europejskich. Zarazem jednak należy pamiętać, że kolejne fazy rozwoju cywilizacyjnego przynoszą nowe wyzwania. Zarówno więc Rada Europy, jak i Unia Europejska powinny stawiać sobie za cel, by za tymi zmianami podążać i oferować adekwatne standardy europejskie, chroniące w sposób optymalny bezpieczeństwo danych osobowych.

Bibliografia

Akty normatywne

- Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, źródło: www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf, data dostępu: 26.07.2019.
- Act 58/2019 of 8 August (the „Data Protection Act"), Date in Force: 9 August 2019.
- Act CXII of 2011 on the Right of Informational Self – Determination and on Freedom od Information (the "Data Protection Act"), Date in force: 26 April 2019.
- Act XLVII of 1997 on the processing and protection of personal data concerning health (the "Health Data Processing Act"), Date in force: 26 April 2019.
- Act on Protection of privacy in Working Life (759/2004) (the "Workplace Privacy Act"), Date in force: 1 April 2019.
- Act amending certain legislations due the adoption of the act on processing of personal data (the "Amending Act") , Date in force: 24 April 2019.
- Act on processing of personal data (the "Data Protection Act"), Date in force: 24 April 2019.
- Act No. 90/2018 on Data Protection and the Processing of Personal Data (in Icelangic Log nr. 90/2018 um personuvernd og vinnslu personuupplysinga).
- Act. No. 18/2018 Coll., on the Protection of Personal Data and Changing and Amending of Other Acta (the „Data Protection Act"), Date in force: 25 May 2018.
- Act on the Implementation of the General Data Protection Regulation (in Cratian: Zakon o provedbi Opce uredbe o zasiti podataka) (the "Implementation Act"), Date in force: 25 May 2018.
- African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014.
- Bundesdatenschultzgesetz, Neufassung 2018 ("BDSG"), Date in force: 25 May 2018.

- Convention for the Protection of Human Rights and Dignity of The Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4. IV.1997, ETS – No. 164.
- Data Protection Act 1 § 2 on the Amendment of Material Laws (Federal Law Gazette I Nr. 32/2018 & Nr. 37/2018).
- Data Protection Act, CAP 586, Date in force: 28 May 2018.
- Data Protection Act, Federal Law Fazette I Nr. 165/1999 (the "Data Protection Act") amended to reflect GDPR requirements by two Data Protection Amendmend Acts in 2018.
- Databeskyttelsesloven (the „Data Protection Act"), Date in Force: 25 May 2018.
- Data Sharing and Governance Act 2019, Date in force: part commenced 18 April 2019.
- Datenschultzgesetz (the "Data Protection Act"), Date in force: 1 January 2019.
- Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers Deputies).
- Declaration of the Council of Europe's First Summit (Vienna, 9 October 1993), źródło: www.cvce.eu/en/obj/declaration, data dostępu: 14.09.2018.
- Decyzja Ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.Urz.UE L 350/60, 30.12.2008).
- Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the Protection of privacy in the electronic communication sector, Official Journal L 201, 31/07/2002 P. 0037-0047.
- Directive No. 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with regard to the processing of personal data and on the Free Movents of such data, October 24, 1995.
- 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, OJ L 119, 4.5.2016, p. 89-131.

- Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz.Urz.UE L 337/11 z 18.12.2009, s. 11-36).
- Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnieniem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.Urz. UE L 105/54 z 13.04.2006).
- 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 178/1 z 17.7.2000).
- Dyrektywa 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz.Urz. UE L 337/11 z 18.12.2009).
- 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.U. L 281 z 23.11.1995, s. 31).

- Finnish Data Protection Act (1050/2018) (the “Data Protection Act”), Date in force: 1 January 2019.
- French Data Protection Act (as amendment by the Law No. 2018-493 of 20 June 2018 on the protection of personal data and by the Decree No. 2018-687 of 1 August 2018), (The “FDPA”, Date in force: 21 June 2018.
- Karta Praw Podstawowych Unii Europejskiej (Dz.Urz. UE C 303 z 14.12.2007).
- Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., (Dz.U. 1993 nr 61 poz. 284).
- 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. 2003 nr 3 poz. 25).
- Konwencja Wykonawcza do Układu z Schengen z dnia 14 czerwca 985 roku między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, Dz.Urz. nr L 239 22/09/2000.
- Law 4624/2019 („Data Protection Law“), which entered into force on 29 August 2019.
- Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (the “Law of 30 July 2018”), Date in force: 5 September 2018.
- Law of 5 September 2018 establishing the information security committee and modifying various laws regarding the implementation of 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 procession of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Date in force: 10 September 2018.
- Law of 1 August 2018 organising the National Commission on Data Protection and implementing the GDPR (the “Data Protection Law”), Date in force: 20 August 2018.
- Law of 3 December 2017 establishing in DPA, Date in force: 25 May 2018.
- Law of 21 March 2018 amending the existing Act of 21 March 2007 on camera surveillance, Date in force: 25 May 2018.

- Law providing for the protection of natural persons with regard to the processing of personal data and for free movement of such data (Law 125 (I) of 2018 (the "Data Protection Act"), Date in force: 31 July 2018.
- Law on Amendment and Supplement to the Personal Data Protection Act, Date in force: 29 February 2019.
- Law No. 190 of 18 July 2018 regarding the Measures for the Application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 re the Protection of Natural Persons With regard to the Processing Personal Data and on the Free Movements of Such Data, and Repeal of the Directive 95/46/EC (General Data Protection Regulation), (the „Data Protection Act"), Date in force:
- Law No. 129 of 15 June 2018 re the Amendment and Supplementation of Law No. 102 of 2005 regarding the Organisation and Functioning of the National Supervisory Authority for Personal Data Processing and for repealing Law No. 677/2001 regarding the Protection of the Individuals re the Processing of Personal Data and Free Movement of Such Data, Date in force: 24 June 2018.
- Legislative Decree No. 101/2018 setting out rules adapting Italia law to the GOPR, chich amendment Legislative Decree No. 196/2003 setting out Italian privacy code (the "Italian Privacy Code", Date in force: 19 September 2018.
- Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. 1977 nr 38 poz. 167).
- Order No. 2018 – 1125 of 12 December 2018 reorganising the FDPA and various provisions concerning the protection of personal data, Date in force: 1 June 2019.
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights ("Ley Organica 3/2018, de 5 de diciembre de Protecction de Datos Personales y garantia de los derechos digitales"), (the "Data Protection Act"), Date in force: 7 December 2018.
- Personal Data Protection Act (the „PDPA"), Date in force: 15 January 2019.
- Personal Data Protection Act Implementation Act, Date in force: 15 March 2019.
- Personal Data Processing Law ("PDPL"), Date in force: 5 July 2018.

- Powszechna Deklaracja Praw Człowieka przyjęta 10 grudnia 1948 r. źródło: libr.sejm.gov.pl/tek01/txt/ONZ/1948.html, data dostępu: 19.07.2018.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych (Dz.U. nr 80, poz. 521).
- 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, PE/31/2018/REV/1, Doc. 32018R1725.
- 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 osobowych).
- Rozporządzenie nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.
- Statut Rady Europy, przyjęty w Londynie w dniu 5 maja 1949 r. (Dz.U. z 1994 r., Nr 118, poz. 565).
- The General Assembly Resolution 34/169, Code of Conduct for Law Enforcement Officials, 17 December 1979, A/RES/34/169.
- The General Assembly Resolution 45/95, Guidelines for the Regulation of computerized personal data files, adopted on 14 December 1990, A/RES/45/95.
- The Law on Legal Protection of Personal Data ("Data Protection Law"), Date in force: 16 July 2018.
- The Norwegian Data Protection Act, Date in force: 20 July 2018.

- The Swedish Data Protection Act (2018;218), (Swe. Lag(2018;218) med kompletterande bestammesler till EU: s dataskyddsforording, (the “Data Protection Act”), Date in force: 25 May 2018.
- The Universal Declaration on the Human Genome and Human Rights was adopted by the General Conference of UNESCO at its 29th session on 11 November 1997.
- Traktat o funkcjonowaniu Unii Europejskiej, Dz. Urz. UE 2016 C 202, s. 1.
- Traktat z Nicei zmieniający Traktat o Unii Europejskiej. Traktat ustanawiający Wspólnotę Europejską oraz niektóre związane z nim akty prawne, Nicea, 26.02.2001.
- Traktat o Unii Europejskiej podpisany 7 lutego 1992 r. w Maastricht, wszedł w życie 1 listopada 1993 r. (Dz.U. z 2004 r. Nr 90, poz. 864/30.
- Uitvoeringswet Algemene Veordening Gegevenscherming (General Data Protection Regulation Implementation Act), Date in force; 25 May 2018.
- UK Data Protection Act 2018, Date in force: 25 May 2018.
- Układ pomiędzy Rządami Państw Unii Gospodarczej Beneluksu oraz Republiki Federalnej Niemiec i Republiki Francuskiej dotyczący stopniowego znoszenia kontroli na wspólnych granicach zawarty w Schengen 14 czerwca 1985 r. (Opublikowany w języku polskim przez Departament ds. Migracji i Uchodźstwa MSWiA, seria: „Dokumenty”, zeszyt 2, Warszawa 1998.
- 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 roku 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 poz. 730).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 133, poz. 883 z późn. zm).
- Videosurveillance Monitoring Act (the “CCTV Act”), Date in force: 25 May 2018.

Dokumenty

- *2018 Annual Report – a new era in data protection,* źródło: www.edps.europa.eu/data-protection/our/publications/annual-reports/2018, data dostępu: 09.01.2020.
- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory Authorities and transborder data flows, ETS nr 181.
- *Annual report 2012,* European Data Protection Supervisor, Publications Office, Luxemburg 2013.
- Case Law of the European Court of Human Rights Concerning the Protection of Personal Data, Council of Europe, Strasbourg, 15 November 2017, T-PD(2017)23.
- Committee of Ministers The Council of Europe Resolution 73/22 on the Protection of the privacy of Individuals vis-a-vis electronic data banks in the private sektor, adopted by the Committee of Ministers on 26 September 1973 at the 224th Meeting of the Ministers' Deputies.
- Committee of Ministers of The Council of Europe Resolution 74/29, On the Protection of the Privacy of Individuals Vis-A Electronic Data Banks in the Public Sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.
- Communication from the Commission to the European Parliament and the Council-Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation as 25 May 2018, COM/2018/043 final, Doc. 52018DC0043.
- Council of Europe Committee of Ministers Declaration on Compliance with Commitments (Adopted by the Committee of Ministers on 10 November 1994 at its 95th Session).
- Decyzja Komisji z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich,

na mocy dyrektywy 95/46/WE (notyfikowana jako dokument nr C(2001)1539), Tekst mający znaczenie dla EOG, Doc. 32001DO497.

- Decyzja Rady 2009/936/WSiSW z 30 listopada 2009. r. w sprawie przyjęcia przepisów wykonawczych dotyczących plików roboczych do celów analizy stosowanych przez Europol (Dz.Urz.UE L 325 z 11.12.2009, s. 14.
- Decyzja ramowa Rady 2008/9777/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.Urz. UE L 350 z 30.12.2008 r., s. 60).
- DLA Piper GOPR Data Breach Survey, A report by DLA Piper's cybersecurity team, February 2019, źródło: www.dlapiper.com/-/media/files/data dostępu: 30.12.2019.
- European Commission Communication from the Commission to the European Parliament, the Council, The Economic and Social Committee and The Committee of the Regions", *A comprehensive approach on personal data protection in the European Union,* Brussels, 4.11.2010, COM(2010)609 final.
- Explanatory Memorandum to Recommendation No. R (2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes, Adopted by the Committee of Ministers on 18 September 2002 at the 808 th meeting of the Minister's Deputies.
- Explanatory Report to the Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine, Convention on Human Rights and Biomedicine, ETS- No. 164, źródło: www.rm.coe.int/16800cde5, data dostępu: 13.09.2018.
- Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS nr 181.
- Guidelines The European Data Protection Supervisor, *Assessing the proportionality of measures limit the fundamental rights to privacy and to the protection of personal data,* 19 December 2019, źródło: www.eds.europa.eu, data dostępu: 09.01.2020.

- Komunikat Komisji do Parlamentu Europejskiego i Rady: Wymiana i ochrona danych osobowych w zglobalizowanym świecie, COM/2017/07/ final.
- Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów , Inteligentne sieci energetyczne: od innowacji do wdrożenia, SEK(2011) 463, Komisja Europejska, Bruksela, dnia 12.4.2011, KOM (2011) 202 wersja ostateczna.
- Ministers' Deputies Decisions, CM/Del/Dec(2006)962, Decisions adopted 2.5.2006.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23.9.1980.
- Opinia Grupy Roboczej z dnia 13 lipca 2011 r. 01197/11/EN,WP187.
- Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych, COM(2005) 475 wersja ostateczna, źródło: www.eur-lex.europa.eu/legal-content/ENTXT/?uri=CELEX:52006XX0225(01), data dostępu: 23.04.2019.
- Opinia Europejskiego Inspektora Ochrony Danych dotycząca komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów – "Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", (2011/C 181/01), źródło: www.eds.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_pl.pdf, data dostępu: 20.05.2019.
- Protocol amending the Convention for the Protection of Individuals with regard to Automatic Pressing of Personal Data, Strasbourg, 10/10/2018 – Treaty open for signature by the Contracting States to Treaty ETS 108.
- Rapport explicatif concernant la Convention pour la protectiondes personnes a l'egard du traitement automatise des donnees a caractere personel, Strasbourg 1981.
- Reflections Paper on Harnessing Globalisation, COM(2017)240.
- Resolution 1986 (2014), Improving user protection and security in cyberspace, Parliamentary Assembly debate on 9 April 2014 (14th Sitting(, Doc. 13451).

- Resolution 1843 (2011), The protection of privacy and personal data on the internet and online media, Parliamentary Assembly debate on 7 October 2011 (36th Sitting), Doc. 12695.
- Resolution calling for the Organisation of an intergovernmental Conference with a view to developing a binding International instrument on privacy and the protection of personal data, International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 27-29.10.2010.
- Resolution No. 3 on data protection and privacy in the third millennium, 30th Council of Europe Conference of Ministers of Justice, Istanbul, Turkey, 24-26 November 2010), MJU-30(2010) RESOL. 3E.
- Resolution AP (95) 3 on a Charter on the Vocational Assessment of People with Disabilities, Adopted by the Committee of Ministers on 12 October 1995 at the 545th meeting of the Minister's Deputies.
- Resolution (78)29 on Harmonisation of Legislations of Member States Relating to Removal, Grafting and Transplantation of Human Substances, Adopted by the Committee of Ministers on 11 May 1978 at the 287th meeting of the Ministers' Deputies.
- Resolution (74)29 on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Public Sector ,Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.
- Resolution (73)22 on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in The Private Sector, Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Minister's Deputies.
- Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.
- Recommendation No. R (95) 4 of the Committee of Ministers to Member States on the Protection of Personal Data in the Area of Telecommunication Service with Particular Reference to Telephone Service, Adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the Minister's Deputies.

- Recommendation No. R (81)1 of the Committee of Ministers to Member States on regulations for automated medical data banks (Adopted by the Committee of Ministers on 23 January 1981, at the 328th meeting of the Minister's Deputies).
- Recommendation of the Council concerning guidelines governing the Protection of privacy and transborder flows of personal data, OECD 23 September 1980.
- Recommendation No. R (97)5 on the Protection of Medical , 13 February 1997.
- Recommendation No. R (97)18 on the Protection of Personal Data Collected and Processed for Statistical Purposes, 30 September 1997.
- Recommendation No. R (99) 5 for the Protection of Privacy on the Internet, 23 February 1999.
- Recommendation No. R (2002)9 on the Protection of Personal Data Collected and Processed for Insurance Purposes, 18 September 2002.
- Recommendation CM/Rec (2010)13 of the Committee of Ministers to member states on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, 23 November 2010.
- Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines.
- Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services.
- Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Minister's Deputies.
- Recommendation No. R (85)20 of the Committee of Ministers to Member States on the Protection of Personal Data Used for the Purposes of Direct Marketing, Adopted by the Committee of Ministers on 25 October 1985 at the 389th meeting of the Minister's Deputies.
- Recommendation No. R (84)10 of the Committee of Ministers to Member States on the Criminal Record and Rehabilitation of Convicted Persons, Adopted by the Committee of Ministers on 21 June 1984 at the 374th meeting of the Minister's Deputies.

- Report containing guiding principles for the Protection of Individuals with regard to collection and processing of data by means of video surveillance, as adopted by the European Committee on Legal Co-operation (CDCJ) at its 78th meeting (20-23 May 2003), źródło: www.rm.coe.int/1680684b, data dostępu: 26.07.2019.
- *Sprawozdanie na temat praw podstawowych 2017. Opinie FRA,* European Union Agency, źródło: www.fra.europa.eu/sites/.../fra-2017-fundamental-rights-report-2017-opinions_pl, data dostępu: 07.01.2019.
- The Council of Europe Progress Report on The Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data, Tilburg Institute for Law, Technology and Society, Tilburg University, April 2013.
- Trybunał Sprawiedliwości Unii Europejskiej, Komunikat Prasowy nr 117/15, Luksemburg, 6 października 2015 r.
- Uwagi ogólne Komitetu Praw Człowieka z 23.03.1988 r., [w:] *Wspólny standard do osiągnięcia. Stan urzeczywistnienia. W pięćdziesięciolecie Powszechnej Deklaracji Praw Człowieka z 10 grudnia 1948 roku,* red. T. Jasudowicz, Toruń 1998.

Orzecznictwo

- Wyrok Europejskiego Trybunału Praw Człowieka w sprawie 27798/95 Amann v. Switzerland, 16.02.2000.
- Wyrok Europejskiego Trybunału Praw Człowieka w sprawie 62332/00 Segerstedt-Wiberg and others v. Sweden, 06.06.2006.
- Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 31 stycznia 1978 r. w sprawie Fratelli Zerbone SNc przeciwko Amministrazione delle finanse dello Stato, sprawa 94/77, ECLI:EU:C:1978:17.
- Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r. w sprawie Google Spain SL i Google Inc. Przeciwko Agencia Espanola de Protection de Datos (AEPD) i Mario Sosteja Gonzale, sygn. akt. C-131/12.
- Wyrok Trybunału Sprawiedliwości Unii Europejskiej w wyroku z dnia 16 lipca 2020 r. ws. C-311/18 (Schrems II).

Opracowania zwarte

- *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych,* Biuro Generalnego Inspektora Danych Osobowych, Warszawa 2009.
- *ABC zasad kontroli przetwarzania danych osobowych,* Generalny Inspektor Ochrony Danych (GIODO), Wydawnictwo Sejmowe, Warszawa 2011.
- *AI in Cybersecurity*, red. L.F. Sikos, Springer International Publishing, Cham 2019.
- *AI Love You Developments in Human-Robot Intimate Relationships,* red. Y. Zhou, M.H. Fischer, Springer International Publishing, Cham 2019.
- Andrzejak K., Glen P., Janiszewski P., Onysyk Ł, Kręcisz-Sarna A., Sarna M., Stępień A., Szczygielska W., Tyski J., *Dokumentacja ochrony danych osobowych według RODO*, Wiedza i Praktyka, Warszawa 2018
- Arora P., *The Next Billion Users: Digital Life Beyond the West*, Harvard University Press, Cambridge 2019.
- Ausloos J., *The right to erasure in EU data protection law : from individual rights to effective protection,* Oxford University Press, Oxford 2020.
- Bach-Golecka D., *Demokracja w prawie międzynarodowym,* Wydawnictwo DANTE, Kraków 2007.
- Banyś T., Łuczak A.J., *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Prescom, Wrocław 2017.
- Barański M., *Informacja w ujęciu prawnym przez pryzmat zagadnień terminologicznych*., Uniwersytet Śląski, Katowice 2017.
- Bernitz U., Groussot X., S., de Vries S.A., Paju J., *General principles of EU law and the EU digital order*, Wolters Kluwer, Aplphen aan den Rijn 2020.
- Betkier M., *Privacy online, law and the effective regulation of online services*, Intersentia, Cambridge 2019.
- *Bezpieczeństwo informacji w administracji publicznej*, red. D. Fleszer, Wyższa Szkoła Humanitas, Sosnowiec 2017.

- Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz,* Kraków 2004.
- Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz,* 5. wyd., LEX a Wolters Kluwer business, Warszawa 2011.
- *Bezpieczeństwo danych i IT w kancelarii prawnej, radcowskiej, adwokackiej, notarialnej, komorniczej czyli jak bezpiecznie przechowywać dane w kancelarii prawnej*, red. D. Szostek, Warszawa 2018.
- Bidziński M., Chmaj M., Szustakiewicz P., *Ustawa o dostępie do informacji publicznej. Komentarz*, wyd. 3, C. H. Beck, Warszawa 2018.
- Bielak-Jomaa E., *Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?*, „Monitor Prawniczy" 2017, dodatek specjalny do nr. 20.
- Bourka A., Drogkaris P., *Online platform for security of personal data processing: reinforcing trust and security in the area of electronic communications and online services*, Publications Office, Luxembourg 2019.
- Burkat P., McCourt T., *Why Hackers Win: Power and Disruption in the Network Society*, University of California Press, Berkeley 2020.
- Carey M.J. , Tribe *of hackers : cybersecurity advice from the best hackers in the world Cybersecurity advice from the best hackers in the world*, Wiley, Indianopolis 2019.
- Chuvakin A., Williams B.R., W. Spangerberg W., *PCI compliance understand and implement effective PCI data security standard compliance.Payment Card Industry compliance*, Syngress, Amsterdam 2010.
- *Consumer informatics and digital health: solutions for health and health care*, red. M. Edmunds, E. Holve, Springer, Cham 2019.
- *Data quality and artificial intelligence: mitigating bias and error to protect fundamental rights*, Publication Office, Luxembourg 2019.
- Denley A., Foulsham M., Hitchen B., *GDPR: how to achieve and maintain compliance*, Routledge, London-New York 2019.
- *Digital Transformation*, red. R. Neugebauer, Springer, Berlin-Heidelberg 2019.
- *Digital transformation in business and society: theory and cases*, Palgrave Macmillan, red. P.B. George, J. Paul, Cham 2020.

- *Digital Twin Technologies and Smart Cities*, red. M. Farsi, A. Daneskhah, A. Hoseinian-Far, H. Jahankhani, Springer International Publishing, Cham 2020.
- Drożdż A., *Protection of natural persons with regard to automated individual decision-making in the GDPR*, Kluwer Law International, Alpen aan den Rijn 2020.
- *Edge Computing From Hype to Reality*, red. F. Al-Turjman, Springer International Publishing, Cham 2019.
- Elżanowski F., *Polityka energetyczna. Prawne instrumenty realizacji,* Lexis Nexis, Warszawa 2008.
- Erdos D., *European data protection regulation, journalism and traditional publishers: balancing on a tightrope?*, Oxford University Press, Oxford 2019.
- *EU General Data Protection Regulation (GDPR): an implementation and compliance guide*, IT Governance Publishing, Ely 2017.
- Farrell H., Newman A., *Of privacy and power: the transatlantic struggle over freedom and security*, Princeton University Press, Princeton – Oxford 2019.
- Fromm E., *Rewolucja nadziei,* Wydawnictwo Rebis, Poznań 1996.
- *5G Enabled Secure Wireless Networks*, red. D.N.K. Jayakody, K. Srinivasan, V. Sharma, Springer International Publishing, Cham 2019.
- Gałaj-Emiliańczyk K, *Dokumentacja wdrożenia RODO (z suplementem elektronicznym),* ODDK**,** Gdańsk 2018.
- Gałaj-Emiliańczyk K., *Dokumentacja ochrony danych osobowych. Praktyczny przewodnik krok po kroku*, Difin, Warszawa 2016.
- Gawronski M., *Guide to the GDPR*, Kluwer Law International, Alpena aan den Rijn 2019.
- *General principles of EU law and the EU digital order*, red. U. Bernitz, X. Groussot, S.A. de Vries, J. Paju, Wolters Kluwer, Aplphen aan den Rijn 2020.
- *Guidelines for SMEs on the security of personal data processing*, ENISA, Heraklion 2016.
- *Handbook on security of personal data processing,* ENISA, Heraklion 2017.
- Hassan N.A., Hijazi R., Salminen H., *Data hiding techniques in Windows OS: a practical approach to investigation and defense*, Syngress, Amsterdam 2017.

- Irion K., *Digital Single Market Strategy (DSM Strategy),* European Parliament, Brussels 2018.
- Jabłoński M., Węgrzyn J., *Ochrona tajemnic osób wykonujących prawnicze zawody zaufania publicznego*, wyd. 2., Wrocławskie Wydawnictwo Naukowe Atla 2, Wrocław 2018.
- Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie,* Oficyna a Wolters Kluwer business, Warszawa 2010.
- Jasiński F., *Karta Praw Podstawowych Unii Europejskiej,* Dom Wydawniczy ABC, Warszawa 2003.
- Jaskiernia J., *Funkcje Konstytucji RP w dobie integracji europejskiej i radykalnych przemian politycznych*, Wydawnictwo Adam Marszałek, Toruń 2020.
- Jaskiernia J., *Zgromadzenie Parlamentarne Rady Europy,* Uniwersytet Warszawski, Biuro Informacyjne Rady Europy, Warszawa 2000.
- Kawecki M., *Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych*, Wolters Kluwer, Warszawa 2017.
- Kim S.-J, Suh K.-J, Lee H.-J, Yu H.-I, Park J.H., Lee H.-J., *Apparatus and method for enhancing personal information data security*, ESP, Cenet 2019.
- Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Wolters Kluwer Polska**,** Warszawa 2018.
- Krasuski A., *Ochrona danych osobowych na podstawie RODO*, wyd. 2., Wolters Kluwer Polska Warszawa 2018.
- Kropf J.W., N. Cohen N., *U.S. government practice on global sharing of personal information*, 3rd ed., International Association of Privacy Professionals IAPP, Portsmouth 2000.
- Krzysztofek M., *GDPR, General Data Protection Regulation (EU) 2016/679 : post-reform personal data protection in the European Union*, Kluwer Law International, Alphen aan den Rijn 2019.
- Kuner Ch., *European Data Protection Law Compliance and Regulation,* Oxford – New York 2007.

- Ladley J., *Data governance: how to design, deploy and sustain an effective data governance program*, Academic Press, London 2020.
- Lambert P., *The right to be forgotten: interpretation and practice*, Bloomsbury, London 2019.
- *Law, policy and the Internet*, red. L. Edwards, Hart, London 2019.
- Łasak K., *Prawa społeczne w orzecznictwie Europejskiego Trybunału Praw Człowieka,* Instytut Wydawniczy EuroPrawo, Warszawa 2013.
- Mironenko Enerstvedt O., *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*, Springer International Publishing, Cham 2017.
- Pan M., Wang J., Errapotu S.M., Zhang X., Ding J., Han Z., *Big Data Privacy Preservation for Cyber-Physical Systems*, Springer International Publishing, Cham 2019.
- Pang Z.-H., Liu G.-P, Zhou D., Sun D., *Networked Predictive Control of Systems with Communication Constraints and Cyber Attacks*, Springer, Singapore 2019.
- Parzymies S., *Unia Europejska od Maastricht do Lizbony. Polityczne aspekty aktywności,* Wydawnictwo Dialog, Warszawa 2012.
- *PCI compliance: understand and implement effective PCI data security standard compliance. Understand and implement effective PCI data security standard compliance*, 4 ed., red. B.R. Wiliams, A.A. Chuvakin, D. Milroy, Syngress, Waltham 2015.
- Pemble M., Goucher W., *CIO's guide to security incident management*, CRS Press, New York 2019.
- *Personal data in competition, consumer protection and intellectual property law: towards a holistic approach?*, red. M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Sulbryte-Namavičiene, Springer, Berlin 2018.
- *Personalized Medicine in Healthcare Systems Legal, Medical and Economic Implications*, red. N. Bodriga-Vukobrat, D. Rukavina, K. Pavelić, G.G. Sander, Springer International Publishing, Cham 2019.

- *Post-reform personal data protection in the European Union: general data protection regulation (EU) 2016/679 Subjects*, Wolters Kluwer, Alphen aan den Rijn 2017.
- *Privacy and data protection seals*, red. R. Rodrigues, V. Papakonstantinou, T.M.C. Asser Press, The Hague 2018.
- *Privacy and security in personal data clouds: final report*, ENISA, Heraklion 2016.
- Puwalski M., *Prawo do prywatności osób publicznych,* Wydawnictwo TNOiK, Toruń 2003.
- *Regulating industrial internet through IPR, data protection and competition law*, red. R.M. Ballardini, I. Pitkänen, P. Kuoppamäki, Kluwer Law International, Alphen aan den Rijn 2019.
- *Regulating new technologies in uncertain times*, red. L. Reins, Asser Press, Springer, The Hague 2019.
- *Reinforcing trust and security in the area of electronic communications and online services: sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*, ENISA, Heraklion 2018.
- Robel J., *Wpływ Rady Europy na realizację koncepcji bezpieczeństwa demokratycznego w państwach członkowskich.* Wydawnictwo Adam Marszałek, Toruń 2016.
- *RODO w e-commerce*, red. D. Lubasz, Wolters Kluwer Polaska, Warszawa 2018.
- *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, C.H. Beck, Warszawa 2018.
- Schifreen R., *Data Protection and Security for Personal Computers: A manager's guide to improving the confidentiality, availability and integrity of data on Personal Computers and Local Area Networks*, Elsevier Science, Amsterdam 2014.
- Sears A., Dehesne F., Georgieva I., Tani T., van der Hof S., *EU personal data protection in policy and practice*, T.M.C. Asser Press, The Hague 2019.

- *Security and privacy in cyber-physical systems: foundations, principles, and applications*, red. H. Song, G.A. Fink, S. Jeschke, *Security and privacy in cyber-physical systems : foundations, principles, and applications*, John Wiley & Sons, Chichester – Hoboken 2019.
- *Security in Smart Cities: Models, Applications, and Challenges*, red. A.E. Hassanien, M. Elhoseny, S.H. Ahmed, A.K. Singh, Springer International Publishing 2019.
- *Security/Mobility Politics of Movement*, red. S. Wittendorp, M. Leese, Manchester University Press, Manchester 2017.
- Sharpe S., *National security, personal privacy and the law : surveying electronic surveillance and data acquisition*, Routlege, London-New York 2020.
- *Smart Cities of Today and Tomorrow Better Technology, Infrastructure and Security*, red. J.P. Pelton, I.B. Singh, Springer International Publishing, Cham 2019.
- Snowden E., *Mémoires vives*, Éditions du Seuil, Paris 2019.
- Sozański J., *Prawo Unii Europejskiej po Traktacie Lizbońskim,* Polskie Wydawnictwo Prawnicze „IURIS", Warszawa – Poznań 2010.
- Sweeney J.A., *The European Court of Human Rights in the Post-Cold War Era: Universality in Transition,* Routledge, Abington 2012.
- Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem,* Oficyna a Wolters Kluwer business, Warszawa 2010.
- *The EU general data protection regulation (GDPR): a commentary*, red. C. Kuner, Oxford University Press, Oxford 2019.
- *The European Union: facing the challenge of multiple security threats*, red. A. Bakardijeva Engelbrekt, A. Michalski, N. Nillson, L. Oxelheim, Edward Elgar Publishing, Cheltenham – Portsmouth 2018.
- Trombski M., Kosowski B., *Współczesny wymiar bezpieczeństwa w aspekcie zmienności zagrożeń,* Wyższa Szkoła Zarządzania Ochroną Pracy, Katowice 2010.
- *Trusting records in the Cloud*, red. L. Duranti, C. Rogers, Facet, London 2019.

- Tsirigotis A.A. *Cybernetics, Warfare and Discourse The Cybernetisation of Warfare in Britain*, Springer International Publishing, Cham 2017.
- *Ubiquitous Computing and Computing Security of IoT*, red. J. Jeyjanyhi, A. Abraham, H. Mcheick, Springer International Publishing, Cham 2019.
- *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Wolters Kluwer Warszawa 2018.
- Volchkov A., *Information security governance : framework and toolset for CISOs and decision makers*, CRS Press. Boca Raton 2019.
- Walters R., Trakman L., Zeller B., *Data Protection Law A Comparative Analysis of Asia-Pacific and European Approaches*, Springer, Singapore 2019.
- Weiss J.B., *Data processing agreements: coordination, drafting & negotiation*, International Association of Privacy Professionals IAPP, Portsmouth 2019.
- Williams R.R., Chuvakin A.A., Milroy D. (red.), *PCI compliance: understand and implement effective PCI data security standard compliance. Understand and implement effective PCI data security standard compliance*, Syngress, Waltham 2015.

Studia i artykuły naukowe

- Abbott K., Sindal D., *Hard and Soft Law in International Governance,* [w:] *International Law: Classic and Contemporary Readings,* red. C. KU. P.F. Dietl, Lynne Rienner, Boulder 2009.
- Abu Gholeh M., *Pozycja ustrojowa organu nadzorczego ochrony danych osobowych na przykładzie Polski*, „Przegląd Prawa Konstytucyjnego" 2019, nr 4.
- Adamowicz M., *Traktat o Unii Europejskiej,* „Problemy Integracji Rolnictwa" 1997, nr 3.
- Adamski D., *Unijne modele regulacji jawności i jej ograniczeń oraz ich wpływ na systemy krajowe,* [w:] *Jawność i jej ograniczenia,* red. G. Szpor, C. Mik, C.H. Beck, Warszawa 2016.

- Altenhoener Ch., *Review of the Monitoring Process of the Council of Europe Framework Convention for the Protection of National Minorities,* "European Yearbook of Minority Issues" 2012, Vol. 9.
- Anciaux N., Buganim L., Pucheral P., Popa I.S., Scerri G., *Personal Database Security and Trusted Execution Environments: A Tutorial at the Crossroads,* [w:] *Proceedings of the VLDB Endowment*, 28 August 2019.
- Arnold R., *Znaczenie prawa europejskiego dla polskiego porządku prawnego,* „Monitor Prawniczy" 1996, nr 7.
- Aromińska K., *Ochrona danych osobowych w procesie rekrutacji i zatrudnienia,* „Bezpieczeństwo Pracy" 2014, nr 3.
- Bajorek J., *Ochrona i bezpieczeństwo danych osobowych w organizacji,* „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2016, nr 1.
- Balcerzak M., *Kategoria jawności i prawo do informacji z perspektywy orzecznictwa Europejskiego Trybunału Praw Człowieka,* [w:] *Jawność i jej ograniczenia,* red. G. Szpor, C. Mik, t. 11. *Standardy europejskie*, Wydawnictwo Beck, Warszawa 2016.
- Balcerzak M., *Zalecenia Komitetu Ministrów Rady Europy jako forma pozatraktatowej działalności normatywnej i harmonizującej w dziedzinie praw człowieka,* [w:] *Rada Europy – 60 lat na rzecz jedności europejskiej,* Bielsko – Biała 2009.
- Ball K.M., *African Union Convention on Cyber Security and Personal Data Protection*, "International Legal Materials" 2017, nr 1.
- Ball K.M., *Introductory note to African Union convention on cyber security and personal data protection*, "International Legal Materials", 2017, nr 1.
- Banyś T., Łuczak A.J., *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Presscom, Wrocław 2017.
- Bańczyk W., *„Miękkie prawo, ale prawo", czyli o obowiązku przestrzegania soft law,* „Internetowy Przegląd Prawniczy TB ŚP UJ" 2016, nr 1.
- Baran B., Południak-Gierz K., *Aspekt podmiotowy udostępniania informacji publicznej na przykładzie regulacji polskich i szwedzkich,* „Przegląd Prawa Publicznego" 2017, nr 10.

- Barański M., Giermak M., *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego, (uwagi na tle ferenda),* „Państwo i Prawo" 2017, nr 10.
- Barcz J., *Struktura Unii Europejskiej,* [w:] *Zasady ustrojowe Unii Europejskiej,* red. J. Barcz, t. 2, Instytut Wydawniczy EuroPrawo, Warszawa 2010.
- Barkin S.J., *The Revolution of the Constitutions of Sovereignty and the Emergence of Human Rights Norms,* "Millenium – Journal of International Studies" 1998, No. 2.
- Bąba M., *Zasada proporcjonalności (adekwatności) a zgoda pracownika na przetwarzanie danych osobowych*, „Praca i Zabezpieczenie Społeczne" 2018, nr 2.
- Bąba M., *Zgoda pracownika jako podstawa legalizująca gromadzenie przez pracodawcę danych biometrycznych pracownika*, „Praca i Zabezpieczenie Społeczne" 2018, nr 1.
- Bernatowicz G., *Traktat Amsterdamski a kwestia rozszerzenia Unii Europejskiej,* „Zeszyty Naukowe Wyższej Szkoły Zarządzania i Marketingu w Warszawie" 1998, nr 4.
- Biczysko-Pudełko A., *Administrator danych osobowych i przetwarzający dane na zlecenie a chmura obliczeniowa - problemy interpretacyjne*, „Prawo Mediów Elektronicznych" 2016, nr 1.
- Bielaszka R., *Kształtowanie polskich rozwiązań prawnych przez Unię Europejską w zakresie efektywności energetycznej,* Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2013.
- Bielecki M., *Przetwarzanie danych osobowych przez Świadków Jehowy*, „Przegląd Prawno-Ekonomiczny" 2017, nr 3.
- Biernat S., *Czy Karta Prawo Podstawowych Unii Europejskiej obowiązuje w Polsce?,* [w:] *Państwo prawa i prawo karne: księga jubileuszowa profesora Andrzeja Zolla,* Wydawnictwo Lex a Wolters Kluwer business, Warszawa 2012.
- Biernat S., *Źródła prawa Unii Europejskiej,* [w:] *Prawo Unii Europejskiej,* red. J. Barcz, Warszawa 2006.
- Bienias M., *Zasada czasowego ograniczenia przechowywania danych osobowych na gruncie RODO*, „ Prawo Mediów Elektronicznych" 2017, nr 4.

- Biliński M., *Ochrona danych osobowych w sferze sportu w świetle aktualnych zmian legislacyjnych*, „Przegląd Naukowy Disputatio" 2017, t. 24, nr 2.
- Biliri E., Kokkinakos B., Michailitsi A., Papaspyror D., Tsapelas J., Mouzakitis S., Koussouris S., Glickaman Y., Kirstein F., *Big data analytics in public safety and personal security: Challenges and potential*, [w:] 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), 2017.
- Bińkowska-Artowicz B., *W sprawie obowiązków posła jako administratora w kontekście ogólnego rozporządzenia o ochronie danych (RODO*), „Przegląd Sejmowy" 2018, nr 5.
- Bloom M., *Protecting personal data: a model data security and breach notification statute*, "St. John's Law Review", 2018, nr 4.
- Błaszczuk M., *Rozszerzenie Unii Europejskiej – Bułgaria i Rumunia nowymi państwami członkowskimi,* „Wspólnoty Europejskie" 2006, nr 10.
- Błoński T., *Wyzwania stojące przed Zakładem Ubezpieczeń Społecznych w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych (2016/679),* „Ubezpieczenia Społeczne" 2016, nr 3.
- Bochentyn A., Ważny K., *Udostępnianie informacji publicznej przez podmioty prowadzące działalność gospodarczą*, [w:] *Administracja publiczna a gospodarka*, red. B. Jaworska-Dębska, A. Dobaczewska, Wydawnictwo Ius Publicum, Warszawa 2018.
- Bogucka L., *Bezpieczeństwo danych osobowych w świecie Facebooka,* „Zarządzanie Innowacyjne w Gospodarce i Biznesie" 2017, nr 1.
- Boehme-Nebler V., *Privacy: a matter of democracy. Why democracy needs privacy and data protection,* "International Data Privacy Law", Vol. 6.
- Borecka J., *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych,* „Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie" 2006, z. IV.
- Borowicz J., *Obowiązki poufności pracowników współpracujących z wykonawcami wolnych zawodów*, „Praca i Zabezpieczenie Społeczne" 2017, nr 12.
- Bowring B., *Russia's Accession to the Council of Europe and human rights. Four years on,* "Helsinki Monitor" 2000, vol. 11.

- Braciak J., *Prawo do prywatności,* [w:] *Prawa i wolności obywatelskie w Konstytucji RP,* red. B. Banaszak, A. Preisner, Warszawa 2002.
- Brkan M., *The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core,* "European Constitutional Law Review" 2018, nr 2.
- Bronfman J., *I'm ready for my close-up, Mr. Spielberg: creating a working model for data security and personal privacy in the use case of unmanned aerial systems in film and video game productions*, "Whittier Law Review", 2018, nr 2.
- Brzezińska M.M., *Skutki zmian systemowych Unii Europejskiej po ratyfikacji Traktatu Lizbońskiego,* [w:] *Traktat Lizboński, Co po Irlandii?,* red. M.M. Brzezińska, R. Zenderowski, UKSW, Warszawa 2009.
- Buchalska J., *Prawo do bycia zapomnianym – w orzecznictwie polskim,* [w:] *Prawo prywatności jako reguła społeczeństwa informacyjnego,* red. K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak, Wydawnictwo C.H. Beck, Warszawa 2017.
- Byrski J., *Nowe zasady przekazywania danych osobowych do państwa trzeciego, jako instrument prawny oddziaływania na gospodarkę,* [w:] *Prawne instrumenty oddziaływania na gospodarkę,* red. A. Powałowski, Wydawnictwo C.H. Beck, Warszawa 2016.
- Byrski J., Hoser H., *Zakres zmian w ustawie o działalności ubezpieczeniowej i reasekuracyjnej w związku z dostosowaniem do unijnych regulacji dotyczących ochrony danych osobowych*, „Prawo Asekuracyjne" 2019, nr 2.
- Cegiełko S., *Kultura użytkowa zabezpieczeń biometrycznych klientów banków w Polsce na podstawie sondażu internetowego*, „Bezpieczny Bank" 2018, t. 72, nr 3.
- Ceglarek K., *Ochrona danych osobowych a rozwój społeczeństwa informacyjnego,* „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2012, nr 88.
- Celarek K., *Informacja istotą demokracji - szczególna rola administracji publicznej w procesie urzeczywistniania Prawa informacyjnego*, [w:] *Stulecie polskiej administracji. Doświadczenia i perspektywy*, red. W. Federczyk, Krajowa Szkoła Administracji Publicznej, Warszawa 2018.

- Cern G., *Realizacja zasady jawności i dostępu do informacji publicznej w "spółkach gminnych",* [w:] *Źródła prawa w samorządzie terytorialnym*, red. B. Dolnicki, Wolters Kluwer Polska, Warszawa 2018.
- Cha S.C., Yeh K.-H, *A Data-Driven Security Risk Assessment Scheme for Personal Data Protection*, Institute of Electrical and Electronics Engineers (IEEE) Access, 2018, vol. 6.
- Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych,* „Europejski Przegląd Prawa" 2017, nr 5.
- Ciechomska M., *Zmiana Konwencji nr 108 Rady Europy o ochronie danych osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych,* „Monitor Prawniczy" 2017, nr 16.
- Ciesielski J., *Rejestry przedsiębiorców a ochrona danych osobowych*, „Acta Universitatis Wroclaviensis. Przegląd Prawa i Administracji" 2018, nr 112.
- Czarnecki K., *Ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych,* [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X – lecie polskiej ustawy o ochronie danych osobowych,* red. G. Goździewicz, M. Szabłowska, Wydawnictwo TNOiK, Toruń 2008.
- Chodorowski M., *Nowe prawa i obowiązki administratorów bezpieczeństwa informacji (inspektorów ochrony danych osobowych w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29,* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia,* red. M. Kawecki, T. Osiej, Wydawnictwo C.H. Beck, Warszawa 2017.
- Chojnowski L., *Polityczny sektor bezpieczeństwa,* „Zeszyty Naukowe WSOWL" 2012, nr 3.
- Chrzanowska J., *Problematyka tymczasowego aresztowania w praktyce Komitetu Ministrów Rady Europy (art. 46 EKPC),* [w:] *Przewlekłość tymczasowego aresztowania w Polsce w świetle europejskich standardów ochrony praw człowieka,* red. P. Turek, Prokuratura Generalna, Warszawa 2013.

- Cwener M., *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych,* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia,* red. M. Kawecki, T. Osiej, Wydawnictwo C.H. Beck, Warszawa 2017.
- Czarnowski A., Gawroński M., Naklicka P., *Powierzenie danych oraz elementy nowej umowy powierzenia danych*, [w:] *RODO. Przewodnik ze wzorami*, red. M. Gawroński, Wolters Kluwer Polska, Warszawa 2018.
- Czarnowski A., Gawroński M., P. Punda P., *Prawo do przenoszenia danych, czyli jak przenieść dane od jednego administratora danych do drugiego (art. 20 RODO)*, [w:] *RODO. Przewodnik ze wzorami*, red. M. Gawroński, Wolters Kluwer Polska, Warszawa 2018.
- Czarnowski A., Gawroński M., Punda P., *Pseudonimizacja i szyfrowanie - preferowane środki zabezpieczania danych osobowych*, [w:] *RODO. Przewodnik ze wzorami*, red. M. Gawroński, Wolters Kluwer Polska, Warszawa 2018.
- Czech A., *Uwarunkowania polskiej polityki energetycznej w kontekście postulatu zrównoważonego rozwoju,* „Studia Ekonomiczne. Zeszyty Naukowe" 2016, nr 269.
- Czermiński J., *Bezpieczeństwo danych osobowych w aplikacjach umieszczonych w „chmurze",* „Logistyka" 2015, nr 3.
- Czosnek M., Piaskowski G., *Tajemnica telekomunikacyjna. Analiza NAT jako narzędzie do identyfikacji sprawców*, „Przegląd Policyjny" 2018, nr 4.
- Czyżewski R., Babś A., Madajewski K., *Sieci inteligentne – wybrane cele i kierunki działania operatora systemu dystrybucyjnego,* „ActaEnergetica", źródło: www.actaenergetica_org.pl, data dostępu: 17.07.2018.
- Degeling C, Chen G., Gilbert G.L., Brookes W., Thai T., Wilson A., Johnson J., *Changes in public preferences for technologically enhanced surveillance following the COVID-19 pandemic: a discrete choice experiment*, "British Medical Journal" 2020, nr 11.
- de Hert P., Papakonstantinou V., *The Council of Europe Data Protection Convention reform: Analysis of the new text and Critical Comments on its*

global ambition, "Computer Law & Security Review: The International Journal of Technology Law and Practice" 2014, vol. 30.

- Denkiewicz E., *Płaszczyzny oddziaływania Rady Europy na przemiany systemowe w Federacji Rosyjskiej – wpływ Europejskiej Konwencji Praw Człowieka oraz Europejskiego Trybunału Praw Człowieka na zmiany systemu prawnego w Rosji,* [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989 – 2009,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2010.
- Desiree Dodd J., *Data security law—state statutory requirements for protecting personal data*, "The American Journal of Trial Advocacy", 2015-04-01, nr 3.
- Diggelmann O., Cleis M.N., *How to Right to Privacy Became a Human Right,* "Human Rights Law Review" 2014, vol. 14.
- Długosz Z., Mostowik M., *Dysponowanie danymi z rachunku w świetle przepisów PSD2 oraz RODO*, „Monitor Prawa Bankowego" 2018, nr 5.
- Dmochowska A., *Obowiązek informacyjny,* [w:] *Unijna ochrona danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art.. 29, Ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, 2. wyd. Wydawnictwo C.H. Beck, Warszawa 2018.
- Dmochowska A., *Prawa osoby, której dane dotyczą,* [w:] *Unijna ochrona danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art.. 29, Ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, 2. wyd. Wydawnictwo C.H. Beck, Warszawa 2018.
- Dmochowska A., *Europejska Rada ochrony Danych,* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018.
- Dobkowski J., *Rejestry publiczne o charakterze personalnym prowadzone w systemie teleinformatycznym i administracyjne prawo dowodowe*, „Casus" 2018, nr 91.
- Dobroczyńska A., Juchniewicz L., *Polityka energetyczna Polski,* „Nowe Życie Gospodarcze" 2003, nr 1.

- Domańska-Szaruga B. Prokopowicz D., *Ochrona transferu danych osobowych w cyberprzestrzeni,* „SECRETUM. Służby Specjalne, Bezpieczeństwo i Informacja" 2016, nr 2.
- Domański Z., *Bezpieczeństwo socjalne,* „Journal of Modern Science" 2017, nr 2.
- Dörre-Kolasa D., *Administrator danych osobowych w zbiorowym prawie zatrudnienia*, Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019, nr 4.
- Du Z.-Y., *Personal Data Security and Supervision in the Age of Large Data*, "Intelligent Automation and Soft Computing" 2019, nr 1.
- Dyrda K., *Prawo i obowiązek przetwarzania danych osobowych byłych wyznawców przez kościoły i inne związki wyznaniowe*, „Studia z Prawa Wyznaniowego" 2018, t. 21.
- Dziembała M., *Koncepcja polityki bezpieczeństwa w świetle zmian w ochronie danych osobowych w placówce medycznej,* „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 355.
- Dziewięcka-Bokun L., *Bezpieczeństwo socjalne jako podstawa pokoju społecznego,* „Prace Naukowe/Akademia Ekonomiczna w Katowicach" 2003, tom: Bezpieczeństwo socjalne.
- Dzięgiel A.M., *Naruszenie dóbr osobistych w Internecie,* „Jurysta" 2017, nr 1.
- Dmochowska A., *Współadministratorzy danych – ułatwienie dla grup przedsiębiorców,* „Jurysta" 2017, nr 3.
- Drzemczewski A., *Procedura monitoringowa Komitetu Ministrów a Rada Europy. Użyteczny mechanizm „praw człowieka",* [w:] *Polska w Radzie Europy. 10 lat członkostwa – wybrane zagadnienia,* red. H. Machińska, Ośrodek Informacji Rady Europy, Centrum Europejskiego Uniwersytetu Warszawskiego, Warszawa 2002.
- Drzemczewski A., *Monitoring by the Committee of Ministers of the Council of Europe: A Useful 'Human Rights' Mechanisms?,* "Baltic Yearbook of International Law Online" 2002, Vol. 2.
- Dygasiewicz K., *Kradzież tożsamości w czasach społeczeństwa informacyjnego,* [w:] *Internet. Strategie bezpieczeństwa. Security strategy,* red. G. Szpor, A. Gryszczyńska, Wydawnictwo C.H. Beck, Warszawa 2017.

- Fajgielski P., *Ochrona danych osobowych przedsiębiorcy będącego osobą fizyczną*, [w:] *Dysfunkcje publicznego prawa gospodarczego*, red. M. Zdyb, E. Kruk, G. Lubeńczuk, C. H. Beck, Warszawa 2018.
- Fajgielski P., *Unijna reforma ochrony danych osobowych a działalność urzędów stanu cywilnego*, „Metryka" 2017, nr 2.
- Feri F., Jenzsch N., *Disclosure of personal information under risk of privacy shocks*, "Journal of Economic Behavior & Organization", 2016, vol. 123.
- Fitzmaurice M.A., *The Identification and Character of Treaties and Treaty Obligations between States in International Law,* "British Year Book of International Law" 2002, vol. 73.
- Fleischmann A., *Personal Data Security: Divergent Standards in the European Union and the United States*, "Fordham International Law Journal" 1995, nr 1.
- Fleszer D., *Zabezpieczenie danych osobowych – zakres, obowiązki i sankcje za jego naruszenie,* [w:] *Bezpieczeństwo informacji w administracji publicznej,* red. D. Fleszer, Wyższa Szkoła Humanitas, Sosnowiec 2017.
- Foltyn T., *German chat site faces fine under GDPR after data breach,* źródło: www.welivesecurity.com/2018/11/27, data dostępu: 09.01.2020.
- Furmanek W., *Zagrożenia wynikające z rozwoju technologii informacyjnych,* „Dydaktyka Informatyki" 2014, nr 9.
- Furrer H.P., Gutzkow J., *The Concept of Democratic Security and It's Implementation by the Council of Europe,* "Romanian Journal of International Affairs" 1996, vol. II.
- Gałaj-Emiljańczyk K., *Ochrona danych osobowych podczas głosowania*, „Jurysta" 2018, nr 4.
- Ganczar M., Sytek A., *Jednostki samorządu terytorialnego wobec ogólnego rozporządzenia o ochronie danych (RODO)*, [w:] *Źródła prawa w samorządzie terytorialnym*, red. B.Dolnicki, Wolters Kluwer Polska, Warszawa 2018.
- Ganfalean I., Tudorascu M., Cojan M., *Human Rights Protection in Europe,* "Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2014, nr 11.
- Gawkowski K., *Informacja i jej bezpieczeństwo w jednostkach administracji samorządowej*, [w:] *Koncepcje i instrumenty zarządzania w administracji*

publicznej, red. A. Gołębiowska, P. B. Zientarski, Kancelaria Senatu, Warszawa 2017.

- Gawkowski K., *Wpływ Rady Europy na rozwój samorządności terytorialnej,* [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989 – 2009,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2010.
- Gawroński M., Kloc K., Wojtas M., *Administrator i podmiot przetwarzający*, [w:] *RODO*. *Przewodnik ze wzorami*, red. M. Gawroński, Wolters Kluwer Polska, Warszawa 2018.
- Glen P., *Umowa powierzenia przetwarzania danych osobowych*, [w:] K. Andrzejak, P. Glen, P. Janiszewski, Ł. Onysyk, A. Kręcisz-Sarna, M. Sarna, A. Stępień, W. Szczygielska, J. Tyski, *Dokumentacja ochrony danych osobowych według RODO*, Wiedza i Praktyka, Warszawa 2018
- Goerick J., *Współpraca międzynarodowa organów ochrony danych osobowych państw członkowskich Unii Europejskiej przed wejściem w życie ogólnego rozporządzenia o ochronie danych,* „Przegląd Naukowy. Disputio" 2017, nr 2.
- Gołda-Sobczak M., *Unia Europejska wobec potrzeby ochrony danych osobowych,* [w:] *Europejski system ochrony praw człowieka. Aksjologia-instytucje-efektywność,* red. J. Jaskiernia, t. III, Wydawnictwo Adam Marszałek, Toruń 2015.
- Gonschior A., *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej,* [w:] *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego. Aspekty teoretyczne i praktyczne,* red. D. Kornobis-Romanowska, Uniwersytet Wrocławski, Wrocław 2017.
- Gonzalez G. F.., *Security and the future of personal data protection in the European Union,* "Security and Human Rights" 2013, vol. 23.
- Gonzalez G.F., Gutwirth S., *Opening up personal data Protection: A conceptual controversy,* "Computer Law & Security Review: The International Journal of Technology Law and Practice" 2013, vol. 29.
- Gonschior A., *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej,* [w:] *Aktualne problemy prawa Unii Europejskiej i prawa*

międzynarodowego. Aspekty teoretyczne i praktyczne, red. D. Kornobis – Romanowska, Uniwersytet Wrocławski, Wrocław 2017.

- Gonzalez Fuster G.F., *Security and the Future of Personal Data Protection in the European Union,* "Security and Human Rights" 2013, nr 4.
- Graham P., Platten N., *Achieving Personal Data Protecting in the European Union,* "Journal of Common Market Studies" 1998, Vol. 26.
- Greenleaf G., Witzleb N., Lindsay D., Paterson M., Rodrick S., *A World Data Privacy Treaty?, 'Globalisation' and 'Modernisation' of Council of Europe Convention 108,* Cambridge University Press, Cambridge 2014.
- Greenleaf G., *'Modernising' data Protection Convention 108: A safe Basic for a global,* "Computer Law and Security Review: The International Journal of Technology and Practice" 2013, vol. 29.
- Grondys G., *Zagrożenia bezpieczeństwa informacji w Straży Miejskiej jako organizacji publicznej*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Warszawa-Siedlce 2018.
- Grzelak A., *Współpraca między organami ochrony danych osobowych w obszarze współpracy policyjnej i wymiaru sprawiedliwości w sprawach karnych – nadchodzące wyzwania prawne,* [w:] *Wdrożenie ogólnego rozporządzenia o ochronie danych osobowych. Aspekty proceduralne,* red. E. Bielak-Jomaa, U. Góral, Wolters Kluwer Polska, Warszawa 2018.
- Grzelak M., Lidel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe" 2012, nr 22.
- Grzeszczak R., *Zupełny i efektywny system ochrony praw podstawowych w Unii Europejskiej,* [w:] *Unia Europejska w roli gwaranta i promotora praw podstawowych,* red. D. Kornobis-Romanowska, Currenda, Sopot 2016.
- Gumularz M., Kawecki M., *RODO a doradcy podatkowi*, „Przegląd Podatkowy" 2018, nr 5.
- Gumzej N., *The Council of Europe and the Right to Personal Data Protection: Embracing Postmodernity,* "Journal of Arts & Sciences" 2013, No 6.

- Heinze M., *Poszukiwanie nowych instrumentów ochrony praw człowieka przez Radę Europy, Organizację Bezpieczeństwa i Współpracy w Europie i Unię Europejską,* [w:] *Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania,* red. J. Jaskiernia, t. 1, Wydawnictwo Sejmowe, Warszawa 2014.
- Hemphil T.A., Longstreet P.*, Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards*, "Technology in Society, 2016, vol. 44.
- Hillion Ch., *Rozszerzenie Unii Europejskiej – analiza prawna,* [w:] *Odpowiedzialność i legitymizacja Unii Europejskiej,* red. A. Arnull, D. D. Wincott, Wydawnictwo Sejmowe, Warszawa 2007.
- Hofmański P., *Prawo do poszanowania prywatności (art. 17 Paktu i art. 8 Europejskiej Konwencji Praw Człowieka), a rozwiązania polskiego prawa karnego materialnego i procesowego* [w:] *Standardy praw człowieka a polskie prawo karne,* red. J. Skupiński, Warszawa 1995.
- Indan-Pykno M., *Współpraca Rady Europy oraz Unii Europejskiej w zakresie ochrony praw człowieka,* [w:] *Prawa człowieka wczoraj i dziś. W 60. rocznicę powstania Rady Europy oraz 20 – lecia przyjęcia Konwencji Praw Dziecka,* UAM, Toruń 2010.
- Jabłoński M., Wygoda K., *Reforma ochrony danych osobowych - konsekwencje ograniczonego stosowania ogólnego rozporządzenia o ochronie danych w sferze publiczno-prawnej (zagadnienia wybrane),* [w:] *Dookoła Wojtek... Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Presinerowi*, red. R. Balicki, M. Jabłoński, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2018.
- Jackowiak U., *Ochrona danych osobowych w prawie pracy,* „Prawo i Zabezpieczenie Społeczne" 1998, nr 7-8.
- Jackowski M., Ciesielska M., *Adwokat według RODO - administrator czy procesor*, „Palestra" 2018, nr 10.
- Jaczyński S., *Bezpieczeństwo militarne II Rzeczypospolitej: aspekty wewnętrzne,* „Doctrina. Studia Społeczno-Polityczne" 2016, nr 13.

- Jasiński F., *Ochrona danych osobowych w porządku prawnym Unii Europejskiej,* „Kwartalnik Prawa Publicznego" 2003, nr 3.
- Jaskiernia J., *Wpływ Rady Europy na jedność aksjologiczną systemu prawa w rozwijających się państwach demokratycznych Europy,* [w:] *Jedność aksjologiczna systemu prawa w rozwijających się państwach demokratycznych Europy,* red. L. Stadniczeńko, Uniwersytet Opolski, Opole 2011.
- Kaczmarek A., *Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych*, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Wolters Kluwer, Warszawa 2018.
- Kaniewski S., *Geneza i znaczenie Systemu Informacyjnego Schengen,* „Edukacja Humanistyczna" 2015, nr 2.
- Kalita P., *Bezpieczeństwo energetyczne jako przesłanka poczucia bezpieczeństwa obywateli (doświadczenia Europy i Afryki),* [w:] *Ochrona praw człowieka w Afryce. Aksjologia – instytucje – nowe wyzwania – praktyka,* red. J. Jaskiernia, K. Spryszak, tom II, Wydawnictwo Adam Marszałek, Toruń 2017.
- Kamińska-Pietnoczko A., *Wpływ RODO na zasady przetwarzania danych osobowych związanych z zatrudnieniem - w oczekiwaniu na nowelizację Kodeksu pracy*, „Monitor Prawa Pracy" 2018, nr 6.
- Karpiuk M., *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*., „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, t. 40, nr 1.
- Kawka R., *Kontrola ochrony informacji niejawnych w jednostkach organizacyjnych MON*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski. Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Warszawa - Siedlce 2018.
- Keshu L., Meixia S., *Personal Information Security Crisis in the Era of Big Data*, "Journal of physics. Conference series", 2020, vol. 1486.
- Kierkegaard S., Waters N., Greenleaf G., Bygrave L.A., Lloyd L., Saxby S., *30 Years on – The review of the Council of Europe Data Protection Convention 108,* "Computer & Security Review" 2011, Vol. 27.
- Kirkham T., Winfield S., Ravet S., Kellomaki S., "IEEE Security & Privacy", 2013, nr 5.

- Kleinsorge T.E., *The Parliamentary Assembly: Europe's Motor and Conscience,* [w:] *Council of Europe,* red. T. Kleinsorge, Kluwer Law International, Alhen aan den Rijn 2010.
- Klimek R., *Demokracja czy bezpieczeństwo w sieci. Aspekty społeczno-polityczne bezpieczeństwa informacyjnego w XXI wieku,* „Przegląd Naukowo-Metodyczny „Edukacja dla Bezpieczeństwa" 2012, nr 4.
- Koller A., *The Legal Heritage of the Council of Europe,* "Human Rights Law Journal" 1990, nr 1-2.
- Konaszczuk W., *Realizacja przez państwo modelu bezpieczeństwa energetycznego jako prawa obywateli do odpowiedniego poziomu życia,* [w:] *Uniwersalny system ochrony praw człowieka. Aksjologia – instytucje – efektywność,* red. J. Jaskiernia, tom I, Wydawnictwo Adam Marszałek, Toruń 2015.
- Kontapka M., *Bezpieczeństwo obywatela w społeczeństwie informacyjnym - casus profilowania w sieciach handlowych*, [w:] *Współczesne wyzwania i zagrożenia wobec ochrony informacji niejawnych i danych osobowych*, red. M. Kubiak, S. Topolewski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Warszawa-Siedlce 2018.
- Kościuk D., *General Data Protection Regulation (GDPR) - The EU Law Strengthening the Information Society in Poland*, "Białostockie Stud.Prawnicze" 2018, nr 2.
- Kozioł M., *Bezpieczeństwo informacji i ochrona systemów informatycznych w przedsiębiorstwie,* „Zeszyty Naukowe/Uniwersytet Ekonomiczny w Krakowie" 2009, nr 770.
- Krasińska M., *Ochrona danych osobowych – prawo a rzeczywistość,* „Gazeta Bankowa" 2007, nr 7.
- Księżniakiewicz M., *Stosowanie Karty Praw Podstawowych Unii Europejskiej: Protokół brytyjski i Sprawozdania ze stosowania KPP UE,* „Rocznik Integracji Europejskiej" 2012, nr 6.
- Księżopolski K., *Wpływ rozszerzenia Unii Europejskiej na bezpieczeństwo ekonomiczne państw Europy Środkowej,* „Stosunki Międzynarodowe" 2006, nr 3/4.

- Kucharski O., Wolnicki P., *Prawo kościołów i innych związków wyznaniowych do żądania od kandydata na pracownika danych osobowych o jego wyznaniu lub religii*, Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019, nr 2.
- Kucharski O., Wolnicki P., *Przetwarzanie danych osobowych dotyczących zatrudnienia w Kościołach i innych związkach wyznaniowych*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2018, nr 4.
- Kuczma E., Kuczma P., *Generalny Inspektor Ochrony Danych Osobowych i ochrony prawa,* „Zeszyty Naukowe Dolnośląskiej Wyższej Szkoły Przedsiębiorczości i Techniki w Polkowicach. Studia z nauk społecznych" 2013, nr 6.
- Kujawa M., *Pseudonimizacja danych - co to właściwie jest?*, „Jurysta" 2018, nr 5.
- Kulesza E., *Wpływ regulacji Rady Europy i konwencji dotyczącej ochrony danych osobowych na ustawodawstwo polskie,* [w:] *Polska w Radzie Europy 10 lat członkostwa – wybrane zagadnienia,* red. H. Machińska, Ośrodek Informacji Rady Europy Centrum Europejskiego Uniwersytetu Warszawskiego, Warszawa 2002.
- Kumar L., Rishival V., *Design of Retrievable Data Perturbation Approach and TPA for Public Cloud Data Security*, "Wireless Personal Communications", 2019, nr 1.
- Kunasiewicz M., *Wybrane aspekty ochrony danych osobowych w systemach informatycznych,* „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 2002, nr 955.
- Kuźnicka D., *Monitorowanie pracownika w miejscu pracy a ochrona prywatności*, „Przegląd Prawniczy Uniwersytetu Warszawskiego" 2018, nr 1.
- Lambert P.B., *Security of Personal Data*, [w:] *Essential Introduction to Understanding European Data Protection Rules*, CRS Press, Boca Raton 2018.
- Lach A., *Uzyskiwanie przez osoby prywatne danych telekomunikacyjnych oraz danych internetowych*, „Państwo i Prawo" 2018, nr 6.
- Lang M., Devitt J., Kelly S., Kinneen A., O'Malley J., D. Prunty, *Social Networking and Personal Data Security: A Study of Attitudes and Public*

Awareness in Ireland, [w:] 2009 International Conference on Management of e-Commerce and e-Government, 2009.

- Lee D., Park N., Kim G., Jin J., Jo S., Han J., *De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment*, "Peer-to-Peer Networking and Applications", 2018-11, nr 6.
- Lewoc M., *Ocena stanu realizacji przez Polskę Zaleceń Komitetu Ministrów Rady Europy,* „Probacja" 2009, nr 2.
- Liu Y., Greene C., *The Dark Side of Big Data: Personal Privacy, Data Security, and Price Discrimination*, "Digital Transformation in Business and Society", 15 October 2019.
- Lubbe A., *Bezpieczeństwo ekonomiczne państwa,* „Sprawy Międzynarodowe" 1997, nr 4.
- Lund H., *Choice awareness: the Development of technological and institutional choice in the public debate of Danish energy planning,* "Journal of Environmental Policy and Planning" 2000, Vol. 2.
- Lynch J.K., Fisk M., *mHealth, Trust and the Security of Personal Data*, "Mobile e-Health", 2 December 2017.
- Łuczak J., *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji,* „Studia Oeconomia Posnaniensia" 2016, nr 12.
- Magnusson Sjőberg C., *Threats to personal data security: how does the EU protect its citizens?*, "The European Union", 27 April 2018.
- Majchrzak K., *Wzmacnianie świadomości obywateli Unii Europejskiej na temat gromadzenia i przetwarzania danych osobowych oraz ich ochrony,* [w:] *Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania,* red. J. Jaskiernia, t. 2, Wydawnictwo Sejmowe, Warszawa 2014.
- Maldini P., *Croatian Accession to the European Union: UE Democratization Potential and Issues of Democratic Consolidation,* [w:] *Croatia and the European Union. Changes and Development,* red. P. Maldini, D. Pauković, Routledge, London-New York 2016.

- Maliszewska-Nienartowicz J., *Ochrona danych osobowych,* „Prawo i Podatki Unii Europejskiej w Praktyce" 2006, nr 10.
- Mantelero A., *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework,* "Computer Law & Security Review: The International Journal of Technology Law and Practice" 2017, vol. 33.
- Mâţă D.C., *The protection of personal data in the context of national security protection measures*, Universul Juridic, 2018 (Suplement).
- Mednis A., *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej,* „Państwo i Prawo" 1997, nr 6.
- Mendyk B., *Nowe Rozporządzenie Unii Europejskiej w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych,* [w:] *Współczesne wyzwania państwa i prawa. Księga jubileuszowa prof. Jerzego Jaskierni z okazji 45 lecia pracy naukowej,* red. Ł. Baratyński, P. Ramiączek, K. Spryszak, Wydawnictwo Adam Marszałek, Toruń 2017.
- Merill M., *An Uneasy Love Triangle Between Alexa, Your Personal Life, and Data Security: Exploring Privacy in the Digital New Age*, "Mercer Law Review", 2020, nr 2.
- Miedzińska I., *Polska w systemie ochrony praw człowieka Rady Europy,* [w:] *Konstytucja w dobie europejskich wyzwań,* red. M. Zubik, A. Paprocka, R. Puchta, „Legislator", Warszawa 2010.
- Mik C., *Standardy Rady Europy dotyczące prasy,* „Palestra" 1993, nr 9-10.
- Miller V., *Effects of the EU Charter of Rights in the UK,* Standard Note SN/IA/6765, 17 March 2014, House of Commons Library.
- Mochocki R., *Prawnokarna ochrona danych osobowych,* [w:] *Nowe wyzwania i rozwiązania w polskim systemie ochrony praw człowieka,* red. J. Jaskiernia, K. Spryszak, Wydawnictwo Adam Marszałek, Toruń 2018.
- Mokrosiński J., *Reformy instytucji w Unii Europejskiej po „szczytach" w Nicei i Goteborgu,* 'Studia Europejskie Centrum Europejskie Uniwersytetu Warszawskiego" 2001, nr 2.

- Motyka K., *Prawo do prywatności,* „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach Seria: Administracja i Zarządzanie" 2010, nr 85.
- Morawski F., *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według Ogólnego Rozporządzenia o Ochronie Danych Osobowych*., „Acta Iuris Stetinensis" 2019, nr 2.
- Mrózek A., *Ochrona danych osobowych w Szwajcarii,* „OMT" 1984, nr 1.
- Mrózek A., *Zachodnioniemiecka ustawa o ochronie danych osobowych w procesach automatycznego przetwarzania,* „Studia Prawnicze" 1978, nr 1.
- Nehrebecki A.J., *Wspólna polityka energetyczna Unii Europejskiej,* „Stosunki Międzynarodowe" 2009, nr 3/4.
- Niczyporuk J., *Administracja ochrony danych osobowych,* „Zeszyty Naukowe/Wyższa Szkoła Informatyki i Zarządzania" 1999, nr 1.
- Niedźwiecki M., *Pseudonimizacja jako nowy środek zabezpieczenia danych osobowych w świetle zmian prawnych w UE - wybrane aspekty*, „Studia Erasmiana Wratislaviensis" 2018, nr 12.
- Nowotka M., *Współpraca między Unią Europejską a Radą Europy w kontekście ochrony praw człowieka w Europie,* [w:] *Państwo i prawo wobec współczesnych wyzwań. Integracja Europejska i stosunki międzynarodowe. Księga jubileuszowa Profesora Jerzego Jaskierni,* red. R.M. Czarny, K. Spryszak, t. V, Wydawnictwo Adam Marszałek, Toruń 2012.
- Ognik H., *Rada Europy,* [w:] *Europejskie struktury współpracy. Informator,* red. S. Parzymies, Polski Instytut Spraw Międzynarodowych, Warszawa 1995.
- Olszowiec P., *W kierunku inteligentnych sieci. Innowacje i tendencje dla przyszłych systemów elektroenergetycznych,* „Automatyka Elektroenergetyczna" 2010, nr 4.
- Osypowicz T., *Standardy uniwersalne w obszarze bezpieczeństwa danych osobowych,* „Przegląd Prawno-Ekonomiczny" 2019, nr 46.
- Papucki M., *Grupa Państw przeciwko Korupcji (GRECO) jako instrument oddziaływania Rady Europy na zwalczanie korupcji,* [w:] *Europejski system ochrony praw człowieka. Inspiracja uniwersalna – uwarunkowania kulturowe –*

bariery realizacyjne, red. J. Jaskiernia, K. Spryszak, tom III, Wydawnictwo Adam Marszałek, Toruń 2016.

- Paruch S.A., *Czynniki wpływające na skuteczność systemu instytucjonalnego ochrony praw człowieka w Radzie Europy,* [w:] *Ochrona praw człowieka w Europie. Aksjologia – instytucje – nowe wyzwania – praktyka,* red. J. Jaskiernia, K. Spryszak, tom III, Wydawnictwo Adam Marszałek, Toruń 2017.
- Patoglou D., Dunkerley F., Patil S., Robinson N., *Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study*, "Computers in Human Behavior", 2017, vol. 75
- Pelewicz R., *Ujawnianie danych osobowych zarejestrowanych w systemie dozoru elektronicznego w kontekście konstytucyjnych i międzynarodowych gwaranci ochrony życia prywatnego,* [w:] *Efektywność europejskiego systemu ochrony praw człowieka. Obszary analizy skuteczności europejskiego systemu ochrony praw człowieka,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2012.
- Phua C., *Protecting organisations from personal data breaches*, "Computer Fraud & Security", 2009, nr 1.
- Pieńczykowski M., *Ochrona danych osobowych jako negatywna przesłanka udostępniania informacji publicznej*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2018, nr 2.
- Pittiglio R., F. Reganati, F. Ricci, C. Tedeshi, [w:] *The Palgrave Handbook of Corporate Sustainability in the Digital Era*, Springer International Publishing, Cham 2020.
- Pizzetti F., *Europejska ochrona danych osobowych,* „Zeszyty Naukowe USz Praw." 2010, nr 22.
- Pliżys J., *Zarządzanie ochroną informacji w systemach zarządzania kryzysowego,* „DOCTRINA. Studia Społeczno-Polityczne" 2010, nr 7.
- Poboży M., *Obywatelstwo i obywatelskość w Unii Europejskiej,* „Przegląd Europejski" 2014, nr 1.
- Podgórski B., *Rada Europy w procesie integracji europejskiej,* [w:] *Efektywność europejskiego systemu ochrony praw człowieka. Efektywność mechanizmów*

ochrony praw człowieka Rady Europy, Unii Europejskiej i OBWE, red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2012.

- Polyakova E.N., Filonova O.I., Prokofjev K.G., Sutiagin S.A., *Ensuring the information security of personal data when submitting electronic appeals to the public authorities*, "Journal of physics. Conference series", 2019, vol. 1210.
- Pozzato V., *2014 Opinion of the European Data Protection Supervisor: Interplay Between Data Protection and Competition Law,* "Journal of European Competition Law & Practice" 2014, Vol. 5.
- Przyborowska-Klimczak A., *Prawne aspekty integracji europejskiej – rys historyczny,* [w:] *Prawo Unii Europejskiej. Zagadnienia systemowe,* red. J. Barcz, Wydawnictwo Prawio i Praktyka Gospodarcza, Warszawa 2002.
- Pshehotskaya E., *Theft Preventive Measures for Interconnected Personal Computer Devices as Proactive Physical Security of Data*, "International Journal of Embedded and Real-Time Communication Systems (IJERTCS)", 2018, nr 2.
- Purtova N., *Private Law Solutions in European Data Protection,* "Netherlands Quarterly of Human Rights" 2010, No. 28.
- Raman J., *European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland, no. 20511/03, 17 July 2008*, "The Computer Law and Security Report", 2008, nr 6.
- Rejmus M., *Zadania Prezesa Urzędu Regulacji Energetyki a polityka energetyczna państwa,* „Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza" 2014, nr 3.
- Regner Ł., *Aktualne problemy i wyzwania w obszarze jawności działania administracji publicznej oraz kierunki dalszego kształtowania modelu*, [w:] *Stulecie polskiej administracji. Doświadczenia i perspektywy*, red. W. Federczyk, Krajowa Szkoła Administracji Publicznej, Warszawa 2018.
- Robel J., *Kongres Władz Lokalnych i Regionalnych Europy na straży europejskiej samorządności terytorialnej,* „Zeszyty Naukowe Instytutu Administracji AJD w Częstochowie, Gubernaculum et Administration" 2016, nr 2.

- 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, nr 4.
- Romkowski A., *Przepisy karne ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. w kontekście standardów ochrony danych osobowych w rozporządzeniu GOPR (RODO) z dnia 27 kwietnia 2016 r.,* „Przegląd Prawno – Ekonomiczny" 2018, nr 1.
- Rotmans J., Kemp R., van Asselt M., *More Evolution than Revolution: Transition Management in Public Policy,* "Foresight" 2001, No. 1.
- Rzucidło J., Węgrzyn J., *Wybrane problemy ochrony danych dotyczących zdrowia pacjenta w kontekście ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz RODO*, [w:] *Dookoła Wojtek... Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Presinerowi,* red. R. Balicki, M. Jabłoński., Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2018.
- Ryter J., Ryter E., *Rejestr sprawców przestępstw na tle seksualnym a prawo do prywatności i prawo do bycia zapomnianym w świetle ogólnego rozporządzenia o ochronie danych osobowych (RODO), dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27.04.2016 r. oraz innych ustaw*, „Probacja" 2018, nr 4.
- Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym,* „Państwo i Prawo" 2002, nr 6.
- Schultz E., *Security views: security breaches threaten personal and financial data*, "Computers & Security", 2004, nr 4.
- Siegel K.M., *Protecting the most valuable corporate asset: electronic data, identity theft, personal information, and the role of data security in the information age*, "Penn State law review", 2007, nr 3.
- Sieńczyło-Chlabicz J., *Wkład Rady Europy w tworzenie i kodyfikację norm prawa międzynarodowego,* „Białostockie Studia Prawnicze" 1994, nr 2.
- Sierpowska I., *Bezpieczeństwo socjalne jako dobro publiczne,* „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2015, nr 16.

- Skoczkowski T., *Zrównoważona polityka energetyczna,* „Przegląd Komunalny" 2004, nr 3.
- Skoczylas D., *Przetwarzanie danych osobowych a prawo do bycia zapomnianym i prawo do przenoszenia danych na gruncie RODO*, „Acta Iuris Stetinensis" 2018, nr 4.
- Sobczak J., *Ochrona danych osobowych – standardy unijne i rzeczywistość polska,* [w:] *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka,* red. J. Jaskiernia, t. 2, Wydawnictwo Sejmowe, Warszawa 2013.
- Sobczyk P., *Ochrona danych osobowych jako element prawa do prywatności,* „Zeszyty Prawnicze UKSW" 2009, nr 9.
- Soluamni A., Alti A., Laouamer L., *A Blind Image Watermarking Method for Personal Medical Data Security*, [w:] 2019 International Conference on Networking and Advanced Systems (ICNAS), 2019.
- Spryszak K., *Wpływ Rady Europy na transformację prawnokonstytucyjną na Węgrzech,* [w:] *Ochrona praw człowieka w Europie. Aksjologia – instytucje – nowe wyzwania – praktyka,* red. J. Jaskiernia, K. Spryszak, t. III, Wydawnictwo Adam Marszałek, Toruń 2017.
- Stegen J.G., *The Parliamentary Assembly of the Council of Europe and its Relations with Central and Eastern Europe,* [w:] *Working Paper on Comparative Legislative Studies,* red. L.D. Longley, Appleton 1994.
- Strzyżakowska Z., *Bezpieczeństwo i ochrona informacji,* „Pomiary, Automatyka, Kontrola" 2005, nr 4.
- Szałowski R., *Data protection officer in the light of the provisions of the general data protection regulation (GDPR)*, "Ius Novum "2018, nr 4.
- Szczepańska-Kulik I., *W sprawie problematyki prawa do informacji publicznej w kontekście przepisów rozporządzenia o ochronie danych osobowych*, „Przegląd Sejmowy" 2018, nr 5.
- Szubrycht T., *Współczesne aspekty bezpieczeństwa państwa,* „Zeszyty Naukowe Akademii Marynarki Wojennej im. Bohaterów Westerplatte" 2006, nr 4.
- Szumski O., *Ochrona danych osobowych w społeczeństwie informacyjnym,* „Acta Universitatis. Lodziensis. Folia Oeconomia" 2007, t. 2.

- Szustakiewicz P., *Pozycja prawna Prezesa Urzędu Ochrony Danych Osobowych - ustrój i kompetencje polskiego organu nadzoru*, „Kontrola Państwowa" 2018, nr 6.
- Szymańska J., *Reformy na jubileusz: Unia Europejska w 50. i 60. rocznicę podpisania traktatów rzymskich,* „Sprawy Międzynarodowe" 2017, nr 4.
- Szymczyk Ł., *Wszedł w życie Traktat Amsterdamski,* „Wspólnoty Europejskie" 1999, nr 5.
- Szymczyk-Madej K., Madej J., *Bezpieczeństwo informatycznych systemów rachunkowości,* „Zeszyty Naukowe/Akademia Ekonomiczna w Krakowie" 2000, nr 553.
- Szymczyk P., *Bezpieczeństwo systemów i sieci komputerowych,* „Automatyka/Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie" 2003, z. 1-2.
- Szwed K., *Inspektorat Ochrony Danych Osobowych*, [w:] *Ustrój państwowy Republiki Estonii*, red. S. Sagan, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2018.
- Świeboda H., Stobiecki P., *Bezpieczeństwo urządzeń mobilnych w przestrzeni cyfrowej*, „Przegląd Policyjny" 2018, nr 4.
- Świtalski P.A., *Miejsce Rady Europy w Europejskiej architekturze instytucjonalnej,* [w:] *Sześćdziesiąt lat Rady Europy. Tworzenie i stosowanie standardów prawnych,* red. H. Machińska, Oficyna Prawa Polskiego, Warszawa 2009.
- Świtalski P.A., *Rola Rady Europy w systemie organizacji międzynarodowych,* [w:] *Rada Europy a przemiany demokratyczne w państwach Europy Środkowej i Wschodniej w latach 1989-2009,* red. J. Jaskiernia, Wydawnictwo Adam Marszałek, Toruń 2010.
- Tabrez A., *Technology Convergence and Protection of Data Privacy: Human Rights, Democracy Issues and Judical Responses in USA, European Union and India,* "University of Petroleum and Energy Studies (UPES) – College of Legal Studies" 2009, źródło: www.papers.ssrn.com/sol3/papers.cfm?abstract_id=1480718, data dostępu: 18.07.2018.
- Thomson J., *The Right to Privacy,* "Philosophy and Public Affairs" 1975, t. 4.

- Tomkiewicz M., *Sądowa kontrola pozyskiwania danych telekomunikacyjnych, internetowych i pocztowych*, „Państwo i Prawo" 2018, nr 4.
- Tor K., *Wybrane zagadnienia prawnej ochrony danych osobowych w działalności przedsiębiorstwa,* „Zeszyty Naukowe/Akademia Ekonomiczna w Krakowie" 2004, nr 657.
- Tran E., Atkinson M., *Security of personal data across national borders,* "Information Management & Computer Security" 2002, Vol. 10.
- Trela-Smalarz A., *Dostęp do informacji o ochronie środowiska*, „Przegląd Prawa Publicznego" 2018, nr 1.
- Tylec G., *Monitoring wizyjny jako ingerencja w sferę dóbr osobistych*, „Przegląd Prawno-Ekonomiczny" 2018, nr 2.
- Yildrim E.Y., Adali E., *The threats and risks in personal data security*, [w:] 2017 International Conference on Computer Science and Engineering (UBMK), 2017.
- Vlad I.M., *Security of Personal Data in Social Networks*, "International Journal of Information Security and Cybercrime (IJISC)", 2018, nr 2.
- Waligórski M.A., *Polityka energetyczna państwa jako sektorowa polityka administracyjna,* „Biuletyn Urzędu Regulacji Energetyki" 2008, nr 4.
- Warren S.D., Brandeis L.D., *The Right to Privacy,* "Harvard Law Review" 1890, vol. 4.
- Wącior J., *Zniesienie kontroli granicznych a bezpieczeństwo: System Informacyjny Schengen,* „Zeszyty Naukowe AON" 2010, nr 3.
- Wierzbicka A., *Ochrona danych osobowych w publicznych zakładach opieki zdrowotnej w Polsce,* „Przedsiębiorczość i Zarządzanie" 2014, z. 9.
- Wiewiórowski A. Nowe ramy ochrony danych osobowych w Unii Europejskiej, dodatek „MoP" 2012, nr 7
- Winkler H., *Democracy and human Rights – a Survey of the Admission Practice of the Council of Europe*, "Austrian Journal of Public and International Law" 1995, t. 47.
- Wojciechowski Ł., *Bezpieczeństwo informacji i ochrona danych osobowych jako polityka publiczna – analiza wprowadzania mechanizmów i uregulowań prawnych,* „Polityka i Społeczeństwo" 2016, nr 4.

- Wojarnik G., *Bezpieczeństwo przetwarzania danych w modelu cloud computing: uwarunkowania w kontekście ochrony danych osobowych w warunkach prawa polskiego,* „Zeszyty Naukowe. Studia Informatica/Uniwersytet Szczeciński" 2013, nr 33.
- Wojnowska-Radzińska J., *Obywatelstwo Unii Europejskiej,* „Studia BAS" 2015, nr 4.
- Wolny W., Sadecki B., *Bezpieczeństwo danych w systemach ERP,* „Prace Naukowe/Akademia Ekonomiczna w Katowicach" 2009, t. 1.
- Wolska-Bagińska A., *Ochrona danych osobowych a cele procesu karnego*, „Palestra" 2018, nr 7-8.
- Wolters P.T.J., *The Security of Personal Data under the GDPR: a harmonized duty or a shared responsibility?,* „International Data Privacy Law" 2017, nr 3.
- Wolters R., Trakman L., Zeller B., *Personal Data and Cybersecurity*, "Data Protection Law", 5 September 2019.
- Woszczyk M., *Bezpieczeństwo dostaw energii elektrycznej – stan obecny i podstawowe wyzwania,* [w:] *W kierunku nowoczesnej polityki energetycznej. Energia elektryczna,* red. M. Swora, Instytut Obywatelski, Warszawa 2011.
- Wrzesiński P., *Bariery prawne rozwoju cyfrowych kanałów dystrybucji w działalności zakładów ubezpieczeń w Polsce*, „Prawo Asekuracyjne" 2019, nr 2.
- Wrześniewska-Wal I., Janiszewska L., *Prywatność pacjenta jako dobro osobiste. Nowe wyzwania w świetle regulacji RODO*, „Studia Prawnoustrojowe" 2019, nr 43.
- Wyrozumska A. *Protokół w sprawie stosowania Karty Praw Podstawowych Unii Europejskiej w stosunku do Polski i Zjednoczonego Królestwa,* [w:] *Ochrona Praw Podstawowych w Unii Europejskiej,* red. J. Barcz, Wydawnictwo C.H. Beck, Warszawa 2008.
- Zadrożny M., *Reorganizacja systemu ochrony danych,* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018.
- Zadrożny M., *Środki ochrony prawnej* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29,*

ustawy o ochronie danych osobowych z 2018 r., red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018.

- Zadrożny M., *Uprawnienia organu nadzorczego,* [w:] *Unijna reforma ochrony danych osobowych. RODO w praktyce z uwzględnieniem: wytycznych GR Art. 29, ustawy o ochronie danych osobowych z 2018 r.,* red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, wyd. 2, Warszawa 2018.
- Zając P., *RODO a Kościół Katolicki w Polsce. Określenie zakresu działalności Unii Europejskiej*, „Biuletyn - Stowarzyszenie Kanonistów Polskich" 2018, nr 31.
- Zalewski D., *Bezpieczeństwo społeczne i socjalne – kontrowersje wokół pojęć,* „Polityka Społeczna" 2016, nr 10.
- Zalewski S., *Strategia jako instrument bezpieczeństwa politycznego państwa,* „DOCTRINA Studia Społeczno-Polityczne" 2009, nr 6.
- Zalozhnev A.Y., Andros D.A., Ginz V.N., Loktionov A.E., *Information Systems and Network Technologies for Personal Data Cyber Security in Public Health*, [w:] 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019.
- Zeidler K., *W sprawie genezy, dynamiki i charakterystyki współczesnych konfliktów zbrojnych,* „Międzynarodowe Prawo Humanitarne" 2010, t. 1.
- Zharova A.K., V.M. Elin, *The use of Big Data: A Russian perspective of personal data security*, "The Computer Law and Security Report", 2017-08, nr 4.
- Zubik M., Podkowik J., Rybski R., *Prywatność. Wolność u progu D-day*, „Gdańskie Studia Prawnicze" 2018, t. XL.

Netografia

- *Accession to the EU,* źródło: www.ec.europa.eu/neighbourhood-enlargement/policy/glossary/terms/accessior, data dostępu: 16.05.2019.
- Adamski A., Redo S., *Globalna wioska i gminna rzeczywistość. Ochrona danych osobowych a rządy prawa,* „Rzeczpospolita" 1996, nr 160.

- *Amendments to Convention 108,* źródło: www.coe.int/en/web/data-protection/convention108/amendments, data dostępu: 13.09.2018.
- *A New Swiss – U.S. Privacy Shield Replaces the U.S. – Swiss Safe Harbor,* źródło: www.jonesday.com/en/insights/2017/01/a-new-swissus-privacy-shield-replaces-the-usswiss-safe-harbor, data dostępu: 07.01.2020.
- *Baza wiedzy RODO,* źródło: www.gov.pl/web/cyfryzacja/baza-wiedzy-rodo, data dostępu: 08.01.2020.
- *Belgian and German data protection authorities cooperate on Mastercard's data,* źródło: www.data protectionauthority.be/news, data dostępu: 08.01.2020.
- Borowska A., *Czym jest incydent w ochronie danych osobowych?,* źródło: www.poradnikprzedsiębiorcy.pl/-incydent-w-ochronie-danych-osobowych, data dostępu: 18.07.2018.
- *Brexit. Wielka Brytania i UE osiagnęły porozumienie w sprawie umowy handlowej*, https://www.bankier.pl/wiadomosc/Brexit-Wielka-Brytania-i-UE-osiagnely-porozumienie-ws-umowy-handlowej-8026891.html, data dostępu: 27.1.2020.
- *Case – law overview,* źródło: www.eds.europa.eu/data -protection/eu-institutions-dpo/case-law-guidance_en, data dostępu: 23.04.2019.
- *Congress of Europe,* The Hague, 7-11 May 1948, Council of Europe Publishing, Strasbourg 1999.
- *Consultative Committee,* źródło: www.coe.int/web/data-protection/consultative-committee-tpd, data dostępu: 13.09.2018.
- *Coraz więcej kar za RODO w Unii Europejskiej*, źródło: https://ictmarketexperts.com/aktualnosci/coraz-wiecej-kar-za-rodo-w-unii-europejskiej/, data dostępu: 26.12.2020.
- *Co to jest RODO i jakie zmiany wprowadza ustawa*, https://www.pwc.pl/pl/artykuly/co-to-jest-rodo-i-jakie-zmiany-wprowadza-ustawa.html, data dostępu: 26.12.2020.
- *Council of Europe, Data Protection Day,* źródło: www.coe.int/t/dghl/standardsetting/dataprotection/Data, data dostępu: 12.09.2018.

- *Council of Europe Discusses Amendments to Convention 108,* źródło: www.personaldata.ge/en/strasburgshi-108-e-konventsiashi-shesat-tsvlilbebze-msdjelebon/610, data dostępu: 13.09.2018.
- *Council of Europe modernises Convention 108,* źródło: www.privacylaws.com/Publications/enews/International=E-news-Dates/2018/5/Council-of-Europe-modernises-Convention-108/, data dostępu: 14.09.2018.
- *Council of Europe issues recommendation on health – related data,* źródło: www.insideprivacy.com/uncategorized/council-of-europe-issues-resommendation-on-health-related-data, data dostępu: 03.01.2020.
- *Croatia is the Second country to ratify Convention 108+,* źródło: www.coe.int/en/web/data-protection/-/croatia-is-the -second-country-to-ratify-convention-108, data dostępu: 03.01.2020.
- *Czego dotyczy ogólne rozporządzenie o ochronie danych (RODO)?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pl, data dpstpu: 26.12.2020.
- *Czym jest RODO i jakie zmiany wprowadza nowa ustawa Parlamentu Europejskiego*, https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-rodo-i-jakie-zmiany-wprowadza-nowa-ustawa-parlamentu-europejskiego, data dostępu: 26.12.2020.
- *Data Protection,* źródło: www.edps.europa.eu/data-protection_en, data dostępu: 08.01.2020.
- *Data Protection Enforcement in Belgium,* źródło: www.globalcompliancenews.com/data-privacy/data-protection-enforcement-in-belgium/&prev=search, data dostępu: 08.01.2020.
- *Denmark: Data Protection 2019,* źródło: www.iclg.com/practice-areas/data-protection-laws-and-regulations/denmark, data dostępu: 09.01.2020.
- *Energetyka - charakterystyka podstawowa (autor – zespół),* źródło: www.ure.gov.pl/download.php?s=1&d=710, data dostępu: 16.07.2018.
- *European Data Protection Supervisor,* źródło: www.eds.europa.eu/data -protection/eu-institutions-dpo/case-law-guidance_en, data dostępu: 23.04.2019.

- *European Data Protection Board,* źródło: www.ec.europa.eu/info/law-topic/data-protection/, data dostępu: 24.04.2019.
- *Europejski Inspektor Ochrony Danych (EIOD),* źródło: www.europa.eu>european-data-protection-supervisor.pl, data dostępu: 08.01.2020.
- *EU Member States to ratify Convention 108+,* źródło: www.coe.int/en/web/data-protection/-/eu-member-states-to-ratify-convention-108-, data dostępu: 03.01.2020.
- *EU contracts with Microsoft raising 'serious' data concerns, says watchdog,* źródło: www.techcrunch.com/2019/10/21/eu-contracts-with-microsoft-raising-serious, data dostępu: 09.01.2019.
- *First ratification of Convention 108+ Congratulations Bulgaria,* źródło: www.coe.int/en/web/data-protection/-/first-ratification-of-convention-108-congratulations-bulgaria, data dostępu: 03.01.2020.
- *First GDPR fine in Portugal Issues against hospital for three violations,* źródło: www.iapp.org/news/a /first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations, data dostępu: 09.01.2020.
- *GDPR Guide to National Implementation: Austria. A practical guide to national GDPR compliance requirements across the EEA,* źródło: www.whitecase.com/publications/article/gdpr-guide-national-implementation, data dostępu: 09.01.2020.
- *GIODO: instytucje socjalne muszą szczególnie dbać o dane osobowe,* źródło: www.lex.pl/czytaj/-/artykul/giodo-instytucje-socjalne-musza-szczegolnie-dbac-o-dane-osobowe, data dostępu: 17.07.2018.
- Glen P., *Ochrona danych osobowych w pomocy społecznej. Co musisz wiedzieć?,* www.pomocspoleczna24.pl/nr-1/ochrona-danych-osobowych-w-pomocy-spolecznej-co-musisz-wiedziec-55.html, data dostępu: 17.07.2018.
- Greser J., *Nowe zasady ochrony danych osobowych. Analiza ryzyka,* źródło: www.poradnik.ngo.pl/wiadomości/2158375.html, data dostępu: 18.07.2018.
- *Guide to the reparation of contractual clauses governing data protection the transfer of personal data to third not bound by an adequate level of data protection (2002),* Prepared by the Consultative Committee of the Convention

for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) in 2002, źródło: www.rm.coe.int/168068416c, data dostępu: 26.07.2019.

- *Handbook on European Data Protection Law – 2018 edition,* Publications Office of the European Union, Luxembourg 2018.
- *Historia danych osobowych,* źródło: www.ochronainformacji.com.pl/historia-danych-osobowych, data dostępu: 26.06.2018.
- Hodge N., *GDPR enforcement varies widely by country,* źródło: www.complianceweek.com/gdpr-enforcement-varies-widely-by-country, data dostępu: 31.12.2019.
- *Hungarian to the National Authority for Data Protection and Freedom of Information,* źródło: www.naih.hu/general-information.html, data dostępu: 08.01.2020.
- Irwin L., *How to write a GDPR data protection policy – with template examples,* źródło: www.itgovernance.co.uk, data dostępu: 07.01.2020.
- Kawecki M., *Wdrażanie ogólnego rozporządzenia unijnego do polskiego porządku prawnego a techniczne aspect zabezpieczenia danych osobowych – wystąpienie Macieja Kaweckiego,* źródło: www.gov.pl/web/cyfryzacja/wdrazanie-ogolnego-rozporzadzenia-unijnego-do-polskiego-porzadku-prawnego-a-techniczne-aspekty-bezieczenstwa-danych-osobowych, data dostępu: 21.12.2019.
- *LaLiga fined EUR 250, 000 for using smartphone microphones to detect illegal feeds,* źródło: www.telecompaper.com/news/la-liga-fined-eur-250000-for-using-smartphone-microphones-to-detect-illegal-feeds-1296384, data dostępu: 09.01.2020.
- Madecki M, *Transfer danych osobowych – rekomendacje Europejskiej Rady Ochrony Danych po wyroku Schrems II*, https://rodoradar.pl/transfer-danych-osobowych-rekomendacje-europejskiej-rady-ochrony-danych-po-wyroku-schrems-ii/, data dostępu: 28.12.2020.
- Majczak K., *RODO rok od stosowania nowych przepisów,* źródło: www.rp.pl/Firma.306039975-RODO-rok-od-stosowania-nowych-przepisow-html, data dostępu: 21.12.2019.

- Maroszek W., *RODO czyli ochrona danych 2.0. Nowe unijne przepisy oznaczają trudności dla przedsiębiorców*, https://businessinsider.com.pl/firmy/przepisy/rodo-gdpr-regulacje-o-ochronie-danych-osobowych-zmiany-w-firmach/21p6svs, data dostępu: 26.12.2020.
- *New Technologies: a challenge to Privacy Protection?*, Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1989, źródło: www.coe.int/en/web/data-protection/reports-studies-and-opinions, data dostępu: 26.07.2019.
- *New EDPS mandate 2019 – 2024,* źródło: www.edps.europa.eu, data dostępu: 09.01.2019.
- *Ochrona danych osobowych,* źródło: www.europarl.eu/factsheet/pl/sheet/157/ochrona-danych-osobowych, data dostępu: 08.02.2019.
- *Ochrona danych w UE,* https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pl, data dostępu: 26.12.2020.
- *Ochrona danych osobowych w przypadku ich wykorzystywania przez Policję i organy wymiaru sprawiedliwości (od 2018),* źródło: www.eur-lex.eu/legal-content/PL/ALL/?uri=uriserv:310401_3, data dostępu: 08.02.2019.
- *Opinions and Recommendations,* źródło: *European Data Protection Supervisor,* źródło: www.eds.europa.eu/data -protection/eu-institutions-dpo/case-law-guidance_en, data dostępu: 23.04.2019.
- *Po co nam RODO, czyli jak będą chronione nasze dane osobowe i co nam dają unijne regulacje*, https://portal.librus.pl/artykuly/po-co-nam-rodo-czyli-jak-beda-chronione-nasze-dane-osobowe-i-co-nam-daja-unijne-regulacje, data dostępu: 26.12.2020.
- Polanowski A., *Brixit a ochrona danych osobowych. Jak wystąpienie Wielkiej Brytanii z Unii Europejskiej wpłynie na polskich przedsiębiorców?*, https://www.parp.gov.pl/component/content/article/64651:brexit-a-ochrona-danych-osobowych-jak-wystapienie-wielkiej-brytanii-z-unii-europejskiej-wplynie-na-polskich-przedsiebiorcow, data dostępu: 26.12.2020.

- *Prezes Urzędu Ochrony Danych Osobowych,* źródło: www.uodo.gov.pl/pl/preses-i-urzad, data dostępu: 08.01.2020.
- *Protection of Personal Data and Privacy,* źródło: www.coe.int/en/web/portal/personal-data-protection-and-privacy?deskopt, data dostępu: 13.09.2018.
- *Pseudonimizacji danych,* źródło: www.odo24.pl/blog-post.pseudonimizacja-anonimizacja-danych-wyjasniamy-pojecie, data dostępu: 21.12.2019.
- Raczek K., *Przetwarzanie danych w USA jest niezgodne z RODO*, https://itwiz.pl/tsue-przetwarzanie-danych-usa-jest-niezgodne-rodo/, data dostępu: 26.12.2020.
- *Raising Awareness Activities 2017 – 2019,* źródło: www.azop.hr/data-protection-agency, data dostępu: 08.01.2020.
- *Reforma unijnych przepisów o ochronie danych w 2018 roku,* źródło: www.ec.europa.eu/commission/priorites/justice-and-fundamental-rights/data -protection/2018-reform-eu-data-protection-rules_pl, data dostępu: 06.03.2019.
- *RODO i przepisy danych osobowych na świecie,* źródło: źródło: *https://www.dnvgl.pl/article/rodo-i-przepisy-o-ochronie-danych-osobowych-na-swiecie-161457*, data dostępu: 26.12.2020.
- *RODO jednak chroni,* źródło: www.ec.europa.eu/poland/news/190724_RODO_pl, data dostępu: 21.12.2019.
- *RODO – rozporządzenie o ochronie danych osobowych*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/topics/RODO-ochrona-danych-osobowych.html, data dostępu: 26.12.2020.
- Roguska E., *Systemy ochrony danych osobowych w Unii Europejskiej i Stanach Zjednoczonych*, źródło: https://www.temidium.pl/artykul/systemy_ochrony_danych_osobowych_w_unii _europejskiej_i_stanach_zjednoczonych-5398.html, data dostępu: 26.12.2020.
- Romanowicz M., *Ochrona danych osobowych – ważny komunikat Komisji Europejskiej,* źródło: www.portalmorski.pl/prawo-polityka/38479-ochrona-danych-osobowych-wazny-komunikat-komisji-europejskiej-, data dostępu: 23.04.2019.

- Sobczak K., *KE ponagla państwa ws wdrożenia RODO,* źródło: www.prawo.pl/prawnicy-sady/ke-ponagla-panstwa-ws-wdrazania-rodo,73668.html, data dostępu: 21.12.2019.
- Staśkiewicz J., *Wymogi dla systemów informatycznych w RODO,* źródło: www.opensecurity.pl/wymogi-dla-systemow-informatycznych-rodo/, data dostępu: 17.07.2018.
- *The Bulgarian Commission for Personal Data Protection,* źródło: www.privacyconference2018.org/en/about/bulgarian-commission-personal-data-protection.html&prev, data dostępu: 08.01.2020.
- *The Data Protection Commission,* źródło: www.dataprotection.ie, data dostępu: 08.01.2020.
- *The introduction and use of personal identification numbers: the data Protection Issues (1991),* Study prepeared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1991, źródło: www.rm.coe.int/16806845b3, data dostępu: 26.07.2019.
- *Transfer danych osobowych poza terytorium Unii Europejskiej*, https://poradnikprzedsiebiorcy.pl/-rodo-transfer-danych-osobowych-poza-terytorium-unii-europejskiej, data dostępu: 26.12.2020.
- *Uber fines E600, 000 in the Netherlands,* źródło: www.cloudprivacycheck.eu, data dostępu: 09.01.2020.
- *Vade-mecum on the Committee of Ministers monitoring Procedure,* Document prepared by the Secretary General's Monitoring Unit, Strasbourg – 1 March 1999.
- *Walka z terroryzmem i ochrona danych osobowych,* źródło: www.europarl.europa.eu/sides/getDoc/do?pubRef=-//EP//TEXT+IM-PRESS+20080901BRI35769+ITEM-003-PL+DOC+XML+VO//PL&language+PL, data dostępu: 16.07.2018.
- Walther A., *Protection Privacy also Means Preserving Democracy,* źródło: www.phys.org/news/2014-09-privacy-democracy.html, data dostępu: 18.07.2018.

- *What are Data Protection Authorities (DPAs)?,* źródło: www.europa.eu/info/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en&prev=search, data dostępu: 08.01.2020.
- *Wojciech Wiewiórowski mianowany Europejskim Inspektorem Ochrony Danych Osobowych*, https://www.consilium.europa.eu/pl/press/press-releases/2019/12/05/wojciech-wiewiorowski-appointed-european-data-protection-supervisor/#, data dostępu: 26.12.2020.
- Woolen R., *GDPR Compliance – The Fines Have Begun,* źródło: www.infogoto.com/gdpr-compliance-the-fines-have-begun, data dostępu: 09.01.2020.
- Wystąpienie posła M. Lewandowskiego na 112. posiedzeniu Sejmu w dniu 30 lipca 1997 r., przedstawiającego sprawozdanie Komisji Administracji i Spraw Wewnętrznych, Komisji Sprawiedliwości i Praw Człowieka oraz Komisji Ustawodawczej o poselskim oraz rządowym projektach ustaw o ochronie danych osobowych (*Sprawozdanie Stenograficzne).*
- Zajdler R., *Ochrona danych osobowych a systemy inteligentnych sieci,* Biuletyn URE, źródło: www.wnp.pl/wiadomosci/ochrona-danych-osobowych-a-systemy-inteligentnych-sieci,-6589_1_0.html, data dostępu: 17.07.2018.
- Zygmunt M., *RODO w Polsce i innych krajach członkowskich. Różnice w podejściu do wdrożenia,* źródło: www.bezowijania.com/rodo-w-polsce-i-innych-krajach-czlonkowskcih-roznice-w -podejsciu-do-wdrozenia, data dostępu: 21.12.2019.
- Zygmunt-Jakuć M., *RODO w Polsce i w innych krajach członkowskich. Różnice w podejściu do wdrożenia*, https://bezowijania.com/rodo-w-polsce-i-innych-krajach-czlonkowskich-roznice-w-podejsciu-do-wdrozenia, data dostępu: 26.12.2020.
- W. Żółcińska W., *RODO – ranking kar*, https://www.computerworld.pl/news/RODO-ranking-kar,422090.html, data dostępu: 26.12.2020.

Strony internetowe

- www.coe.int – Strona internetowa Rady Europy
- www.eds.europa.eu – Europejski Inspektor Ochrony Danych
- www.europarl.europa.eu – Strona internetowa Parlamentu Europejskiego
- www.gov.pl – Serwis Rzeczypospolitej Polskiej
- www.ochronainformacji.com.pl – Strona internetowa firmy „AGABOR" zajmującej się ochroną danych osobowych
- www.privacycommission.be – Komisja ochrony prywatności (Belgia)
- www.uodo.gov.pl – Urząd Ochrony Danych Osobowych