PRAWO DO OCHRONY DANYCH OSOBOWYCH

REDAKCJA
MIKOŁAJ BRZÓSTOWICZ

TOM III

INTERDYSCYPLINARNE FORUM OCHRONY DANYCH OSOBOWYCH

ARCHAEGRAPH
Wydawnictwo Naukowe

PRAWO DO OCHRONY DANYCH OSOBOWYCH

Tom III

Redakcja
Mikołaj Brzóstowicz

PRAWO DO OCHRONY DANYCH OSOBOWYCH

REDAKCJA
MIKOŁAJ BRZÓSTOWICZ

TOM III

INTERDYSCYPLINARNE FORUM OCHRONY DANYCH OSOBOWYCH

ARCHAEGRAPH
Wydawnictwo Naukowe

Redakcja
Mikołaj Brzóstowicz

Recenzja naukowa
dr hab. Agnieszka Laskowska-Hulisz, prof. UMK
dr hab. Mariusz Krzysztofek, prof. AKP
dr Maria Jędrzejczak
dr Damian Kaczan
dr Julia Kapelańska-Pręgowska
dr Karol Kosiński
dr Krzysztof Kucharski
dr Paweł Litwiński
dr Dominika Skoczylas
dr Dominika Zawadzka-Klonowska

Korekta, skład i projekt okładki
Karol Łukomiak

ISBN: 978-83-68410-86-0

Wersja elektroniczna dostępna na stronie internetowej wydawcy:
www.archaegraph.pl

ARCHAEGRAPH
Wydawnictwo Naukowe

ŁÓDŹ-STAROWA GÓRA, CZERWIEC 2026

SPIS TREŚCI

OD REDAKCJI

Trzeci tom monografii „Prawo do ochrony danych osobowych" oddaję do rąk Czytelnika w momencie, w którym europejski i krajowy system ochrony danych osobowych wkracza w fazę głębokiej rekonfiguracji. Od wejścia w życie ogólnego rozporządzenia o ochronie danych („RODO") minęło już blisko osiem lat, a praktyka jego stosowania – wzbogacona o orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, decyzje organów nadzorczych oraz dorobek doktrynalny – ujawnia obszary, w których pierwotne instrumenty ochrony okazują się niewystarczające wobec dynamiki rozwoju technologicznego. Równolegle prawodawca unijny buduje wokół RODO gęstą siatkę aktów uzupełniających: akt w sprawie sztucznej inteligencji, akt o danych, akt o zarządzaniu danymi, rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia, a także dyrektywę NIS 2. Każdy z tych aktów wchodzi w interakcję z RODO, niekiedy dopełniając jego mechanizmy, a niekiedy stawiając przed administratorami i procesorami danych pytania, na które brakuje jednoznacznych odpowiedzi.

Niniejszy tom stanowi próbę zmierzenia się z najistotniejszymi z tych pytań. Zgromadzone w nim opracowania przedstawicieli młodszego pokolenia naukowców łączy przekonanie, że ochrona danych osobowych nie może być analizowana w izolacji od kontekstu sektorowego, w którym dane są przetwarzane. Stąd też w układzie monografii obok rozważań o charakterze ogólnym znalazły się studia poświęcone konkretnym dziedzinom, w których problematyka przetwarzania danych nabiera szczególnego znaczenia praktycznego.

Znaczącą część tomu zajmują opracowania dotyczące tych obszarów, w których ochrona danych osobowych pozostaje w napięciu z innymi wartościami chronionymi prawnie. Autorzy podejmują problematykę transgranicznych transferów danych pomiędzy Unią Europejską a Stanami Zjednoczonymi – ze szczególnym uwzględnieniem ram *Data Privacy Framework*, amerykańskich regulacji stanowych oraz zjawiska hybrydowej adekwatności – jak również zagadnienie danych jako

aktywa przedsiębiorstwa, w którym krzyżują się przepisy RODO, art. 55^1 Kodeksu cywilnego oraz prawo *sui generis* do baz danych. Ten ostatni nurt rozważań prowadzi do pytania o granice komercjalizacji zanonimizowanych zbiorów danych, a tym samym do napięcia pomiędzy ochroną osoby, której dane dotyczą, a swobodą obrotu gospodarczego.

Odrębny krąg zagadnień tworzą studia poświęcone wybranym dziedzinom zawodowym i sektorowym. Czytelnik znajdzie w tomie rozważania o statusie notariusza jako administratora danych osobowych – z konfrontacją przepisów Prawa o notariacie z reżimem RODO, w szczególności z jego art. 6 i 9 – a także analizy dotyczące ochrony danych w edukacji cyfrowej, której pandemia COVID-19 oraz upowszechnienie narzędzi opartych na sztucznej inteligencji nadały zupełnie nowy wymiar. W tym kontekście pojawiają się m.in. zagadnienia proctoringu, ochrony danych dzieci oraz wpływu AI Act na praktykę edukacyjną. Osobny głos w tomie zabierają autorzy podejmujący problematykę ochrony danych sportowców w sprawach dopingowych, osadzając ją w kontekście Światowego Kodeksu Antydopingowego oraz najnowszego orzecznictwa Trybunału Sprawiedliwości – w szczególności w sprawach C-115/22 i C-474/24.

Wyraźnie zaznaczonym wątkiem tomu jest cyberbezpieczeństwo danych, ze szczególnym uwzględnieniem sektora ochrony zdrowia. Opracowania dotyczące tej problematyki analizują relację między rozporządzeniem EHDS a dyrektywą NIS 2, a także krajowy system cyberbezpieczeństwa – w tym projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa oraz szczególną pozycję szpitali jako podmiotów kluczowych w rozumieniu dyrektywy NIS 2.

Nie mniej istotny krąg tematów stanowią rozważania o charakterze pojęciowym i metodologicznym. Autorzy powracają do fundamentalnego rozróżnienia między anonimizacją a pseudonimizacją – pojęciami, których prawidłowe rozumienie warunkuje stosowanie RODO – odwołując się do motywu 26 rozporządzenia oraz przepisów ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Ten kierunek refleksji znajduje rozwinięcie w opracowaniach poświęconych styku ochrony danych i sztucznej inteligencji: skuteczności prawa do sprzeciwu, o którym mowa w art. 21 RODO, wobec danych wywnioskowanych przez systemy AI ze szczególnym uwzględnieniem znaczenia wyjaśnialnej sztucznej inteligencji jak również wykorzystaniu dużych modeli językowych do anonimizacji orzeczeń sądowych. Te ostatnie rozważania, dotykające problemu halucynacji modeli oraz nieprzejrzystości mechanizmu ich działania (*black box*), wykraczają poza ramy klasycznej ochrony danych i otwierają pole do dyskusji o granicach automatyzacji w wymiarze sprawiedliwości.

Mam nadzieję, że oddawany do rąk Czytelnika tom – podobnie jak dwa poprzednie – stanie się przyczynkiem do dalszej dyskusji naukowej oraz źródłem inspiracji dla praktyków stosujących przepisy o ochronie danych osobowych. Składam serdeczne podziękowania Autorom za wkład w powstanie niniejszej publikacji, a także Recenzentom, których uwagi przyczyniły się do podniesienia jej merytorycznego poziomu.

Monografia uwzględnia stan prawny na 2 marca 2026 r.

mgr **Mikołaj Brzóstowicz**
Uniwersytet Mikołaja Kopernika w Toruniu
mikolaj.brzostowicz@outlook.com
https://orcid.org/0009-0001-0920-8751

TRANSGRANICZNE TRANSFERY DANYCH W ERZE INFLACJI REGIONALNYCH REGULACJI: KOMPARATYSTYKA MECHANIZMÓW TRANSFEROWYCH RODO I SYSTEMU STANOWEGO W USA PO WYKSZTAŁCENIU SIĘ WIELOWARSTWOWYCH REŻIMÓW PRYWATNOŚCI

Streszczenie: Artykuł analizuje zmieniający się krajobraz transferów danych między UE a USA w warunkach kryzysu zaufania po wyroku Schrems II oraz w obliczu proliferacji regulacji prywatności w Stanach Zjednoczonych. Badamy pojęcie „adekwatności", rekonstruując na poziomie federalnym założenia Ram Ochrony Prywatności Danych UE-USA (EU-U.S. Data Privacy Framework, DPF) oraz Rozporządzenia Wykonawczego 14086, a także wskazując luki w amerykańskiej ochronie danych w obrocie komercyjnym wynikające z braku federalnej, kompleksowej (omnibusowej) ustawy o prywatności. W ramach analizy porównawczej trzech modelowych stanowych reżimów ochrony prywatności – kalifornijskiej CPRA, wirginijskiej VCDPA oraz koloradzkiej CPA – oceniamy: (1) sposób definiowania danych wrażliwych na tle art. 9 RODO, (2) zakres praw osób, których dane dotyczą (ze szczególnym uwzględnieniem pytania, czy wirginijskie prawo do usunięcia danych jest równoważne art. 17 RODO), oraz (3) mechanizmy egzekwowania prawa (kalifornijska CPPA w zestawieniu z kompetencjami stanowymi Prokuratorów Generalnych). Ocenie poddano również funkcjonalność ustaw stanowych jako „środków uzupełniających" w ramach *Transfer Impact Assessments* (TIA). Zwracamy uwagę, że przepisy stanowe mogą wzmacniać gwarancje RODO poprzez wypełnianie luk w komercyjnej ochronie danych, jednak ich efektywność jest ograniczona przez klauzulę supremacji oraz federalne uprawnienia w zakresie nadzoru (w szczególności FISA, sekcja 702). Ustalenia przemawiają za postulatem „hybrydowej adekwatności": zasadniczo równoważny poziom ochrony wyłania się dopiero z łącznego oddziaływania gwarancji federalnych (zwłaszcza w obszarze zabezpieczeń związanych z bezpieczeństwem narodowym) oraz stanowych praw do prywatności, które powinny być oceniane łącznie. Brak federalnej preempcji rodzi jednak ryzyko nierównomiernych standardów ochrony obywateli UE w zależności od

stanu USA, w którym działa importer, co uwypukla potrzebę wielowarstwowego podejścia do adekwatności.

Słowa kluczowe: RODO; transfery transatlantyckie; adekwatność; Ramy Ochrony Danych UE-USA (DPF); Executive Order 14086; prawo prywatności stanów USA; CPRA; VCDPA; CPA; Transfer Impact Assessment (TIA); FISA 702; klauzula supremacji.

WPROWADZENIE

Miniona dekada przyniosła poważny kryzys zaufania w transatlantyckim przepływie danych osobowych. Ingerencje amerykańskich służb ujawnione przez Edwarda Snowdena oraz dwa przełomowe wyroki Trybunału Sprawiedliwości UE (inwalidujące mechanizmy *Safe Harbor* i *Privacy Shield*) doprowadziły do wzrostu napięć między UE a USA w obszarze prywatności danych[1]. Unia Europejska, opierając się na zasadzie „istotnej równoważności" poziomu ochrony (wynikającej z art. 45 RODO oraz sprecyzowanej w orzecznictwie TSUE), zaczęła kwestionować adekwatność ochrony danych w Stanach Zjednoczonych, szczególnie wobec nieograniczonego dostępu amerykańskich władz do danych europejskich użytkowników[2]. Powstała luka zaufania wymusiła poszukiwanie nowych paradygmatów prawnych dla transgranicznych transferów danych, łączących rozwiązania polityczne i techniczne, a także ponowną negocjację ram prawnych między Brukselą a Waszyngtonem.

Równolegle do tych wydarzeń obserwujemy zjawisko określane w literaturze mianem „inflacji regulacyjnej" – lawinowego przyrostu przepisów ochrony danych na poziomie regionalnym i krajowym, które regulują tożsame obszary w odmienny

[1] Zob. Wyrok TSUE z dnia 6 października 2015 r., C362/14, („*Schrems I*"), stwierdzający nieważność decyzji Komisji z dnia 26 lipca 2000 r. przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz. U. UE. L. z 2000 r. Nr 215, str. 7) oraz wyrok TSUE z dnia 16 lipca 2020 r., C311/18 („*Schrems II*"), LEX nr 3029449, unieważniający decyzję wykonawczą Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności (Dz. U. UE. L. z 2016 r. Nr 207, str. 1). TSUE podkreślił brak zapewnienia w USA ochrony ekwiwalentnej z art. 7 i 8 Karty Praw Podstawowych UE, m.in. ze względu na nieograniczone uprawnienia służb (programy PRISM, UPSTREAM) i brak skutecznych środków odwoławczych dla osób spoza USA. Por. D. Karwala, *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018, s. 408-419.

[2] Zgodnie z art. 45 ust. 1 RODO, Komisja może stwierdzić, że dane państwo trzecie zapewnia „odpowiedni stopień ochrony", co skutkuje swobodą transferów z UE do tego kraju bez dodatkowych zezwoleń.

sposób[3]. Koncepcja inflacji regulacyjnej, zapożyczona z teorii ekonomii, opisuje nadprodukcję norm skutkującą fragmentacją systemu, wzrostem kosztów zgodności oraz paradoksalnym spadkiem pewności prawa mimo formalnego podniesienia standardów ochrony[4]. W kontekście transatlantyckim zjawisko to uwidacznia się szczególnie ostro: z jednej strony dąży się do stabilizacji i odbudowy zaufania na poziomie międzynarodowym poprzez nowe porozumienia (jak *EU-US Data Privacy Framework*, „DPF") i odpowiadającą mu decyzję Komisji Europejskiej o adekwatności[5]; z drugiej zaś – w Stanach Zjednoczonych trwa bezprecedensowy wysyp legislacji stanowych dotyczących prywatności. Do roku 2025 ponad dwadzieścia stanów USA przyjęło kompleksowe ustawy o ochronie danych osobowych, tworząc mozaikę *(„patchwork")* niespójnych wymogów prawnych w obrębie jednego kraju[6]. W rezultacie, europejscy eksporterzy danych stają wobec systemu wielowarstwowego: obok prawa federalnego pojawia się nowa warstwa prawa stanowego i lokalnych standardów prywatności.

Niniejszy artykuł przyjmuje perspektywę prawnoporównawczą i krytyczną wobec powyższych procesów. Sformułowano tezę, że choć nowe reżimy stanowego i w USA – na przykładzie *California Privacy Rights Act*[7] („CPRA"), *Virginia Consumer Data Protection Act*[8] („VCDPA") oraz *Colorado Privacy Act*[9] („CPA") – zbliżają

[3] Por. Regulation Taskforce, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, Report to the Prime Minister and the Treasurer, Canberra, Styczeń 2006. W kontekście ochrony danych, inflacja regulacyjna przejawia się rosnącą liczbą nieskoordynowanych reżimów (np. stanowych), co utrudnia pełną zgodność.

[4] Taką paradoksalną konsekwencję (obniżenie pewności prawa mimo wzrostu formalnych standardów) odnotowano m.in. w kontekście różnic między poszczególnymi ustawami stanowymi USA. Analiza *Alpha Architect* wskazuje, że "*regulatory fragmentation*" rodzi koszty administracyjne i ryzyko nieświadomego naruszenia przepisów przez firmy działające w wielu jurysdykcjach por. E. Basilico, *Regulatory fragmentation drags down efficiency*, AlphaArchitect, 2025 [dostęp: 2.03.2026]. W przypadku ochrony danych fragmentacja może też obniżać poziom ochrony obywateli, gdyż przedsiębiorstwa mogą *„forum shopping"* wybierać siedziby w stanach o niższych wymaganiach.

[5] Decyzja wykonawcza Komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE-USA (Dz. U. UE. L. z 2023 r. Nr 231, str. 118). Decyzja stwierdza, że Stany Zjednoczone w zakresie, w jakim podmioty amerykańskie przestrzegają Zasad Ram Ochrony Danych (DPF) – zapewniają poziom ochrony zasadniczo równoważny gwarancjom RODO (art. 1 decyzji). Akt ten jest prawnie wiążący od daty przyjęcia i do czasu ewentualnego uchylenia go przez TSUE pozostaje podstawą legalnych transferów do sygnatariuszy DPF.

[6] Według stanu na koniec 2025 r., ogólne ustawy o prywatności przyjęły m.in. Kalifornia, Wirginia, Kolorado, Utah, Connecticut, Teksas, Oregon, Iowa, Indiana, Tennessee, Montana, Wirginia, Karolina Południowa i Delaware (część z nich wejdzie w życie w 2026). Ponadto kilkanaście stanów proceduje podobne projekty. Zob. *The Great Privacy Patchwork of 2025: Eight New State Laws Reshape America's Data Protection Landscape*, ComplianceHub Wiki https://www.compliancehub.wiki/the-great-privacy-patchwork-of-2025-eight-new-state-laws-reshape-americas-data-protection-landscape/ [dostęp 3.01.2026].

[7] https://www.caprivacy.org/cpra-text/ [dostęp: 2.03.2026].

[8] https://law.lis.virginia.gov/vacode/ [dostęp: 2.03.2026].

[9] https://www.consumerprivacyact.com/colorado-privacy-act-cpa/ [dostęp 3.01.2026].

się terminologicznie do RODO (tzw. *Brussels Effect*), to ich strukturalna odmienność oraz brak federalnego aktu kreują system o wysokiej nieprzewidywalności z perspektywy unijnych zasad ochrony danych. W kolejnych częściach publikacji przeanalizowano, w jakim stopniu te nowe, „inflacyjne" warstwy regulacyjne mogą pełnić rolę „środków uzupełniających" (*supplementary measures*) w rozumieniu wyroku *Schrems II* i Wytycznych Europejskiej Rady Ochrony Danych („EROD") nr 01/2020, służących zabezpieczeniu transferów danych do państw trzecich[10].

1. DEKOMPOZYCJA POJĘCIA „ADEKWATNOŚCI"

Po unieważnieniu decyzji *Privacy Shield* w 2020 r. (sprawa *Schrems II*), UE i USA wypracowały nowe porozumienie mające przywrócić stabilność transferów danych – tzw. *EU-US Data Privacy Framework*. Komisja Europejska 10 lipca 2023 r. wydała decyzję wykonawczą stwierdzającą odpowiedni poziom ochrony danych osobowych w ramach DPF. Decyzja ta wprowadza domniemanie adekwatności dla transferów do organizacji amerykańskich, które dobrowolnie uzyskały certyfikację DPF przy Departamencie Handlu USA. Kluczową podstawą tej decyzji były zmiany w prawie USA na szczeblu wykonawczym: w szczególności Prezydent Biden w październiku 2022 r. wydał Rozporządzenie Wykonawcze nr 14086 *„Enhancing Safeguards for United States Signals Intelligence Activities"*[11]. *Executive Order 14086* („EO 14086") wprowadził do amerykańskiego systemu prawnego dwie zasadnicze gwarancje wcześniej nieobecne: (a) materialnoprawną zasadę konieczności i proporcjonalności w działalności wywiadu sygnałowego („SIGINT") oraz (b) mechanizm dochodzenia roszczeń dla osób objętych inwigilacją – powołano nowy *Data Protection Review Court* („DPRC"), czyli quasi-sądowy organ odwoławczy rozpatrujący skargi osób fizycznych spoza USA na naruszenia ich prywatności przez amerykańskie służby. W ocenie Komisji Europejskiej, te reformy wzmacniają ochronę danych

[10] EROD, *Zalecenia 01/2020 w sprawie środków uzupełniających dotyczących transferów*, wersja 2.0 z 18 czerwca 2021 r. https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pl_0.pdf [dostęp: 2.03.2026]. W pkt 48-49 zaleceń EROD wskazano, że analizując przepisy państwa trzeciego należy brać pod uwagę zarówno brzmienie prawa (*de jure*), jak i praktykę stosowania (*de facto*), w tym np. raporty dotyczące częstotliwości żądań organów itp.

[11] Executive Order 14086 z 7 października 2022 r., *Enhancing Safeguards for United States Signals Intelligence Activities*, opublikowany w Federal Register Vol. 87, No 198 (7 października 2022), EO 14086 ustanawia m.in. nowe zasady dla działań wywiadu: w sekcji 2 wylicza zasady konieczności, proporcjonalności, ograniczenia celów oraz mechanizmy kontroli wewnętrznej nad działaniami służb. Ponadto sekcja 3 nakazuje utworzenie *Data Protection Review Court* przy Departamencie Sprawiedliwości (w formie 28 CFR Part 201, https://www.ecfr.gov/current/title-28/chapter-I/part-201#part-201 [dostęp: 2.03.2026]) https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf [dostęp: 2.03.2026].

Europejczyków przed nieproporcjonalną inwigilacją, co w powiązaniu z istniejącymi już wcześniej gwarancjami praw obywatelskich w USA pozwoliło stwierdzić istnienie „istotnie równoważnego" poziomu ochrony w zakresie dostępu władz publicznych do danych.

Należy podkreślić, że adekwatność przyznana przez decyzję Komisji ma charakter sektorowy i warunkowy – dotyczy wyłącznie podmiotów, które przystąpią do DPF i zobowiążą się do przestrzegania szczegółowych *Privacy Principles* określonych w decyzji. Udział w programie jest dobrowolny; przedsiębiorstwa amerykańskie muszą samodzielnie zarejestrować się i poddać nadzorowi Departamentu Handlu oraz Federalnej Komisji Handlu. W praktyce DPF przypomina poprzedni mechanizm *Privacy Shield* – jego skuteczność zależy od dobrowolnej certyfikacji i państwowego egzekwowania naruszeń zasad u sygnatariuszy. Transfery danych do przedsiębiorstw, które nie uzyskały certyfikacji DPF, pozostają poza zakresem decyzji adekwatności. W takich wypadkach nadal stosuje się art. 46 RODO, głównie standardowe klauzule umowne (*Standard Contractual Clauses*, „SCC"), uzupełnione obowiązkiem dokonania przez eksportera Oceny Skutków Transferu (*Transfer Impact Assessment*, „TIA")[12]. Innymi słowy, warstwa federalna (DPF oparta na EO 14086) tworzy nowy reżim bezpieczeństwa dla danych w kontekście dostępu na szczeblu federalnym, ale nie rozwiązuje automatycznie problemów ochrony danych w komercyjnym obrocie poza programem certyfikacji.

Pomimo znaczących zmian w obrębie nadzoru wywiadowczego, struktura amerykańskiego systemu ochrony danych osobowych w sektorze prywatnym pozostała fragmentaryczna. Stany Zjednoczone wciąż nie posiadają federalnego aktu *omnibus* o ochronie danych porównywalnej z RODO. Ochrona na szczeblu federalnym opiera się wyłącznie na przepisach sektorowych (dotyczących m.in. ochrony finansowej, zdrowotnej, dzieci online) oraz ogólnych zasadach odpowiedzialności deliktowej

[12] Zob. EROD, *Informacja nt. transferów danych do USA po przyjęciu DPF* https://www.edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf [dostęp: 2.03.2026]. EROD przypomina, że podmioty nieobjęte DPF nie korzystają z domniemania adekwatności, zatem nadal wymagane jest stosowanie odpowiednich zabezpieczeń z art. 46 RODO oraz ocena ryzyka w trybie Schrems II. W praktyce oznacza to konieczność dalszego wykorzystania SCC i ewentualnie dodatkowych środków. Por. także Wytyczne EROD 01/2020 https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pl_0.pdf oraz 02/2020 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_pl.pdf [dostęp: 2.03.2026].

i ochrony konsumentów (akt o Federalnej Komisji Handlu)[13]. W latach 2019-2022 w Kongresie podejmowano próby uchwalenia kompleksowej ustawy o prywatności (m.in. projekt *American Data Privacy and Protection Act*, „ADPPA"), jednak nie osiągnięto konsensusu politycznego co do standardu ochrony ani kwestii preempcji przepisów stanowych[14]. W efekcie brak federalnej preempcji – czyli dominującego aktu unifikującej standard w całym kraju – pozostawia poszczególnym stanom swobodę stanowienia własnych regulacji. Nowa decyzja DPF nie obejmuje tych kwestii: odnosi się przede wszystkim do ograniczenia dostępu władz publicznych, uznając, że w sferze komercyjnej minimalny poziom ochrony zapewnią same zasady DPF (których przestrzegania pilnuje FTC) w odniesieniu do podmiotów certyfikowanych. Należy jednak zauważyć, że zasady DPF – podobnie jak wcześniej *Privacy Shield* – są w istocie zbliżone do dawnych zasad programu *Safe Harbor* z 2000 r. i nie odzwierciedlają wszystkich wymogów RODO (np. nie przewidują pełnego zestawu praw osób, których dane dotyczą). Tym samym, w odniesieniu do znacznej liczby transferów (szczególnie do podmiotów nieobjętych DPF) powstaje pytanie, czy obecne realia prawne USA spełniają unijne kryterium „istotnej równoważności" w zakresie praktyk komercyjnych. To zagadnienie prowadzi do analizy roli, jaką zaczęły odgrywać nowe ustawy stanowe wypełniające luki pozostawione przez prawo federalne.

2. ANALIZA KOMPARATYSTYCZNA GWARANCJI STANOWYCH (CPRA, VCDPA, CPA)

W obliczu *vacuum* legislacyjnego na szczeblu federalnym, poszczególne stany USA wprowadziły własne, szeroko zakrojone regulacje dotyczące prywatności konsumenckiej. Kalifornia, Wirginia i Kolorado należą do stanów, które przyjęły akty

[13] Najważniejsze federalne ustawy sektorowe to m.in.: *Gramm-Leach-Bliley Act* (1999) dla sektora finansowego (nakłada obowiązki informacyjne i bezpieczeństwa na instytucje finansowe wobec danych klientów); *Health Insurance Portability and Accountability Act* (HIPAA, 1996) dla danych medycznych (wprowadza standardy poufności i bezpieczeństwa informacji zdrowotnych); *Children's Online Privacy Protection Act* (COPPA, 1998) dla danych dzieci poniżej 13 lat (wymóg zgody rodzica na zbieranie danych); oraz *Fair Credit Reporting Act* (FCRA, 1970) dot. danych w rejestrach kredytowych. Ponadto *Federal Trade Commission Act* (1914) w sekcji 5 zakazuje nieuczciwych lub wprowadzających w błąd praktyk – FTC używa tego przepisu do karania firm, które nie dochowują własnych polityk prywatności lub dopuszczają wycieki danych (argumentując, że to *unfair business practice*). Brak jednak kompleksowej regulacji pokrywającej całość gospodarki, analogicznej do RODO.

[14] W lipcu 2022 r. projekt ADPPA (H.R. 8152) uzyskał ponadpartyjne poparcie w komisji Izby Reprezentantów, lecz ostatecznie nie doszło do głosowania na forum Kongresu przed końcem kadencji. Spór dotyczył m.in. klauzuli preempcji – projekt przewidywał, że ustawa federalna uchyli większość przepisów stanowych (co popierał biznes i część republikanów), z wyjątkiem kilku najsilniejszych standardów stanowych (co z kolei budziło sprzeciw np. reprezentacji Kalifornii, obawiającej się osłabienia CCPA/CPRA). Por. H.R.8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act. (2022, grudzień 30). https://www.congress.gov/bill/117th-congress/house-bill/8152 [dostęp: 2.03.2026].

prawne mogące uchodzić za wzorce dla kolejnych stanów. Poniżej porównano wybrane elementy tych reżimów z rozwiązaniami RODO, aby ocenić zakres konwergencji (pod wpływem europejskiego standardu) oraz rozbieżności mogących wpływać na ocenę adekwatności.

2.1 DEFINICJE „DANYCH WRAŻLIWYCH" VS. ART. 9 RODO

Kluczowym punktem odniesienia jest art. 9 RODO, który definiuje szczególne kategorie danych osobowych (potocznie dane wrażliwe) i co do zasady zakazuje ich przetwarzania, chyba że zachodzi jedna z enumeratywnie wymienionych przesłanek legalizujących (m.in. wyraźna zgoda osoby, ważny interes publiczny, ochrona żywotnych interesów itp.). Dane wrażliwe w rozumieniu RODO obejmują m.in. informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych, zdrowiu, seksualności, a także dane genetyczne i biometryczne pozwalające na jednoznaczną identyfikację osoby (art. 9 ust. 1)[15]. *California Privacy Rights Act*, który od 2023 r. aktualizuje standard ochrony w Kalifornii, wprowadził do prawa stanowego pojęcie *"sensitive personal information"* zbliżone zakresem do art. 9 RODO. Obejmuje ono m.in. dane o pochodzeniu rasowym/etnicznym, poglądy religijne lub filozoficzne, przynależność do związków zawodowych, dane genetyczne, biometryczne identyfikatory, informacje zdrowotne, seksualne, orientację seksualną, a także dane lokalizacyjne (dokładna geolokalizacja) oraz zawartość prywatnej komunikacji (np. maile, SMS)[16]. Virginia Consumer Data Protection Act oraz Colorado Privacy Act posługują się pojęciem *"sensitive data"*, również definiowanym w zbliżony sposób (włącznie z danymi dot. rasy, etniczności, zdrowia,

[15] Zob. szerzej P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych*. Komentarz, wyd. III, Warszawa 2025, art. 9. Autor wskazuje, że unijny ustawodawca uznał te dane za wymagające *„szczególnej ochrony"* z uwagi na kontekst społeczny ich przetwarzania (np. ryzyko dyskryminacji).

[16] California Consumer Privacy Act (CCPA) 2018, znowelizowana California Privacy Rights Act (CPRA) 2020 – ustawa skodyfikowana w Cal. Civil Code § 1798.100 ff. Definicja *"Sensitive Personal Information"* została dodana przez CPRA (Cal. Civ. Code § 1798.140(ae)): obejmuje m.in. numer ID, dane finansowe + dostęp do konta, geolokalizację dokładną, rasę, pochodzenie etniczne, poglądy religijne/filozoficzne, przynależność do związków zawodowych, treść poczty/komunikacji (jeśli nie publiczna), genetyczne, biometria identyfikacyjna, zdrowotne, seksualne, orientacja seksualna. Prawo do ograniczenia użycia/ujawniania danych wrażliwych przyznaje Cal. Civ. Code § 1798.121 – konsument może w każdym czasie zażądać, by firma wykorzystywała jego *SPI* tylko w celach "niezbędnych" (tamże § 1798.121(a)). Obowiązek umieszczenia linku "Limit the Use of My Sensitive Personal Information" nakłada § 1798.135(b).

genetyki, biometria, przekonania, życie seksualne, orientacja seksualna, a także dane o nieletnich)[17].

Mimo podobieństw definicyjnych, istotne są różnice w reżimie przetwarzania danych wrażliwych. RODO ustanawia tu model *opt-in* – przetwarzanie szczególnych kategorii jest zabronione, chyba że administrator wykaże istnienie wyjątku ustawowego lub uzyska wyraźną zgodę osoby (art. 9 ust. 2 RODO). Ustawy stanowe i Wirginii i Kolorado przyjęły analogiczną filozofię: wymagają zgody konsumenta na przetwarzanie jego danych wrażliwych, z pewnymi wyjątkami przewidzianymi w ustawie[18]. Wprost stanowi o tym np. sekcja 59.1-578(A)(5) Kodeksu Wirginii, nakładając na administratora obowiązek uzyskania zgody przed gromadzeniem i użyciem wrażliwych informacji[19]. Z kolei Kolorado nie tylko wymaga zgody, ale też precyzuje formę jej uzyskania (musi być odrębna dla każdej kategorii danych wrażliwych, zgodnie z regulacjami wykonawczymi CPA)[20]. Kalifornijski CPRA odbiega nieco od tego podejścia – zamiast wymogu uprzedniej zgody, przyznaje konsumentom prawo do ograniczenia wykorzystania i ujawniania ich informacji wrażliwych (*Right to Limit the Use and Disclosure of Sensitive Personal Information*)[21]. W praktyce CPRA operuje modelem opt-out dla danych wrażliwych: konsument może w dowolnym momencie zażądać od przedsiębiorstwa zaprzestania wykorzystywania jego danych wrażliwych do celów innych niż niezbędne (ustawa wylicza m.in. możliwość wewnętrznego wykorzystania danych wrażliwych do świadczenia usługi, bezpieczeństwa, krótkoterminowego marketingu bez profilowania itp.). Dopóki jednak konsument nie skorzysta z prawa *"Limit Use of My Sensitive Personal Information"*, przedsiębiorstwo może te

[17] Virginia Consumer Data Protection Act (VCDPA) 2021, Kodeks Wirginii Tyt. 59.1, rozdz. 53 (§ 59.1-571 ff.). Definicje: "*Sensitive data*" oznacza dane osobowe obejmujące: pochodzenie rasowe lub etniczne, przekonania religijne, zdrowie psychiczne lub fizyczne, informacje genetyczne, dane biometryczne w celu jednoznacznej identyfikacji, dane dzieci, orientację seksualną lub życie intymne (Va. Code § 59.1- 575). Zgoda wymagana jest na przetwarzanie danych wrażliwych – zob. Va. Code § 59.1-578(A)(5): *"Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.)."*.

[18] *Ibidem*.

[19] *Ibidem*.

[20] Colorado Privacy Act (SB 21-190), przyjęta 8 czerwca 2021 r. Definicje i prawa w CPA są zbliżone do VCDPA: *"Sensitive data"* obejmuje rasę, pochodzenie etniczne, przekonania religijne, zdrowotne, seksualne, orientację, genetyczne, biometria ident., dane dzieci – zob. Colorado Revised Statutes § 6-1-1303(24). Wymagana jest zgoda opt-in na ich przetwarzanie (§ 1308(7)). Dodatkowo Kolorado jako pierwsze opracowało centralny mechanizm Global Privacy Control: przedsiębiorstwa muszą respektować uniwersalny sygnał opt-out wysyłany np. przez przeglądarkę – zob. L. White, *Colorado's approach to universal opt-out requirements*, https://iapp.org/news/a/colorados-approach-to-universal-opt-out-requirements [dostęp 3.01.2026]

[21] Prawo do ograniczenia użycia/ujawniania danych wrażliwych przyznaje Cal. Civ. Code § 1798.121 – konsument może w każdym czasie zażądać, by firma wykorzystywała jego *SPI* tylko w celach "niezbędnych" (ibidem § 1798.121(a)).

dane przetwarzać na zasadach *opt-out*. Takie rozwiązanie odbiega od rygoru RODO (gdzie domyślnie przetwarzanie jest niedozwolone). Można zatem stwierdzić, że Wirginia i Kolorado wdrożyły w zakresie danych wrażliwych mechanizm zbliżony do europejskiego (wymóg zgody na dane szczególnie chronione sugeruje daleko idącą inspirację RODO), podczas gdy Kalifornia zachowała model charakterystycznych dla systemu amerykańskiego (szerszą swobodę działania administratorów, ograniczaną jedynie inicjatywą konsumenta).

Warto odnotować, że zakres ochrony kategorii wrażliwych nie jest identyczny we wszystkich stanach. CPRA dodaje pewne elementy (np. dane finansowe w połączeniu z loginem/hasłem, które mogą umożliwić kradzież tożsamości, są traktowane jako *"sensitive personal information"*, „SPI"), podczas gdy np. VCDPA nie chroni informacji o karalności czy wyrokach (które w UE mieszczą się w art. 10 RODO). RODO zaś nie wyróżnia danych geolokalizacyjnych jako szczególnych, a w CPRA i VCDPA dokładna geolokalizacja (np. dane z GPS) są *explicite* wymienione jako wrażliwe[22]. Te rozbieżności mogą powodować, że pewne dane chronione w UE jako wrażliwe nie będą objęte takim samym statusem prawnym w relacji transgranicznej.

2.2 PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

RODO przyznaje osobom fizycznym szereg praw względem ich danych, co stanowi centralny element modelu europejskiego. Jednym z najważniejszych jest prawo do usunięcia danych (art. 17 RODO), zwane także potocznie „prawem do bycia zapomnianym". Uprawnia ono osobę do żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, m.in. gdy cele przetwarzania zostały zrealizowane, zgoda została cofnięta, dane były przetwarzane niezgodnie z prawem albo wniesiono skuteczny sprzeciw – chyba że zachodzą wyjątki (np. nadrzędny obowiązek prawny przechowania danych, wolność wypowiedzi lub konieczność ustalenia lub dochodzenia roszczeń prawnych, por. art. 17 ust. 3)[23]. Virginia CDPA (podobnie jak większość nowych ustaw stanowych) przewiduje analogiczne uprawnienie konsumenta do żądania usunięcia swoich danych osobowych. Co istotne, jest

[22] Cal. Civ. Code § 1798.140(ae) oraz Va. Code § 59.1- 575.

[23] Zob. szerzej P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679*… op. cit., art. 17. Warto zaznaczyć, że prawo do usunięcia na gruncie RODO nie ma charakteru bezwzględnego – ważenie z innymi prawami (np. wolność słowa, obowiązki prawne) jest integralną częścią przepisu. W kontekście transatlantyckim ciekawym problemem był tzw. transfer *"right to be forgotten"* – np. usunięcie danych z Google w Europie vs ich dostępność w USA. TSUE w sprawie C507/17 (*Google LLC przeciw CNIL*, 2019) orzekł, że wyszukiwarka nie jest zobowiązana do stosowania prawa do bycia zapomnianym globalnie, a jedynie w domenach europejskich – co pokazuje potencjalne tarcia jurysdykcyjne w egzekwowaniu art. 17 poza UE.

ono sformułowane szeroko – dotyczy zarówno danych *"provided by the consumer"* (przekazanych przez konsumenta), jak i danych *"obtained about the consumer"* (uzyskanych o konsumencie)[24]. Zgodnie z oficjalnym podsumowaniem od Prokuratora Generalnego Wirginii, konsument ma prawo zażądać, aby administrator usunął wszystkie jego dane osobowe, niezależnie od źródła ich pozyskania[25]. Jest to szersze ujęcie niż pierwotna kalifornijska ustawa CCPA z 2018 r. (gdzie prawo do usunięcia początkowo obejmowało tylko dane zebrane od konsumenta bezpośrednio), przy czym nowelizacja CPRA usunęła to ograniczenie także w Kalifornii. Zatem co do zakresu podmiotowego i przedmiotowego, prawo do usunięcia w VCDPA z grubsza odpowiada art. 17 RODO – obejmuje wszelkie dane osobowe danej osoby będące pod kontrolą administratora.

Istnieją jednak różnice w warunkach realizacji i wyjątki. Akty stanowe przewidują liczne wyłączenia, które zwalniają administratora z obowiązku usunięcia danych na żądanie konsumenta. Na przykład VCDPA zwalnia z realizacji prawa do usunięcia w sytuacjach, gdy zachowanie danych jest niezbędne do: wykonania umowy z konsumentem, zapewnienia bezpieczeństwa, zapobiegania oszustwom, wykonywania obowiązków prawnych (np. prowadzenia dokumentacji finansowej), ustalenia lub obrony roszczeń prawnych, wewnętrznych celów zgodnych z oczekiwaniami konsumenta lub zgodnych z prawem kontekstem zbierania danych itp. RODO również przewiduje wyjątki (art. 17 ust. 3), ale ich zakres nie jest identyczny – w RODO nacisk położono m.in. na ochronę prawa do informacji (wolność prasy) czy obowiązki publiczne administratora, podczas gdy stany amerykańskie kładą akcent na uzasadniony użytek biznesowy i zgodność z innymi przepisami krajowymi. Ponadto, unijna koncepcja *„bycia zapomnianym"* idzie dalej w odniesieniu do danych upublicznionych: art. 17 ust. 2 RODO nakłada na administratora, który upublicznił dane (np. w internecie), obowiązek podjęcia „rozsądnych działań", aby poinformować innych administratorów przetwarzających te dane o żądaniu ich usunięcia – co *de facto* przenosi skutki żądania na dalszy ekosystem danych. Amerykańskie akty konsumenckie nie mają odpowiednika tej regulacji; obowiązek usunięcia dotyczy jedynie administratora, do którego konsument się zwraca, i jego bezpośrednich kontrahentów-przetwarzających (np. przedsiębiorstwo musi nakazać swoim podmiotom przetwarzającym skasowanie danych, co wynika z ogólnych obowiązków umownych.

[24] AG Virginia, *The Virginia Consumer Data Protection Act*, https://www.oag.state.va.us/consumer-protection/files/tips-and-info/Virginia-Consumer-Data-Protection-Act-Summary-2-2-23.pdf [dostęp: 2.03.2026]. W sekcji *"What rights do Virginia consumers have"* enumeratywnie wymieniono pięć uprawnień (potwierdzenie przetwarzania, sprostowanie, usunięcie, dostęp/kopia, opt-out od ads/sale/profilowania) wraz z objaśnieniami. Tamże wyraźnie: "*delete personal data provided by or obtained about the consumer*" – co potwierdza szeroki zakres prawa do usunięcia.

[25] *Ibidem*.

Reasumując, prawo do usunięcia w VCDPA jest w założeniu zbieżne funkcjonalnie z art. 17 RODO, co świadczy o wpływie europejskiego modelu na ustawodawstwo stanowe USA. Zakres ochrony konsumenta w Wirginii wydaje się jednak nieco węższy w praktyce ze względu na szersze przesłanki odmowy realizacji żądania. Dla obywatela UE, którego dane trafią do podmiotu w Wirginii, oznacza to wciąż możliwość skutecznego usunięcia danych osobowych w wielu sytuacjach – ale nie we wszystkich, w których RODO by to gwarantowało. W pewnych scenariuszach (np. utrzymywanie danych ze względów wewnętrznych zgodnych z kontekstem transakcji) przedsiębiorstwo z Wirginii może legalnie odmówić pełnego „zapomnienia" konsumenta, podczas gdy analogiczna odmowa w UE musiałaby znaleźć podstawę w wąsko interpretowanych wyjątkach z art. 17 ust. 3.

Warto również wspomnieć o innych prawach podmiotów danych. Wszystkie trzy analizowane ustawy stanowe przyznają prawa dostępu do danych oraz sprostowania nieścisłości – wprost wzorowane na art. 15 i 16 RODO. Konsumenci mają też prawo do przenoszenia swoich danych, czyli otrzymania kopii danych w formacie nadającym się do ponownego wykorzystania – to również zbieżne z art. 20 RODO. Istotną różnicą jest natomiast prawo sprzeciwu: podczas gdy RODO zapewnia prawo do sprzeciwu wobec przetwarzania w dowolnym momencie z przyczyn związanych z sytuacją osoby (oraz absolutne prawo sprzeciwu wobec marketingu bezpośredniego, art. 21 RODO), akty prawne w Stanach Zjednoczonych formułują prawo sprzeciwu głównie jako prawo *opt-out* od określonych działań: sprzedaży danych, profilowania i użycia do reklamy behawioralnej. Przykładowo, VCDPA daje konsumentowi prawo cofnięcia zgody na profilowanie oraz prawo wyrażenia sprzeciwu wobec wykorzystania jego danych do targetowanej reklamy lub sprzedaży danych. Nie ma jednak ogólnego prawa sprzeciwu obejmującego wszelkie inne cele przetwarzania oparte np. na uzasadnionym interesie – co istnieje w RODO. W pewnym sensie, stany amerykańskie ograniczyły katalog sprzeciwów do tych sytuacji, które najczęściej budzą niepokój konsumentów (handel danymi i profilowanie reklam). Można zatem mówić o częściowej ekwiwalencji praw podmiotów danych: podstawowe prawa (dostęp, poprawienie, usunięcie, przeniesienie) są uznawane wszędzie, natomiast prawo sprzeciwu ma w USA węższe zastosowanie.

3. FUNKCJONALNOŚĆ PRAW STANOWYCH W PROCESIE TIA: ŚRODKI UZUPEŁNIAJĄCE A GRANICE SKUTECZNOŚCI

Zgodnie z obowiązującym regulacji oraz orzecznictwem Trybunału Sprawiedliwości UE w sprawie *Schrems II*, eksporterzy danych z UE zobowiązani są

przeprowadzić *Transfer Impact Assessment* dla transferów opartych na art. 46 RODO, by ocenić czy prawo i praktyka państwa trzeciego zapewniają ochronę zasadniczo równoważną unijnemu standardowi[26]. Dotyczy to zwłaszcza sytuacji, gdy brak jest decyzji adekwatności – a zatem np. transferu do podmiotu w USA, który nie jest objęty DPF. Europejska Rada Ochrony Danych wyraźnie zaleca, by taka analiza uwzględniała całość systemu prawnego importera, w tym regulacje sektorowe i praktykę stosowania prawa[27]. W kontekście federalnego systemu USA oznacza to konieczność spojrzenia nie tylko na prawo federalne (jak *FISA, Patriot Act, CLOUD Act*), lecz także na poziom stanowy. Dynamiczna ekspansja aktów stanowych dostarcza nowych argumentów potencjalnie wzmacniających ochronę danych w toku TIA.

Przepisy stanowe mogą pełnić rolę „środków o charakterze prawnym" poprawiających poziom ochrony, komplementarnie do środków technicznych i organizacyjnych wdrażanych przez eksportera. W szczególności:

(1) Wszystkie analizowane akty stanowe nakładają na administratorów obowiązek zawierania umów powierzenia z podmiotami przetwarzającymi (procesorami), które muszą regulować m.in. cel i czas przetwarzania, wymagania bezpieczeństwa oraz zobowiązanie do działania wyłącznie na polecenie administratora. Wymóg ten jest zbieżny z art. 28 RODO. Skutek praktyczny polega na tym, że jeśli unijny eksporter korzysta z usług amerykańskiego procesora (np. dostawcy chmury) w stanie posiadającym taki przepis, to nie tylko klauzule umowne SCC wiążą procesora, ale również prawo krajowe USA nakazuje mu przestrzegać analogicznych warunków. To czyni zobowiązania ochronne bardziej egzekwowalnymi lokalnie, gdyż naruszenie umowy powierzenia oznacza jednocześnie złamanie prawa stanowego – grożą za to sankcje nakładane przez AG lub (w Kalifornii) CPPA[28]. Ten mechanizm podwójnego zabezpieczenia podnosi poziom zaufania do SCC: ryzyko, że procesor zignoruje ustalenia umowne, jest mniejsze, gdy nad jego działaniami czuwa również lokalny regulator.

(2) Prawa stanowe wypełniają luki, które dawny *Privacy Shield* pozostawiał nietknięte – zwłaszcza w zakresie niekontrolowanego udostępniania danych stronom trzecim. Przykładowo, definicja „sprzedaży danych" przyjęta w CPRA i CPA obejmuje każde udostępnienie danych osobowych za „korzyść pieniężną lub inną

[26] Zob. EROD, *Zalecenia 01/2020 w sprawie środków uzupełniających dotyczących transferów*, wersja 2.0 z 18 czerwca 2021 r., https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pl_0.pdf [dostęp: 2.03.2026].

[27] Ibidem, s. 8.

[28] *California Privacy Protection Agency*, ustanowiona na mocy CPRA (dodała § 1798.199.10 ff. do California Civil Code). Zob. *California Privacy Protection Agency: About*, https://cppa.ca.gov [dostęp: 2.03.2026].

wartościową”[29]. To znacznie szersze ujęcie niż potoczne rozumienie sprzedaży, które obejmuje tylko transakcje za pieniądze. Dzięki temu, przedsiębiorstwa nie mogą omijać obowiązku oferowania konsumentom *opt-out* poprzez twierdzenie, że wymieniają dane za usługi lub inne świadczenia (a nie za gotówkę). W ten sposób stanowe legislacje uniemożliwiają praktyki dzielenia się danymi z brokerami czy partnerami reklamowymi bez wiedzy osoby – co w braku prawa stanowego mogłoby odbywać się w szarej strefie, nie wprost zabronione na gruncie samych SCC. Z perspektywy TIA, fakt podlegania przez importera takiej regulacji redukuje ryzyko niekontrolowanego dalszego transferu danych do kolejnych podmiotów, bo każda taka operacja wymaga podstawy prawnej lub zgody konsumenta. Innymi słowy, prawa stanowe uszczelniają obieg komercyjny danych tam, gdzie kontrakty czy samoregulacja mogłyby nie wystarczyć.

(3) Wiele nowych aktów stanowych wprowadza wymogi inspirowane zasadami RODO, jak *data minimization* (np. CPRA wymaga, by zbierane dane były “rozsądnie niezbędne i proporcjonalne” do celu[30]) czy obowiązek przeprowadzania ocen ryzyka związanego z przetwarzaniem (Virginia i Kolorado wymagają od administratorów dokonywania *Data Protection Assessments* dla operacji wysokiego ryzyka, np. profilowania lub sprzedaży danych wrażliwych)[31]. Takie oceny są odpowiednikami unijnych DPIA (*Data Protection Impact Assessment*, art. 35 RODO). Co istotne, wyniki tych ocen mogą być weryfikowane przez organ (np. AG Kolorado może zażądać przedstawienia dokumentacji oceny ryzyka – Colorado CPA § 6-1-1309). Zatem przedsiębiorstwa w tych stanach muszą wykazać się procesem identyfikacji i mitigacji ryzyk prywatności, co sprzyja transparentności wobec partnerów z UE. Dla unijnego eksportera lub audytora fakt, że importer przygotował i archiwizuje takie oceny, jest dodatkowym zabezpieczeniem: ułatwia zrozumienie, jakie dane są przetwarzane i w jakim celu, co pozytywnie wpływa na wiarygodność oceny TIA.

Podsumowując, regulacje stanowe mogą pełnić rolę katalizatora, podnoszącego poziom ochrony tam, gdzie prawo federalne milczy. W pewnych aspektach (np. wymóg zgody na dane wrażliwe, ocena skutków) prawodawcy stanowi wdrożyli standard nawet wyższy niż minimalny poziom wymagany do certyfikacji DPF. Z punktu widzenia unijnego oceniającego transfer, jest racjonalne uznać te przepisy za środki uzupełniające o charakterze prawnym, które – łącznie ze środkami umownymi

[29] Patrz Colorado Privacy Act (SB 21-190)(23)(a) oraz California Civil Code § 1798.140(ad)(1).
[30] California Civil Code § 1798.100(c).
[31] Code of Virginia § 59.1-580. oraz Colorado Privacy Act (SB 21-190) 6-1-1305 (2)(c).

i technicznymi – mogą pomóc zapewnić *„essentially equivalent"* ochronę[32]. W rekomendacjach EROD podkreśla się, że dopuszczalne są środki uzupełniające wynikające z obowiązującego prawa lokalnego, byleby rzeczywiście przekładały się na ograniczenie dostępu władz lub innych podmiotów do danych transferowanych[33]. Prawa stanowe ograniczają dostęp podmiotów komercyjnych – więc w zakresie ryzyk prywatności konsumenckiej stanowią istotne uzupełnienie.

3.1. GRANICE SKUTECZNOŚCI: KLAUZULA SUPREMACJI I DOSTĘP NA PODSTAWIE FISA 702

Mimo niewątpliwych korzyści, reżimy stanowe mają także strukturę ograniczenia, której nie są w stanie przekroczyć. Najważniejszą z nich jest nadrzędność prawa federalnego nad stanowymi na gruncie Konstytucji USA (*Supremacy Clause*, art. VI Konstytucji). W praktyce oznacza to, że żadna ustawa stanowa nie może uchylić ani ograniczyć uprawnień przyznanych agencjom federalnym w ustawach Kongresu. Dotyczy to zwłaszcza kompetencji w zakresie bezpieczeństwa narodowego i egzekwowania prawa. Ustawy CPRA, VCDPA, CPA wprost zawierają wyłączenia wskazujące, że ich postanowienia nie stosują się do przetwarzania danych, jeśli jest to konieczne do spełnienia wymogów prawa federalnego lub współpracy z organami ścigania[34]. Na przykład CPRA stwierdza, iż nic w ustawie nie stoi na przeszkodzie podporządkowaniu się nakazowi sądowemu, wezwaniu lub obowiązkowi prawnemu[35]. W konsekwencji, jeśli przedsiębiorstwo z Kalifornii otrzyma prawnie wiążący nakaz ujawnienia danych na podstawie *Foreign Intelligence Surveillance Act* (dalej także: FISA) Section 702[36] lub innego przepisu federalnego, to prawo stanowe nie zapewni osobie żadnej ochrony – przedsiębiorstwo będzie musiało przekazać dane zgodnie z federalnym prawem, nie narażając się na sankcje stanowe (gdyż akt stanowy nie obowiązuje w tym zakresie). Innymi słowy, w obszarze kluczowego problemu zidentyfikowanego w *Schrems II* – dostępu służb wywiadowczych – legislacja stanowa jest bezsilna, ponieważ nie może ani zabronić współpracy ze służbami, ani ustanowić dla niej własnych ograniczeń.

---

[32] Zob. EROD, *Zalecenia 01/2020 w sprawie środków uzupełniających dotyczących transferów*, wersja 2.0 z 18 czerwca 2021 r., https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pl_0.pdf [dostęp: 2.03.2026].
[33] Ibidem.
[34] California Privacy Rights Act, sec. 30, Code of Virginia § 59.1-582 oraz Colorado Privacy Act (SB 21-190)(3)(a)(I).
[35] California Privacy Rights Act, sec. 28.
[36] 50 U.S. Code § 1881a.

Konsekwencją powyższego jest stwierdzenie, że z perspektywy TIA prawa stanowe nie mogą być uznane za skuteczny środek uzupełniający w zakresie ochrony przed dostępem rządowym. Ryzyko inwigilacji i masowego gromadzenia danych przez władze USA musi być adresowane wyłącznie na poziomie federalnym – i tym właśnie zajęły się mechanizmy DPF/EO 14086, czego wyrazem jest adekwatność w decyzji Komisji. Jednak w zakresie ryzyk czysto komercyjnych (wykorzystanie danych przez sam podmiot importera lub dalsze przekazywanie innym firmom), prawo stanowe może znacząco obniżyć poziom zagrożenia dla praw osób z UE. Powstaje zatem dwupoziomowy system ochronny: warstwa federalna (DPF z reformami wywiadu) ma chronić przed naruszeniem prywatności przez państwo, a warstwa stanowa – przed nadużyciami ze strony sektora prywatnego.

Brak federalnej preempcji powoduje jednak kolejny problem – niejednolitość standardu ochrony w zależności od miejsca prowadzenia działalności w USA. Dla obywatela UE przekazującego dane do Stanów oznacza to potencjalnie nierówne traktowanie: jeśli dane trafią do przedsiębiorstwa w Kalifornii czy Kolorado, to będą tam chronione licznymi prawami konsumenta (jak opisane powyżej), podczas gdy transfer do przedsiębiorstwa np. w Teksasie (stanie, gdzie na dzień 3 stycznia 2026 nie wprowadzono ustawy dot. ochrony danych osobowych) oznacza brak takich gwarancji. Z punktu widzenia oceny adekwatności rodzi się pytanie, czy USA jako całość mogą zapewnić równoważny poziom ochrony, skoro wewnątrz kraju występują strefy o odmiennych reżimach prawnych. Komisja Europejska, wydając decyzję DPF, *de facto* pominęła tę kwestię – skupiła się na mechanizmach federalnych i przyjęła, że każdy sygnatariusz DPF niezależnie od lokalizacji musi przestrzegać jednolitych zasad programu (co zapewnia pewną minimalną ochronę komercyjną). Jednakże DPF obejmuje ograniczoną liczbę podmiotów; ci spoza ram muszą być oceniani indywidualnie. Tu zaś TIA może prowadzić do wniosku, że np. importer z siedzibą w stanie A (bez ustawy) stwarza większe ryzyko niż importer w stanie B (z ustawą), mimo że obaj podlegają temu samemu rządowi federalnemu. Brak preempcji skutkuje więc geograficzną dysproporcją ochrony – co samo w sobie może być postrzegane jako element niepewności prawnej dla UE. Europejski organ nadzorczy w swojej opinii nt. projektu decyzji DPF zwracał uwagę, że fragmentacja prawna USA powinna

być monitorowana pod kątem wpływu na spójność ochrony i wezwał Komisję do analiz w ramach przyszłych rewizji adekwatności[37].

PODSUMOWANIE

Przeprowadzona powyżej analiza pozwala sformułować następujące wnioski.

Po pierwsze, prawa stanowe w USA pełnią rolę komplementarną, a nie substytucyjną wobec federalnych gwarancji bezpieczeństwa. Nie zastępują one mechanizmów DPF/EO 14086 w zakresie ograniczania dostępu władz publicznych, ale są ich niezbędnym uzupełnieniem w sferze prywatnoprawnej (komercyjnej). W erze po *Schrems II* należy więc postrzegać ochronę danych transatlantyckich warstwowo: dopiero połączenie reform na poziomie federalnym (zapewniających gwarancje konstytucyjne i ścieżkę dochodzenia naruszeń przez DPRC) z wysokimi standardami stanowymi (zapewniającymi prawa podmiotów i obowiązki przedsiębiorstw) tworzy system mogący aspirować do miana adekwatnego względem RODO. Innymi słowy, proponowany jest postulat uznania „hybrydowej adekwatności" – gdy ocenie podlegałby łącznie pakiet wielowarstwowych środków ochronnych obowiązujących w danym państwie trzecim.

Po drugie, w praktyce prawo stanowe w USA wykazuje cechy zbieżne z modelem europejskim, co wpisuje się w szersze zjawisko oddziaływania unijnego standardu RODO jako punktu odniesienia dla regulacji pozaeuropejskich, z którymi dzieli on wspólny rdzeń w strukturze i podstawowych koncepcjach[38]. Pomimo odmiennych założeń (np. *opt-out vs opt-in*) wiele mechanizmów materialnych upodabnia się do RODO: wymaganie zgody na dane wrażliwe (VA, CO), zasady minimalizacji i ograniczenia celu, obowiązek oceny skutków (VA, CO), prawo do sprostowania (CA, VA, CO) itp. – to wszystko świadczy o rosnącym wpływie standardów RODO na ustawodawstwo amerykańskie. Nawet jeżeli reżimy stanowe nie są identyczne

[37] EROD, *Opinia 5/2023 dotycząca projektu decyzji wykonawczej Komisji Europejskiej w sprawie stwierdzenia zapewnienia odpowiedniego stopnia ochrony danych osobowych w ramach unijno-amerykańskich ram ochrony danych (EU–US Data Privacy Framework)*, https://www.edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [dostęp 3.01.2026]. EROD z zadowoleniem przyjął zapowiedź Komisji, że pierwsza rewizja decyzji adekwatności odbędzie się w ciągu roku od jej wejścia w życie (tj. do lipca 2024 r.), a kolejne co najmniej raz na cztery lata. Zarekomendowano, by w ramach przeglądów ocenić wpływ zmian w prawie USA, w tym ewentualnego uchwalenia ustawy federalnej lub nowych ustaw stanowych na trwałość adekwatności. Rada stwierdziła też *expressis verbis*, że obecna ocena adekwatności koncentruje się na mechanizmach federalnych, lecz nie wyklucza potrzeby analizy poziomu ochrony zapewnianego przez inne czynniki (np. praktyki biznesowe, inicjatywy stanowej). Sformułowano wręcz uwagę, że "system ochrony danych w USA opiera się na mozaice instrumentów prawnych" i tylko kompleksowa ocena pozwoli stwierdzić jego efektywność.

[38] M. Krzysztofek, *Porównanie prawa ochrony danych osobowych w największych gospodarkach świata. Regulacji Unii Europejskiej (RODO), CHIN (PIPL) i Kalifornii (CCPA)*, Warszawa 2025, s. 4.

z RODO, to jednak zmierzają ku „europeizacji" filozofii ochrony danych. Dla unijnych obserwatorów jest to sygnał pozytywny, wskazujący na globalne podnoszenie poprzeczki ochrony prywatności (efekt zaraźliwy regulacji).

Po trzecie, fragmentacja systemu USA stawia wyzwania dla zgodności z RODO pod kątem operacyjnym. Europejscy administratorzy nie mogą już traktować USA jako monolitu prawnego – muszą brać pod uwagę, do jakiego stanu trafią dane. Mapa ryzyka regulacyjnego USA jest zróżnicowana terytorialnie: np. Kalifornia czy Kolorado oferują znacznie pełniejszy „przyjazny port" dla danych (*safe harbor* w szerokim tego słowa znaczeniu) niż stany nieuregulowane. Dla przedsiębiorstw europejskich oznacza to dodatkowy ciężar zgodności – konieczność śledzenia i analizy przepisów w poszczególnych jurysdykcjach oraz potencjalnie różnicowania środków zabezpieczających przy transferach (np. inne postanowienia umowne lub środki techniczne, jeśli importer nie podlega rygorom ustaw stanowych). Z punktu widzenia zasady równości i pewności prawa rodzi się też pytanie, czy taka sytuacja jest docelowo akceptowalna – tj. czy obywatel UE powinien mieć różny poziom ochrony w zależności od tego, czy jego dane trafią do np. Oregonu czy do Kalifornii.

Konkludując, obecny kształt transatlantyckiego reżimu transferowego można określić mianem hybrydowego i wielowarstwowego. Wobec braku federalnej ustawy prywatności, ciężar zapewnienia równoważnej ochrony spoczął na dwóch filarach: zreformowanym prawie federalnym (bezpieczeństwo narodowe) oraz aktywnym prawie stanowym (prywatność konsumencka). Adekwatność powinna zatem być oceniana łącznie w odniesieniu do obu tych warstw. Komisja Europejska, przyznając decyzję DPF, wzięła pod uwagę głównie warstwę pierwszą – mechanizmy EO 14086 i powiązane z nim zobowiązania USA. W kolejnych latach (zgodnie z zapowiedzią przeglądu decyzji po roku obowiązywania) Unia powinna jednak uwzględnić także rozwój sytuacji na poziomie stanowym. Możliwe, że w trakcie rewizji adekwatności pewna liczba kolejnych stanów będzie już wdrażać własne regulacje – być może niektóre nawet ostrzejsze niż omawiane pionierskie akty. Uznanie "hybrydowej adekwatności" oznaczałoby docenienie faktu, że choć USA nie ma jednolitego RODO, to sumaryczny efekt różnych norm (federalnych i stanowych) może zapewnić *de facto* porównywalny poziom ochrony. Taka perspektywa zachęcałaby również USA do utrzymania i rozszerzania reform – zarówno na szczeblu stanowym (zachęta dla kolejnych stanów do przyjmowania ustaw pro-privacy), jak i federalnym (docelowo przyjęcie ustawy ogólnokrajowej z preempcją, co wyeliminowałoby problem patchworku).

Na chwilę obecną należy jednak zachować ostrożność. Jak wskazano, granice supremacji powodują, że pewnych kluczowych różnic (dostęp służb) prawo stanowe

nie zniweluje. DPF stara się te różnice zminimalizować poprzez reformy wykonawcze – lecz skuteczność nowych mechanizmów (np. DPRC) dopiero zostanie zweryfikowana w praktyce. Z punktu widzenia unijnego prawa prywatności, konstrukcja transferów do USA będzie najprawdopodobniej nadal opierać się na warunkowej adekwatności (tylko dla certyfikowanych) oraz indywidualnych środkach zabezpieczających dla reszty przypadków. W tych zabezpieczeniach warto uwzględniać, jako argument zmniejszający ryzyko, fakt podlegania importera restrykcyjnemu prawu stanowemu. Nie zastąpi to wymogów wskazanych przez TSUE (jak ocena przepisów wywiadowczych), ale stanowi element szerszej układanki budującej zaufanie. Można prognozować, że finalnie droga do pełnej odbudowy zaufania w relacjach UE-USA będzie wiodła albo przez ustanowienie jednej, spójnej ustawy federalnej (co wymaga kompromisu politycznego w Kongresie), albo przez dalsze zacieśnianie standardów stanowych i ich uznaniowe "skorelowanie" z wymogami UE. W tym drugim scenariuszu, Komisja Europejska musiałaby w przyszłości formalnie czy nieformalnie uznać rolę prawa stanowego w ocenie poziomu ochrony – co niniejszy artykuł określa mianem postulatu hybrydowej adekwatności. Tylko poprzez łączne uwzględnienie obu wymiarów prawnych – bezpieczeństwa (federalnego) i prywatności (stanowego) – można oddać sprawiedliwy obraz ochrony danych w Stanach Zjednoczonych ery post-Privacy Shield.

BIBLIOGRAFIA

LITERATURA

Fajgielski P. [w:] *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych*. Komentarz, wyd. III, Warszawa 2025.

Karwala D., *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018.

Krzysztofek M. *Porównanie prawa ochrony danych osobowych w największych gospodarkach świata. Regulacji Unii Europejskiej (RODO), CHIN (PIPL) i Kalifornii (CCPA)*, Warszawa 2025.

AKTY PRAWNE

California Civil Code

Children's Online Privacy Protection Act of 1998 (COPPA) (Pub. L. No. 105–277, div. C, title XIII, 112 Stat. 2681-728).

Code of Virginia

Colorado Privacy Act

Executive Order 14086 z 7 października 2022 r., Enhancing Safeguards for United States Signals Intelligence Activities (Vol. 87, No 198).

Fair Credit Reporting Act (FCRA) (Pub. L. No. 91-508, 84 Stat. 1114).

Federal Trade Commission Act (Ch. 311, 38 Stat. 717).

Gramm-Leach-Bliley Act (Pub. L. No. 106–102, 113 Stat. 1338).

Health Insurance Portability and Accountability Act of 1996 (HIPAA). (Pub. L. No. 104-191, 110 Stat. 1936)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

ORZECZNICTWO

Decyzja wykonawcza Komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE-USA (Dz. U. UE. L. z 2023 r. Nr 231, str. 118).

Wyrok TSUE z 6 października 2015 r., C362/14, ZOTSiS 2015, nr 10, poz. I-650.

Wyrok TSUE z 16 lipca 2020 r., C311/18, LEX nr 3029449

Wyrok TS z 24 września 2019 r., C-507/17, LEX nr 2720952.

INNE PUBLIKACJE

ComplianceHub Wiki, *The Great Privacy Patchwork of 2025: Eight New State Laws Reshape America's Data Protection Landscape*, https://www.compliancehub.wiki/the-great-privacy-patchwork-of-2025-eight-new-state-laws-reshape-americas-data-protection-landscape/ [dostęp: 2.03.2026].

E. Basilico, *Regulatory fragmentation drags down efficiency*, https://alphaarchitect.com/regulatory-fragmentation-drags-down-efficiency/ [dostęp: 2.03.2026].

EROD, *Informacja nt. transferów danych do USA po przyjęciu DPF,* https://www.edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf [dostęp: 2.03.2026].

EROD, *Opinia 5/2023 dotycząca projektu decyzji wykonawczej Komisji Europejskiej w sprawie stwierdzenia zapewnienia odpowiedniego stopnia ochrony danych osobowych w ramach unijno-amerykańskich ram ochrony danych (EU-US Data Privacy Framework),* https://www.edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [dostęp: 2.03.2026].

EROD, *Zalecenia 01/2020 w sprawie środków uzupełniających dotyczących transferów, wersja 2.0 z 18 czerwca 2021 r.,* https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pl_0.pdf [dostęp: 2.03.2026].

Kongres, Izba Reprezentantów, *American Data Privacy and Protection Act: Reported in House*, [https://www.congress.gov/bill/117th-congress/house-bill/8152 [dostęp: 2.03.2026].

L. White, *Colorado's approach to universal opt-out requirements*, https://iapp.org/news/a/colorados-approach-to-universal-opt-out-requirements [dostęp: 2.03.2026].

Regulation Taskforce, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business*, https://treasury.gov.au/sites/default/files/2019-03/Reducing_Regulatory_Burdens_on_Business_Final_Government_Response.pdf [dostęp: 2.03.2026].

TRANSBORDER DATA TRANSFERS IN AN ERA OF REGIONAL REGULATORY INFLATION: A COMPARATIVE ANALYSIS OF GDPR TRANSFER MECHANISMS AND THE U.S. STATE LAW SYSTEM IN THE CONTEXT OF EMERGING MULTI-LAYERED PRIVACY REGIMES

Summary: The article examines the evolving landscape of EU–U.S. data transfers amid a crisis of trust following the Schrems II judgment and the proliferation of privacy regulations in the United States. We analyze the concept of "adequacy" by dissecting the EU-U.S. Data Privacy Framework (DPF) and Executive Order 14086 at the federal level, alongside the gaps in U.S. commercial data protection due to the lack of a federal omnibus privacy law. A comparative study of three model U.S. state privacy regimes – California's CPRA, Virginia's VCDPA, and Colorado's CPA – evaluates their definitions of sensitive data versus GDPR's Article 9, the scope of data subject rights (with a focus on whether Virginia's right to delete is equivalent to GDPR's Article 17), and enforcement mechanisms (California's CPPA vs. state Attorneys General). The functionality of state laws as "supplementary measures" in Transfer Impact Assessments (TIAs) is assessed, noting that state statutes can complement GDPR safeguards by filling commercial protection gaps, yet their effectiveness is bounded by the Supremacy Clause and federal surveillance powers (FISA Section 702). The findings support a "hybrid adequacy" postulate, arguing that an essentially equivalent level of protection emerges only from the combined effect of federal guarantees (national security safeguards) and state-level privacy rights, which should be jointly evaluated. The absence of federal preemption, however, risks uneven protection standards for EU citizens depending on the importer's U.S. state, underscoring the need for a multi-layered approach to adequacy.

Keywords: GDPR; transatlantic data transfers; adequacy; EU–US Data Privacy Framework (DPF); Executive Order 14086; U.S. state privacy law; CPRA; VCDPA; CPA; Transfer Impact Assessment (TIA); FISA 702; Supremacy Clause.

mgr **Dominika Filipek**
Akademia Leona Koźmińskiego w Warszawie
filipek.dominika.9.8@gmail.com
https://orcid.org/0000-0002-9659-6245

DANE JAKO AKTYWO PRZEDSIĘBIORSTWA – PRAWNE ASPEKTY KOMERCJALIZACJI I OBROTU ZANONIMIZOWANYMI ZBIORAMI DANYCH

Streszczenie: Rozdział analizuje transformację postrzegania danych z produktu ubocznego działalności gospodarczej w kluczowy składnik aktywów przedsiębiorstwa, determinujący pozycję konkurencyjną i możliwości rozwoju organizacji w dobie gospodarki cyfrowej. W pierwszym podrozdziale omówiono fundamentalną zmianę w podejściu do zasobów informacyjnych przedsiębiorstw, wskazując na ich rosnące znaczenie w kontekście transformacji cyfrowej, gdzie odpowiednio przetworzone i przeanalizowane dane stanowią istotną wartość ekonomiczną. Drugi podrozdział przedstawia ewolucję pojmowania danych jako przedmiotu prawa własności intelektualnej oraz została omówiona koncepcję „prawa własności danych" jako postulowanego nowego typu prawa własności intelektualnej oraz alternatywne modele oparte na kontroli dostępu i współdzieleniu danych. Podrozdział trzeci koncentruje się na prawnych aspektach procesu anonimizacji danych jako kluczowego mechanizmu umożliwiającego wyłączenie zbiorów danych spod reżimu RODO. Czwarty podrozdział analizuje standardy anonimizacji w świetle wytycznych Europejskiej Rady Ochrony Danych, podkreślając konieczność traktowania anonimizacji jako ciągłego procesu uwzględniającego rozwój technologii i nowe zagrożenia dla prywatności. Podsumowanie zawiera wnioski, postulujące m.in. wprowadzenie przepisów szczegółowo regulujących status prawny danych jako składnika przedsiębiorstwa oraz opracowanie jednolitych standardów anonimizacji.

Słowa kluczowe: gospodarka oparta na danych; anonimizacja danych; komercjalizacja danych; własność danych

WPROWADZENIE

Dynamiczny rozwój gospodarki opartej na danych (*data-driven economy*) doprowadził do fundamentalnej zmiany w postrzeganiu zasobów informacyjnych przedsiębiorstw. Dane, niegdyś traktowane wyłącznie jako produkt uboczny działalności gospodarczej, dziś stanowią jedno z kluczowych aktywów organizacji, decydujących o ich pozycji konkurencyjnej oraz możliwościach rozwoju. Zjawisko to nabrało szczególnego znaczenia w dobie transformacji cyfrowej, gdy coraz więcej aspektów działalności gospodarczej generuje ogromne ilości danych, które odpowiednio przetworzone i przeanalizowane mogą stanowić istotną wartość ekonomiczną. W tym kontekście niezwykle istotne staje się określenie prawnego statusu danych jako aktywów przedsiębiorstwa oraz analiza możliwości ich komercjalizacji, szczególnie po przeprowadzeniu procesu anonimizacji.

Celem niniejszego rozdziału jest analiza prawnych aspektów traktowania danych jako składnika aktywów przedsiębiorstwa, ze szczególnym uwzględnieniem możliwości komercjalizacji i obrotu zanonimizowanymi zbiorami danych w świetle 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 („RODO"). Opracowanie koncentruje się na problematyce prawnej dotyczącej statusu danych w obrocie gospodarczym, procesów anonimizacji jako mechanizmu umożliwiającego wyłączenie zbiorów danych spod reżimu RODO, instrumentów prawnych służących wycenie zasobów danych, a także wpływu nowych regulacji europejskich na krajowe ramy prawne obrotu danymi.

Znaczenie tej problematyki wykracza daleko poza akademickie rozważania. W praktyce gospodarczej przedsiębiorstwa coraz częściej stają przed pytaniami dotyczącymi możliwości legalnego obrotu posiadanymi zbiorami danych, metod ich wyceny w bilansie czy zabezpieczenia transakcji obejmujących transfer danych. Jednocześnie, brak jednoznacznych regulacji prawnych w tym zakresie stwarza istotne wyzwania zarówno dla przedsiębiorców, jak i dla doradców prawnych oraz instytucji regulacyjnych.

1. EWOLUCJA POJMOWANIA DANYCH JAKO PRZEDMIOTU PRAWA WŁASNOŚCI INTELEKTUALNEJ

Koncepcja danych jako przedmiotu prawa własności intelektualnej przeszła znaczącą ewolucję w ciągu ostatnich dekad. Początkowo dane były postrzegane

wyłącznie przez pryzmat ich potencjalnej ochrony na gruncie prawa autorskiego lub prawa *sui generis* do baz danych. Z czasem jednak, wraz z rosnącym znaczeniem gospodarczym danych samych w sobie, niezależnie od sposobu ich uporządkowania czy prezentacji, pojawiła się potrzeba wypracowania nowych koncepcji prawnych dotyczących własności danych[1].

Prawna kwalifikacja danych jako składnika przedsiębiorstwa wymaga w pierwszej kolejności odniesienia się do art. 55[1] ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2025 r., poz. 1071 ze zm.), który zawiera otwarty katalog składników przedsiębiorstwa. Zgodnie z tym przepisem, przedsiębiorstwo stanowi zorganizowany zespół składników niematerialnych i materialnych przeznaczonych do prowadzenia działalności gospodarczej, obejmujący m.in. oznaczenie indywidualizujące przedsiębiorstwo lub jego wyodrębnione części, własność nieruchomości lub ruchomości, prawa wynikające z umów najmu i dzierżawy nieruchomości, wierzytelności, prawa z papierów wartościowych, środki pieniężne, koncesje, licencje, zezwolenia, patenty, wzory użytkowe i inne prawa własności przemysłowej, majątkowe prawa autorskie i majątkowe prawa pokrewne, tajemnice przedsiębiorstwa, księgi i dokumenty związane z prowadzeniem działalności gospodarczej. Choć przepis ten nie wymienia wprost zbiorów danych, to w doktrynie i orzecznictwie przyjmuje się, że mogą one stanowić składnik przedsiębiorstwa, mieszczący się w kategorii „innych praw" lub „tajemnicy przedsiębiorstwa".

W kontekście ochrony prawnoautorskiej danych, należy zwrócić uwagę na wyrok Trybunału Sprawiedliwości Unii Europejskiej („TSUE") z dnia 29 lipca 2019 r. w sprawie C-469/17, w którym Trybunał stwierdził, że: „[…] Aby można było uznać twórczość intelektualną za własną twórczość jej autora, musi ona odzwierciedlać jego osobowość, co ma miejsce wówczas, gdy autor mógł wyrazić swoje możliwości twórcze przy realizacji utworu poprzez dokonywanie swobodnych i twórczych wyborów[2]. Po drugie, zakwalifikowanie jako „utworu" w rozumieniu dyrektywy 2001/29 jest zastrzeżone dla elementów stanowiących wyraz takiej twórczości intelektualnej[3]". Przedmiotowe orzeczenie potwierdza, że same dane, bez elementu twórczego w ich organizacji, nie mogą korzystać z ochrony prawnoautorskiej.

Ochrona danych na podstawie prawa *sui generis* do baz danych, uregulowanego dyrektywą 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r.

---

[1] W. Hydzik, *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych,* „Przegląd Ustawodawstwa Gospodarczego" 2019, s. 32.

[2] Wyrok TSUE z dnia 29 lipca 2019 r., C-469/17; zob. Wyrok TSUE z dnia 1 grudnia 2011 r., C-145/10, EU:C:2011:798, pkt 87-89.

[3] Zob. Wyrok TSUE z dnia 13 listopada 2018 r., C310/17, EU:C:2018:899, pkt 37 i przytoczone tam orzecznictwo; także Wyrok TSUE z dnia 29 lipca 2019 r., C-469/17.

w sprawie ochrony prawnej baz danych[4], implementowaną w Polsce przez ustawę z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2024 r., poz. 1769 ze zm.), także napotyka na istotne ograniczenia. Prawo to chroni bowiem nie tyle same dane, co istotne co do jakości lub ilości nakłady inwestycyjne na sporządzenie, weryfikację lub prezentację zawartości bazy danych[5].

W związku z tymi ograniczeniami, w doktrynie i praktyce gospodarczej coraz częściej postuluje się wprowadzenie nowego typu prawa własności – „prawa własności danych" (*data ownership right*). Koncepcja ta opiera się na założeniu, że dane jako dobro niematerialne o istotnej wartości gospodarczej, powinny być objęte szczególnym reżimem prawnym, umożliwiającym ich efektywną ochronę i komercjalizację[6].

Jednocześnie należy zauważyć, że koncepcja „własności danych" budzi liczne kontrowersje. Krytycy wskazują na potencjalne zagrożenia związane z monopolizacją dostępu do danych, które mogą prowadzić do ograniczenia innowacji i konkurencji[7]. Dlatego też, alternatywnie do modelu opartego na własności danych, proponuje się modele oparte na kontroli dostępu do danych (*access-based models*) czy też modele oparte na współdzieleniu danych (*data sharing models*). W polskim systemie prawnym dane mogą podlegać ochronie również jako:

1. Tajemnica przedsiębiorstwa - zgodnie z art. 11 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2026 r., poz. 85 ze zm.);
2. Baza danych - na podstawie wspomnianej wcześniej ustawy o ochronie baz danych;
3. Utwór - jeśli spełniają przesłanki ochrony prawnoautorskiej wynikające z ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2025 r., poz. 24 ze zm.);
4. Wynalazek - w ograniczonym zakresie, dane mogą stanowić element rozwiązania technicznego chronionego patentem na podstawie ustawy z dnia 30 czerwca 2000 r. Prawo własności przemysłowej (Dz. U z 2023 r., poz. 1170 ze zm.);

Warto podkreślić, że każda z tych form ochrony ma swoje specyficzne przesłanki i ograniczenia, co sprawia, że w praktyce ochrona danych jako aktywów

[4] Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych (Dz. U. UE. L. z 1996 r. Nr 77, str. 20 z późn. zm.).
[5] I. Kamińska, M. RozbickaOstrowska, *Ochrona danych osobowych a prawo do informacji publicznej*, Warszawa 2021, s. 12.
[6] W. Hydzik, *Cyberbezpieczeństwo i ochrona... op. cit.,* s. 32.
[7] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych*, *Komentarz*, Warszawa 2016, s. 45.

przedsiębiorstwa często wymaga zastosowania kompleksowych strategii prawnych, łączących różne instrumenty ochrony[8].

W kontekście transakcji gospodarczych, dane coraz częściej stanowią kluczowy element wartości przedsiębiorstw, szczególnie w sektorach takich jak *e-commerce*, *fintech* czy *healthtech*. W związku z tym, w praktyce transakcyjnej wykształciły się różnorodne mechanizmy umownego zabezpieczania praw do danych, takie jak szczegółowe postanowienia dotyczące transferu danych w umowach sprzedaży przedsiębiorstwa, umowy o powierzenie przetwarzania danych czy umowy licencyjne dotyczące korzystania z danych[9].

Ewolucja pojmowania danych jako przedmiotu prawa własności intelektualnej jest procesem dynamicznym, ściśle związanym z rozwojem technologicznym i gospodarczym. Wraz z pojawianiem się nowych technologii, takich jak sztuczna inteligencja czy internet rzeczy, które generują ogromne ilości danych, można oczekiwać dalszych zmian w podejściu do prawnej ochrony danych jako aktywów przedsiębiorstwa.

2. PRAWNE ASPEKTY PROCESU ANONIMIZACJI DANYCH

Szczególnego znaczenia w kontekście komercjalizacji danych nabiera problematyka danych osobowych. Zgodnie z art. 4 pkt 1 RODO, dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[10]. Komercjalizacja zbiorów danych zawierających dane osobowe podlega zatem rygorystycznym ograniczeniom wynikającym z przepisów RODO, w szczególności z zasady ograniczenia celu (art. 5 ust. 1 lit. b RODO) oraz zasady zgodności przetwarzania z prawem (art. 5 ust. 1 lit. a RODO).

W tym kontekście szczególnego znaczenia nabiera instytucja anonimizacji danych. Motyw 26 RODO stanowi, że „[…] Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować […]". Skuteczna anonimizacja danych pozwala zatem na wyłączenie zbioru danych spod reżimu RODO, co umożliwia ich swobodną komercjalizację, bez konieczności uzyskiwania

[8] J. Barta, R. Markiewicz, Prawo do prywatności w społeczeństwie informatycznym, „Ethos" 1999, s. 67.
[9] P. Drobek, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak Jomaa (red.), D. Lubasz (red.), Warszawa 2017, s. 18.
[10] P. Barta, P. Litwiński, *Ustawa o ochronie… op. cit.*, s. 78.

zgody osób, których dane dotyczą, czy spełniania innych przesłanek legalizacyjnych przewidzianych w RODO[11].

Warto jednak podkreślić, że proces anonimizacji, aby był skuteczny z perspektywy RODO, musi spełniać wysokie standardy. Zgodnie ze stanowiskiem Europejskiego Trybunału Sprawiedliwości wyrażonym w wyroku z dnia 19 października 2016 r. w sprawie C-582/14[12], dane mogą być uznane za dane osobowe nawet wtedy, gdy ich powiązanie z konkretną osobą wymaga pozyskania dodatkowych informacji od strony trzeciej. Oznacza to, że proces anonimizacji musi być przeprowadzony w sposób uniemożliwiający reidentyfikację nawet przy wykorzystaniu dodatkowych zewnętrznych źródeł danych.

Grupa Robocza Art. 29 w opinii 05/2014 dotyczącej technik anonimizacji przyjęta w dniu 10 kwietnia 2014 r., zidentyfikowała trzy kryteria, które muszą być spełnione, aby proces anonimizacji był skuteczny:

1. Niemożliwość wyodrębnienia (indywidualizacji) – dane nie mogą pozwalać na wyodrębnienie rekordu odnoszącego się do konkretnej osoby;
2. Niemożliwość łączenia – dane nie mogą pozwalać na łączenie ze sobą dwóch lub więcej rekordów dotyczących tej samej osoby;
3. Niemożliwość wnioskowania – na podstawie danych nie można wnioskować z istotnym prawdopodobieństwem o wartościach atrybutów konkretnej osoby.

W praktyce, skuteczna anonimizacja danych może być realizowana przez różne techniki, takie jak:

1. Generalizacja – zastępowanie szczegółowych wartości wartościami bardziej ogólnymi (np. zamiast dokładnego wieku podawanie przedziału wiekowego);
2. Zaburzanie danych (perturbacja) – losowa modyfikacja wartości danych poprzez dodawanie szumu statystycznego;
3. Randomizacja – zastępowanie wartości losowymi danymi;
4. Agregacja – zastępowanie indywidualnych wartości wartościami statystycznymi (średnia, mediana, etc.);
5. K-anonimizacja – technika polegająca na takim przekształceniu zbioru danych, aby każdy rekord nie mógł zostać odróżniony od co najmniej k-1 innych rekordów na podstawie tzw. quasi-identyfikatorów.

[11] W. Hydzik, *Cyberbezpieczeństwo i ochrona... op. cit.,* s. 34.
[12] Zob. wyrok TSUE z dnia 19 października 2016 r., C-582/14.

Wybór odpowiedniej metody anonimizacji powinien być dostosowany do charakteru danych, celu ich komercjalizacji oraz potencjalnych ryzyk związanych z reidentyfikacją[13]. Warto podkreślić, że niektóre metody anonimizacji, jak np. pseudonimizacja, nie są uznawane za wystarczające do wyłączenia zbioru danych spod reżimu RODO. Zgodnie z art. 4 pkt 5 RODO, pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[14].

Istotnym wyzwaniem prawnym związanym z procesem anonimizacji jest kwestia odpowiedzialności za potencjalną reidentyfikację danych. W przypadku, gdy zanonimizowane dane zostaną poddane procesowi reidentyfikacji przez nabywcę danych lub osobę trzecią, powstaje pytanie o odpowiedzialność prawną pierwotnego administratora danych, który przeprowadził proces anonimizacji[15]. W doktrynie prawniczej dominuje pogląd, że administrator danych powinien ponosić odpowiedzialność za skuteczność procesu anonimizacji tylko w zakresie, w jakim reidentyfikacja jest możliwa przy użyciu środków, których zastosowania można racjonalnie oczekiwać w momencie przeprowadzania anonimizacji.

W kontekście odpowiedzialności za skuteczność anonimizacji, istotne znaczenie ma również dokumentowanie procesu anonimizacji oraz przeprowadzanie regularnych przeglądów skuteczności zastosowanych technik. Administrator powinien być w stanie wykazać, że zastosowane środki techniczne i organizacyjne zapewniają skuteczną anonimizację danych z uwzględnieniem aktualnego stanu wiedzy technologicznej.

Coraz częściej w praktyce stosuje się tzw. prywatność różnicową (*differential privacy*), która jest matematycznym modelem zapewniającym silne gwarancje ochrony prywatności, nawet w przypadku posiadania przez atakującego znacznej wiedzy kontekstowej. Technika ta polega na dodaniu precyzyjnie skalibrowanego szumu statystycznego do wyników zapytań do bazy danych, co zapewnia, że włączenie lub wyłączenie pojedynczej osoby ze zbioru danych nie wpływa istotnie na wynik zapytania. Prywatność różnicowa jest coraz częściej uznawana za złoty standard w zakresie ochrony prywatności w analizie danych[16].

---

[13] I. Kamińska, M. RozbickaOstrowska, *Ochrona danych…, op. cit.*, s. 12.
[14] P. Barta, P. Litwiński, *Ustawa o ochronie… op. cit.*, s. 80.
[15] J. Barta, R. Markiewicz, Prawo do prywatności…, op. cit., s. 67.
[16] I. Kamińska, M. RozbickaOstrowska, *Ochrona danych…, op. cit.*, s. 13-14.

Warto również zwrócić uwagę na kwestię prawnych aspektów procesu anonimizacji w kontekście badań naukowych i statystyki publicznej. Odpowiednio w odniesieniu do art. 89 ust. 2 RODO, przetwarzanie danych do celów badań naukowych, historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom, które mogą obejmować pseudonimizację lub anonimizację danych[17]. W polskim porządku prawnym, szczególne znaczenie w tym kontekście ma ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r., poz. 1799 ze zm.), która określa zasady anonimizacji danych dla celów statystycznych.

W kontekście komercjalizacji zbiorów danych, kluczowe znaczenie ma odpowiednie uregulowanie w umowach kwestii związanych z procesem anonimizacji. W szczególności, umowy takie powinny określać:

1. Metodologię anonimizacji, w tym zastosowane techniki i środki bezpieczeństwa,
2. Podział odpowiedzialności za skuteczność anonimizacji,
3. Procedury postępowania w przypadku potencjalnej reidentyfikacji danych,
4. Zasady regularnej weryfikacji skuteczności zastosowanych technik anonimizacji,
5. Gwarancje i zapewnienia dotyczące zgodności procesu anonimizacji z przepisami prawa.

Odpowiednio skonstruowane postanowienia umowne mogą znacząco ograniczyć ryzyko prawne związane z komercjalizacją zanonimizowanych zbiorów danych, zapewniając jednocześnie odpowiednią ochronę interesów wszystkich stron transakcji[18].

3. STANDARDY ANONIMIZACJI W ŚWIETLE WYTYCZNYCH EUROPEJSKIEJ RADY OCHRONY DANYCH

Europejska Rada Ochrony Danych („EROD") w wytycznych 05/2020 dotyczących zgody jednoznacznie podkreśliła konieczność regularnej weryfikacji skuteczności zastosowanych technik anonimizacji w kontekście postępującego rozwoju technologicznego, który potencjalnie może prowadzić do reidentyfikacji uprzednio zanonimizowanych danych. Jest to szczególnie istotne w kontekście ryzyka inferencyjnego, czyli możliwości dedukowania informacji o osobach fizycznych na podstawie pozornie zanonimizowanych zbiorów danych[19].

[17] P. Fajgielski, *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021, s. 34.
[18] A. SaganJeżowska, *Klauzule RODO. Wzory klauzul z praktycznym komentarzem*, Warszawa 2018, s. 56.
[19] C. Banasiński, *Cyberbezpieczeństwo. Zarys wykładu*, wyd. II, Warszawa 2023, s. 23.

Kontynuując prace swojego poprzednika – Grupy Roboczej Art. 29, EROD systematycznie rozwija standardy anonimizacji danych. Zgodnie ze stanowiskiem EROD, anonimizacja powinna być traktowana jako proces ciągły, a nie jednorazowe działanie. Administrator danych zobowiązany jest regularnie weryfikować skuteczność zastosowanych technik, uwzględniając rozwój technologii umożliwiających reidentyfikację, dostępność nowych źródeł danych oraz zmiany w kontekście społeczno-gospodarczym wpływające na możliwość identyfikacji osób.

EROD zwraca uwagę na fundamentalny paradoks anonimizacji – im bardziej szczegółowe i bogate są dane, tym większa ich wartość analityczna, ale jednocześnie tym wyższe ryzyko reidentyfikacji. Dlatego właściwy dobór techniki anonimizacji wymaga precyzyjnego wyważenia między zachowaniem użyteczności danych a skuteczną ochroną prywatności.

Skuteczność technik anonimizacji powinna być oceniana według czterech zasadniczych kryteriów: odporności na celowe ataki reidentyfikacyjne przeprowadzane przez podmioty dysponujące specjalistyczną wiedzą i zasobami, skalowalności niezależnie od wielkości zbioru danych, odporności na przewidywalny rozwój technologiczny oraz odporności na dodatkowe informacje, które potencjalny atakujący może pozyskać z zewnętrznych źródeł[20].

W ocenie EROD, wśród technik anonimizacji szczególnie wartościowe są metody oparte na randomizacji (zwłaszcza prywatność różnicowa, zapewniająca silne gwarancje prywatności) oraz generalizacji (k-anonimizacja, l-różnorodność, t-bliskość), choć te ostatnie wymagają ostrożnego stosowania ze względu na podatność na ataki inferencyjne. Pseudonimizacja sama w sobie nie jest wystarczająca do uznania danych za zanonimizowane, natomiast techniki oparte na kryptografii, choć obiecujące, wymagają odpowiedniego zarządzania kluczami kryptograficznymi[21].

Wybór właściwej techniki anonimizacji powinien być poprzedzony dogłębną analizą ryzyka uwzględniającą charakter danych (szczególnie wrażliwe dane wymagają rygorystycznych technik anonimizacji), kontekst przetwarzania, cel dalszego wykorzystania danych oraz możliwe metody ataku, w tym te oparte na łączeniu z zewnętrznymi źródłami informacji.

Standardy anonimizacji w świetle wytycznych EROD oraz innych organów nadzorczych tworzą kompleksowy system zasad i praktyk, które powinni stosować administratorzy danych planujący komercjalizację zanonimizowanych zbiorów. Przestrzeganie tych standardów nie tylko minimalizuje ryzyko prawne związane

[20] A. SaganJeżowska, *Klauzule RODO…, op. cit.*, s. 56.
[21] T. Wyka, M. A. Mielczarek, *Administrator i inspektor ochrony danych osobowych*, [w:] T. Wyka, M.A. Mielczarek (red.), Warszawa 2019, s. 43.

z potencjalnym naruszeniem przepisów o ochronie danych osobowych, ale również zwiększa zaufanie do komercyjnych produktów opartych na danych[22].

Obok procesu anonimizacji, istotnym aspektem komercjalizacji zbiorów danych jest ich wycena jako składnika aktywów przedsiębiorstwa. Tradycyjne metody wyceny aktywów niematerialnych napotykają na szereg wyzwań w odniesieniu do zbiorów danych ze względu na ich unikatowy charakter, trudności w określeniu okresu ekonomicznej użyteczności oraz dynamiczne zmiany wartości w czasie. W praktyce rynkowej wykształciły się specyficzne metody wyceny zbiorów danych, uwzględniające czynniki takie jak aktualność danych, ich kompletność, dokładność, unikalność, potencjał analityczny czy zgodność z przepisami prawa.

Przy wycenie wartości niematerialnych i prawnych, w tym zbiorów danych, kluczowe znaczenie ma ich zdolność do generowania przyszłych korzyści ekonomicznych dla przedsiębiorstwa. Wartość zbiorów danych powinna być określana przede wszystkim przez pryzmat ich potencjału do tworzenia wartości dodanej, na przykład poprzez optymalizację procesów biznesowych, lepsze zrozumienie preferencji klientów czy identyfikację nowych możliwości rynkowych[23].

W praktyce wycena zbiorów danych opiera się na różnych metodologiach. Metody kosztowe, bazujące na oszacowaniu nakładów na pozyskanie lub odtworzenie zbioru danych, uwzględniają koszty zbierania, przechowywania, przetwarzania oraz zabezpieczania informacji. Zaletą tych metod jest względna prostota, jednak często nie odzwierciedlają one rzeczywistej wartości ekonomicznej danych. Metody dochodowe, szacujące przyszłe korzyści ekonomiczne możliwe do uzyskania dzięki wykorzystaniu zbioru danych, obejmują między innymi analizę zdyskontowanych przepływów pieniężnych, opcji realnych czy nadwyżek przychodów. Uwzględniają one potencjał ekonomiczny danych, choć wymagają przyjęcia wielu założeń dotyczących przyszłych korzyści[24]. Metody porównawcze, oparte na analizie podobnych zbiorów danych o znanej wartości rynkowej, mają tę zaletę, że bazują na rzeczywistych danych rynkowych, jednak ze względu na unikatowy charakter zbiorów danych oraz ograniczoną transparentność rynku, ich zastosowanie bywa utrudnione. Coraz częściej stosowane są również metody mieszane, łączące elementy różnych podejść oraz metody oparte na teorii gier, uwzględniające strategiczne interakcje między podmiotami na rynku danych oraz wartość informacji w różnych scenariuszach współpracy lub konkurencji.

[22] C. Banasiński, *Cyberbezpieczeństwo… op. cit.,* s. 23.
[23] T. Wyka, M. A. Mielczarek, *Administrator… op. cit.,* s. 44.
[24] C. Banasiński, *Cyberbezpieczeństwo… op. cit.,* s. 24-25.

W zakresie prawnych aspektów obrotu zbiorami danych kluczowe znaczenie mają umowy regulujące transfer danych między podmiotami. W praktyce rynkowej wykształciło się kilka typów takich umów. Umowy sprzedaży zbiorów danych regulują jednorazowy transfer w zamian za ustaloną cenę i powinny precyzyjnie określać zakres transferowanych danych, gwarancje dotyczące ich jakości i legalności, zasady odpowiedzialności za wady prawne i fizyczne oraz ewentualne ograniczenia w wykorzystaniu danych[25]. Umowy licencyjne dotyczą czasowego udostępnienia danych w zamian za opłatę licencyjną i określają zakres udzielanej licencji, czas jej trwania, dozwolone sposoby korzystania z danych, zasady sublicencjonowania oraz warunki wypowiedzenia. Umowy o świadczenie usług opartych na danych regulują dostarczanie usług analitycznych, predykcyjnych czy rekomendacyjnych bazujących na zbiorach danych, określając zakres świadczonych usług, standardy jakości, poziom dostępności, zasady raportowania oraz kwestie własności intelektualnej do wyników analiz. Umowy o wspólnym korzystaniu z danych normują zasady współdzielenia informacji między różnymi podmiotami, na przykład w ramach konsorcjów badawczych, partnerstw strategicznych czy platform wymiany danych, określając zasady dostępu, zakres dozwolonego wykorzystania, zasady podziału korzyści oraz mechanizmy rozstrzygania sporów. Umowy o powierzenie przetwarzania danych regulują przetwarzanie danych osobowych przez podmiot przetwarzający na zlecenie administratora danych, zgodnie z art. 28 RODO, co ma szczególne znaczenie, gdy przedmiotem obrotu są dane osobowe lub gdy proces anonimizacji jest przeprowadzany przez podmiot trzeci.

W kontekście fuzji i przejęć zbiory danych stanowią coraz istotniejszy element wpływający na wycenę transakcji oraz strukturę umowy[26]. W ramach procesu *due diligence* szczególną uwagę poświęca się legalności posiadanych zbiorów danych (zgodność z przepisami o ochronie danych osobowych, prawem autorskim, przepisami o ochronie baz danych czy regulacjami sektorowymi), ich jakości i kompletności (aktualność, dokładność i przydatność biznesowa), bezpieczeństwu (stosowane środki techniczne i organizacyjne zapewniające poufność, integralność i dostępność) oraz prawom do wykorzystania (umowy z osobami, których dane dotyczą, umowy z dostawcami danych, ograniczenia wynikające z przepisów prawa)[27].

W strukturze transakcji dotyczących przedsiębiorstw opartych na danych coraz częściej stosuje się zaawansowane mechanizmy zabezpieczające, takie jak *earn-out*

[25] P. Drobek, [w:] *RODO. Ogólne rozporządzenie… op.cit.,* s. 18.
[26] C. Banasiński, *Cyberbezpieczeństwo… op. cit.,* s. 25.
[27] A. Pązik, M. Świerczyński, B. Fischer, *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2023, s. 64.

(uzależnienie części ceny od przyszłych wyników ekonomicznych uzyskanych dzięki wykorzystaniu zbiorów danych), gwarancje i oświadczenia dotyczące zbiorów danych (zgodność z przepisami, kompletność, brak roszczeń osób trzecich) oraz kary umowne związane z wadami prawnymi lub fizycznymi zbiorów danych.

Istotnym aspektem obrotu zbiorami danych są również kwestie podatkowe. W zakresie podatku dochodowego kluczowe znaczenie ma możliwość amortyzacji nabytych zbiorów danych jako wartości niematerialnych i prawnych. Zbiory danych mogą być przedmiotem amortyzacji podatkowej pod warunkiem, że są nabyte (a nie wytworzone we własnym zakresie), możliwa jest ich identyfikacja oraz wiarygodne określenie wartości początkowej[28]. W praktyce możliwość amortyzacji nabytych zbiorów danych może stanowić istotny czynnik wpływający na decyzje inwestycyjne przedsiębiorstw.

PODSUMOWANIE

Prawne aspekty komercjalizacji i obrotu zanonimizowanymi zbiorami danych stanowią złożone i dynamicznie rozwijające się zagadnienie na styku prawa cywilnego, handlowego, własności intelektualnej, ochrony danych osobowych oraz prawa konkurencji. Dynamiczny rozwój gospodarki opartej na danych wymaga wypracowania nowych ram prawnych, które z jednej strony będą stymulować innowacje i umożliwią efektywne wykorzystanie potencjału ekonomicznego danych, a z drugiej – zapewnią odpowiednią ochronę praw jednostek i interesów konsumentów.

Przeprowadzona analiza prowadzi do istotnych wniosków dotyczących statusu prawnego danych. Dane jako składnik aktywów przedsiębiorstwa stanowią szczególny rodzaj dobra niematerialnego, którego status prawny nie jest jednoznacznie uregulowany w obecnym stanie prawnym. W zależności od charakteru danych oraz sposobu ich uporządkowania i prezentacji, mogą one podlegać ochronie na podstawie różnych reżimów prawnych, takich jak prawo autorskie, prawo własności przemysłowej, przepisy o ochronie baz danych czy przepisy o ochronie tajemnicy przedsiębiorstwa.

Proces anonimizacji danych stanowi kluczowy mechanizm umożliwiający komercjalizację zbiorów danych zawierających pierwotnie dane osobowe. Aby anonimizacja była skuteczna z perspektywy RODO, musi ona spełniać wysokie standardy określone w wytycznych Europejskiej Rady Ochrony Danych oraz w orzecznictwie Trybunału Sprawiedliwości UE. Skuteczna anonimizacja powinna uniemożliwiać

[28] P. Drobek, [w:] *RODO. Ogólne rozporządzenie… op.cit.,* s.18.

reidentyfikację osób fizycznych nawet przy wykorzystaniu dodatkowych zewnętrznych źródeł danych.

Wycena zbiorów danych jako aktywów przedsiębiorstwa napotyka na szereg wyzwań wynikających z unikalnego charakteru danych, trudności w określeniu okresu ich ekonomicznej użyteczności oraz dynamicznych zmian ich wartości w czasie. W praktyce rynkowej wykształciły się różnorodne metody wyceny zbiorów danych, uwzględniające takie czynniki jak aktualność danych, ich kompletność, dokładność, unikalność czy potencjał analityczny.

Obrót zanonimizowanymi zbiorami danych odbywa się w ramach różnych modeli umownych, takich jak umowy sprzedaży, umowy licencyjne, umowy o świadczenie usług opartych na danych czy umowy o wspólnym korzystaniu z danych. Umowy te powinny precyzyjnie regulować zakres transferowanych danych, gwarancje dotyczące ich jakości i legalności, zasady odpowiedzialności za wady prawne i fizyczne oraz ewentualne ograniczenia w wykorzystaniu danych.

W polskim porządku prawnym zidentyfikowano szereg luk regulacyjnych, które mogą stanowić barierę dla rozwoju krajowego rynku danych. Należą do nich przede wszystkim: brak szczegółowych regulacji dotyczących własności danych, nieprecyzyjne przepisy dotyczące obrotu zanonimizowanymi danymi, brak regulacji dotyczących wyceny zbiorów danych oraz niespójności między europejskimi inicjatywami legislacyjnymi a krajowymi przepisami prawa handlowego. W świetle powyższych wniosków, można sformułować następujące postulaty *de lege ferenda*:

- Wprowadzenie do polskiego porządku prawnego przepisów szczegółowo regulujących status prawny danych jako składnika przedsiębiorstwa, w tym zasady ich wyceny, amortyzacji oraz obrotu. Przepisy te powinny uwzględniać specyfikę różnych kategorii danych, takich jak dane strukturalne, niestrukturalne, dane maszynowe czy dane sensoryczne.
- Opracowanie i przyjęcie jednolitych standardów anonimizacji danych, które zapewnią odpowiedni poziom ochrony prywatności przy jednoczesnym zachowaniu użyteczności danych dla celów analitycznych i badawczych. Standardy te powinny być elastyczne, aby uwzględniać postęp technologiczny oraz zmieniające się zagrożenia dla prywatności.
- Wprowadzenie typowej umowy nazwanej dotyczącej obrotu danymi, która określałaby standardowe prawa i obowiązki stron takiej umowy. Umowa taka powinna regulować takie kwestie jak zakres transferowanych danych, gwarancje dotyczące ich jakości i legalności, zasady odpowiedzialności za wady prawne i fizyczne, ograniczenia w wykorzystaniu danych czy mechanizmy rozstrzygania sporów.

- Uregulowanie kwestii własności danych generowanych przez systemy automatycznego zbierania danych. Regulacja ta powinna określać prawa i obowiązki różnych podmiotów zaangażowanych w proces generowania, przetwarzania i wykorzystywania danych, takich jak producenci urządzeń, ich użytkownicy czy podmioty świadczące usługi przetwarzania danych.
- Dostosowanie polskich przepisów do wymogów europejskich regulacji dotyczących danych, w szczególności *Data Governance Act* i *Data Act*. Adaptacja ta powinna uwzględniać specyfikę polskiego rynku danych oraz istniejące ramy prawne obrotu aktywami niematerialnymi.
- Wprowadzenie mechanizmów wspierających rozwój krajowego rynku danych, takich jak zachęty podatkowe dla przedsiębiorstw inwestujących w aktywa oparte na danych, programy wsparcia dla startupów działających w obszarze analityki danych czy inicjatywy edukacyjne zwiększające świadomość prawnych aspektów komercjalizacji danych.
- Wprowadzenie regulacji dotyczących transparentności i odpowiedzialności w obrocie danymi, w szczególności w kontekście wykorzystania danych do trenowania systemów sztucznej inteligencji. Regulacje te powinny określać minimalne standardy informacyjne dotyczące pochodzenia i jakości danych oraz zasady odpowiedzialności za szkody wynikające z wykorzystania wadliwych lub niezgodnych z prawem zbiorów danych.
- Stworzenie instytucjonalnych ram współpracy między różnymi organami regulacyjnymi zaangażowanymi w nadzór nad rynkiem danych, takimi jak Prezes Urzędu Ochrony Danych Osobowych, Prezes Urzędu Ochrony Konkurencji i Konsumentów czy organy nadzoru sektorowego. Współpraca ta powinna obejmować wymianę informacji, koordynację działań nadzorczych oraz wypracowywanie spójnego podejścia do regulacji rynku danych.

Niezależnie od przyjętego podejścia legislacyjnego, kluczowe znaczenie ma zapewnienie odpowiedniej równowagi między stymulowaniem innowacji gospodarczych opartych na danych a ochroną praw jednostek i interesów społecznych. *De lege ferenda* dane jako aktywo przedsiębiorstwa powinny uzyskać jasno określony status prawny, uwzględniający unikalną kategorię tych dóbr, łączącą cechy dóbr ekonomicznych z aspektami praw człowieka i interesów zbiorowych. Efektywne ramy prawne komercjalizacji danych muszą zatem uwzględniać tę dualność, zapewniając zarówno możliwości rozwoju gospodarczego, jak i respektowanie fundamentalnych wartości demokratycznego społeczeństwa.

BIBLIOGRAFIA

LITERATURA

Banasiński C., *Cyberbezpieczeństwo. Zarys wykładu,* wyd. II, Warszawa 2023.

Barta J., Markiewicz R., *Prawo do prywatności w społeczeństwie informatycznym*, „Ethos" 1999.

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych*. Komentarz, Warszawa 2016.

Drobek P., [w:] *RODO. Ogólne rozporządzenie o ochronie danych.* BielakJomaa E. (red.), Lubasz D. (red.), Komentarz, Warszawa 2017.

Fajgielski P., *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021.

Hydzik W., *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Przegląd Ustawodawstwa Gospodarczego" 2019.

Kamińska I., RozbickaOstrowska M., *Ochrona danych osobowych a prawo do informacji publicznej*, Warszawa 2021.

Pązik A., Świerczyński M., Fischer B., *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2023.

SaganJeżowska A., *Klauzule RODO. Wzory klauzul z praktycznym komentarzem*, Warszawa 2018.

Wyka T., Mielczarek M.A. [w:] *Administrator i inspektor ochrony danych osobowych*, Wyka T. (red.), Mielczarek M.A. (red.), Warszawa 2019.

AKTY PRAWNE

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.

Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych (Dz. U. UE. L. z 1996 r. Nr 77, str. 20 z późn. zm.).

Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2025 r., poz. 1071 ze zm.).

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2026 r., poz. 85 ze zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2025 r., poz. 24 ze zm.).

Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r., poz. 1799 ze zm.).

Ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej (Dz. U z 2023 r., poz. 1170 ze zm.).

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2024 r., poz. 1769 ze zm.).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r., poz. 902 ze zm.).

ORZECZNICTWO

Wyrok TSUE z dnia 19 października 2016 r., C-582/14.

Wyrok TSUE z dnia 1 grudnia 2011 r., C-145/10.

Wyrok TSUE z dnia 13 listopada 2018 r., C310/17.

Wyrok TSUE z dnia 29 lipca 2019 r., C-469/17.

DATA AS AN ENTERPRISE ASSET – LEGAL ASPECTS OF COMMERCIALIZATION AND TRADE IN ANONYMIZED DATA COLLECTS

Summary: The chapter analyzes the transformation of data perception from a by-product of economic activity into a key asset of the enterprise, determining the competitive position and development opportunities of the organization in the era of the digital economy. The first subchapter discusses a fundamental change in the approach to enterprise information resources, pointing to their growing importance in the context of digital transformation, where properly processed and analyzed data constitute significant economic value. The second subsection presents the evolution of the understanding of data as a subject of intellectual property law and discusses the concept of "data ownership" as a postulated new type of intellectual property law and alternative models based on access control and data sharing. The third subchapter focuses on the legal aspects of the data anonymisation process as a key mechanism enabling the exclusion of data sets from the GDPR regime. The fourth subchapter analyses anonymisation standards in the light of the guidelines of the European Data Protection Board, emphasizing the need to treat anonymisation as a continuous process that takes into account technological developments and new threats to privacy. The summary contains conclusions, including the introduction of provisions specifically regulating the legal status of data as a component of an enterprise and the development of uniform anonymization standards.

Keywords: *data-driven economy; data anonymization; data commercialization; data ownership*

Agnieszka Jagielska
Uniwersytet SWPS z siedzibą w Warszawie
a.jagielska.biuro@gmail.com

STATUS I OBOWIĄZKI NOTARIUSZA JAKO ADMINISTRATORA DANYCH OSOBOWYCH W ŚWIETLE RODO

Streszczenie: Artykuł poświęcono analizie statusu notariusza jako administratora danych osobowych oraz obowiązków związanych z przetwarzaniem danych w świetle RODO. Przedstawiono podstawy prawne przetwarzania danych osobowych w działalności notarialnej, wynikające zarówno z RODO, jak i ustawy – Prawo o notariacie, ze szczególnym uwzględnieniem specyfiki czynności notarialnych, obowiązków publicznoprawnych oraz roli notariusza jako osoby zaufania publicznego. Omówiono zasady przetwarzania danych w kancelarii notarialnej, w tym zasadę legalności, minimalizacji, rozliczalności, obowiązek informacyjny oraz zakres realizacji praw osób, których dane dotyczą. Analiza objęła także problematykę archiwizacji dokumentacji notarialnej, bezpieczeństwa informacji i cyberbezpieczeństwa w warunkach postępującej cyfryzacji czynności notarialnych. Wskazano, że zapewnienie zgodności działalności kancelarii notarialnej z RODO wymaga połączenia środków prawnych, organizacyjnych i technicznych, a także wdrożenia spójnych procedur ochrony danych, które ograniczają ryzyko odpowiedzialności i wzmacniają zaufanie do notariatu.

Słowa kluczowe: RODO; ochrona danych osobowych; kancelaria notarialna; notariusz; cyberbezpieczeństwo; bezpieczeństwo informacji; tajemnica notarialna

WPROWADZENIE

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.[1], powszechnie określane jako Ogólne Rozporządzenie o Ochronie

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L nr 119 z 4.05.2016 r., s. 1-88, „RODO").

Danych Osobowych, wprowadziło jednolite zasady przetwarzania danych osobowych w państwach członkowskich Unii Europejskiej. Postępująca cyfryzacja obrotu prawnego oraz rosnąca skala przetwarzania danych osobowych sprawiają, że ich ochrona stanowi jedno z kluczowych wyzwań współczesnych systemów prawnych. Szczególne znaczenie ma to w odniesieniu do zawodów zaufania publicznego, w tym notariuszy, których działalność wiąże się z przetwarzaniem danych o często wrażliwym charakterze. RODO ustanowiło jednolite ramy ochrony danych w Unii Europejskiej, nakładając na administratorów danych – w tym notariuszy – liczne obowiązki prawne, organizacyjne i techniczne, służące zapewnieniu ochrony praw i wolności osób fizycznych, w szczególności prawa do prywatności.

Dynamiczny rozwój technologii i globalizacja zwiększyły skalę gromadzenia, przetwarzania i wymiany danych osobowych, co rodzi nowe wyzwania w zakresie ich ochrony. Nowoczesne technologie umożliwiają przetwarzanie danych na niespotykaną dotąd skalę, a osoby fizyczne coraz częściej udostępniają swoje dane w przestrzeni publicznej[2].

Postęp technologiczny sprzyja swobodnemu przepływowi danych osobowych w Unii Europejskiej oraz ich przekazywaniu do państw trzecich i organizacji międzynarodowych. Wymaga to jednak zapewnienia wysokiego poziomu ochrony danych oraz spójnych ram prawnych, które wzmacniają zaufanie i umożliwiają rozwój gospodarki cyfrowej, przy jednoczesnym zachowaniu przez osoby fizyczne kontroli nad ich danymi.

Artykuł analizuje wyzwania związane z funkcjonowaniem kancelarii notarialnych w kontekście RODO, przedstawiając rolę notariusza jako administratora danych osobowych. Omawia podstawy prawne przetwarzania danych wynikające z RODO i ustawy – Prawo o notariacie, a także praktyczne problemy dotyczące bezpieczeństwa danych, realizacji praw osób, których dane dotyczą, oraz zarządzania ryzykiem naruszeń.

1. PODSTAWOWE POJĘCIA I ZAKRES ZASTOSOWANIA RODO W KANCELARII NOTARIALNEJ – DANE OSOBOWE I PRZETWARZANIE

RODO, obowiązujące od 25 maja 2018 r., reguluje zasady ochrony danych osobowych osób fizycznych przetwarzanych zarówno przez podmioty prywatne, jak i organy władzy publicznej oraz inne instytucje. W odróżnieniu od wcześniej

[2] E. Bielak-Jomaa, D. Lubasz, *Ogólne rozporządzenie o ochronie danych. Komentarz*, Wolters Kluwer, Warszawa 2018, s. 25.

obowiązującej ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[3], RODO nie zawiera przepisów wprost określających zakres jego zastosowania w ujęciu podmiotowym. Analiza przepisów RODO, w szczególności art. 4 definiującego m.in. administratora danych, podmiot przetwarzający i odbiorcę danych, prowadzi do wniosku, że regulacje te mają zastosowanie także do przetwarzania danych osobowych przez podmioty sektora publicznego. Wyłączenie stosowania RODO wobec tych podmiotów ma charakter wyjątkowy i dotyczy jedynie określonych sytuacji wskazanych w motywach 16 i 19 preambuły oraz w art. 6 ustawy z 10 maja 2018 r. o ochronie danych osobowych[4].

W celu określenia zakresu RODO należy odwołać się do definicji „danych osobowych", „przetwarzania" i „zbioru danych" oraz do art. 1 i art. 2 ust. 1 rozporządzenia. Z motywu 14 preambuły wynika, że RODO dotyczy danych osób fizycznych niezależnie od obywatelstwa i miejsca zamieszkania, natomiast nie obejmuje danych osób zmarłych ani *nasciturusa*[5]. RODO nie ma zastosowania do przetwarzania danych dotyczących osób prawnych, takich jak firma, forma prawna czy dane kontaktowe przedsiębiorstwa. W doktrynie pojawiają się jednak wątpliwości co do dokładnego zakresu tych wyłączeń[6].

Pojęcie danych osobowych ma kluczowe znaczenie w systemie ochrony danych. Zgodnie z art. 4 pkt 1 RODO są to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można ustalić bezpośrednio lub pośrednio, np. na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji czy innych cech określających jej tożsamość. Znaczenie tego pojęcia jest również rozwijane w orzecznictwie i doktrynie prawa[7].

RODO wskazuje jedynie przykładowe kategorie danych osobowych, ponieważ o uznaniu danej informacji za dane osobowe decyduje możliwość bezpośredniego lub pośredniego zidentyfikowania na jej podstawie konkretnej osoby fizycznej. W związku z tym nie jest możliwe z góry przypisanie określonym informacjom charakteru danych osobowych ani stworzenie zamkniętego katalogu tego rodzaju danych[8].

---

[3] Por. art. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 z późn. zm.).

[4] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000, „u.o.d.o.").

[5] D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* E. Bielak-Jomaa (red.), D. Lubasz (red.), Warszawa 2017, s. 168-169.

[6] P. Litwiński, P. Barta, M. Kawecki (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 176.

[7] A. Kręcisz-Sarna, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*. „Roczniki Administracji i Prawa", 2018, *2*(XVIII), s. 199-213.

[8] A. Mednis [w:] *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 23.

Uznanie określonej informacji za daną osobową jest uzależnione od kontekstu, w jakim dana informacja występuje. Dane osobowe obejmują nie tylko informacje wyrażone w formie językowej, lecz również wizerunki utrwalone na fotografiach i nagraniach wideo, zarejestrowany głos, a także dane genetyczne i biometryczne wskazane w art. 4 pkt 13 i 14 RODO[9]. Do tej kategorii zaliczają się wszelkie informacje, niezależnie od ich formy czy sposobu utrwalenia, o ile umożliwiają bezpośrednią lub pośrednią identyfikację konkretnej osoby fizycznej[10].

RODO wprowadza podział danych osobowych na trzy kategorie: dane zwykłe (art. 6 RODO), dane szczególnych kategorii (art. 9RODO) oraz dane dotyczące wyroków skazujących i naruszeń prawa (art. 10 RODO). Dane wcześniej określane jako wrażliwe w ustawie z 1997 r. mieszczą się obecnie głównie w dwóch ostatnich kategoriach[11].

Zakres pojęcia danych osobowych jest bardzo szeroki, co ma na celu zapewnienie osobom fizycznym możliwie najpełniejszej ochrony w związku z przetwarzaniem informacji ich dotyczących[12]. Definicja danych osobowych opiera się na czterech elementach: informacjach, dotyczących, zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[13]. Notariusz prowadzący kancelarię otrzymuje od klientów dane osobowe wykorzystywane wyłącznie do realizacji czynności notarialnych. Pojęcie informacji obejmuje wszelkie dane dotyczące osoby fizycznej, zarówno z życia prywatnego, jak i zawodowego, ekonomicznego czy społecznego, niezależnie od ich prawdziwości i formy (np. pisemnej, liczbowej, graficznej lub akustycznej)[14].

Określenie „dotyczące" oznacza, że informacja odnosi się do osoby fizycznej ze względu na jej treść, cel lub skutek. Osoba jest możliwa do zidentyfikowania, gdy można ją odróżnić od innych, np. na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych lokalizacyjnych czy innych cech określających jej tożsamość. Katalog tych danych ma charakter otwarty[15]. RODO nie ma zastosowania do danych dotyczących osób prawnych, takich jak nazwa firmy, forma prawna czy dane kontaktowe przedsiębiorstwa. W doktrynie pojawiają się jednak

[9] *Ibidem*, s. 23.
[10] *Ibidem*, s. 23-24.
[11] P. Fajgielski, *Przetwarzanie szczególnych kategorii danych w świetle RODO,* „Informacja w Administracji Publicznej" 2017, nr 2, s. 15.
[12] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym*. Warszawa 2018, s. 30.
[13] X. Konarski, G. Sibiga, D. Nowak, K. Syska, I. Małobęcka, *Ogólne rozporządzenie o ochronie danych osobowych (RODO). Poradnik dla radców prawnych i adwokatów*, Warszawa 2018, s. 13.
[14] M. Sakowska-Baryła, *Rozdział 1 Charakterystyka prawa do ochrony danych osobowych, prawa dostępu do informacji publicznej oraz prawa do ponownego wykorzystywania informacji sektora publicznego jako informacyjnych praw podmiotowych* [w:] *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022, s. 21-25.
[15] *Ibidem*.

wątpliwości co do zakresu tych wyłączeń[16]. Wątpliwości dotyczą tego, czy dane osoby prawnej obejmują jedynie informacje takie jak adres, telefon, e-mail czy NIP, czy także dane osób fizycznych wchodzących w skład jej organów. W interpretacji przyjmuje się jednak szerokie rozumienie pojęcia danych osoby prawnej i danych kontaktowych[17].

RODO wyróżnia dane zwykłe, szczególne kategorie danych (art. 9 RODO) oraz dane dotyczące wyroków skazujących i naruszeń prawa (art. 10 RODO). Zgodnie z art. 2 ust. 1 RODO przepisy te stosuje się do przetwarzania danych w sposób zautomatyzowany oraz niezautomatyzowany, jeśli dane stanowią część zbioru danych lub mają do niego należeć[18]. Przetwarzanie danych osobowych obejmuje m.in. ich zbieranie, przechowywanie, organizowanie, modyfikowanie, przeglądanie, wykorzystywanie oraz udostępnianie. Do przetwarzania zalicza się także łączenie, ograniczanie, usuwanie lub niszczenie danych (art. 4 pkt 2 RODO). Wymienione czynności mają charakter przykładowy, ponieważ nie jest możliwe stworzenie zamkniętego katalogu wszystkich operacji przetwarzania danych[19].

Istotne znaczenie dla określenia zakresu stosowania RODO ma art. 2 ust. 1 rozporządzenia, zgodnie z którym przepisy te obejmują dane osobowe przetwarzane zarówno w sposób zautomatyzowany, jak i niezautomatyzowany, o ile stanowią one część zbioru danych lub mają zostać do niego włączone. Przetwarzanie zautomatyzowane polega na wykonywaniu operacji na danych bez bezpośredniego udziału człowieka[20]. Przetwarzanie danych osobowych w sposób niezautomatyzowany podlega RODO tylko wtedy, gdy dane stanowią lub mają stanowić część uporządkowanego zbioru dostępnego według określonych kryteriów. Rozporządzenie nie obejmuje ręcznych zbiorów danych nieuporządkowanych według takich kryteriów (motyw 15 preambuły RODO). W konsekwencji pojedyncze informacje o charakterze danych osobowych nie korzystają z ochrony RODO, o ile nie są gromadzone w celu utworzenia lub uzupełnienia zbioru danych[21].

„Zbiór danych" natomiast stanowi uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów i ma znaczenie przede wszystkim

[16] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016, s. 40-41.
[17] A. Kalisz, *Wykładnia i stosowanie prawa wspólnotowego,* Warszawa 2007, s. 157.
[18] X. Konarski, G. Sibiga, D. Nowak, K. Syska, I. Małobęcka, *Ogólne…*, op.cit. s. 13.
[19] P. Litwiński, P. Barta, M. Kawecki (red.), *Rozporządzenie…* Op. cit, s. 176-177.
[20] W. Chomiczewski [w:] *Polska i europejska reforma ochrony danych,* E. Bielak – Jomaa (red.), D. Lubasz (red.), Warszawa 2016, s. 129.
[21] 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).

w odniesieniu do ręcznego przetwarzania danych. RODO obejmuje zarówno przetwarzanie zautomatyzowane, realizowane przy użyciu systemów informatycznych, jak i przetwarzanie ręczne, jednak wyłącznie wówczas, gdy dane osobowe są częścią zbioru danych lub mają do niego należeć, np. w przypadku akt sprawy sądowej[22].

Klauzula informacyjna dotycząca przetwarzania danych osobowych stanowi jeden z podstawowych instrumentów realizacji obowiązków wynikających z RODO w działalności kancelarii notarialnych. Jest ona wyrazem zasady przejrzystości przetwarzania danych osobowych oraz stanowi element wewnętrznych procedur ochrony danych osobowych obowiązujących w kancelarii notarialnej, służących zapewnieniu zgodności z przepisami prawa.

2. STATUS NOTARIUSZA JAKO ADMINISTRATORA DANYCH I PODSTAWY PRAWNE PRZETWARZANIA

2.1. ADMINISTRATOR DANYCH

Zgodnie z art. 4 pkt 7 RODO administratorem danych jest podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. O uznaniu danego podmiotu za administratora decyduje jego „władztwo nad danymi", czyli możliwość określania celów i sposobów przetwarzania. Cecha ta odróżnia administratora od podmiotu przetwarzającego, który działa w imieniu administratora na podstawie umowy lub innego instrumentu prawnego (art. 28 ust. 3 RODO)[23].

W kancelarii notarialnej funkcję administratora danych pełni notariusz, który – wykonując czynności notarialne na podstawie ustawy z 14 lutego 1991 r. – Prawo o notariacie – decyduje o zakresie i sposobach przetwarzania danych osobowych stron, ich pełnomocników, świadków oraz innych uczestników czynności. Status ten wynika zarówno z przepisów RODO, jak i Prawa o notariacie. Przetwarzanie danych ma charakter obligatoryjny i jest związane z realizacją ustawowych zadań notariusza, co wymaga przestrzegania zasad ochrony danych, w szczególności legalności, minimalizacji i rozliczalności.

2.2. PODSTAWY PRAWNE PRZETWARZANIA

Przetwarzanie danych osobowych przez notariuszy nie opiera się wyłącznie na podstawie art. 6 ust. 1 lit. c RODO, czyli obowiązku prawnego administratora,

[22] *Ibidem*, s. 14.
[23] T. Wyka, M.A. Mielczarek, *Administrator i inspektor ochrony danych osobowych*, Warszawa 2019, s. 23.

lecz również na innych podstawach przewidzianych w rozporządzeniu. Wynika to z faktu, że notariusz realizuje ustawowe zadania publiczne i wykonuje czynności notarialne o charakterze urzędowym. W szczególności przetwarzanie danych osobowych przez notariusza odbywa się:

- na podstawie art. 6 ust. 1 lit. b RODO – gdy przetwarzanie danych jest niezbędne do podjęcia działań na żądanie stron lub do wykonania czynności prawnej dokumentowanej aktem notarialnym;
- na podstawie art. 6 ust. 1 lit. c RODO – w zakresie realizacji obowiązków prawnych wynikających z przepisów powszechnie obowiązujących, takich jak ustawa – Prawo o notariacie[24] (np. identyfikacja stron czynności, sporządzanie aktów notarialnych, prowadzenie repertorium i archiwizacja dokumentów), Kodeks cywilny[25] czy ustawa o księgach wieczystych i hipotece[26];
- na podstawie art. 6 ust. 1 lit. e RODO – jako przetwarzanie niezbędne do realizacji zadania w interesie publicznym przez notariusza jako osobę zaufania publicznego.
- Ponadto, w przypadku przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, podstawę legalizującą to przetwarzanie stanowią:
- art. 9 ust. 2 lit. f RODO – gdy przetwarzanie jest konieczne do ustalenia, dochodzenia lub obrony roszczeń;
- art. 9 ust. 2 lit. g RODO – gdy przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, wynikającym z prawa Unii Europejskiej lub prawa krajowego;
- art. 9 ust. 2 lit. j RODO – w zakresie archiwizacji dokumentacji notarialnej w interesie publicznym, zgodnie z przepisami prawa krajowego.

Ograniczenie podstaw przetwarzania danych przez notariusza wyłącznie do art. 6 ust. 1 lit. c RODO byłoby niepełne. Notariusz wykonuje bowiem zadania publiczne, dlatego zastosowanie ma także art. 6 ust. 1 lit. e RODO dotyczący interesu publicznego. W relacjach ze stronami czynności notarialnych znaczenie ma również art. 6 ust. 1 lit. b RODO odnoszący się do działań niezbędnych do realizacji czynności prawnych.

[24] Ustawa z dnia 14 lutego 1991 r. – Prawo o notariacie (Dz.U. 2023 poz. 1791 ze zm., „PN").
[25] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2021 r. poz. 1509).
[26] Ustawa z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (t.j. Dz. U. z 2025 r. poz. 341).

3. ZASADY PRZETWARZANIA DANYCH W KANCELARII NOTARIALNEJ ORAZ OBOWIĄZEK INFORMACYJNY I PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Zakres pojęcia danych osobowych jest szeroki i obejmuje wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 1 RODO). W praktyce notarialnej są to głównie dane identyfikacyjne, adresowe, informacje o stanie cywilnym, sytuacji majątkowej czy powiązaniach rodzinnych. Zgodnie z zasadą minimalizacji (art. 5 ust. 1 lit. c RODO) notariusz może przetwarzać jedynie dane niezbędne do dokonania danej czynności notarialnej.

Notariusz, prowadząc kancelarię i wykonując czynności zawodowe, przetwarza dane osobowe w rozumieniu RODO. Dane te są niezbędne zarówno do sporządzania czynności notarialnych, jak i realizacji obowiązków publicznoprawnych, w szczególności związanych z poborem podatków i opłat sądowych, gdzie notariusz występuje jako płatnik lub pośrednik organów publicznych.

Podstawą przetwarzania danych osobowych przez notariusza są przede wszystkim obowiązki prawne wynikające z pełnionej funkcji osoby zaufania publicznego. Zgodnie z art. 6 ust. 1 lit. c RODO przetwarzanie jest dopuszczalne, gdy jest niezbędne do wypełnienia obowiązku prawnego administratora. Obowiązki te wynikają z ustawy Prawo o notariacie, a także z przepisów prawa podatkowego, które ustanawiają notariusza płatnikiem m.in. podatku od czynności cywilnoprawnych oraz podatku od spadków i darowizn przy czynnościach dokonywanych w formie aktu notarialnego[27]. Przetwarzanie danych osobowych przez notariusza znajduje również podstawę w art. 6 ust. 1 lit. b RODO, który dopuszcza przetwarzanie danych niezbędnych do wykonania umowy lub podjęcia działań na żądanie osoby, której dane dotyczą. Czynności notarialne są podejmowane na wyraźne żądanie klienta i prowadzą do ukształtowania jego sytuacji prawnej, dlatego sporządzenie aktu notarialnego czy poświadczenia nie jest możliwe bez przetwarzania danych osobowych stron.

Zastosowanie znajduje również art. 6 ust. 1 lit. e RODO, który dopuszcza przetwarzanie danych niezbędne do realizacji zadania w interesie publicznym lub w ramach wykonywania władzy publicznej powierzonej administratorowi. Notariusz pełni funkcję publiczną[28], której celem jest zapewnienie bezpieczeństwa i pewności

[27] Art. 7 § 1-2, art. 79, art. 80 § 2-3 ustawy z dnia 14 lutego 1991 r. – Prawo o notariacie (t.j. Dz.U. z 2024 r. poz. 1001); Art. 10 ust. 2-3 ustawy z dnia 9 września 2000 r. o podatku od czynności cywilnoprawnych (t.j. Dz. U. z 2026 r. poz. 191); Art. 18 ust. 1-3 ustawy z dnia 28 lipca 1983 r. o podatku od spadków i darowizn (t.j. Dz. U. z 2026 r. poz. 478).

[28] Z. Kwiatkowski, *Notariusz jako funkcjonariusz publiczny w świetle nowego prawa o notariacie*, „Przegląd Sądowy" 1993, nr 3, s. 22.

obrotu prawnego[29]. Pobór podatków, opłat sądowych oraz przekazywanie danych właściwym organom publicznym stanowi realizację tego interesu publicznego i jest integralną częścią działalności notarialnej[30]. W orzecznictwie Sądu Najwyższego wskazuje się, że notariusz sprawuje tzw. jurysdykcję prewencyjną, pełniąc funkcję strażnika porządku prawnego w obrocie cywilnym i przyczyniając się do zapewnienia bezpieczeństwa obrotu[31]. Notariusz, mimo że formalnie nie jest urzędnikiem, wykonuje funkcje zbliżone do urzędnika państwowego, gdyż dokonuje czynności notarialnych o charakterze urzędowym[32].

Notariusz jest nosicielem władzy publicznej, przejawiającej się w uprawnieniu do sporządzania dokumentów urzędowych o szczególnej mocy dowodowej. Działa przy tym niezależnie od Ministerstwa Sprawiedliwości, które sprawuje jedynie nadzór nad wykonywaniem funkcji notarialnej[33]. Choć notariusz pozostaje poza strukturą wymiaru sprawiedliwości, pełni w istocie funkcję jurysdykcji prewencyjnej, zapewniając bezpieczeństwo i pewność obrotu prawnego poprzez prawidłowe sporządzanie czynności oraz zabezpieczanie interesów uczestników obrotu[34].

Szczególne znaczenie ma przetwarzanie danych osobowych w związku z pobieraniem danin publicznoprawnych. Dane klientów są wykorzystywane wyłącznie do ustalenia podstawy opodatkowania, sporządzenia deklaracji, pobrania należności i przekazania ich właściwym organom. Przetwarzanie to ma charakter obowiązkowy i nie wymaga zgody osoby, której dane dotyczą, ponieważ wynika bezpośrednio z przepisów prawa[35].

W praktyce notarialnej może dochodzić do przetwarzania szczególnych kategorii danych osobowych (art. 9 RODO). Podstawę stanowią w szczególności art. 9 ust. 2 lit. g RODO – ze względu na ważny interes publiczny, zwłaszcza w sprawach spadkowych, majątkowych i rodzinnych – oraz art. 9 ust. 2 lit. f RODO, dotyczący

---

[29] M. Kulik, *Odpowiedzialność karna osoby pełniącej funkcję publiczną ze szczególnym uwzględnieniem odpowiedzialności notariusza* [w:] *Odpowiedzialność karna notariusza*, A. Oleszko (red.), Warszawa 2010, s. 210-211.

[30] J. Bodio, *Status prawny notariusza – wybrane zagadnienia*, „Rejent" 2011, nr 10, s. 17.

[31] A. Oleszko, *Glosa do uchwały SN z dnia 18 grudnia 2013 r., III CZP 82/13*, NPN 2014, nr 1, s. 63-76; Uchwała SN z dnia 18 grudnia 2013 r., III CZP 82/13; Uchwała SN (7) z 7.12.2010 r., III CZP 86/10, OSNC 2011, nr 5, poz. 49.

[32] W. Boć, *Wokół statusu notariusza*, „Przegląd Prawa i Administracji", t. LXIV, red. J. Frąckowiak, Wrocław 2004, s. 20.

[33] A. Rataj, A. Szereda, *Ustrój notariatu. Komentarz do art. 1-78d Prawa o notariacie,* Warszawa 2019 s. 50.

[34] R. Sztyk, *Funkcja publiczna notariatu*, „Rejent" 1994, nr 12, s. 67-68.

[35] Ustawa z dnia 9 września 2000 r. o podatku od czynności cywilnoprawnych (t.j. Dz. U. z 2026 r. poz. 191); Ustawa z dnia 28 lipca 1983 r. o podatku od spadków i darowizn (t.j. Dz. U. z 2026 r. poz. 478); Ustawa z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych (t.j. Dz. U. z 2025 r. poz. 1228 z późn. zm.).

ustalenia, dochodzenia lub obrony roszczeń. Z kolei art. 9 ust. 2 lit. j RODO znajduje zastosowanie w odniesieniu do archiwizacji akt notarialnych w interesie publicznym, wynikającej z przepisów Prawa o notariacie[36].

W ramach wykonywania obowiązków ustawowych notariusz przekazuje dane osobowe właściwym organom publicznym, w szczególności sądom oraz organom administracji skarbowej. Przekazanie następuje wyłącznie w zakresie niezbędnym do realizacji czynności notarialnych oraz związanych z nimi obowiązków publicznoprawnych, w tym poboru podatków i przekazywania deklaracji podatkowych[37], wnioski o wpisy do ksiąg wieczystych czy realizacja obowiązków sprawozdawczych. Takie udostępnianie danych stanowi formę dalszego przetwarzania, zgodną z zasadami RODO, o ile wynika bezpośrednio z przepisów prawa[38]. Niezależnie od przekazywania danych organom publicznym, notariusz może powierzyć przetwarzanie danych osobowych podmiotom trzecim, takim jak biuro rachunkowe, z którym zawarta została umowa o świadczenie usług księgowych. W takim przypadku biuro rachunkowe działa jako podmiot przetwarzający w rozumieniu art. 28 RODO, a przetwarzanie danych odbywa się wyłącznie na udokumentowane polecenie notariusza oraz w zakresie niezbędnym do realizacji usług księgowych i rozliczeń podatkowych kancelarii[39]. Warunkiem legalności tego przetwarzania jest zawarcie umowy powierzenia przetwarzania danych, określającej m.in. cele, zakres oraz środki bezpieczeństwa przetwarzanych danych osobowych[40].

Istotnym zagadnieniem jest obowiązek podania danych osobowych przez klientów kancelarii notarialnej. Dane te są niezbędne do dokonania czynności notarialnej i wynikają z przepisów ustawy – Prawo o notariacie, w szczególności art. 85 oraz art. 92 § 1 pkt 4, które wymagają wskazania danych identyfikujących uczestników czynności. Podstawę stanowią także przepisy prawa podatkowego dotyczące poboru podatku od czynności cywilnoprawnych oraz podatku od spadków i darowizn[41].

Zgodnie z art. 13 ust. 2 lit. e RODO administrator jest zobowiązany poinformować osobę o obowiązku podania danych oraz konsekwencjach ich niepodania. W przypadku czynności notarialnych brak przekazania danych uniemożliwia

[36] Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie (t.j. Dz. U. z 2026 r. poz. 614).
[37] Ustawa z dnia 9 września 2000 r. o podatku od czynności cywilnoprawnych (t.j. Dz. U. z 2026 r. poz. 191).
[38] Ustawa z dnia 28 lipca 1983 r. o podatku od spadków i darowizn (t.j. Dz. U. z 2026 r. poz. 478); Ustawa z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych (t.j. Dz. U. z 2025 r. poz. 1228 z późn. zm.).
[39] Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie (t.j. Dz. U. z 2026 r. poz. 614).
[40] *Ibidem*.
[41] art. 85, art. 92 § 1 pkt 4 *ibidem*; Art. 10 ust. 2-3 ustawy z dnia 9 września 2000 r. o podatku od czynności cywilnoprawnych (t.j. Dz. U. z 2026 r. poz. 191); Art. 18 ust. 1-3 ustawy z dnia 28 lipca 1983 r. o podatku od spadków i darowizn (t.j. Dz. U. z 2026 r. poz. 478).

dokonanie czynności, gdyż notariusz ma obowiązek ustalenia tożsamości uczestników zgodnie z art. 85 § 1-2 ustawy – Prawo o notariacie[42]. Ustalenie tożsamości powinno nastąpić na podstawie dokumentów przewidzianych prawem, a w razie ich braku – w sposób niebudzący wątpliwości. Zgodnie z art. 85 § 3 Prawa o notariacie notariusz jest zobowiązany wskazać w dokumencie sposób jej ustalenia, działając przy tym ze szczególną starannością oraz z uwzględnieniem ochrony praw i interesów stron[43]. Brak przekazania niezbędnych danych osobowych uniemożliwia notariuszowi ocenę zgodności czynności z prawem oraz wykonanie obowiązków ustawowych. W takiej sytuacji notariusz może odmówić dokonania czynności na podstawie art. 81 PN, co jest stwierdzane w protokole zgodnie z art. 81a § 1 PN.

W ramach czynności notarialnych notariusz gromadzi jedynie dane niezbędne do prawidłowego i zgodnego z prawem dokonania czynności, realizując zasadę minimalizacji danych. Służy temu wdrażanie procedur wewnętrznych określających zakres i cele przetwarzania oraz przeprowadzanie analiz ryzyka i ocen skutków dla ochrony danych[44]. Status i obowiązki notariusza jako administratora danych osobowych znajdują odzwierciedlenie w organizacji pracy kancelarii notarialnej. Zasady jej funkcjonowania określa m.in. Regulamin wewnętrznego urzędowania kancelarii notarialnych wydany na podstawie art. 40 § 1 pkt 1 ustawy – Prawo o notariacie. W praktyce kancelarie wdrażają także wewnętrzne procedury ochrony danych, takie jak polityki bezpieczeństwa informacji czy instrukcje zarządzania systemami informatycznymi, zapewniające zgodność z RODO[45].

W kontekście art. 9 RODO przetwarzanie danych wrażliwych, np. informacji o stanie zdrowia czy pochodzeniu etnicznym, może opierać się na art. 9 ust. 2 lit. g RODO, który dopuszcza takie przetwarzanie ze względu na ważny interes publiczny. Zgoda z art. 6 ust. 1 lit. a RODO co do zasady nie stanowi podstawy przetwarzania, ponieważ relacja notariusz-klient ma charakter ustawowy, a nie dobrowolny[46].

W celu zapewnienia zgodności z RODO kancelarie notarialne wdrażają wewnętrzne regulacje, takie jak polityki ochrony danych, procedury bezpieczeństwa informacji oraz instrukcje zarządzania systemami informatycznymi. Dokumenty te uszczegóławiają obowiązki wynikające z RODO i ustawy Prawo o notariacie.

---

[42] A. Rataj A. Szereda A. (red.), *Ustrój notariatu. Komentarz do art. 1-78d Prawa o notariacie*, Warszawa 2019, s. 147-148

[43] Wyrok Sądu Najwyższego z dnia 14 czerwca 2017 r., IV CSK 104/17, OSNC 2018/3/35.

[44] Krajowa Rada Notarialna, Informacja o ochronie danych osobowych, https://krn.org.pl/rodo [dostęp: 2.03.2026].

[45] Zarządzenie Ministra Sprawiedliwości z dnia 19 grudnia 1989 r. Regulamin wewnętrznego urzędowania państwowych biur notarialnych. (Na podstawie art. 7 oraz w związku z art. 9 ustawy z dnia 24 maja 1989 r. - Prawo o notariacie (t.j. Dz. U. z 2026 r. poz. 614)).

[46] *Ibidem*.

Klauzule informacyjne służą realizacji obowiązku informacyjnego wynikającego z art. 13 i 14 RODO i powinny wskazywać administratora, cele i podstawy przetwarzania, okres przechowywania danych oraz prawa osób, których dane dotyczą.

Realizacja tych praw musi jednak uwzględniać specyfikę Prawa o notariacie oraz tajemnicę notarialną (art. 18 PN). W praktyce prawo do usunięcia danych z art. 17 RODO jest ograniczone ze względu na obowiązek archiwizacji aktów notarialnych, natomiast możliwe jest korzystanie z innych uprawnień, takich jak prawo dostępu do danych czy ich sprostowania, o ile nie narusza to przepisów szczególnych[47]. W przypadku pytań lub wątpliwości dotyczących przetwarzania danych osobowych klienci mogą skontaktować się z notariuszem za pośrednictwem wskazanego adresu poczty elektronicznej. Jeżeli natomiast uznają, że przetwarzanie ich danych osobowych narusza przepisy RODO, przysługuje im prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Zgodnie z art. 32 RODO notariusz jest zobowiązany do stosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych. W dyskusji pojawia się postulat rozszerzenia obowiązków notariuszy o anonimizacji dokumentów przekazywanych do Krajowego Rejestru Sądowego, co spotyka się z krytyką środowiska notarialnego. Wskazuje się, że rozwiązanie to zwiększałoby zakres odpowiedzialności notariuszy w zakresie zasad minimalizacji oraz integralności i poufności danych, mimo że nie pełnią oni funkcji administratora danych w systemie KRS[48].

W praktyce realizacja tych obowiązków wymaga wdrożenia w kancelarii notarialnej polityki bezpieczeństwa informacji oraz odpowiednich procedur organizacyjnych i technicznych, obejmujących m.in. kontrolę dostępu do pomieszczeń, akt i systemów informatycznych, zasady zarządzania hasłami i szyfrowania danych, tworzenie kopii zapasowych oraz ewidencjonowanie upoważnień do przetwarzania danych przez pracowników. Szczególną cechą działalności notarialnej jest długotrwały obowiązek archiwizacji dokumentacji. Prawo o notariacie nakłada na notariuszy obowiązek przechowywania akt i repertoriów przez okresy dłuższe niż w wielu innych sektorach, co stanowi wyjątek od zasady ograniczenia przechowywania danych z art. 5 ust. 1 lit. e RODO. Archiwizacja powinna odbywać się z zastosowaniem środków organizacyjnych i technicznych zapewniających integralność, poufność i dostępność danych[49].

---

[47] *Ibidem*.

[48] Uchwała Nr 98/X/2025 Zarządu Głównego Stowarzyszenia Notariuszy Rzeczypospolitej Polskiej podjęta drogą obiegową w dniu 9 października 2025 r. w sprawie zaopiniowania projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw (UDER49).

[49] Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie (t.j. Dz. U. z 2026 r. poz. 614).

Obowiązki archiwizacyjne notariusza wynikają z przepisów ustawy – Prawo o notariacie[50] oraz aktów wykonawczych wydanych na jej podstawie, natomiast w praktyce kancelarii są one uszczegóławiane przez wewnętrzne procedury dotyczące przechowywania i zabezpieczania dokumentacji w postaci papierowej oraz elektronicznej. Zgodnie z obowiązującymi przepisami notariusz jest zobowiązany do przechowywania dokumentów obejmujących czynności notarialne przez okres 10 lat od dnia ich sporządzenia. Po upływie tego terminu dokumenty podlegają przekazaniu do archiwum ksiąg wieczystych właściwego sądu rejonowego (art. 90 § 1 PN). Przekazanie następuje również w razie zaprzestania działalności kancelarii. Szczegółowe zasady archiwizacji i przekazywania dokumentów określa rozporządzenie Ministra Sprawiedliwości.

4. BEZPIECZEŃSTWO PRZETWARZANIA I CYBERBEZPIECZEŃSTWO

Postępująca cyfryzacja czynności notarialnych, w tym obsługa elektronicznych ksiąg wieczystych oraz komunikacja z systemami KRS i sądów, zwiększa efektywność pracy notariusza, lecz jednocześnie rodzi nowe zagrożenia w obszarze cyberbezpieczeństwa. Dane przetwarzane elektronicznie są narażone na nieautoryzowany dostęp, utratę danych czy ataki hakerskie, dlatego kancelarie powinny stosować odpowiednie procedury bezpieczeństwa, obejmujące ochronę systemów informatycznych, aktualizację zabezpieczeń oraz szkolenia personelu. Istotne znaczenie ma również regulacja korzystania z poczty elektronicznej, urządzeń mobilnych oraz ewentualnej pracy zdalnej. RODO przyznaje osobom fizycznym określone prawa, w tym prawo dostępu do danych, ich sprostowania, ograniczenia przetwarzania, usunięcia, wniesienia sprzeciwu oraz złożenia skargi do organu nadzorczego.

Zgodnie z zasadą rozliczalności notariusz powinien wykazać zgodność przetwarzania danych z RODO. W przypadku naruszenia ochrony danych konieczne jest podjęcie odpowiednich działań, w tym – gdy wymagają tego przepisy – zgłoszenie incydentu Prezesowi Urzędu Ochrony Danych Osobowych oraz poinformowanie osób, których dane dotyczą. Istotną rolę odgrywają w tym zakresie wewnętrzne procedury reagowania na incydenty bezpieczeństwa informacji[51].

Wdrożone i regularnie weryfikowane procedury ochrony danych oraz bezpieczeństwa informacji stanowią podstawowe narzędzie zarządzania ryzykiem

[50] Zob. art. 90 § 1-2 ustawy z dnia 14 lutego 1991 r. – Prawo o notariacie (t.j. Dz. U. z 2026 r. poz. 614) oraz Rozporządzenie Ministra Sprawiedliwości wydane na podstawie art. 90 § 2 PN, określające sposób prowadzenia ksiąg notarialnych oraz warunki przekazywania dokumentów na przechowanie do właściwego sądu rejonowego.

[51] Por. art. 5 ust. 2, art. 24 ust. 1, art. 32 ust. 1, art. 33 oraz art. 34 RODO.

w kancelarii notarialnej. Obejmują m.in. prowadzenie rejestru czynności przetwarzania, audyty bezpieczeństwa, dokumentowanie naruszeń oraz szkolenia personelu. Zapewnienie zgodności z RODO wymaga połączenia działań prawnych, organizacyjnych i technicznych. Skuteczna ochrona danych minimalizuje ryzyko sankcji oraz wzmacnia zaufanie do notariusza jako osoby zaufania publicznego.

PODSUMOWANIE

Zapewnienie zgodności działalności kancelarii notarialnej z RODO wymaga połączenia działań prawnych, organizacyjnych i technicznych. Kluczowe znaczenie mają właściwe podstawy przetwarzania (art. 6 i 9 RODO), stosowanie zasad z art. 5 RODO, realizacja obowiązku informacyjnego oraz wdrożenie odpowiednich środków bezpieczeństwa (art. 32 RODO). W praktyce szczególnie istotna jest bezpieczna archiwizacja dokumentów zgodnie z Prawem o notariacie oraz ocena ryzyk związanych z ewentualnym rozszerzaniem obowiązków, np. w zakresie anonimizacji. Spójne procedury ochrony danych ograniczają ryzyko odpowiedzialności i wzmacniają zaufanie do notariatu.

BIBLIOGRAFIA

LITERATURA

Bielak-Jomaa E., Lubasz D. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Boć W., *Wokół statusu notariusza*, Przegląd Prawa i Administracji, t. LXIV, red. J. Frąckowiak, Wrocław 2004.

Bodio J., *Status prawny notariusza – wybrane zagadnienia*, „Rejent" 2011, nr 10

Chomiczewski W. [w:] Bielak – Jomaa E., Lubasz D. (red.), *Polska i europejska reforma ochrony danych,* Warszawa 2016.

Fajgielski P., *Przetwarzanie szczególnych kategorii danych w świetle RODO,* „Informacja w Administracji Publicznej" 2017, nr 2.

Gumularz M., *Ochrona danych osobowych w sektorze publicznym*. Warszawa 2018.

Kalisz A., *Wykładnia i stosowanie prawa wspólnotowego,* Warszawa 2007.

Konarski X., Sibiga G., Nowak D., Syska K., Małobęcka I., *Ogólne rozporządzenie o ochronie danych osobowych (RODO). Poradnik dla radców prawnych i adwokatów*, Warszawa 2018.

Kręcisz-Sarna, A., Ochrona danych osobowych w ogólnym postępowaniu administracyjnym. „Roczniki Administracji i Prawa", 2018, *2*(XVIII).

Krzysztofek M. , *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* Warszawa 2016.

Kulik M., *Odpowiedzialność karna osoby pełniącej funkcję publiczną ze szczególnym uwzględnieniem odpowiedzialności notariusza*, *[w:] Odpowiedzialność karna notariusza*, A. Oleszko (red.), Warszawa 2010.

Kwiatkowski Z., *Notariusz jako funkcjonariusz publiczny w świetle nowego prawa o notariacie*, „Przegląd Sądowy" 1993, nr 3.

Litwiński P. , Barta P., Kawecki M. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018.

Lubasz D. [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2017.

Mednis A., *Ustawa o ochronie danych osobowych,* Warszawa 1999.

Oleszko A., Glosa do uchwały Sądu Najwyższego z dnia 18 grudnia 2013 r., III CZP 82/13, „Nowy Przegląd Notarialny" 2014, nr 1.

Rataj A. Szereda A. (red.), *Ustrój notariatu. Komentarz do art. 1- 78d Prawa o notariacie*, Warszawa 2019.

Sakowska-Baryła M., *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

Sztyk R., *Funkcja publiczna notariatu*, „Rejent" 1994, nr 12.

Wyka T., Mielczarek M.A., *Administrator i inspektor ochrony danych osobowych*, Warszawa 2019.

AKTY PRAWNE

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L nr 119 z 4.05.2016 r.).

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).

Ustawa z dnia 28 lipca 1983 r. o podatku od spadków i darowizn (t.j. Dz. U. z 2026 r. poz. 478).

Ustawa z dnia 14 lutego 1991 r. – Prawo o notariacie (t.j. Dz. U. z 2026 r. poz. 614).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 z późn. zm.).

Ustawa z dnia 9 września 2000 r. o podatku od czynności cywilnoprawnych (t.j. Dz. U. z 2026 r. poz. 191).

Ustawa z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych (t.j. Dz.U. z 2025 r. poz. 1228 z późn. zm.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781 z późn. zm.).

Zarządzenie Ministra Sprawiedliwości z dnia 19 grudnia 1989 r. Regulamin wewnętrznego urzędowania państwowych biur notarialnych. Na podstawie art. 7 oraz w związku z art. 9 ustawy z dnia 24 maja 1989 r. - Prawo o notariacie (Dz. U. Nr 33, poz. 176)

Rozporządzenie Ministra Sprawiedliwości z dnia 12 kwietnia 1991 r. w sprawie prowadzenia ksiąg notarialnych oraz przekazywania na przechowanie dokumentów sądom rejonowym (t.j. Dz. U. z 2018 r. poz. 2039).

ORZECZNICTWO

Uchwała Sądu Najwyższego (7) z dnia 7 grudnia 2010 r., III CZP 86/10, OSNC 2011, nr 5, poz. 49.

Uchwała Sądu Najwyższego z dnia 18 grudnia 2013 r., III CZP 82/13.

INNE PUBLIKACJE

Uchwała Nr 98/X/2025 Zarządu Głównego Stowarzyszenia Notariuszy Rzeczypospolitej Polskiej z dnia 9 października 2025 r. w sprawie zaopiniowania projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw (UDER49).

Krajowa Rada Notarialna, Informacje dotyczące RODO, https://krn.org.pl/rodo [dostęp: 2.03.2026].

THE STATUS AND OBLIGATIONS OF A NOTARY AS A DATA CONTROLLER UNDER THE GDPR

Summary: This article is devoted to an analysis of the status of a notary as a controller of personal data and of the obligations connected with data processing under the GDPR. It presents the legal bases for the processing of personal data in notarial practice, arising both from the GDPR and from the Polish Notarial Law, with particular emphasis on the specific nature of notarial acts, public-law obligations, and the role of the notary as a public trust professional. The article also discusses the principles governing data processing in a notarial office, including the principles of lawfulness, data minimization, and accountability, as well as the information obligation and the scope of the exercise of data subjects' rights. The analysis further covers the archiving of notarial records, information security, and cybersecurity in the context of the ongoing digitalization of notarial activities. It is argued that ensuring the compliance of notarial practice with the GDPR requires a combination of legal, organizational, and technical measures, as well as the implementation of coherent data protection procedures that reduce the risk of liability and strengthen trust in the notarial profession.

Key words: GDPR; personal data protection; notarial office; notary; cybersecurity; information security; notarial confidentiality.

mgr **Aneta Landrat-Kańtoch**
Uniwersytet Śląski w Katowicach
aneta.landrat@us.edu.pl
https://orcid.org/0009-0007-8323-6535

OCHRONA DANYCH OSOBOWYCH W EDUKACJI CYFROWEJ

Streszczenie: Rozwój edukacji cyfrowej oraz sięganie po dostępne rozwiązania w zakresie kształcenia na odległość wiążą się z nowymi wyzwaniami prawnymi, zwłaszcza w obszarze ochrony danych osobowych. Kwestia rozwoju edukacji cyfrowej stała się praktycznie istotna wraz z rozwojem pandemii koronawirusa, kiedy konieczność zapewnienia bezpieczeństwa i przeciwdziałania rozpowszechnieniu się wirusa spowodowała zawieszenie tradycyjnej formy nauczania w wielu placówkach. Wymusiło to na organizatorach procesu nauczania adaptację innych metod oraz wykorzystanie możliwości oferowanych przez edukację cyfrową. Ponadto, uwzględniając fakt, że współczesny świat cyfrowy charakteryzuje się rosnącą świadomością społeczeństwa oraz coraz większym udziałem technologii w życiu człowieka, konieczne staje się dostosowanie osiągnięć technologicznych do wymogów zgodności z podstawowymi prawami i wolnościami jednostki, w szczególności z prawem do prywatności oraz ochrony danych osobowych w środowisku cyfrowym. Celem niniejszego rozdziału jest ukazanie kluczowych wyzwań, jakie edukacja cyfrowa stawia w zakresie ochrony danych osobowych, z uwzględnieniem obowiązujących regulacji prawnych, wytycznych organu nadzorczego oraz stosowanych praktyk.

Słowa kluczowe: RODO; ochrona danych osobowych; edukacja cyfrowa; kształcenie na odległość, narzędzia IT.

WPROWADZENIE

Dynamiczny rozwój technologii informacyjno-komunikacyjnej ma istotny wpływ na przemiany w sposobie funkcjonowania systemów edukacyjnych[1]. Jedna z wielu definicji edukacji cyfrowej odnosi się do wykorzystywanych narzędzi informatycznych i środków komunikacji elektronicznej w procesie nauczania i uczenia się[2]. Ponadto edukacja cyfrowa[3] definiowana jest również pod względem dwóch różnych, ale uzupełniających się perspektyw[4]. Pierwsza perspektywa odnosi się do rozwoju kompetencji cyfrowych u uczniów i nauczycieli, z kolei druga perspektywa nawiązuje do aspektów wykorzystywania nowoczesnych technologii dla celów wzmacniania edukacji.

Zjawisko edukacji cyfrowej nabrało większego znaczenia w momencie pandemii koronawirusa, która w związku z wdrożeniem działań mających na celu przeciwdziałanie rozpowszechnieniu się pandemii[5], wymusiła na podmiotach świadczących usługi edukacyjne zawieszenie kształcenia w formie stacjonarnej i przejście do świata cyfrowego. Przeniesienie edukacji do sfery cyfrowej doprowadziło do przeniesienia nauczania na inny poziom, wykorzystując do tego dostępne, nowoczesne narzędzia cyfrowe, co istotnie wpłynęło na zmianę dotychczasowych modeli nauczania[6]. Pandemia doprowadziła do powszechnego wdrożenia kształcenia na odległość na wszystkich poziomach edukacji, udowadniając jednocześnie potrzebę odpowiedniego wdrożenia przez państwo zasad funkcjonowania systemu edukacji cyfrowej[7]. Przed eskalacją epidemii koronawirusa zdalna forma kształcenia była już dostępna, w szczególności jako jedna z opcji, a nie konieczność[8]. Mimo tego nie należy utożsamiać procesu rozwoju systemu edukacji cyfrowej tylko z pandemią koronawirusa. Fakt rozwoju edukacji cyfrowej należy postrzegać również jako element szerszego procesu

[1] G. Mazurek, *Transformacja cyfrowa- perspektywa instytucji szkolnictwa wyższego,* [w:] Transformacja akademickiego szkolnictwa wyższego w Polsce w okresie 30-lecia: 1989-2019, Konferencja Rektorów Akademickich Szkół Polskich, J. Woźnicki (red.), Warszawa 2019, s. 313-314.

[2] UNESCO, *Digital Education*, UNESCO, https://www.unesco.org/en/tags/digital-education-0 [dostęp: 2.03.2026].

[3] Zwana również edukacją zdalną, kształceniem na odległość, e-learningiem, edukacją online.

[4] Komisja Europejska /EACEA/Eurydice, *Digital Education at School in Europe*, Eurydice Report. Edukacja cyfrowa w szkołach w Europie. Raport Eurydice, Luksemburg: Urząd Publikacji Unii Europejskiej, 2019, s. 109.

[5] Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. 2020 poz. 493).

[6] OECD, *Education responses to COVID-19: Embracing digital learning and online collaboration*, Paris 2020, s. 3.

[7] OECD Digital Education Outlook, *Towards an Effective Digital Education Ecosystem,* 2023, s. 15.

[8] M. Garlinska, M. Osial, K. Proniewska, A. Pregowska, *The Influence of Emerging Technologies on Distance Education*. „Electronics" 2023, 12, 1550, s. 1, https://doi.org/10.3390/electronics12071550.

transformacji cyfrowej państwa oraz działań zmierzających do dostosowania systemu edukacji do postępujących zmian i warunków społeczno-gospodarczych[9].

Wprowadzenie edukacji cyfrowej w trudnych warunkach pandemicznych, które wymagały od podmiotów świadczących usługi edukacyjne szybkości działania, często pod presją czasu, ujawniło sporo wyzwań o charakterze społecznym, pedagogicznym, psychologicznym, ale również prawnym[10]. Jednym z obszarów, które zwracają uwagę i potrzebę precyzyjnego dookreślenia warunków i zasad postępowania jest ochrona danych osobowych uczestników procesu edukacji zdalnej, ze szczególnym uwzględnieniem sytuacji prawnej uczniów oraz studentów[11]. Proces edukacji zdalnej wiąże się z koniecznością przetwarzania danych osobowych uczestników tego procesu, zarówno danych zwykłych, jak i niejednokrotnie danych szczególnych kategorii w rozumieniu art. 9 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 („RODO")[12].

Proces edukacji cyfrowej nie może być utożsamiany ze stacjonarną formą edukacji i transferowany do cyfrowego świata bez wprowadzenia jakichkolwiek zmian i udoskonaleń[13]. Chociażby kwestia zakresu przetwarzanych danych w edukacji cyfrowej często różni się zakresem od danych, które są przetwarzane w tradycyjnej formie nauczania. Występowanie tej różnicy uzasadnia konieczność jednoznacznego uregulowania sytuacji prawnej uczestników w kontekście ochrony danych osobowych i zapewnienia odpowiedniego stopnia bezpieczeństwa oraz poszanowania prawa do prywatności. Warto podkreślić, że ochrona danych osobowych to nie tylko obowiązek formalnoprawny, ale również realizacja podstawowych praw i wolności jednostki zgodnie z Kartą praw podstawowych Unii Europejskiej[14].

Kwestia ochrony danych osobowych w procesie edukacji cyfrowej zyskuje znaczenie ze względu na fakt, że uczestnikami tego procesu w dużym stopniu są dzieci,

---

[9] J. Aquino, R. Alarcón, L. Guevara, J. Bravo-Jaico, N. Germán, C. Valdivia-Salazar, O. Serquén, G.L.E. Maquen-Niño, A. Tesén-Arroyo, *Impact of digital transformation: assessing the knowledge and adoption of disruptive technologies in a higher education institution*, Front. „Computer Science" 7, 2025, s. 1, 13, https://doi.org/10.3389/fcomp.2025.1611952.

[10] M. Kovacic, *Legal Aspects of Distance Learning*, 2021, s.322, https://doi.org/10.46793/nnu21.321k.

[11] R. Isus, K. Kolesnikova, I. Khlevna, T. Oleksandr, K. Liubov, *Development of a model of personal data protection in the context of digitalization of the educational sphere using information technology tools,* „Procedia Computer Science", Volume 231, 2024, s.348, https://doi.org/10.1016/j.procs.2023.12.215.

[12] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

[13] F. Sabirova, A. Gura, E. Belyanova, A. Sukhorukih, *Distance education in a digital age*, „World Journal on Educational Technology: Current Issues", 14(5), 2022, s. 1416, https://doi.org/10.18844/wjet.v14i5.8051.

[14] Karta praw podstawowych Unii Europejskiej (Dz.U. UE C 326 z 26.10.2012).

których dane podlegają szczególnej ochronie. Zgodnie z motywem 38 RODO dzieci jako podmioty prawa mniej świadome ryzyka, zagrożeń oraz konsekwencji związanych z przetwarzaniem ich danych osobowych powinny podlegać szczególnej ochronie[15]. Ochronie powinny podlegać, w szczególności z perspektywy obecności dzieci w platformach edukacyjnych, w tym usługach społeczeństwa informacyjnego, które są wykorzystywane do prowadzenia procesu edukacji cyfrowej. Dzieci, jako osoby bardziej podatne na wpływ cyfrowego świata, które nie posiadają dostatecznych narzędzi ochrony przed zagrożeniami, powinny być traktowane priorytetowo[16]. Powyższe wiąże się z koniecznością uwzględnienia podwyższonego standardu ochrony danych osobowych małoletnich już na etapie projektowania (*privacy by design)* narzędzi informatycznych, które będą stosowane w procesie edukacji zdalnej.

Pomimo ustania pandemii koronawirusa edukacja cyfrowa wciąż dynamicznie się rozwija i jest wykorzystywana przez placówki edukacyjne. Jednak fakt ciągłego zainteresowania tą formą nauczania oraz większy dostęp uczestników do tego procesu poprzez powstające platformy edukacyjne oraz narzędzia informatyczne nie doprowadziły do zmian w przedmiocie uregulowań sektorowych oraz kompleksowych regulacji odnoszących się wprost do ochrony danych osobowych w edukacji cyfrowej.

Celem niniejszego rozdziału jest wskazanie kluczowych wyzwań prawnych związanych z ochroną danych osobowych w procesie edukacji cyfrowej, które nadal pozostają nieuregulowane i często pomijane przez ustawodawcę. Ponadto celem rozdziału jest kompleksowa analiza zasad przetwarzania danych osobowych, rodzaju i kategorii danych, sposobu ich zabezpieczenia oraz identyfikacja głównych ryzyk dla praw i wolności osób, których dane dotyczą, a także znaczenie dobrych praktyk i rekomendacji organów nadzorczych.

1. REGULACJE PRAWNE ODNOSZĄCE SIĘ DO SYSTEMU EDUKACJI CYFROWEJ ORAZ OCHRONY DANYCH

Kwestia uregulowania przetwarzania danych osobowych w procesie edukacji cyfrowej nie doczekała się kompleksowej regulacji. Podstawowym aktem prawnym, który stanowi podstawę rozważań nad zagadnieniem ochrony danych oraz ich przetwarzaniem, jest RODO. Przepisy RODO nakładają na placówki edukacyjne szereg obowiązków związanych z prawidłowym przetwarzaniem danych osobowych

[15] Grupa Robocza Artykułu 29, Opinia 2/2009, *On the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, 2009, s. 6.
[16] G. Malgieri, G. González Fuster, *The Vulnerable Data Subject: A Gendered Data Subject?,* „European Journal of Law and Technology", 13(1), 2022, s. 1.

uczniów, studentów, nauczycieli, rodziców, w tym zapewnieniem odpowiednich środków technicznych i organizacyjnych wprowadzających odpowiedni stopień ochrony danych. Znaczenie ochrony danych osobowych w edukacji cyfrowej zostało jednak uwzględnione przez organ nadzorczy. Prezes Urzędu Ochrony Danych Osobowych w wydanych poradnikach oraz stanowiskach zwraca szczególną uwagę na zachowanie bezpieczeństwa danych uczestników zdalnej edukacji jako legalnego aspektu przetwarzania danych osobowych oraz zapewnienie odpowiednich środków organizacyjnych i technicznych[17] .

Analiza obowiązujących aktów prawnych w Polsce jednoznacznie wskazuje na pozostawienie luki w krajowych regulacjach prawnych. Zauważalna jest tendencja unikania tematyki kształcenia na odległość w powszechnie obowiązujących przepisach prawa, a tym bardziej kwestii ochrony danych osobowych. Przykładowo w ustawie prawo o szkolnictwie wyższym i nauce znajdziemy jedynie przepis (art. 67 ust. 4), który reguluje funkcjonowanie uczelni i prowadzenie studiów w pewnym zakresie z wykorzystaniem środków kształcenia na odległość oraz drugi i ostatni przepis dot. weryfikacji wyników nauki w sposób zdalny (art. 76a)[18]. Ponadto w ustawie o systemie oświaty czy ustawie oświatowej brak przepisów dot. ochrony danych osobowych uczniów w ramach zajęć zdalnych. Prawodawca ogranicza się jedynie do aspektów możliwości prowadzenia zajęć w formie innej niż stacjonarna, metod i technik, w tym narzędzi, które mogą być zastosowane.

Można również zauważyć, że prawodawca niejako zmusza do traktowania kształcenia zdalnego jako tradycyjnej formy nauczania, co nie jest dobrym rozwiązaniem.

Wartościowy wpływ na funkcjonowanie w Polsce systemu edukacji cyfrowej miała regulacja, która weszła w życie w czasie trwania pandemii koronawirusa. Rozporządzenie dot. czasowego ograniczenia funkcjonowania jednostek systemu oświaty, formalnie wprowadziło możliwość zdalnej realizacji obowiązku szkolnego i obowiązku nauki[19]. Równocześnie wprowadzenie wspomnianej regulacji przyczyniło się do rozpowszechnienia wykorzystywania narzędzi informatycznych oraz różnych platform edukacyjnych oraz aplikacji do prowadzenia procesu nauczania.

Istotny wpływ na rozwój edukacji cyfrowej na poziomie Unii Europejskiej mają przyjęte przez Komisję Europejską programy: *Digital Decade 2030* oraz *Digital Education Action Plan 2021-2027.* Dokumenty są ze sobą powiązane strategicznie

[17] Zob. Poradnik UODO, *Dane osobowe bezpieczne podczas zdalnego nauczania*, 2020, https://uodo.gov.pl/pl/383/1475 [dostęp: 2.03.2026].
[18] Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 r. poz. 1571 z późn. zm.).
[19] Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań…*op.cit.*

oraz celowo, a ich zakres przedmiotowy dotyczy szeroko rozumianej unijnej strategii transformacji cyfrowej, w której edukacja i kompetencje cyfrowe odgrywają znaczącą rolę[20]. Dokument dot. planu działania w dziedzinie edukacji cyfrowej na lata 2021-2027 stanowi strategicznie ramy dla Państw Członkowskich Unii Europejskiej w zakresie cyfrowej transformacji systemów edukacji. Jednocześnie podkreśla istotę rozwijania kompetencji cyfrowych, modernizacji narzędzi informatycznych, zwiększenia dostępności oraz poprawy jakości kształcenia cyfrowego[21]. Z kolei program „Droga ku cyfrowej dekadzie 2030 r.", o którym mowa powyżej, jest głównym dokumentem, który kompleksowo wyznacza szereg celów ogólnych oraz celów cyfrowych. W nawiązaniu do wspomnianego programu, Rada Ministrów jako uzupełnienie unijnej strategii dot. transformacji gospodarki uchwaliła Krajowy plan działania do programu polityki „Droga ku cyfrowej dekadzie 2030 r."[22]. Plan ten zakłada podjęcie działań mających na celu przyśpieszenie transformacji cyfrowej zgodnej z wartościami prezentowanymi przez unijne organy.

Podsumowaniem powyższych rozważań dotyczących stopnia uregulowania edukacji cyfrowej w Polsce oraz podjętych działań przez ustawodawcę mających na celu wdrożenie jak najlepszego stopnia świadczenia usług kształcenia na odległość, istotną rolę odgrywa w tym procesie uchwalona przez Radę Ministrów „Polityka Cyfrowej Transformacji Edukacji"[23]. Powołany dokument ma za zadanie określić cele i kierunki rozwoju edukacji w aspekcie społecznym, gospodarczym i przestrzennym. Polityka określana jako Dekalog Cyfrowej Transformacji Edukacji podzielona została na 10 ściśle powiązanych ze sobą obszarów. W każdym z dziesięciu obszarów uwzględniono diagnozę stanu obecnego, cele strategiczne transformacji i kierunki interwencji[24].

Mając powyższe na względzie, pomimo wprowadzenia programów oraz strategii mających na celu wprowadzenie zmian w przedmiocie edukacji cyfrowej w Polsce, wciąż zauważalne są braki regulacyjne. W szczególności w omawianej w tym rozdziale ochronie danych osobowych, odnośnie której administratorzy danych, w rozumieniu art. 4 pkt 7 RODO, napotykają licznie trudności w kontekście wdrażania

[20] Komunikat komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów*, Plan działania w dziedzinie edukacji cyfrowej na lata 2021-2027, Nowe podejście do kształcenia i szkolenia w epoce cyfrowej,* 2020.

[21] Digital Education Plan 2021-2027, *Resetting education and training for the digital age,* https://education.ec.europa.eu/sites/default/files/document-library-docs/deap-communication-sept2020_en.pdf, s. 2 [dostęp: 2.03.2026].

[22] Uchwała nr 125 Rady Ministrów z dnia 22 października 2024 r. *w sprawie Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie do 2030* r".

[23] Uchwała nr 98 Rady Ministrów z dnia 12 września 2024 r. w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji".

[24] *Ibidem* (załącznik do uchwały), s. 5.

edukacji cyfrowej w swojej organizacji[25]. Finalnie mogą skorzystać z dostępnych poradników, wytycznych czy opinii organu nadzorczego bardzo często postępując intuicyjnie, stosując analogicznie przepisy dot. edukacji w tradycyjnej formie, co w rezultacie i w praktycznym zastosowaniu tych przepisów może doprowadzić do naruszenia podstawowych praw i wolności osób, których dane dotyczą, tj. uczestników procesu edukacji cyfrowej.

2. RODZAJE ORAZ KATEGORIE DANYCH OSOBOWYCH PRZETWARZANYCH W PROCESIE EDUKACJI CYFROWEJ

Przetwarzanie danych osobowych w rozumieniu art. 4 pkt 1 RODO jest nierozerwalnym elementem realizacji procesu edukacji cyfrowej[26]. Zakres danych osobowych gromadzonych i przetwarzanych wykracza poza zakres danych, które są gromadzone w ramach tradycyjnej formy nauczania.

W omawianym procesie ogólną kategorię danych stanowią dane uczestników edukacji cyfrowej. Pod pojęciem uczestnika należy rozumieć nauczyciela, rodzica oraz ucznia, często będącego dzieckiem. Udział dzieci w procesie zdalnej edukacji budzi pewne wątpliwości oraz jest problematyczny z punktu widzenia ochrony danych, gdzie dzieci traktowane są jako jednostki mniej świadome, wrażliwe i podatne na zagrożenia wynikające z obecności w świecie cyfrowym[27]. W związku z powyższym dane dzieci określane jako szczególne powinny być chronione ze wzmożoną ostrożnością w celu zapewnienia poszanowania podstawowych praw i wolności[28].

Rozważając kwestie rodzajów danych osobowych przetwarzanych w procesie edukacji cyfrowej należy je rozgraniczyć na dane identyfikacyjne uczestnika procesu, dane edukacyjne, dane techniczne oraz dane szczególnych kategorii tzw. dane wrażliwe. Nadal podstawową kategorią danych gromadzonych w procesie edukacji cyfrowej pozostają, podobnie jak w tradycyjnej formie kształcenia, dane identyfikacyjne

[25] Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

[26] Dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

[27] A. Bagattini, *Children's Well-Being and Vulnerability*, „Ethics and Social Welfare", 13, 2019, s. 211.

[28] S. Piasecki, J. Chen, *Complying with the GDPR When Vulnerable People Use Smart Devices*, International Data Privacy Law, 12(113), 2022, s. 113.

uczestników, które obejmują w szczególności imię i nazwisko, datę i miejsce urodzenia, adres e-mail, numer PESEL, adres zamieszkania oraz szereg niezbędnych dodatkowych danych gromadzonych dla potrzeb prowadzenia procesu dydaktycznego[29]. Jednak w odróżnieniu od tradycyjnej formy kształcenia istotną grupę danych stanowią dane edukacyjne oraz techniczne. Grupa ta obejmuje w szczególności login użytkownika, który wykorzystywany jest do zakładania kont użytkowników na platformach edukacyjnych, komunikatorach, aplikacjach dokumentujących przebieg i postęp w nauce, takich jak frekwencja, wyniki w nauce, aktywność na platformach edukacyjnych, zadania domowe lub prace zaliczeniowe. Dane te stanowią pośrednie dane osobowe, które w połączeniu z danymi bezpośrednimi pozwolą na utworzenie szczegółowego profilu uczestnika procesu edukacji cyfrowej, co może wpływać na jego poczucie bezpieczeństwa oraz poszanowania prawa do prywatności , zważywszy na fakt, że wszystkie te dane są przetwarzane automatycznie przez systemy informatyczne. Dane techniczne to katalog danych, które rzadziej występują w tradycyjnej formie nauczania, a wynika to z faktu wykorzystywania do edukacji cyfrowej większej liczby narzędzi i systemów informatycznych. W praktyce oznacza to, że dochodzi do przetwarzania adresów IP, identyfikatorów urządzeń logujących się w aplikacji lub platformach, danych logowania, a także niejednokrotnie danych dot. lokalizacji. Powyższe dane stanowią dane osobowe w rozumieniu RODO. Pogląd ten potwierdza wyrok Trybunału Sprawiedliwości Unii Europejskiej („TSUE") z dnia 19 października 2016 r., sygn. akt C-582/14, który uznał dane techniczne, w tym adres IP, za daną osobową, o ile istnieje możliwość dokonania jednoznacznej identyfikacji osoby fizycznej[30].

Problematyczne staje się również przetwarzanie danych szczególnych kategorii w rozumieniu art. 9 RODO w procesie edukacji cyfrowej. Znaczenia nabierają narzędzia informatyczne wykorzystywane do monitorowania uczestników podczas egzaminów (tzw. *proctoring*). Platformy edukacyjne, które wykorzystują algorytmiczne narzędzia monitorujące podczas egzaminów opierają się na systemie nadzoru tj. rozpoznanie twarzy i analizy otoczenia, śledzenie wzroku, stosowanie kamer 360 stopni nagrywających całe pomieszczenie. Takie działanie platformy może doprowadzić do przetwarzania danych biometrycznych, w tym wizerunku uczestnika procesu oraz

[29] Zob. przykładowo §14 i 15 Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (Dz. U. poz. 2787), które określają zakres danych osobowych gromadzonych od studentów, które przechowywane są w teczkach studenta dla potrzeb realizacji procesu dydaktycznego na uczelni wyższej.

[30] Wyrok TSUE z dnia 19 października 2016 r., *Breyer*, sygn. akt C-582/14, Legalis nr 1533445.

często danych behawioralnych, co wiąże się ze sporą ingerencją w podstawowe prawa i wolności[31].

Może się wydawać, że zakres przetwarzanych danych osobowych w procesie edukacji cyfrowej nie różni się znacznie od jej tradycyjnej formy. Jednak dokonując głębszej analizy, należy wziąć pod uwagę, że zakres przetwarzanych danych w przypadku edukacji w formie tradycyjnej jest ściśle określony, jasno wynikający z przepisów prawa oświatowego lub ustawodawstwa odnoszącego się do szkolnictwa wyższego. W przypadku edukacji cyfrowej zakres ten jest elastyczny i bardzo dynamiczny, często uzależniony od rodzaju wykorzystywanych narzędzi informatycznych. Biorąc powyższe pod uwagę, istotne jest odpowiednie zabezpieczenie i zapewnienie ochrony danych przez administratorów danych, co z kolei ponownie uzasadnia konieczność odpowiedniej regulacji i określenia charakteru prawnego gromadzenia i przetwarzania danych osobowych w edukacji cyfrowej.

3. PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH W EDUKACJI CYFROWEJ

Rozwój narzędzi cyfrowych, które stosowane są w procesie dydaktycznym, jak wskazano powyżej, prowadzi do intensyfikacji przetwarzania danych osobowych uczestników procesu dydaktycznego, w szczególności uczniów, studentów oraz nauczycieli. Wykorzystywane platformy e-learningowe, dzienniki elektroniczne, systemy zarządzające procesem nauczania („LMS") oraz aplikacje, których celem jest dodatkowe wsparcie zdalnej edukacji, gromadzą i analizują spore ilości danych osobowych oraz informacji na temat użytkowników korzystających z tych narzędzi. Wobec powyższego, jako konsekwencja korzystania w edukacji cyfrowej z narzędzi wspierających proces dydaktyczny, szczególnego znaczenia nabiera konieczność określenia podstaw prawnych przetwarzania danych osobowych w procesie edukacji cyfrowej.

Zgodnie z art. 6 ust. 1 RODO przetwarzanie danych osobowych jest dopuszczalne i zgodne z prawem tylko w przypadku spełnienia co najmniej jednej z przesłanek legalizujących określonych w art. 6 ust. 1 oraz art. 9 ust. 2 RODO. Dla potrzeb niniejszego rozdziału, omawianej tematyki oraz w kontekście funkcjonowania instytucji edukacyjnych kluczowe znaczenie mają trzy podstawy prawne: realizacja obowiązku prawnego nałożonego na administratora danych (art. 6 ust 1 lit. c RODO),

[31] Dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

wykonanie zadania realizowanego w interesie publicznych lub w ramach sprawowania władzy publicznej (art. 6 ust 1 lit. e RODO) oraz w ostateczności zgoda osoby, której dane dotyczą (art. 6 ust 1 lit. a RODO).

Realizacja obowiązku prawnego ciążąca na administratorze danych osobowych to jedna z najczęściej stosowanych przesłanek przetwarzania danych osobowych w procesie edukacji. Powyższą tezę potwierdza fakt obowiązku gromadzenia i przetwarzania określonych kategorii i rodzajów danych dla potrzeb podtrzymania procesu dydaktycznego przez instytucje edukacyjne[32]. W ramach realizacji ustawowych obowiązków placówki edukacyjne przetwarzają liczne dane identyfikacyjne uczestników procesu dydaktycznego, które są niezbędne do podtrzymania właściwego toku kształcenia. Powyżej już zasygnalizowano, że wraz z rozwojem i postępem cyfryzacji w dziedzinie edukacji coraz częściej dochodzi do przetwarzania danych w systemach teleinformatycznych, takich jak przykładowo dzienniki elektroniczne lub platformy edukacyjne, wykorzystanych nie tylko do prowadzenia nauczania w formie zdalnej, ale również do zarządzania procesem dydaktycznym. Przetwarzanie danych w ramach powyższych działań będzie legalne, o ile niezbędność gromadzenia danych jest kluczowa i niezbędna do realizacji obowiązków wynikających z przepisów prawa.

Kolejną istotną podstawą prawną przetwarzania danych osobowych w procesie edukacji cyfrowej jest wykonywanie zadania realizowanego w interesie publicznym, tj. art. 6 ust. 1 lit. e RODO. Niewątpliwie edukacja stanowi jedno z najważniejszych i podstawowych zadań państwa, a realizacją tych zadań zajmują się instytucje edukacyjne na różnych poziomach oraz w różnych formach opierające swą działalność na głównym celu, tj. realizacji ww. zadania państwowego. Biorąc powyższe pod uwagę, jeśli w ramach wykonywania zadania publicznego polegającego na zapewnieniu prawidłowego funkcjonowania procesu kształcenia konieczne jest przetwarzanie danych osobowych, wówczas administratorzy danych sięgają po podstawę prawną przetwarzania w ramach realizacji zadania publicznego nałożonego na nich[33]. W edukacji cyfrowej przetwarzanie danych w oparciu o tę podstawę

[32] Zob. Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (t.j. Dz. U. z 2023 r. poz. 2787 z późn. zm.) oraz Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (t.j. Dz. U. z 2024 r. poz. 50). Wskazane akty wykonawcze wskazują na obwiązek prawny placówek edukacyjnych gromadzenia określonych danych osobowych, które są niezbędne do świadczenia usług edukacyjnych.

[33] Zob. art. 11 ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 r. poz. 1571 z późn. zm.). W wskazanym artykule ustawodawca określił szereg zadań publicznych nałożonych na publiczne uczelnie wyższe, których realizacja jest elementem koniecznym funkcjonowania każdej uczelni wyższej. Jeśli, w skutek realizacji jednego z wskazanych tam zadań konieczne będzie przetwarzanie i gromadzenia danych osobowych administratorzy danych powinni skorzystać z podstawy przetwarzania z art. 6 ust 1 lit c RODO.

można uzasadnić w przedmiocie korzystania z platform e-learningowych, aplikacji mobilnych dla uczestników procesu, systemów zarządzania nauczaniem, w zakresie postępów w nauce, wyników, czasu pracy. Należy podkreślić, że przetwarzanie danych w oparciu o podstawę realizacji zadania publicznego nie może być nadużywane przez jednostki świadczące usługi edukacyjne, dlatego też przetwarzanie musi spełniać zasady minimalizacji danych oraz ograniczania celu, które zostały określone w art. 5 RODO[34].

Analizują kwestie podstaw prawnych przetwarzania danych, nie sposób odnieść do zgody osoby, której dane dotyczą, tj. art. 6 ust. 1 lit. a RODO. Niewątpliwie w trakcie procesu edukacji cyfrowej niejednokrotnie pojawia się problem z doborem odpowiedniej przesłanki do gromadzenia i przetwarzania danych, w szczególności, że ustawodawca nie uregulował tego procesu. W praktyce oznacza to, że zgoda będzie stosowana przez niektóre podmioty do świadczenia edukacji cyfrowej w sytuacjach, które nie wynikają z obowiązków ustawowych instytucji edukacyjnych, a analogiczne odwołanie się do przepisów odnoszących się do tradycyjnej formy kształcenia nie znajdzie zastosowania. W przypadku stosowania zgody jako przesłanki prawnej przetwarzania danych w relacji uczeń/nauczyciel - placówka edukacyjna pojawia się pewna wątpliwość oraz zagrożenie wynikające z braku równowagi pomiędzy stronami[35]. Zgodnie z art. 4 pkt 11 RODO jednym z elementów prawidłowej i ważnej zgody na przetwarzanie danych jest jej dobrowolność. Trudno szukać dobrowolności w relacji, w której równowaga jest zachwiana. Tym samym administratorzy danych powinni unikać stosowania przesłanki zgody jako podstawy przetwarzania danych w procesie edukacji cyfrowej. Dobrą praktyką jest korzystanie z tej podstawy jedynie dla potrzeb publikacji wizerunku uczestników procesu kształcenia na odległość, ewentualnie jako zgoda na korzystanie z dodatkowych nieobowiązkowych narzędzi informatycznych wspomagających proces edukacji zdalnej.

4. STATUS ORAZ ROLA ADMINISTRATORA DANYCH W SYSTEMACH EDUKACJI CYFROWEJ

Szczególnie ważne z perspektywy ochrony danych osobowych w edukacji cyfrowej jest precyzyjne określenie statusu podmiotów uczestniczących w tym procesie

[34] S. Rozmus, *E- learning w świetle RODO*, „Ekonomiczne Problemy Usług" 2018(2), https://doi.org/10.18276/epu.2018.131/1-30, s. 307-308.

[35] Zob. motyw 43 RODO, zgodnie z którym aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach.

i realizujących go. Zgodnie z art. 4 pkt 7 RODO administratorem danych jest podmiot, który samodzielnie decyduje o sposobach i celach przetwarzania danych osobowych. W praktyce funkcję administratora danych w dziedzinie edukacji zazwyczaj pełnią szkoły, uczelnie oraz inne placówki edukacyjne świadczące usługi edukacyjne, bez względu na ich formę[36,37]. Posiadanie statusu administratora danych wiąże się z licznymi obowiązkami nałożonymi na ten podmiot przez RODO. To na administratorze ciąży obowiązek przestrzegania zasad wskazanych w art. 5 RODO, w szczególności zasady zgodnego z prawem przetwarzania danych. Z perspektywy omawianej tematyki, administrator podejmuje decyzje w zakresie środków, które będą wykorzystywane do procesu dydaktycznego w formie zdalnej, zwłaszcza narzędzi informatycznych pozwalających na świadczenie kształcenia na odległość. Należy podkreślić, że odpowiedzialność ciążąca na administratorze nie może zostać przeniesiona na dostawców narzędzi informatycznych bądź platform edukacyjnych, bez względu na to, czy podmioty te zapewniają wsparcie techniczne. Głównym powodem, dla którego przeniesienie odpowiedzialności jest niemożliwe, jest fakt, że to administrator danych jest obowiązany wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić adekwatny stopień ochrony danych oraz ich przetwarzania zgodnego z prawem oraz podstawowymi zasadami wynikającymi z art. 5 RODO[38]. Co więcej, rola administratora nie sprowadza się jedynie do wdrożenia dowolnych jakichkolwiek środków technicznych i organizacyjnych. Biorąc pod uwagę złożoność procesu edukacji cyfrowej, w tym zakres przetwarzanych danych, administrator powinien wdrożyć środki i zabezpieczenia proporcjonalnie do zakresu, formy i celu oraz ilości przetwarzanych danych. Zatem administrator powinien dokonać oceny ryzyka oraz jego wpływu na prawa i wolności osób, których dane dotyczą, w szczególności poszanowania prawa do prywatności[39]. Administrator danych w swojej działalności powinien dostosować wdrożone zabezpieczenia pod względem rodzaju przetwarzanych danych, sposobu ich przetwarzania oraz ryzyka, które powiązane jest z przetwarzaniem i gromadzeniem danych[40].

---

[36] E. Day, K. Pothong, A. Atabey, S. Livingstone, *Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech*, „Learning, Media and Technology", 49(3), 2024, s. 360, https://doi.org/10.1080/17439884.2022.2152838.

[37] Por. Poradnik UODO i MEiN, *Ochrona danych osobowych w szkołach i placówkach oświatowych,* 2018, s. 8.

[38] P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa o ochronie danych osobowych. Komentarz [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz,* P. Litwiński (red.), wyd. 2, Warszawa 2025, artykuł 24.

[39] D. Lubasz, [w:] *RODO. Ogólne rozporządzenie o ochronie danych*, E. Bielak-Jomaa (red.), D. Lubasz (red.), Warszawa 2017, s. 587.

[40] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. 3, Warszawa 2025, s. 317.

Poza kluczową rolą administratora danych w systemach edukacji cyfrowej należy również zwrócić uwagę na podmioty przetwarzające w rozumieniu art. 4 pkt 8 RODO. Za podmioty przetwarzające uważa się podmiot przetwarzający dane w imieniu administratora.

W przypadku edukacji cyfrowej do podmiotów tych można zaliczyć dostawców platform edukacyjnych, narzędzi informatycznych, dostawców aplikacji mobilnych lub innych systemów, które mogą być wykorzystywane do prowadzenia procesu dydaktycznego zdalnie lub w chmurze. Podmioty przetwarzające są wybierane przez administratora danych, a legalność przetwarzania przez nich danych osobowych wynika z zawartej pomiędzy stronami umowy powierzenia danych osobowych lub innego instrumentu spełniającego wymogi określone w art. 28 ust. 3 RODO[41]. W kwestii podmiotów przetwarzających rola administratora ponownie ma decydujące znaczenie, bowiem to na administratorze spoczywa obowiązek wyboru podmiotu, który będzie przetwarzał dane w jego imieniu. Wybór podmiotu przetwarzającego nie może być przypadkowy, dopiero po ocenie kompetencji i adekwatności podmiotu przetwarzającego, administrator może zawrzeć stosowne umowy[42]. Zgodnie z wytycznymi Europejskiej Rady Ochrony Danych („EROD") administrator danych wybierając podmiot przetwarzający powinien oprzeć swój wybór na odpowiednich kryteriach, w szczególności powinien zwrócić uwagę na odpowiedni stopień wiedzy fachowej podmiotu przetwarzającego (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń ochrony danych), wiarygodność podmiotu przetwarzającego, zasoby podmiotu przetwarzającego oraz stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji[43]. Co więcej przed przystąpieniem do zawarcia umowy powinien stworzyć tzw. listę kontrolną dotyczącą podmiotu przetwarzającego oraz świadczonych przez niego usług[44]. Wspomniana weryfikacja ma charakter trwały, administrator już w trakcie trwania współpracy nadal obowiązany jest kontrolować, czy podmiot przetwarzający wciąż spełnia kryteria wyboru, a dane, które przetwarza, są odpowiednio zabezpieczone[45].

W kontekście omawiania statusu i roli administratora w procesie edukacji cyfrowej, poza licznymi odpowiedzialnościami, pozostaje również obowiązek przeprowadzenia oceny skutków dla ochrony danych („DPIA"). Zgodnie z art. 35 RODO jeśli

[41] P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa…op.cit.*, artykuł 28.
[42] Decyzja PUODO z dnia 16 sierpnia 2022 r., DKN.5131.29.2022, LEX nr 3482711.
[43] Wytyczne EROD 07/2020*, dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO,* 2021, s. 35.
[44] M. Sakowska-Baryła [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, M. Sakowska-Baryła (red.), wyd. 1, Warszawa 2018, artykuł 28.
[45] Wytyczne EROD 07/2020*, dotyczące pojęć…*op.cit., s. 30.

dane osobowe są przetwarzane w sposób szczególny, zwłaszcza z wykorzystaniem nowych technologii na administratorze spoczywa obowiązek przeprowadzenia DPIA w porozumieniu z Inspektorem Ochrony Danych („IOD"). Nie ulega wątpliwości, że proces edukacji cyfrowej opiera się na wykorzystywaniu platform, narzędzi informatycznych oraz rozwiązań, które opierają się na systemach sztucznej inteligencji lub nowoczesnych technologiach, co z kolei może prowadzić do wysokiego ryzyka naruszenia podstawowych praw i wolności osób, których dane dotyczą[46].

Ukazanie roli administratora danych oraz podmiotu przetwarzającego w procesie edukacji cyfrowej prowadzi do wniosku, że posiadanie jedynie statusu administratora danych na papierze nie jest wystarczające. Zapewnienie skutecznej ochrony danych uczestników procesu edukacji cyfrowej nie kończy się tylko na formalnym spełnieniu przepisów RODO, ale na faktycznym wdrożeniu ich w organizacji, w tym stałej kontroli ze strony administratora jako podmiotu, który ponosi odpowiedzialność za prawidłowe i zgodne z prawem przetwarzanie danych osobowych[47].

5. WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI I ZAUTOMATYZOWANEGO PODEJMOWANIA DECYZJI W EDUKACJI CYFROWEJ

Poruszając problematykę ochrony danych w procesie edukacji cyfrowej, nie sposób nawiązać do kwestii wykorzystywania narzędzi opartych na systemach sztucznej inteligencji („systemy AI"). Systemy wykorzystywane w procesie edukacji cyfrowej umożliwiają dokonanie analiz zbiorów danych dotyczących aktywności uczestników procesu edukacji cyfrowej, w szczególności analiz w zakresie wyników w nauce, aktywności na platformach edukacyjnych, realizacji zadań lub sposobów korzystania z udostępnionych materiałów edukacyjnych[48]. Systemy AI, bazując na pozyskanych danych, mogą zidentyfikować słabe strony uczestnika edukacji lub trudności w nauce, jednocześnie proponując spersonalizowane metody edukacyjne, które mogą wpłynąć na poprawę wyników i zwiększyć rozwój naukowy uczestników[49]. O ile wykorzystywane narzędzia informatyczne oparte na systemach AI są ułatwieniem i zdecydowanie mogą wpłynąć na poprawę jakości świadczonych usług edukacyjnych oraz procesu dydaktycznego i wydajności jednostki, to administratorzy danych,

[46] P. Barta, M. Kawecki, P. Litwiński [w:], *Ustawa…op.cit.*, artykuł 35.
[47] Wyrok WSA w Warszawie z dnia 21 października 2020 r., II SA/Wa 2826/19, LEX nr 3067899.
[48] H. Hariyanto, F.X.D. Kristianingsih, R. Maharani, *Artificial intelligence in adaptive education: a systematic review of techniques for personalized learning*, „Discover Education", 458(4), 2025, https://doi.org/10.1007/s44217-025-00908-6, s. 2-3.
[49] UNESCO, *Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development,* 2019, s. 12.

decydując się na stosowanie systemów AI, są obowiązani do zapewnienia zgodności z zasadami ochrony danych osobowych wynikającymi z RODO.

Z punktu widzenia RODO wykorzystanie systemów AI nabiera szczególnego znaczenia z perspektywy ochrony danych osobowych. Skutki działania i możliwości, które oferują systemy AI, często polegają na profilowaniu (art. 4 pkt 4 RODO) użytkowników danego narzędzia[50]. Szczególnego znaczenia w kontekście stosowania narzędzi opartych na systemach AI nabiera kwestia zautomatyzowanego podejmowania decyzji, czyli podejmowania decyzji w sposób zautomatyzowany bez udziału człowieka. Zgodnie z art. 22 RODO stosowanie zautomatyzowanych systemów jest dopuszczalne jedynie w ściśle określonych przypadkach[51]. W odniesieniu do edukacji cyfrowej, administratorzy danych podejmujący decyzje o stosowaniu zautomatyzowanych systemów decyzyjnych powinni zachować szczególną ostrożność, zwłaszcza w aspekcie udziału dzieci w tym procesie. Z tego względu ponownie należy odnieść się do obowiązku przeprowadzenia przez administratora danych DPIA, zgodnie z art. 35 RODO w przypadku stosowania i wdrażania przez administratora danych systemów opartych na sztucznej inteligencji lub systemów zautomatyzowanego podejmowania decyzji. Konieczność przeprowadzenia DPIA w tym zakresie jest niezbędna z uwagi na bardzo wysokie ryzyko naruszenia podstawowych praw i wolności jednostki.

Wykorzystywanie sztucznej inteligencji dynamicznie się rozwija. Znaczenie problematyki w zakresie ochrony danych osobowych, oraz systemów AI zostało podkreślone w regulacji odnoszącej się do sztucznej inteligencji na poziomie Unii Europejskiej. Wprowadzenie rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące wykorzystywania systemów opartych na sztucznej inteligencji („AI Act") wprowadza system klasyfikacji systemów AI ze względu na poziom ryzyka ich stosowania[52]. Tym samym wykorzystywanie systemów AI w procesie edukacji cyfrowej, nakłada na administratorów danych dodatkowe obowiązki w przedmiocie zapewnienia odpowiedniego stopnia ochrony i poszanowania podstawowych praw i wolności

[50] Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

[51] L. Colonna, *Teachers in the loop? An analysis of automatic assessment systems under Article 22 GDPR*, „International Data Privacy Law". 14, https://doi.org/10.1093/idpl/ipad024, s. 8-10.

[52] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), Dz.U. L, 2024/1689, art. 6-7.

osób uczestniczących w tym procesie[53]. Stosowanie systemów AI lub innych nowoczesnych technologii stawia przed administratorami wyzwanie spełnienia szeregu dodatkowych wymogów. W pierwszej kolejności administratorzy powinni czuwać nad przejrzystością, jasnością działania narzędzi sztucznej inteligencji oraz zapewnieniem nadzoru i udziału czynnika ludzkiego[54], który w głównej mierze powinien czuwać nad ograniczeniem ryzyka dyskryminacji, błędnych decyzji podejmowanych przez zautomatyzowane systemy lub nieuzasadnionego profilowania i ingerencji w prywatność, w szczególności uczniów i studentów w trakcie świadczenia procesu edukacji cyfrowej[55].

Dokonując podsumowania tej części, warto przekazać pewnego rodzaju wiadomość w stronę administratorów danych. Korzystanie i stosowanie systemów AI w obecnych czasach są potrzebne, stanowią pewnego rodzaju udogodnienie, jednak to, co jest w tym kluczowe, to świadomość administratorów. Nie wystarczy jedynie zapłacić za system i bezwiednie z niego korzystać; trzeba go jeszcze poznać i zrozumieć jego funkcjonalność.

6. ZAGROŻENIA ORAZ RYZYKA DLA OSÓB, KTÓRYCH DANYCH DOTYCZĄ W PROCESIE KSZTAŁCENIA NA ODLEGŁOŚĆ

Charakter procesu edukacji cyfrowej wiąże się z możliwością wystąpienia licznych zagrożeń dla bezpieczeństwa danych osobowych uczestników procesu, w szczególności dla prawa do prywatności. Wystąpienie zagrożeń prowadzi do naruszenia podstawowych zasad przewidzianych w art. 5 RODO, a co z tym związane, finalnie prowadzi do naruszenia podstawowych praw i wolności osób.

Zagrożenia mogą mieć zarówno charakter techniczny, jak i organizacyjny[56]. Podstawowym zagrożeniem dla danych osobowych w kształceniu na odległość jest nieuprawniony dostęp do systemów informatycznych, na podstawie których funkcjonują wykorzystywane do procesu narzędzia informatyczne lub platformy edukacyjne. Zagrożenie to zazwyczaj jest wynikiem stosowania słabych haseł lub udostępnienia dostępu do systemu nieuprawnionym osobom trzecim. Powodem wspomnianego zagrożenia może być również niewłaściwe zabezpieczenie platform.

[53] L. Yan, L. Sha, L. Zhao, Y.Li, R. Martinez-Maldonado, G. Chen, X. Li, Y. Jin,D. Gašević, D., *Practical and ethical challenges of large language models in education: A systematic scoping review.* „British Journal of Educational Technology", 2024(55). https://doi.org/10.1111/bjet.13370, s. 102

[54] L. Colonna, *Teachers in the loop?*...op.cit, s.14-16.

[55] F. Panagopoulou, C. Parpoula, K. Karpouzis, *Legal perspectives on AI and the right to digital literacy in education*, „Front. Comput. Sci.", 7:1692268, 2025, https://doi.org/10.3389/fcomp.2025.1692268, s. 9-10.

[56] P. Fajgielski, *Ogólne… op.cit*, 2025, s. 373.

Skutek powyższych zagrożeń to głównie ujawnienie danych osobowych zgromadzonych w systemach, co może mieć istotny wpływ na prawa i wolności osób będących uczestnikami procesu edukacji zdalnej. Kolejnym zagrożeniem w obszarze edukacji cyfrowej jest niewłaściwa konfiguracja narzędzi wykorzystywanych do prowadzenia procesu dydaktycznego[57]. Przykładowo, pozornie nieszkodliwe publiczne publikowanie linków do spotkań/zespołów lub brak odpowiedniego zarządzania w kwestii nagrywania lub robienia zrzutów ekranu podczas spotkania może w rezultacie doprowadzić do naruszenia integralności i poufności całej grupy danego spotkania online. Do naruszenia może dojść poprzez nieautoryzowany dostęp osób trzech, które mogą, jeśli nie ma wprowadzonych odpowiednich konfiguracji i zabezpieczeń, ujawnić dane, wykorzystać profile uczestników, skopiować ich wizerunek bądź wykorzystać zgromadzone dane dla potrzeb przyszłych potencjalnych wyłudzeń.

Z obszaru zagrożeń znaczenia nabiera budzące spore kontrowersje zjawisko wspomnianego już wcześniej *proctoringu.* Metoda mająca na celu kontrolę uczestników zajęć online podczas egzaminów. Kontrowersją w tym przypadku są stosowane narzędzia, których systemy wykorzystują sztuczną inteligencję do monitorowania zachowania uczestników, co często prowadzi do zgromadzenia danych biometrycznych, a w rezultacie do wysokiego ryzyka narażenia podstawowych praw i wolności, zwłaszcza prawa do prywatności. Należy podkreślić, że *protoring* prowadzi do nadmiernej ingerencji w sferę prywatną uczestników procesu edukacji cyfrowej, nie spełniając jednocześnie kryterium proporcjonalności przetwarzania danych osobowych. Tezę tę potwierdza orzeczenie krajowego sądu niemieckiego, który uznał, że monitorowanie egzaminów z wykorzystaniem *proctoringu* narusza RODO, w szczególności art. 9 RODO w zakresie niedopuszczalnej ingerencji w fundamentalne prawa osób, których dane dotyczą[58]. Dodatkowo warto zwrócić uwagę na orzeczenie, które zawiesiło decyzję jednego z paryskich uniwersytetów odnośnie do stosowania jednej z platform *proctoringowych*. Zgodnie z postanowieniem francuskiego sądu administracyjnego wstępnie zawieszono użycie platformy *TestWe*, która wykorzystuje algorytmiczne narzędzie monitorujące studentów podczas egzaminów[59]. *TestWe* opiera się na systemie nadzoru, tj. rozpoznaniu twarzy i analizie otoczenia, śledzeniu wzroku, stosowaniu kamer 360 stopni nagrywających całe pomieszczenie. Takie działania platformy określono jako wykraczające i nadmierne oraz rażąco naruszające zasadę minimalizacji.

[57] Poradnik UODO, *Jak bezpiecznie korzystać z wideokonferencji,* 2020, https://chopin.edu.pl/uploaded_files/1602064265_1601989594wideokonferencja-porady.pdf [dostęp: 2.03.2026].

[58] Wyrok Wyższego Sądu Krajowego (Thüringer Oberlandesgericht) z dnia 17 listopada 2025r., sygn. akt 3 U 885/24.

[59] Postanowienie z dnia 15 grudnia 2022r. nr 2216570, https://consultation.avocat.fr/blog/florent-verdier/article-45977-la-telesurveillance-des-examens-et-rgpd-pourquoi-est-ce-illegal.html? [dostęp: 2.03.2026].

Rozwój edukacji cyfrowej ma bezpośredni wpływ na dynamiczny wzrost wykorzystania przez placówki edukacyjne dostępnych platform edukacyjnych oraz innych narzędzi informatycznych, w tym aplikacji mobilnych. Dlatego nie bez znaczenia pozostają narzędzia informatyczne oraz platformy edukacyjne wykorzystywane do procesu edukacji cyfrowej jako czynniki wywołujące zagrożenia dla ochrony danych, w szczególności, na uwadze należy mieć prawo do prywatności[60]. W obszarze szkolnictwa można wyróżnić dwa najczęściej wykorzystywane systemy edukacji zdalnej: *Learning Management System* oraz *Massive Open Online Courses* („MOOC"). LMS to system wykorzystywany do zarządzania nauczaniem, częściej stosowany w szkolnictwie, z kolei MOOC to forma otwartych kursów online, głównie wykorzystywana do prowadzenia szkoleń dla dużych grup. Zdecydowanie częściej bowiem około 48% organizatorów usług edukacyjnych sięga po system LMS, z kolei 21% korzysta z systemów MOOC[61]. Skupiając się na platformach wykorzystujących system LMS, warto zwrócić uwagę na polityki prywatności przykładowych platform. Istotne jest, aby administrator danych przed wyborem odpowiedniego narzędzia zapoznał się z kluczowymi zasadami związanymi z tym, jak dostawca platformy przetwarza dane osobowe oraz z tym, co się dzieje z danymi w momencie założenia kont użytkowników. Sięgając do polityki prywatności popularnej platformy Microsoft Teams, pierwsze, co budzi wątpliwość to fakt scalenia polityki prywatności z inną aplikacją tej firmy tj. Skype[62]. Takie działanie nie do końca spełnia przesłanki jasności informacji dla użytkowników tych platform. Ze względu na ogólność polityki prywatności użytkownicy nie wiedzą, które dane osobowe są wykorzystywane do funkcjonalności jednej z dwóch wspomnianych platform[63]. Problematyczna staje się również kwestia potencjalnego transferu danych do państw trzecich wskutek korzystania z dostępnych platform oraz narzędzi informatycznych. Dostawcy niektórych z platform mają siedziby lub infrastrukturę poza Europejskim Obszarem Gospodarczym, co oznacza, że podczas korzystania z nich może dojść do transferu danych do państw trzecich, w związku z przechowywaniem danych na serwerach, obsługą od strony technicznej lub zachowaniem bezpieczeństwa usługi. Problematyczny w tym zakresie nie jest sam fakt transferu, a forma przekazania informacji użytkownikom odnośnie możliwości transferowania danych oraz konkretnego celu dokonywania transferu.

[60] G. Achilleos, K. Limniotis, N. Kolokotronis, *Exploring Personal Data Processing in Video Conferencing Apps,* „Electronics" 2023, 12(5), 1247, s. 1, https://doi.org/10.3390/electronics12051247.
[61] A. Palanci, R.M. Yılmaz, Z. Turan, *Learning analytics in distance education: A systematic review study*, „Educ Inf Technol" 29, 22629-22650, 2024, s. 22640 https://doi.org/10.1007/s10639-024-12737-5.
[62] Oświadczenie o ochronie prywatności w firmie Microsoft, https://www.microsoft.com/pl-pl/privacy/privacystatement [dostęp: 2.03.2026].
[63] G. Achilleos, K. Limniotis, N. Kolokotronis, *Exploring… op.cit.,* s.15.

Na koniec rozważań dot. zagrożeń nie sposób wspomnieć o braku procedur wewnętrznych, braku szkoleń w zakresie ochrony danych osobowych osób pełniących rolę edukatorów. Dominującym czynnikiem wystąpienia wielu zagrożeń wciąż jest błąd ludzki, a niski poziom świadomości w zakresie zasad przetwarzania danych oraz brak dokumentacji jedynie pogłębia ryzyko wystąpienia naruszeń[64]. Jak wynika ze sprawozdania Prezesa Urzędu Ochrony Danych Osobowych za rok 2024, większość zgłoszonych naruszeń była spowodowana błędem ludzkim. Co więcej 328 zgłoszeń dot. naruszeń pochodziło ze szkolnictwa wyższego i oświaty, co dowodzi powyższej tezie dot. licznych zagrożeń i nieprawidłowości u administratorów, które prowadzą do naruszeń ochrony danych osobowych[65].

Przedstawione powyżej przykłady zagrożeń mogących wystąpić w procesie edukacji cyfrowej udowadniają, że obszar ten jest bardzo podatny na zagrożenia i kluczowy z perspektywy bezpieczeństwa danych osobowych. Prawidłowe wdrożenie procedur organizacyjnych i technicznych mających na celu zabezpieczenie danych i stosowanie rozwiązań minimalizujących możliwość wystąpienia naruszeń jest szczególnie ważne pod kątem poszanowania praw i wolności uczestników procesu edukacji cyfrowej oraz jednym z najistotniejszych zadań i odpowiedzialności administratorów danych osobowych.

7. DOBRE PRAKTYKI W ZAKRESIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH I POSZANOWANIA PODSTAWOWYCH PRAW I WOLNOŚCI

Stały rozwój edukacji cyfrowej i wykorzystywanych do tego procesu narzędzi informatycznych powiązany jest z koniecznością wdrożenia przez administratorów danych odpowiednich zasad odnoszących się do ochrony danych osobowych. Potwierdzeniem powyższej tezy jest zasada rozliczalności, o której mowa w art. 5 ust. 2 RODO. Zgodnie z ww. zasadą administrator danych przejmuje na siebie obowiązek przestrzegania zasad ochrony danych oraz odpowiedzialność za przestrzeganie przepisów, w tym również wewnętrznych uregulowań wprowadzonych w organizacji administratora[66]. Wobec powyższego, dobrą praktyką w zakresie bezpieczeństwa danych osobowych w procesie edukacji cyfrowej, w szczególności, jest wdrażanie

[64] Por. raport Duńskiego organu nadzorczego dot. naruszeń ochrony danych, w którym wskazano, że 80,62% naruszeń stanowią niezamierzone incydenty wywołane ludzkim błędem, https://www.cyberpilot.io/cyberpilot-blog/the-most-common-gdpr-breaches oraz raport Litewskiego organu nadzorczego dot. naruszeń ochrony danych w pierwszej połowie 2025 roku, który wskazał, że 57% incydentów naruszeń danych zostały wywołane błędem ludzkim, https://www.thehackerwire.com/human-error-caused-57-of-lithuanias-data -breaches-in-early-2025-report-finds/ [dostęp: 2.03.2026].

[65] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2024, s.73-82.

[66] P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa…op.cit.*, artykuł 5.

środków organizacyjnych. Przykładowo w postaci wewnętrznych procedur takich jak polityki bezpieczeństwa danych oraz regulaminy korzystania i doboru platform edukacyjnych oraz sporządzenia dokumentacji, która w jasny sposób i prostym językiem wskaże osobom, których dane dotyczą sposoby oraz środki jakie podjął administrator, aby zapewnić zgodność przetwarzania danych z przepisami o ochronie danych[67].

Dobre praktyki obejmują zarówno działania techniczne, jak i organizacyjne. Do podstawowych działań o charakterze technicznym należy uwzględnić szyfrowanie danych oraz przechowywanie danych na wewnętrznych serwerach administratora danych, wprowadzenie wieloskładnikowego uwierzytelniania, które głównie ma na celu ograniczenie nieuprawnionego dostępu osób trzecich do kont użytkowników platform, regularne wykonywanie kopii zapasowych jako działanie zmierzające do zachowania atrybutu integralności danych oraz tzw. segmentacja uprawnień tj. zachowanie granic w zakresie nadawania uprawnień dostępowych do systemu w zależności od pełnionej roli w procesie dydaktycznym[68,69]. Działania o charakterze organizacyjnym głównie sprowadzają się do zapewnienia przez administratora jasnych i prostych komunikatów skierowanych do osób, których dane dotyczą, w zakresie sposobów i celów przetwarzania danych, w tym przysługujących im praw w związku z przetwarzaniem ich danych. Niniejszy środek dotyczy również udostępniania polityk prywatności wykorzystywanych narzędzi informatycznych, w tym informowaniu rodziców, w przypadku małoletnich uczestników o wszelkich kwestiach dot. gromadzenia i przetwarzania danych w trakcie procesu edukacji cyfrowej[70]. Nie bez znaczenia dla dobrych praktyk w zakresie bezpieczeństwa danych pozostają szkolenia i ciągłe podnoszenie świadomości personelu, ale również wszystkich uczestników procesu dydaktycznego. Szkolenia identyfikowane są jako działania, które mogą zmniejszyć ryzyko wystąpienia naruszeń wynikających z błędu ludzkiego[71].

Podejmując próbę podsumowania wyżej wymienionych przykładów środków organizacyjnych i technicznych rozumianych jako dobre praktyki, które mogą mieć wpływ na zwiększenie bezpieczeństwa danych osobowych, można sformułować rekomendację dla placówek edukacyjnych świadczących usługi edukacyjne w ramach

[67] Opinia Grupy Roboczej art. 29 z dnia 13 lipca 2010, 3/2010, *w sprawie zasady rozliczalności*, https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/pisma-urzedowe/opinia-grupy-roboczej-art-29-w-sprawie-zasady-184992976, [dostęp: 2.03.2026].

[68] Por. P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa…op.cit.*, artykuł 32.

[69] *Technical and Organisational Measures Under GDPR*, https://www.gdprregulation.eu/technical-and-organisational-measures/, [dostęp: 2.03.2026].

[70] Por. Poradnik UODO, *Dane osobowe*…op.cit.

[71] Por. Decyzja PUODO z dnia 21 sierpnia 2020r., sygn. akt ZSOŚS.421.25.2019, LEX nr 3285238 oraz Decyzja PUODO z dnia 17 maja 2023, sygn. akt DKN.5131.31.2022, LEX nr 3564718 w zakresie uznania przez Prezesa UODO szkoleń za istotny środek organizacyjny zapewniający bezpieczeństwo danych oraz zmniejszający ryzyko wystąpień naruszeń.

procesu edukacji cyfrowej. Po pierwsze, zapewnienie dostępu do aktualnych polityk prywatności wykorzystywanych narzędzi informatycznych. Po drugie, ciągłe wdrażanie nowych środków organizacyjno-technicznych, w tym, co istotne, przed wdrożeniem jakiegokolwiek nowego narzędzia informatycznego przeprowadzenie analizy ryzyka i, jeśli jest to konieczne, również DPIA. Sprawowanie nadzoru nad zawieraniem umów powierzenia z dostawcami platform edukacyjnych, w których jasno zostaną określone zasady powierzenia danych. Finalnie przeprowadzanie regularnych audytów oraz kontrola działań związanych z działaniami wskazanymi powyżej.

PODSUMOWANIE

Konkludując, zjawisko ochrony danych osobowych w procesie edukacji cyfrowej jest zagadnieniem, które wymaga sporo pracy zarówno na szczeblu krajowym, jak i unijnym. Prowadzenie edukacji w formie zdalnej stawia wiele wyzwań oraz zagrożeń dla placówek edukacyjnych nie tylko w kwestii ochrony danych osobowych. Mimo to, zważając na obecne realia, postęp i rozwój technologiczny oraz fakt, że społeczeństwo zwraca się ku światu cyfrowemu, proces ten już się nie zatrzyma. Wręcz przeciwnie wraz z nowymi osiągnięciami i rozwojem nowoczesnych technologii edukacja cyfrowa przybierze w siłę i stanie się nieodłącznym elementem systemu edukacyjnego, o ile już takim się nie stała. W takiej sytuacji administratorom danych osobowych tj. organizatorom procesu dydaktycznego pozostanie jedynie wdrożenie środków technicznych i organizacyjnych, świadome korzystanie z udogodnień, które zaoferuje technologia oraz ciągłe budowanie zaufania społecznego ze strony uczestników tego procesu jako fundamentu bezpiecznego i zgodnego z prawem przetwarzania danych osobowych i wzmocnienia cyfrowego kształcenia, poprzez stosowanie najlepszych praktyk.

BIBLIOGRAFIA

LITERATURA

A. Bagattini, *Children's Well-Being and Vulnerability*, 13 "Ethics and Social Welfare", 2019.

A. Palanci, R.M. Yılmaz, Z. Turan, Learning analytics in distance education: A systematic review study. „Educ Inf Technol" 29, 22629-22650, 2024, https://doi.org/10.1007/s10639-024-12737-5.

D. Lubasz, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa (red.), D. Lubasz (red.), Warszawa 2017.

E. Day, K. Pothong, A. Atabey, S. Livingstone, *Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech*, „Learning, Media and Technology", 49(3), 2024, https://doi.org/10.1080/17439884.2022.2152838.

F. Panagopoulou, C. Parpoula, K. Karpouzis, *Legal perspectives on AI and the right to digital literacy in education*, „Front. Comput. Sci.", 7:1692268, 2025, https://doi.org/10.3389/fcomp.2025.1692268.

F. Sabirova, A. Gura, E. Belyanova, A. Sukhorukih, *Distance education in a digital age*, „World Journal on Educational Technology: Current Issues" 14(5), 2022, https://doi.org/10.18844/wjet.v14i5.8051.

G. Achilleos, K. Limniotis, N. Kolokotronis, *Exploring Personal Data Processing in Video Conferencing Apps*, „Electronics", 2023, 12(5), https://doi.org/10.3390/electronics12051247.

G. Malgieri, G. González Fuster, *The Vulnerable Data Subject: A Gendered Data Subject?*, 13 „European Journal of Law and Technology", 1, 2022.

G. Mazurek, Transformacja cyfrowa- perspektywa instytucji szkolnictwa wyższego, [w:] *Transformacja akademickiego szkolnictwa wyższego w Polsce w okresie 30-lecia: 1989–2019, Konferencja Rektorów Akademickich Szkół Polskich*, J. Woźnicki (red.), Warszawa 2019.

H. Hariyanto, F.X.D. Kristianingsih, R. Maharani, *Artificial intelligence in adaptive education: a systematic review of techniques for personalized learning*, „Discover Education" 4, 458, 2025, https://doi.org/10.1007/s44217-025-00908-6.

J. Aquino, R. Alarcón, L. Guevara, J. Bravo-Jaico, N. Germán, C. Valdivia-Salazar, C., O. Serquén, GLE. Maquen-Niño, A. Tesén-Arroyo *Impact of digital transformation: assessing the knowledge and adoption of disruptive technologies in a higher education institution*, „Front. Computer Science", 7:1611952, 2025, https://doi.org/10.3389/fcomp.2025.1611952.

L. Colonna, *Teachers in the loop? An analysis of automatic assessment systems under Article 22 GDPR*, „International Data Privacy Law", 14, https://doi.org/10.1093/idpl/ipad024.

L. Yan, L. Sha, L. Zhao, Y.Li, R. Martínez-Maldonado, G. Chen, X. Li, Y. Jin,D. Gašević, D., *Practical and ethical challenges of large language models in education: A systematic scoping review.* „British Journal of Educational Technology", 55, 2024. https://doi.org/10.1111/bjet.13370.

M. Garlinska, M. Osial, K. Proniewska, A. Pregowska, *The Influence of Emerging Technologies on Distance Education* „Electronics" 2023, 12, 1550. https://doi.org/10.3390/electronics12071550.

M. Kovacic, *Legal Aspects of Distance Learning*, 2021, https://doi.org/10.46793/nnu21.321k.

M. Sakowska-Baryła [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, M. Sakowska-Baryła (red.), wyd. 1, Warszawa 2018, artykuł 28.

P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa o ochronie danych osobowych. Komentarz [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, P. Litwiński (red.), wyd. 2, Warszawa 2025.

P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2025.

R. Isus, K. Kolesnikova, I. Khlevna, T. Oleksandr, K. Liubov, *Development of a model of personal data protection in the context of digitalization of the educational sphere using information technology tools,* „Procedia Computer Science", Vol. 231, 2024, https://doi.org/10.1016/j.procs.2023.12.215.

S. Piasecki, J. Chen, *Complying with the GDPR When Vulnerable People Use Smart Devices*, 12 „International Data Privacy Law" 113, 2022.

S. Rozmus, *E-learning w świetle RODO*, „Ekonomiczne Problemy Usług" nr 2, 2018, https://doi.org/10.18276/epu.2018.131/1-30.

AKTY PRAWNE

Karta praw podstawowych Unii Europejskiej (Dz.U. UE C 326 z 26.10.2012).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE. L. z 2024 r. poz. 1689).

Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 r. poz. 1571 z późn. zm.).

Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. poz. 493 z późn. zm.).

Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (t.j. Dz. U. z 2024 r. poz. 50).

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (t.j. Dz. U. z 2023 r. poz. 2787 z późn. zm.).

Uchwała nr 125 Rady Ministrów z dnia 22 października 2024 r. w sprawie Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r.

Uchwała nr 98 Rady Ministrów z dnia 12 września 2024 r. w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji".

ORZECZNICTWO

Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r.

Decyzja PUODO z dnia 17 maja 2023, sygn. akt DKN.5131.31.2022, LEX nr 3564718.

Decyzja PUODO z dnia 21 sierpnia 2020 r., sygn. akt ZSOŚS.421.25.2019, LEX nr 3285238.

Decyzja PUODO z dnia 7 września 2022 r., sygn. akt DKN.5131.29.2022, LEX nr 3482711.

Wyrok TSUE z dnia 19 października 2016 r., C-582/14.

Wyrok WSA w Warszawie z dnia 21 października 2020 r., II SA/Wa 2826/19, LEX nr 3067899.

Wyrok Wyższego Sądu Krajowego (Thüringer Oberlandesgericht) z dnia 17 listopada 2025 r., sygn. akt 3 U 885/24.

INNE PUBLIKACJE

Komisja Europejska, Digital Education Plan 2021-2027, Resetting education and training for the digital age, https://education.ec.europa.eu/sites/default/files/document-library-docs/deapcommunication-sept2020_en.pdf [dostęp: 2.03.2026].

Grupa Robocza Artykułu 29, Opinia 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools), 2009.

Komisja Europejska /EACEA/Eurydice, Digital Education at School in Europe, Eurydice Report., 2019.

Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego i Rady, Europejskiego Komitetu ekonomiczno-społecznego i Komitetu Regionów, Plan działania w dziedzinie edukacji cyfrowej na lata 2021-2027: Nowe podejście do kształcenia i szkolenia w epoce cyfrowej, 2020.

OECD, Digital Education Outlook, Towards an Effective Digital Education Ecosystem, 2023.

OECD, Education responses to COVID-19: Embracing digital learning and online collaboration, Paris 2020.

Grupa Robocza Artykułu 29, Opinia Grupy Roboczej art. 29 z dnia 13 lipca 2010, 3/2010, w sprawie zasady rozliczalności, https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/pisma-urzedowe/opinia-grupy-roboczej-art-29-w-sprawie-zasady-184992976, [dostęp: 2.03.2026].

Microsoft, Oświadczenie o ochronie prywatności w firmie Microsoft, https://www.microsoft.com/pl-pl/privacy/privacystatement [dostęp: 2.03.2026].

Poradnik UODO i MEiN, Ochrona danych osobowych w szkołach i placówkach oświatowych, 2018.

Poradnik UODO, Jak bezpiecznie korzystać z wideokonferencji, 2020, https://chopin.edu.pl/uploaded_files/1602064265_1601989594wideokonferencja-porady.pdf, [dostęp: 2.03.2026].

Poradnik UODO, Dane osobowe bezpieczne podczas zdalnego nauczania, 2020, https://uodo.gov.pl/pl/383/1475, [dostęp: 2.03.2026].

Postanowienie z dnia 15 grudnia 2022 r. nr 2216570, https://consultation.avocat.fr/blog/florent-verdier/article-45977-la-telesurveillance-des-examens-et-rgpd-pourquoi-est-ce-illegal.html? [dostęp: 2.03.2026].

Datatilsynet, Raport duńskiego organu nadzorczego dot. naruszeń, https://www.cyberpilot.io/cyberpilot-blog/the-most-common-gdpr-breaches [dostęp: 2.03.2026].

Valstybinė duomenų apsaugos inspekcija, Raport litewskiego organu nadzorczego dot. statystyk naruszeń, https://www.thehackerwire.com/human-error-caused-57-of-lithuanias-data-breaches-in-early-2025-report-finds/, [dostęp: 2.03.2026].

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2024.

GDPRREGULATION, Technical and Organisational Measures Under GDPR, https://www.gdprregulation.eu/technical-and-organisational-measures/ [dostęp: 2.03.2026].

UNESCO, Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development, 2019.

UNESCO, Digital Education, UNESCO, https://www.unesco.org/en/tags/digital-education-0 [dostęp: 2.03.2026].

EROD, Wytyczne EROD 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO, 2021.

PERSONAL DATA PROTECTION IN DIGITAL EDUCATION

Summary: The development of digital education and the use of available distance learning solutions are associated with new legal challenges, particularly in the area of personal data protection. The development of digital education has become increasingly important amid the coronavirus pandemic, when the need to ensure safety and prevent the spread of the virus led to the suspension of traditional teaching in many institutions. This has forced educational providers to adopt alternative methods and to take advantage of the opportunities offered by digital education. Furthermore, given that the modern digital world is characterized by growing public awareness and the increasing involvement of technology in human life, it is essential to adapt technological advancements to the requirements of compliance with fundamental rights and freedoms of individuals, particularly the right to privacy and personal data protection in the digital environment. The purpose of this chapter is to highlight the key challenges digital education poses in the field of personal data protection, taking into account applicable legal regulations, supervisory authority guidelines, and current practices.

Keywords: GDPR; personal data protection; digital education; distance education, IT tools.

Agnieszka Szymczak
Uniwersytet Mikołaja Kopernika w Toruniu
ag.szymczak02@gmail.com

ANONIMIZACJA A PSEUDONIMIZACJA W ŚWIETLE RODO: IMPLIKACJE PRAWNE I PRAKTYCZNE

Streszczenie: Artykuł poświęcony jest analizie prawnej i praktycznej dwóch fundamentalnych technik depersonalizacji danych osobowych – anonimizacji oraz pseudonimizacja – w świetle ogólnego rozporządzenia o ochronie danych. Autor wskazuje, że precyzyjne rozgraniczenie obu procesów ma kluczowe znaczenie w dobie gospodarki opartej na danych oraz rozwoju systemów sztucznej inteligencji, dla których dostęp do wysokiej jakości zbiorów informacji stanowi zarazem warunek postępu i jego wąskie gardło. W opracowaniu wykazano, że RODO definiuje i reguluje wprost wyłącznie pseudonimizację, traktując ją jako środek bezpieczeństwa przetwarzania, podczas gdy informacje skutecznie zanonimizowane tracą charakter danych osobowych i wymykają się spod reżimu rozporządzenia. Omówiono ramy pojęciowe i prawne depersonalizacji, status anonimizacji jako operacji przetwarzania wymagającej podstawy prawnej, a także zasadę ochrony danych w fazie projektowania. Przedstawiono praktyczne techniki anonimizacji (randomizacja, dodawanie szumu, prywatność różnicowa, k-anonimowość, l-dywersyfikacja, t-bliskość) oraz metody pseudonimizacji (szyfrowanie, haszowanie, tokenizacja), wraz z towarzyszącymi im wyzwaniami technicznymi, w szczególności kompromisem między użytecznością analityczną a ochroną prywatności. Artykuł konkluduje, że skuteczność anonimizacji nie ma charakteru absolutnego ani trwałego, lecz stanowi proces dynamiczny, wymagający stałego monitorowania, oceny skutków dla ochrony danych (DPIA) oraz stosowania testu racjonalności w obliczu rosnącego ryzyka reidentyfikacji.

Słowa kluczowe: anonimizacja; pseudonimizacja; RODO; ochrona danych osobowych; depersonalizacja; reidentyfikacja; prywatność różnicowa; k-anonimowość.

WPROWADZENIE

Obecnie dane stanowią kluczowy zasób determinujący postęp innowacyjny, w szczególności w zakresie systemów opartych na sztucznej inteligencji, dla których swobodny dostęp do informacji jest głównym czynnikiem warunkującym, a zarazem

stanowiącym wąskie gardło rozwoju. Z tego względu niezbędne staje się gromadzenie zbiorów danych o wysokiej jakości. Przez pojęcie to należy rozumieć obszerne, reprezentatywne oraz należycie przygotowane repozytoria informacji, pełniące funkcję niezbędnego materiału treningowego dla modeli uczenia maszynowego. Przedmiotowe zbiory obejmują z jednej strony precyzyjne dane ustrukturyzowane, przybierające najczęściej postać wielowymiarowych tabel odzwierciedlających określone zjawiska statystyczne. Z drugiej zaś strony w ich skład wchodzą dominujące we współczesnym obrocie cyfrowym dane nieustrukturyzowane, do których zalicza się między innymi obszerne korpusy dokumentów tekstowych, nagrania dźwiękowe oraz zróżnicowane dane obrazowe, w tym specjalistyczne fotografie medyczne.

W tym kontekście wymóg wysokiej jakości oznacza konieczność zapewnienia odpowiedniej dokładności, zachowania właściwych korelacji i rozkładów statystycznych oraz integralności semantycznej pozyskiwanych informacji. Spełnienie tego kryterium stanowi warunek bezwzględny dla poprawnego funkcjonowania algorytmów i wyciągania przez nie logicznych wniosków, a także dla minimalizacji ryzyka ich wadliwego działania czy powielania ludzkiej stronniczości.

Modele poddane właściwemu trenowaniu na tak rzetelnych zbiorach służą następnie usprawnianiu szerokiego spektrum procesów, które w świetle najnowszych trendów technologicznych nie ograniczają się do jednej dziedziny, lecz znajdują zastosowanie w zaawansowanych operacjach o charakterze badawczym, decyzyjnym, produkcyjnym i usługowym w niemal każdej branży gospodarki. W ujęciu praktycznym wdrożenie omawianych rozwiązań pozwala na radykalną optymalizację, automatyzację i obniżenie kosztów wielu działań. Obejmuje to w szczególności wspomaganie i przyspieszanie procesów diagnostycznych w opiece zdrowotnej, weryfikację oraz obsługę transakcji w sektorze usług finansowych, bezpieczne sterowanie w procesie rozwoju pojazdów autonomicznych, a także usprawnianie procesów komunikacyjnych i analitycznych poprzez automatyczne generowanie spójnych raportów, tłumaczeń czy odpowiedzi w systemach obsługi klienta.

Tak szerokie wykorzystanie danych rodzi jednak konflikt między ich swobodnym przepływem a prawem do prywatności, zmuszając do poszukiwania równowagi między dążeniem do swobodnego przepływu danych a koniecznością zapewnienia skutecznej ochrony prywatności oraz podstawowych praw i wolności osób fizycznych. W odpowiedzi na to wyzwanie administratorzy stosują techniczne metody depersonalizacji. Stanowią je anonimizacja i pseudonimizacja, które mają na celu minimalizację ryzyka naruszenia dóbr osobistych przy jednoczesnym zachowaniu użyteczności informacji dla celów analitycznych i biznesowych. Kluczowe zagadnienie współczesnego prawa ochrony danych osobowych koncentruje się wokół

precyzyjnego rozgraniczenia procesów anonimizacji i pseudonimizacji. Właściwa identyfikacja tych procesów jest niezbędna w dobie gospodarki opartej na danych oraz zaawansowanych analizach *Big Data*. Precyzyjne odróżnienie anonimizacji od pseudonimizacji pozwala administratorom na pogodzenie szerokiego wykorzystania informacji z koniecznością ochrony prywatności i autonomii informacyjnej jednostki. Jest to szczególnie istotne w sektorze publicznym oraz w zaawansowanych badaniach naukowych, gdzie dane statystyczne o wysokiej jakości są niezbędne do optymalizacji usług, takich jak projektowanie przestrzeni publicznej czy systemy transportowe.

Należy przy tym uwzględnić, że w dobie dynamicznego rozwoju technologii anonimizacja stanowi nieustanne wyzwanie techniczne i prawne, gdyż postęp w metodach analizy danych zwiększa ryzyko reidentyfikacji osób fizycznych. Z tego powodu interpretacja przepisów RODO w powiązaniu z krajową ustawą o otwartych danych oraz wytycznymi europejskich organów nadzorczych staje się niezbędnym elementem zarządzania ryzykiem w nowoczesnych systemach informatycznych. Prawidłowe zastosowanie tych instytucji nie tylko gwarantuje zgodność z prawem, ale również buduje zaufanie obywateli oraz innych użytkowników do procesów cyfryzacji i automatyzacji.

1. RAMY POJĘCIOWE I PRAWNE DEPERSONALIZACJI DANYCH

Depersonalizacja danych stanowi zespół metod technicznych i organizacyjnych ukierunkowanych na usunięcie bądź maskowanie identyfikatorów osób fizycznych w celu zapewnienia skutecznej ochrony prywatności przy jednoczesnym zachowaniu użyteczności informacji. W systemie prawnym ukształtowanym przez ogólne rozporządzenie o ochronie danych („RODO")[1] kluczowe znaczenie ma dychotomiczny podział procesów depersonalizacji na anonimizację i pseudonimizację. Należy jednak wyraźnie zaznaczyć, że przepisy RODO definiują i regulują wprost wyłącznie pseudonimizację, traktując ją jako środek zapewnienia bezpieczeństwa przetwarzania danych osobowych. Pojęcie anonimizacji w ogóle nie występuje w normatywnej części tego rozporządzenia, ponieważ – jak wynika z jego motywów – informacje skutecznie zanonimizowane tracą charakter danych osobowych i w konsekwencji całkowicie wymykają się spod reżimu RODO. Podział ten w sposób fundamentalny

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1)

determinuje odmienny status regulacyjny tak przetworzonych informacji oraz zakres obowiązków spoczywających na administratorze[2].

1.1. DEFINICJA DANYCH OSOBOWYCH I IDENTYFIKOWALNOŚCI

Zgodnie z art. 4 pkt 1 RODO fundamentem całego systemu ochrony jest prawna definicja danych osobowych, przez które należy rozumieć wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Owa identyfikowalność może przybrać postać bezpośrednią lub pośrednią. Bezpośrednie wskazanie tożsamości następuje zazwyczaj poprzez identyfikatory o charakterze jawnym, takie jak imię i nazwisko. Natomiast identyfikacja pośrednia wymaga zestawienia posiadanych wiadomości z dodatkowymi czynnikami określającymi fizyczną, fizjologiczną, ekonomiczną lub społeczną tożsamość jednostki. W doktrynie oraz orzecznictwie podkreśla się, że proces ten nie sprowadza się wyłącznie do ustalenia zestawu deskryptorów tożsamości, lecz do obiektywnej możliwości fizycznego wyodrębnienia konkretnego człowieka z grupy innych osób. Co istotne, pojęcie danych osobowych jest kategorią dynamiczną i relatywną. Kwalifikacja konkretnej wiadomości jest bowiem zależna od kontekstu przetwarzania oraz dostępności narzędzi pozwalających na powiązanie określonego atrybutu z podmiotem danych. Oznacza to, że nawet informacje, które same w sobie wydają się niepozorne – jak identyfikatory internetowe, numery kart bankowych czy dane lokalizacyjne – zyskują przymiot danych osobowych w momencie, gdy administrator ma realną możliwość przypisania ich do konkretnej osoby fizycznej[3].

Kluczowy instrument służący do wyznaczenia granicy między daną osobową a informacją anonimową jest wskazany w motywie 26 RODO. Zgodnie ze standardem tam wskazanym, przy ocenie stopnia identyfikowalności administrator winien uwzględnić obiektywne czynniki. Czynniki te stanowią nakłady czasu i kosztów niezbędne do ustalenia tożsamości, a także stan wiedzy technicznej oraz prognozowany postęp technologiczny w momencie operacji przetwarzania. Test racjonalności wymaga analizy sposobów, co do których istnieje uzasadnione prawdopodobieństwo ich wykorzystania nie tylko przez samego administratora, ale również przez osoby

[2] M. Garstka, A. Gos, G. Sibiga, D. Sybilski, I. Szelenbaum [w:] *Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, wyd. 1*, G. Sibiga (red.), D. Sybilski (red.), Warszawa 2022, Legalis/el, art. 2 (I. Anonimizacja).

[3] P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa o ochronie danych osobowych. Komentarz, wyd. 2*, P. Litwiński (red.), Warszawa 2025, Legalis/el, Art. 4 (I. Definicja danych osobowych, w szczególności Nb 1 (Pojęcie „dane osobowe"), Nb 14 (Osoba zidentyfikowana lub możliwa do identyfikacji) oraz Nb 16 (Relatywizacja pojęcia danych osobowych)).

trzecie. Jednakże za sposoby nieracjonalne uznaje się te, które są prawnie zakazane lub ich realizacja wiąże się z nadmiernym wysiłkiem czyniącym ryzyko identyfikacji znikomym. Takie ujęcie identyfikowalności pozwala na precyzyjne określenie progu skutecznej depersonalizacji, gdzie dane zanonimizowane w sposób trwały i nieodwracalny tracą status informacji osobowych i przestają podlegać rygorom rozporządzenia. Należy jednak pamiętać, że w dobie zaawansowanej analityki danych osiągnięcie pełnej anonimowości stanowi wyzwanie. Wymaga ono od administratorów ciągłego monitorowania odporności zbiorów na próby deanonimizacji przy użyciu rozsądnie dostępnych środków technicznych[4].

1.2. ANONIMIZACJA W SYSTEMIE PRAWNYM

Anonimizacja stanowi proces przekształcenia danych osobowych w informacje anonimowe, które przestają odnosić się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Fundamentem tego procesu jest jego nieodwracalność. Oznacza to, że po poprawnym przeprowadzeniu procesu anonimizacji identyfikacja danych podmiotu staje się obiektywnie niemożliwa lub trudna do zrealizowania. Wobec czego odwrócenie procesu wymagałoby nakładu niewspółmiernych kosztów, czasu oraz specyficznych działań technicznych. Sprawia to, że odwrócenie procesu anonimizacji jest okupione zbyt wieloma kosztami, które zasadniczo przewyższają korzyści jakie mogłoby przynieść odwrócenie tego procesu. Takie ujęcie wynika bezpośrednio z założeń zawartych w motywie 26 RODO. Wyznacza on granicę stosowania reżimu ochrony danych wskazując, że zasady te nie znajdują zastosowania do informacji, które nie pozwalają na wyodrębnienie konkretnej jednostki przy użyciu wszelkich rozsądnie prawdopodobnych sposobów.

Choć pojęcie to od lat funkcjonowało w doktrynie to jego definicja legalna na poziomie unijnym została wprowadzona dopiero przez dyrektywę 2019/1024[5] w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego. Polska ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego[6] stanowi bezpośrednią implementację tych założeń. Wprowadza ona w art. 2 pkt 1 definicję anonimizacji. Stanowi, że anonimizacja jest procesem zmiany informacji sektora publicznego w informacje anonimowe

[4] M. Siwicki, *Anonimizacja jako narzędzie służące ochronie danych osobowych*, Warszawa 2022, s. 42-43.
[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 172 z 26.06.2019, s. 56).
[6] Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (t.j. Dz. U. z 2023 r. poz. 1524).

w sposób uniemożliwiający identyfikację. Relacja między RODO a ustawą o otwartych danych opiera się na mechanizmie komplementarności[7].

Zastosowanie anonimizacji jest uzasadnione potrzebą pogodzenia szerokiego wykorzystania informacji z koniecznością respektowania autonomii informacyjnej jednostki. Skuteczna depersonalizacja prowadzi do trwałego wyłączenia informacji spod rygorów RODO. Dane po zanonimizowaniu tracą bowiem przymiot danych osobowych, co jest dopuszczalne jedynie wtedy, gdy administrator dołoży starań koniecznych do wyeliminowania możliwości ponownego połączenia danych z konkretną osobą fizyczną. W konsekwencji anonimizacja pełni w porządku prawnym rolę kluczowego narzędzia ochrony. Umożliwia realizację praw dostępowych bez naruszania sfery życia osobistego osób trzecich przy jednoczesnym zachowaniu użyteczności udostępnianych dokumentów[8].

1.3. PSEUDONIMIZACJA JAKO ŚRODEK BEZPIECZEŃSTWA

Pseudonimizacja, zgodnie z definicją zawartą w art. 4 pkt 5 RODO, stanowi proces przetwarzania danych osobowych w sposób uniemożliwiający przypisanie danych do konkretnej osoby, której dane dotyczą, bez użycia dodatkowych informacji. Kluczowym wymogiem tej instytucji jest to, aby owe dodatkowe informacje były przechowywane osobno i objęte były rygorystycznymi środkami technicznymi oraz organizacyjnymi, uniemożliwiającymi ich przypadkowe przypisanie do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

W systemie ochrony danych pseudonimizacja jest postrzegana jako swoiste stadium pośrednie między informacją w pełni anonimową a danymi osobowymi. Polega ona na zastąpieniu identyfikatorów rzeczywistych, np. imię i nazwisko, odpowiednio wygenerowanymi pseudonimami lub numerami identyfikacyjnymi. Podstawową cechą różniącą ten proces od anonimizacji jest jego odwracalność, co oznacza, że przy użyciu odpowiedniego „klucza" lub dodatkowych danych możliwe jest ponowne odtworzenie tożsamości podmiotu danych. Z tego powodu dane spseudonimizowane nie tracą charakteru danych osobowych. Jest tak, gdyż przy dołożeniu rozsądnych starań lub wykorzystaniu zabezpieczonych informacji pomocniczych osoba fizyczna nadal pozostaje możliwa do zidentyfikowania. Takie ujęcie prawne powoduje,

[7] M. Garstka, A. Gos, G. Sibiga, D. Sybilski, I. Szelenbaum, [w:] *Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, wyd. 1*, G. Sibiga (red.), D. Sybilski (red.), Warszawa 2022, Legalis/el, Komentarz do art. 2.

[8] M. Sakowska-Baryła, *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022, podrozdział 6.9.5.1. Pojęcie anonimizacji, Lex/el.

że informacje poddane pseudonimizacji stanowią kategorię danych osobowych podlegającą pełnej regulacji oraz wszystkim rygorom i zasadom ochrony przewidzianym w rozporządzeniu. Administratorzy decydujący się na to rozwiązanie muszą mieć świadomość, że choć pseudonimizacja łagodzi ryzyka naruszenia praw i wolności jednostek, to jednak nie wyłącza ona stosowania przepisów RODO. W przeciwieństwie do skutecznej i nieodwracalnej anonimizacji[9].

Pseudonimizacja jest wprost wymieniona w art. 25 oraz art. 32 RODO jako jeden z odpowiednich środków technicznych i organizacyjnych służących realizacji zasady ochrony danych w fazie projektowania oraz zapewnieniu bezpieczeństwa przetwarzania. Wybór tej techniki pozwala administratorom na realizację obowiązków w zakresie minimalizacji danych i zwiększenia ich poufności. Jednocześnie technika ta pozwala zachować pierwotną wartość i użyteczność zbiorów dla celów analitycznych czy badawczych. W praktyce pseudonimizacja służy zatem jako istotne zabezpieczenie przed niedozwolonym lub niezgodnym z prawem przetwarzaniem. Nie zwalnia ona jednak administratora z obowiązku wykazania zgodności całego procesu z prawem w ramach zasady rozliczalności[10].

2. PRAWNE ASPEKTY PROCESU ANONIMIZACJI

Proces anonimizacji stanowi podstawowy instrument ochrony prywatności osób fizycznych. Zgodnie z motywem 26 RODO zasady ochrony danych nie mają zastosowania do informacji anonimowych. Przez co skuteczne pozbawienie danych charakteru osobowego pozwala na legalne wykorzystanie informacji poza zakresem rygorów tego rozporządzenia. W analizie procesu anonimizacji istotną rolę odgrywa art. 4 pkt 2 RODO. Porusza on kwestię kwalifikacji anonimizacji jako operacji przetwarzania danych, co jest kluczowe dla ustalenia, iż proces ten podlega zasadzie legalności i wymaga posiadania odpowiedniej podstawy prawnej. Istotny element analizy prawnych aspektów anonimizacji stanowi obowiązek uwzględniania ochrony danych w fazie projektowania - *data protection by design*. Wynika on z art. 25 ust. 1 RODO. Regulacja ta nakłada na administratorów konieczność

[9] P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa o ochronie danych osobowych. Komentarz, wyd. 2*, P. Litwiński (red.), Warszawa 2025, Legalis/el, Art. 4 (V. Definicja pseudonimizacji).

[10] D. Lubasz, K. Witkowska-Nowakowska [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa (red.), D. Lubasz (red.), Warszawa 2018, Lex/el, Art. 25 (w szczególności Nb 2, 8 (Pseudonimizacja jako środek techniczny i organizacyjny), Nb 9 (Minimalizacja i użyteczność danych) oraz Nb 15 (Zasada rozliczalności)) oraz D. Lubasz, Art. 32 (w szczególności Nb 4 (Zasada poufności i ochrona przed niedozwolonym przetwarzaniem) oraz Nb 18, 19 (Pseudonimizacja jako środek bezpieczeństwa)).

implementacji zabezpieczeń i mechanizmów ochronnych już na etapie planowania rozwiązań technologicznych czy usług[11].

2.1. ANONIMIZACJA JAKO OPERACJA PRZETWARZANIA DANYCH

Analiza statusu prawnego anonimizacji wymaga w pierwszej kolejności ustalenia, w którym momencie proces ten podlega rygorom RODO. Choć końcowy rezultat skutecznie przeprowadzonej anonimizacji, czyli informacje anonimowe, znajduje się poza zakresem stosowania przepisów o ochronie danych, to samo działanie administratora zmierzające do osiągnięcia tego stanu jest kwalifikowane jako czynność przetwarzania danych osobowych. Wynika to z faktu, że w trakcie trwania tego procesu operacje są wykonywane na informacjach, które wciąż posiadają charakter osobowy. Natomiast celem administratora jest ich transformacja w taki sposób, aby przestały odnosić się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W ujęciu art. 4 pkt 2 RODO anonimizacja może być klasyfikowana jako operacja „usunięcia" lub „zniszczenia" danych osobowych. Takie przypisanie znajduje uzasadnienie w skutku, jaki wywołuje ten zabieg. Polega on bowiem na uniemożliwieniu dalszego wykorzystania danych identyfikujących, co merytorycznie odpowiada definicji usunięcia rozumianego jako działanie blokujące dostęp do informacji lub niszczenia będącego destrukcją powiązania między danymi a jednostką. Nawet gdyby odmówić anonimizacji bezpośredniej przynależności do tych kategorii należy ją uznać za nienazwaną formę przetwarzania. Mimo wszystko jednak nakłada to na podmiot ją wykonujący obowiązek zachowania pełnej zgodności z przepisami rozporządzenia na tym etapie prac.

Kwalifikacja anonimizacji jako formy przetwarzania rodzi fundamentalną konsekwencję prawną w postaci konieczności wykazania odpowiedniej podstawy legalizującej ten proces (zgodnie z zasadą zgodności z prawem). Administrator podejmujący się depersonalizacji zbioru musi legitymować się jedną z przesłanek wymienionych w art. 6 RODO dla danych zwykłych lub art. 9 RODO w przypadku szczególnych kategorii danych. Jest to niezbędne, ponieważ prawo do ochrony danych obejmuje również ochronę przed ich samowolnym lub bezprawnym niszczeniem i usuwaniem przez administratora. W praktyce taką podstawę stanowić może zgoda osoby, której dane dotyczą. Jednakże musi ona obejmować również czynność anonimizacji po zrealizowaniu pierwotnego celu przetwarzania. Często jednak proces ten opiera się na niezbędności do wypełnienia obowiązku prawnego lub na prawnie uzasadnionym

[11] M. Siwicki, *Anonimizacja jako narzędzie służące ochronie danych osobowych*, Warszawa 2022, s. 41-44.

interesie administratora. Ten ostatni interes bywa wywodzony bezpośrednio z zasady minimalizacji danych, która zobowiązuje do usuwania identyfikatorów w momencie, gdy przestają być one konieczne do osiągnięcia celu, dla którego zostały zebrane[12].

W przypadku przetwarzania danych wrażliwych brak wyraźnego uregulowania kwestii ich usuwania czy anonimizacji w art. 9 RODO powoduje, że administrator musi szczególnie starannie dbać o wykazanie podstawy uchylającej zakaz przetwarzania (np. poprzez niezbędność operacji do celów statystycznych, badawczych lub uzyskanie wyraźnej zgody). Takie rygorystyczne podejście służy zapewnieniu rozliczalności i zapobiega sytuacjom, w których anonimizacja mogłaby zostać wykorzystana do ukrycia niezgodnych z prawem operacji na danych. Wyjaśnia to, dlaczego proces anonimizacji – pomimo dążenia do zwiększenia bezpieczeństwa prywatności – musi być od samego początku osadzony w ścisłych ramach prawnych. Proces ten musi bowiem gwarantować, że każde działanie na informacjach o osobie fizycznej jest przejrzyste i znajduje oparcie w obowiązujących przepisach[13].

2.2. ZASADY OCHRONY DANYCH W FAZIE PROJEKTOWANIA (DATA PROTECTION BY DESIGN)

Fundamentem nowoczesnego systemu ochrony informacji jest obowiązek uwzględniania ochrony danych w fazie projektowania uregulowany w art. 25 ust. 1 RODO, który nakłada na administratorów konieczność implementacji odpowiednich środków technicznych i organizacyjnych. Obowiązek ten znajduje zastosowanie już w momencie planowania konkretnych usług lub systemów. Zasada ta znana jako *data protection by design* wymaga, aby ochrona prywatności stała się immanentnym elementem każdego projektu od samego etapu jego powstawania. Ma to zapewniać realne bezpieczeństwo przetwarzania i ochronę praw osób, których dane dotyczą. Należy wyjaśnić, że obowiązek ten ma charakter dynamiczny i rozciąga się na cały cykl życia informacji. Od określania sposobów przetwarzania aż po realizację operacji na danych. Takie rozwiązanie wynika z konieczności oparcia procesów na analizie ryzyka dla praw i wolności osób fizycznych, co wymusza na administratorze proaktywne działanie. Zapobiega to także ewentualnym zagrożeniom jeszcze przed ich faktycznym wystąpieniem[14].

---

[12] M. Siwicki, *Anonimizacja jako narzędzie służące ochronie danych osobowych*, Warszawa 2022, s. 39, 41-44.

[13] M. Siwicki, *Anonimizacja jako narzędzie służące ochronie danych osobowych*, Warszawa 2022, s. 47-49.

[14] P. Barta, M. Kawecki, P. Litwiński [w:] *Ustawa o ochronie danych osobowych. Komentarz, wyd. 2*, P. Litwiński (red.), Warszawa 2025, Legalis/el, Art. 25 (pkt 1. Nowe zasady ochrony danych oraz . Zasada privacy by design (ochrona danych w fazie projektowania)).

Centralne miejsce w projektowaniu bezpiecznych rozwiązań zajmuje zasada minimalizacji danych. Zobowiązuje ona do tego, aby zbierane informacje były adekwatne, stosowne i ograniczone wyłącznie do celów prawnie uzasadnionych. Realizacja tego postulatu już w fazie tworzenia systemów pozwala uniknąć gromadzenia nadmiernych identyfikatorów, co w świetle postępu technologicznego znacząco redukuje prawdopodobieństwo niepożądanej reidentyfikacji jednostek. Integralnie powiązana z tym wymogiem jest zasada ograniczenia przechowywania. Zgodnie z jej założeniami dane osobowe mogą być utrzymywane w formie pozwalającej na identyfikację podmiotów jedynie przez okres konieczny do osiągnięcia celu ich zebrania. Powyższe normy uzasadniają traktowanie anonimizacji jako standardu projektowego. Proces ten pozwala zachować użyteczność informacji. Jednocześnie umożliwia spełnienie wymogów dotyczących czasu przechowywania danych. Wdrożenie wyżej wskazanych zasad już na etapie koncepcyjnym służy zapewnieniu pełnej rozliczalności administratora, który na mocy art. 5 ust. 2 RODO jest odpowiedzialny za wykazanie, iż każda operacja przetwarzania odbywa się w sposób rzetelny i z poszanowaniem autonomii informacyjnej osób fizycznych[15].

3. PRAKTYCZNE TECHNIKI DEPERSONALIZACJI DANYCH

Skuteczna implementacja zasad ochrony danych wymaga przejścia od teorii do praktyki poprzez zastosowanie precyzyjnych technik depersonalizacji, które pozwalają pogodzić wymogi bezpieczeństwa z analityczną wartością informacji. W celu trwałego uniemożliwienia identyfikacji osoby fizycznej wykorzystuje się rodziny metod randomizacji. Wprowadzają one do zbiorów szum lub permutacje oraz techniki uogólniania takie jak k-anonimowość, redukujące szczegółowość danych na rzecz ich statystycznej agregacji. Odmienną funkcję pełni pseudonimizacja. Realizowana jest ona za pomocą szyfrowania lub tokenizacji, która nie usuwa całkowicie powiązania z tożsamością, lecz jedynie je maskuje stanowiąc tym samym kluczowy środek bezpieczeństwa danych, a nie metodę ich trwałej anonimizacji. Wybór właściwego mechanizmu jest zatem zawsze pochodną konieczności rozwiązania dylematu między głębokością ingerencji w strukturę danych a zachowaniem ich pierwotnej użyteczności dla celów badawczych czy gospodarczych. Ostatecznie o adekwatności przyjętego rozwiązania decyduje zdolność administratora do precyzyjnego oszacowania ryzyka

[15] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. III*, Warszawa 2025, art. 5 (w szczególności Nb 15 (Zasada adekwatności i minimalizacji danych), Nb 19 (Zasada ograniczenia przechowywania) oraz Nb 23, 28 (Zasada rozliczalności)) oraz art. 25 (w szczególności Nb 5, 6, 9 (Ochrona w fazie projektowania i domyślna ochrona danych)), Lex/el.

reidentyfikacji przy jednoczesnym utrzymaniu potencjału informacyjnego przetwarzanych zbiorów[16].

3.1. RODZINY TECHNIK ANONIMIZACJI

Skuteczna anonimizacja danych ma na celu doprowadzenie zbiorów informacji do stanu opisanego w motywie 26 RODO, w którym przestają one stanowić dane osobowe. Anonimizacja danych opiera się na dwóch fundamentalnych rodzinach technik: randomizacji oraz uogólnianiu. Wybór konkretnej metody wynika z konieczności rozwiązania dylematu między zapewnieniem nieodwracalności procesu a zachowaniem użyteczności analitycznej zbioru. W doktrynie taki stan rzeczy określa się mianem kompromisu między prywatnością a przydatnością danych.

Randomizacja stanowi podejście, które zmienia prawdziwość danych wejściowych w celu trwałego zerwania silnego związku między informacją a konkretną osobą fizyczną, przy czym jej skuteczność opiera się na wprowadzeniu do zbioru kontrolowanej niepewności. Jedną z najczęściej implementowanych technik w tej grupie jest dodawanie zakłóceń, czyli tzw. szumu. Polega to na celowej modyfikacji atrybutów tak, aby stały się one mniej dokładne przy jednoczesnym zachowaniu ich ogólnych właściwości statystycznych. Proces ten znajduje uzasadnienie w potrzebie uniemożliwienia odtworzenia indywidualnych wartości oryginalnych. Pozwala to na bezpieczne udostępnianie danych np. o lokalizacji czy parametrach liczbowych bez ryzyka precyzyjnej identyfikacji jednostki[17].

Odmiennym mechanizmem jest permutacja. Znana również jako tasowanie danych, które polega na reorganizacji wartości atrybutów wewnątrz zbioru w taki sposób, aby przestały one odpowiadać pierwotnym rekordom. Mimo to same wartości pozostają autentyczne. Technika ta jest szczególnie użyteczna, gdy administrator dąży do zachowania dokładnego rozkładu cech w populacji. Wymaga ona jednak grupowania skorelowanych logicznie atrybutów w celu uniknięcia wykrycia zmian przez potencjalnego atakującego[18].

Najbardziej zaawansowaną formą randomizacji jest prywatność różnicowa (*differential privacy*). Definiowana jest ona jako matematyczna gwarancja wskazująca, iż wynik analizy statystycznej pozostanie zasadniczo niezmieniony bez względu na

[16] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 14-15, 27.
[17] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 10-12.
[18] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 14.

obecność lub też brak danych konkretnej osoby w zbiorze. Rozwiązanie to opiera się na generowaniu zanonimizowanych widoków danych z celowo dodanym szumem. Dzięki temu administrator może zachować kopię danych pierwotnych przy jednoczesnym skutecznym blokowaniu wnioskowania o tożsamości jednostek przez osoby trzecie[19].

Druga rodzina technik określana jest jako uogólnianie (generalizacja). Koncentruje się ona na redukcji szczegółowości informacji poprzez modyfikację skali lub rzędu wielkości atrybutów identyfikujących. Podstawowym narzędziem w tym obszarze jest agregacja danych, która zastępuje wartości punktowe szerszymi przedziałami, co pozwala uniknąć tworzenia unikalnych quasi-identyfikatorów przy jednoczesnym zachowaniu trendów statystycznych. Ewolucją tego podejścia jest model k-anonimowości. Gwarantuje on bezpieczeństwo poprzez grupowanie każdego rekordu z co najmniej k-1 innymi rekordami o identycznych cechach pośrednich, takich jak wiek czy kod pocztowy. Mechanizm ten tworzy tzw. klasy równoważności, w których prawdopodobieństwo identyfikacji osoby fizycznej staje się równe lub mniejsze niż 1/k. Ma to za zadanie uniemożliwić wyodrębnienie konkretnego wiersza z tabeli. Należy jednak wyjaśnić, że k-anonimowość bywa podatna na ataki oparte na wiedzy podstawowej[20].

Wobec czego w praktyce stosuje się jej modyfikację w postaci l-dywersyfikacji. Wymaga ona, aby w każdej klasie równoważności znajdowało się co najmniej l dobrze reprezentowanych wartości atrybutów wrażliwych. Chroni to przed wnioskowaniem probabilistycznym w sytuacjach, gdy wszystkie osoby w grupie k-anonimowej cierpią na tę samą przypadłość[21].

Dalszym udoskonaleniem tych zabezpieczeń jest model t-bliskości, który nakłada rygorystyczny warunek mówiący o tym, aby rozkład wartości wrażliwych w każdej grupie był zbliżony do rozkładu w całym zbiorze pierwotnym. Stosowanie t-bliskości rozwiązuje ograniczenia poprzednich metod w zakresie ujawniania atrybutów, choć dzieje się to kosztem użyteczności danych. Wymusza to na administratorze precyzyjny dobór parametrów ochronnych w oparciu o analizę ryzyka reidentyfikacji[22].

Zastosowanie powyższych technik, często w sposób hybrydowy, stanowi obecnie standard projektowy pozwalający na realizację praw obywatelskich

[19] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 21-23.
[20] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 15-16.
[21] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 18-19.
[22] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 20-21.

przy jednoczesnym poszanowaniu autonomii informacyjnej osób, których dane są przetwarzane.

3.2. METODY PSEUDONIMIZACJI

Pseudonimizacja, zgodnie z art. 4 pkt 5 RODO, jest to proces przetwarzania danych osobowych w sposób uniemożliwiający ich bezpośrednie przypisanie do konkretnej osoby. Jest to jednak proces odwracalny, przez co informacje poddane temu mechanizmowi w dalszym ciągu zachowują status danych osobowych.

Podstawową metodą realizacji tego wymogu jest szyfrowanie z kluczem tajnym. W tym procesie algorytmy przekształcają dane w postać dostępną wyłącznie dla dysponenta klucza. Wykorzystanie tej samej sekwencji do szyfrowania i deszyfrowania upraszcza implementację. Wymaga jednak wdrożenia ścisłych protokołów dystrybucji. Tylko one pozwalają wyeliminować ryzyko przechwycenia klucza przez osoby nieuprawnione. Skuteczność ochrony zależy tu bezpośrednio od długości i złożoności bitowej klucza. Stanowi to barierę dla ataków typu *brute force*, które polegają na sprawdzaniu wszystkich możliwych kombinacji znaków. Z tego powodu współczesne standardy wymuszają stosowanie odpowiednio długich kluczy. Jest to konieczne, gdyż postęp technologiczny może z czasem osłabić odporność starszych algorytmów[23].

Alternatywną metodą depersonalizacji są funkcje skrótu, znane jako hashowanie. Mechanizm ten przekształca dane wejściowe w ciąg znaków o stałej długości. Jego użyteczność wynika z jednokierunkowego charakteru operacji. Wyznaczenie skrótu jest proste obliczeniowo, lecz proces odwrotny pozostaje niezwykle trudny. Nie da się łatwo odtworzyć danych wejściowych na podstawie samego hasha. Aby dodatkowo zabezpieczyć system przed atakami siłowymi, stosuje się funkcje z kluczem kryptograficznym (np. HMAC lub UMAC). Wówczas wartość skrótu zależy także od tajnego klucza, a nie tylko od samych danych. Bez dostępu do niego odtworzenie pierwotnej informacji przez osoby trzecie jest niemożliwe[24].

Inną formą maskowania danych jest tokenizacja. Wyróżnia się ona brakiem matematycznego związku między pseudonimem a oryginałem. Technika ta polega na zastąpieniu rzeczywistych danych losowymi ciągami znaków, zwanymi tokenami. Tokeny same w sobie nie mają żadnej wartości analitycznej. Kluczowym elementem

[23] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 29.
[24] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 30.

systemu jest przeniesienie danych pierwotnych do odizolowanej, silnie strzeżonej bazy (tzw. skarbca). Tylko tam uprawnieni użytkownicy mogą powiązać token z tożsamością osoby fizycznej. Dzięki temu odkodowanie informacji w pozostałych systemach jest praktycznie niemożliwe. Ze względu na wysoki poziom bezpieczeństwa, rozwiązanie to zdominowało sektor finansowy. Stało się standardem przy autoryzacji transakcji i obsłudze wniosków kredytowych. Umożliwia bezpieczne przetwarzanie danych w obrocie giełdowym, zachowując ich pełną użyteczność gospodarczą[25].

3.3. WYZWANIA TECHNICZNE

Kluczowym problemem depersonalizacji jest konflikt dwóch wartości. Chodzi o wyważenie użyteczności analitycznej zbioru i ochrony prywatności. Wzmocnienie bezpieczeństwa ma swoją cenę. Każde maskowanie identyfikatorów obniża wartość statystyczną danych. Zależność ta ma charakter odwrotnie proporcjonalny. Im pełniejsza anonimizacja, tym mniejszy potencjał informacyjny materiału. W efekcie dane całkowicie bezpieczne mogą okazać się bezużyteczne dla zaawansowanych analiz, w tym dla rozwoju sztucznej inteligencji.

Trudności w kalibracji systemu wynikają ze specyfiki technik randomizacji, takich jak dodawanie szumu. Wymagają one precyzyjnego doboru parametrów statystycznych. Zbyt niski poziom zakłóceń nie zapewnia wystarczającej ochrony. Z kolei zbyt silna modyfikacja niszczy dokładność danych, czyniąc je bezużytecznymi. Szczególnym wyzwaniem są tzw. wartości odstające (*outliers*). Te nietypowe rekordy są najbardziej podatne na reidentyfikację. Ich skuteczne ukrycie wymusza zastosowanie znacznie wyższego poziomu szumu niż dla reszty zbioru. Niestety, zaburza to spójność całej bazy danych. Dla badacza oznacza to niepożądaną utratę informacji[26].

Wdrożenie rygorystycznych modeli, takich jak t-bliskość, generuje istotne koszty analityczne. Wymóg dopasowania rozkładu cech wrażliwych do populacji ma swoje konsekwencje. Ogranicza on bowiem możliwość wykrywania korelacji między atrybutami. Podobny problem dotyczy prywatności różnicowej. Ilość dodanego szumu musi skutecznie ukryć jednostkę. Nie może jednak zniekształcić wyniku statystycznego, który jest kluczowy dla odbiorcy danych. Ostatecznym weryfikatorem dopuszczalności techniki w świetle RODO jest test racjonalności. Uwzględnia on czynniki obiektywne: czas, koszty oraz dostępną technologię. Analiza ta pozwala ocenić, czy ryzyko identyfikacji spadło do poziomu znikomego.

[25] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 31.
[26] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 12-14.

4. ZARZĄDZANIE RYZYKIEM I OCENA SKUTECZNOŚCI

Zarządzanie ryzykiem w depersonalizacji realizuje systemowe podejście RODO (*risk-based approach*). Fundamentem tego procesu jest ocena skutków dla ochrony danych („DPIA"). Należy ją przeprowadzić jeszcze przed udostępnieniem zanonimizowanych zbiorów. Jest to kluczowe zwłaszcza przy operacjach wysokiego ryzyka lub wykorzystaniu nowych technologii. Wymóg ten wynika z prostego założenia: sama anonimizacja też jest przetwarzaniem danych. Musi więc przejść weryfikację pod kątem rzetelności i bezpieczeństwa. DPIA służy tu identyfikacji zagrożeń, w tym ryzyka reidentyfikacji. Pozwala także na udokumentowany wybór właściwych metod, np. randomizacji. Prawidłowa ocena potwierdza, czy po wdrożeniu zabezpieczeń ryzyko rozpoznania osoby spadło do poziomu znikomego[27].

Kluczowym narzędziem weryfikacji odporności zbioru jest tzw. test zdeterminowanego intruza. Polega on na empirycznym sprawdzeniu bezpieczeństwa danych. Administrator symuluje, czy zmotywowana osoba trzecia zdoła odtworzyć tożsamość ukrytą w teoretycznie anonimowym zbiorze. Analiza ta musi uwzględniać realne możliwości ataku. W tym celu stosuje się test racjonalności. Bierze on pod uwagę czynniki obiektywne: czas, koszty oraz dostępną technologię. Istotnym problemem jest tu jednak ciągły postęp techniczny. Metody uznawane dawniej za bezpieczne tracą skuteczność. Wynika to z rosnącej mocy obliczeniowej systemów. Dynamiczny rozwój algorytmów sprawia, że utrzymanie pełnej anonimowości w długim okresie jest wyzwaniem niezwykle złożonym[28].

Krytycznym czynnikiem ryzyka jest możliwość łączenia danych z różnych źródeł. Często są to informacje niezależne i ogólnodostępne. Nawet zbiór poddany wstępnej anonimizacji nie jest w pełni bezpieczny. Jego zestawienie z rejestrami publicznymi lub wiedzą powszechną może ujawnić tożsamość konkretnych osób. Zagrożenie to ma charakter kumulacyjny. Administratorzy muszą więc monitorować nie tylko własne zasoby, ale także ich otoczenie informacyjne. Ocena skuteczności anonimizacji nie może być działaniem jednorazowym. Musi stać się procesem ciągłym. Tylko stały nadzór pozwala reagować na nowe metody korelacji danych[29].

---

[27] M. Sakowska-Baryła, *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022, podrozdział 6.9.5.3. Techniki anonimizacji oraz 6.9.5.5. Anonimizacja jako środek ochrony prywatności i danych osobowych jednostki niezależny od decyzji o odmowie realizacji praw dostępowych, Lex/el.

[28] Europejska Rada Ochrony Danych, *Opinia 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli AI przyjęta 17 grudnia 2024 r.*, s. 15-17.

[29] Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022, s. 10-11.

PODSUMOWANIE

Przeprowadzona analiza wskazuje na istotny i złożony dualizm prawny oraz techniczny w obszarze depersonalizacji informacji. Kluczowe rozróżnienie między anonimizacją a pseudonimizacją determinuje reżim prawny, któremu podlegają zbiory danych, a w konsekwencji kształtuje zakres obowiązków ciążących na administratorze. Skutecznie przeprowadzona anonimizacja powoduje, że informacje w sposób trwały i nieodwracalny tracą status danych osobowych, co skutkuje wyłączeniem ich spod RODO. Z kolei pseudonimizacja, stanowiąca proces odwracalny przy użyciu dodatkowych, odrębnie przechowywanych informacji (tzw. klucza), nie pozbawia danych ich osobowego charakteru. Z tego względu informacje spseudonimizowane wciąż podlegają pełnej ochronie na gruncie RODO, a administrator jest zobligowany do bezwzględnego przestrzegania wszystkich zasad przetwarzania.

Wnioski płynące z badanej materii prowadzą do jednoznacznego stwierdzenia, że skuteczność procesu anonimizacji nie ma charakteru absolutnego, trwałego ani ostatecznego. W dobie zaawansowanej analityki oraz powszechności zjawiska *Big Data,* anonimizację należy postrzegać jako proces o charakterze ciągłym i dynamicznym, a nie jako statyczny stan. Prawdopodobieństwo reidentyfikacji jednostki stanowi zmienną, która jest ściśle uzależniona od upływu czasu, nakładów finansowych oraz dostępności i rozwoju nowoczesnych technologii. Zjawisko korelacji informacji pochodzących z wielu różnorodnych źródeł stało się obecnie standardem analitycznym, co sprawia, że zagwarantowanie całkowitej i bezwzględnej nieodwracalności procesu depersonalizacji w perspektywie długoterminowej jest wysoce utrudnione, a niekiedy wręcz niemożliwe. Weryfikacja skuteczności anonimizacji wymaga zatem stałego monitorowania i stosowania tzw. testu racjonalności (rozsądnego prawdopodobieństwa), uwzględniającego obiektywne czynniki technologiczne i koszty potrzebne do identyfikacji.

Z drugiej strony, pseudonimizacja pełni fundamentalną funkcję jako jeden z głównych środków technicznych i organizacyjnych służących zabezpieczeniu danych, wprost rekomendowany przez prawodawcę unijnego w art. 25 oraz art. 32 RODO. Wykorzystanie tej techniki stanowi wyraz realizacji koncepcji ochrony danych w fazie projektowania (*privacy by design*) oraz domyślnej ochrony danych (*privacy by default*). Choć pseudonimizacja nie wyłącza stosowania przepisów rozporządzenia, jej wdrożenie drastycznie minimalizuje ryzyko naruszenia praw i wolności osób fizycznych w przypadku incydentów bezpieczeństwa. Jednocześnie technika ta pozwala na zachowanie wysokiej użyteczności i wartości analitycznej przetwarzanych zbiorów, co jest warunkiem niezbędnym (*conditio sine qua non*) dla prowadzenia

zaawansowanych badań naukowych, analiz statystycznych czy trenowania modeli sztucznej inteligencji.

Wybór pomiędzy omawianymi technikami depersonalizacji każdorazowo wymaga od administratora głębokiej analizy i wyważenia dwóch przeciwstawnych wartości: stopnia użyteczności analitycznej zbioru danych oraz poziomu ochrony prywatności. Rozwiązaniem tego swoistego kompromisu jest oparcie działań na podejściu opartym na ryzyku (*risk-based approach*), które stanowi fundament RODO. Przed wdrożeniem i udostępnieniem zbiorów administrator winien przeprowadzić rzetelną ocenę skutków dla ochrony danych, szczególnie w przypadku operacji wykorzystujących nowe technologie lub mogących powodować wysokie ryzyko dla podmiotów danych. Takie proaktywne podejście jest jedyną drogą do zrealizowania nadrzędnej zasady rozliczalności (art. 5 ust. 2 RODO), wymagającej nie tylko przestrzegania prawa, ale i udowodnienia przed organem nadzorczym podjęcia wszelkich niezbędnych i adekwatnych środków bezpieczeństwa.

Reasumując, przyszłość i skuteczność ochrony danych osobowych będzie w głównej mierze uzależniona od odnalezienia optymalnego kompromisu pomiędzy dynamicznym rozwojem innowacyjnych technologii a stabilnością ram prawnych. Techniki ochrony prywatności, takie jak zaawansowana anonimizacja, dodawanie szumu (prywatność różnicowa) czy generowanie danych syntetycznych, stanowią w tym procesie narzędzia absolutnie niezbędne. Prawodawstwo i praktyka stosowania prawa muszą jednak nieustannie nadążać za ewolucją technologiczną, aby z jednej strony tworzyć bezpieczne i przyjazne środowisko dla rozwoju innowacyjnej gospodarki cyfrowej, z drugiej zaś w żadnym wypadku nie ustępować pola w kluczowej kwestii, jaką pozostaje niezbywalne prawo do ochrony prywatności i gwarancja pełnej autonomii informacyjnej jednostki.

BIBLIOGRAFIA

LITERATURA

Bielak-Jomaa E., Lubasz D., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018.

Centrum Nowych Technologii dla Polityk Publicznych NASK-PIB, *Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych*, Warszawa 2022.

Europejska Rada Ochrony Danych, *Opinia 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli AI przyjęta 17 grudnia 2024 r.*

Fajgielski P., Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. III, Warszawa 2025.

Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, wyd. 2, Warszawa 2025.

Sakowska-Baryła M., *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

Sibiga G., Sybilski D., *Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, wyd. 1, Warszawa 2022.

Siwicki M., *Anonimizacja jako narzędzie służące ochronie danych osobowych*, Warszawa 2022.

ANONYMIZATION AND PSEUDONYMIZATION UNDER GDPR: LEGAL AND PRACTICAL IMPLICATIONS

Summary: This article provides a legal and practical analysis of two fundamental data depersonalization techniques – anonymization and pseudonymization – in light of the General Data Protection Regulation. The author argues that a precise distinction between the two processes is of key importance in the era of the data-driven economy and the development of artificial intelligence systems, for which access to high-quality datasets constitutes both a precondition for progress and its bottleneck. The study demonstrates that the GDPR explicitly defines and regulates only pseudonymization, treating it as a measure to ensure the security of processing, whereas effectively anonymized information loses its personal-data character and falls outside the scope of the Regulation. The article discusses the conceptual and legal framework of depersonalization, the status of anonymization as a processing operation requiring a legal basis, and the principle of data protection by design. It presents practical anonymization techniques (randomization, noise addition, differential privacy, k-anonymity, l-diversity, t-closeness) and pseudonymization methods (encryption, hashing, tokenization), together with the accompanying technical challenges, in particular the trade-off between analytical utility and privacy protection. The article concludes that the effectiveness of anonymization is neither absolute nor permanent, but rather a dynamic process requiring continuous monitoring, a Data Protection Impact Assessment (DPIA), and the application of the reasonableness test in the face of growing re-identification risk.

Key words: anonymization, pseudonymization, GDPR, personal data protection, depersonalization, re-identification, differential privacy, k-anonymity

mgr **Joanna Walkowiak**
Universiteit Maastricht
jw.walkowiak@student.maastrichtuniversity.nl
https://orcid.org/0009-0001-2630-4956

RODO A OCHRONA DANYCH SPORTOWCÓW W SPRAWACH ZWIĄZANYCH Z DOPINGIEM

Streszczenie: Unijne prawo ochrony danych osobowych przenika do wielu dziedzin życia społecznego, mając wpływ Artykuł analizuje pytania prejudycjalne zadane TSUE, rozważając, gdzie przebiega granica między ochroną zawodników a interesem publicznym i potrzebą zapewnienia integralności sportu. Omawia zakres i status danych sportowców dostępnych publicznie, zwłaszcza w przypadkach naruszeń przepisów antydopingowych. Artykuł dokonuje także oceny zgodności obecnych rozwiązań z wymogami prawa Unii, odnosząc się do opinii Rzeczników Generalnych w sprawie C-474/24 oraz w sprawie C-115/22. Proponuje również model publikacji danych, łączący interes publiczny związany z przejrzystością w sporcie z prawem zawodników do prywatności i ochrony danych.

Słowa kluczowe: RODO; prawo sportowe; prawo antydopingowe; ochrona zawodników; TSUE.

WPROWADZENIE

Mimo braku wyraźnych kompetencji legislacyjnych w zakresie regulacji sportu[1], Unia Europejska („UE", „Unia") zwiększa swoją rolę w kształtowaniu standardów jego funkcjonowania w państwach członkowskich i w skali globalnej. Dzieje się tak dzięki jej wpływowi pośredniemu, wynikającemu z obowiązywania przepisów prawa Unii regulujących inne dziedziny życia społecznego. Do jednej z nich należy ochrona danych osobowych, której ramy w UE wyznacza Ogólne Rozporządzenie Ochronie Danych Osobowych („RODO")[2]. Interakcja pomiędzy interesem indywidualnego sportowca a prawem i praktyką organizacji sportowych to złożony temat, w którym ochrona danych osobowych jednostki – prawo fundamentalne gwarantowane w Art. 8 Karty Praw Podstawowych („KPP", „Karta")[3] – zderza się z dążeniem do zapewnienia integralności współzawodnictwa sportowego.

Niniejszy artykuł omawia zastosowanie przepisów RODO do publikacji danych sportowców, na których nałożono kary za złamanie przepisów antydopingowych, odpowiadając na pytanie badawcze: w jaki sposób stosować przepisy RODO do publikacji danych i informacji o sportowcach i karach nałożonych na nich za przekroczenie przepisów antydopingowych w Unii Europejskiej? Artykuł posługuje się metodą doktrynalną. Analizuje relewantne przepisy prawa, wyroki TSUE, a dodatkowo posługuje się aktualną literaturą naukową.

Na początek, artykuł przedstawi zasady publikowania tych informacji obowiązujące zgodnie z regulacjami międzynarodowymi i krajowymi. Następnie, omówi możliwość zastosowania przepisów RODO do danych zawodników opublikowanych w sprawach antydopingowych oraz, czy ich publikacja w obecnej formie zgodna jest z reżimem RODO. Przyczynek do rozważań stanowią opinie Rzeczników

[1] Zob. Art. 165 Traktatu o funkcjonowaniu Unii Europejskiej, Dz.U. C 202 z 7.06.2016. pp. 1-388 (TFUE). Zgodnie z Art. 165(1) TFEU, UE przyczynia się do rozwoju edukacji o wysokiej jakości, poprzez zachęcanie do współpracy między Państwami Członkowskimi oraz, jeśli jest to niezbędne, poprzez wspieranie i uzupełnianie ich działalności, w pełni szanując odpowiedzialność Państw Członkowskich za treść nauczania i organizację systemów edukacyjnych, jak również ich różnorodność kulturową i językową. Unia przyczynia się do wspierania europejskich przedsięwzięć w zakresie sportu, uwzględniając jego szczególny charakter, jego struktury oparte na zasadzie dobrowolności oraz uwzględniając jego funkcję społeczną i edukacyjną. Jak wskazuje Art. 165(3) TFUE, Unia oraz jej Państwa Członkowskie sprzyjają współpracy z państwami trzecimi oraz z kompetentnymi organizacjami międzynarodowymi w dziedzinie edukacji i sportu, zwłaszcza z Radą Europy. Zakres kompetencji UE w dziedzinie sportu oraz jego konsekwencje prawne zostaną omówione w dalszej części artykułu.

[2] 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) (Tekst mający znaczenie dla EOG).

[3] Karta praw podstawowych Unii Europejskiej (t.j. Dz. U. UE. C. z 2016 r. Nr 202, str. 389).

Generalnych („Rzecznik") wydane w sprawie C-474/24[4] oraz C-115/22[5]. Artykuł próbuje także odpowiedzieć na pytanie, jaki model publikacji danych zapewniłby poszanowanie wymogów unijnego prawodawcy w zakresie ochrony danych osobowych, a jednocześnie odpowiadałby potrzebom sportu międzynarodowego.

1. ZASADY PUBLIKOWANIA INFORMACJI O KARACH DOPINGOWYCH W PRAWIE SPORTOWYM

Istotne dla prawa antydopingowego są standardy międzynarodowe. Pierwszy międzynarodowy standard wypracowała Rada Europy („CoE"), ustanawiając w 1989 r. Konwencję Anty-Dopingową[6], która jednak nie reguluje praw zawodników. W 2005 r. Uchwalono Międzynarodową Konwencję UNESCO przeciwko dopingowi w sporcie[7], która weszła w życie w 2007 r. i której członkami są wszystkie państwa członkowskie UE[8]. Celem konwencji jest zwalczanie dopingu w sporcie. Ponadto, Konwencja zobowiązuje jej strony do wspierania misji Światowej Agencji Antydopingowej („WADA")[9].

Najistotniejszym źródłem regulującym zasady publikowania informacji o sportowcach, w przypadku których stwierdzono naruszenie przepisów antydopingowych, jest Światowy Kodeks Antydopingowy („WADC", „Kodeks")[10]. WADC to prywatny instrument prawny, jednak jego efektywność i moc wiążąca gwarantowana jest wspomnianą Konwencję UNESCO[11].

WADC jest wydawany przez WADA; obowiązująca wersja została ustanowiona w 2021 r. W 2025 r., WADC przeszedł proces nowelizacji[12]. Najnowsza wersja

[4] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24..
[5] Wyrok TS z dnia 7 maja 2024 r., C-115/22, LEX nr 3714444.
[6] Rada Europy, Konwencja Antydopingowa 1989 r. https://rm.coe.int/168007b0e0 [dostęp: 2.03.2026].
[7] UNESCO, Międzynarodowa Konwencja o Zwalczaniu Dopingu w Sporcie (2005) https://antydoping.pl/wp-content/uploads/2017/07/konwencja_antydopingowa_unesco.pdf [dostęp: 2.03.2026].
[8] *Ibidem*.
[9] *Ibidem*, art. 14.
[10] WADA, Światowy Kodeks Antydopingowy (2025). Wersja WADC obowiązująca od 1 stycznia 2027 r., jak i wcześniej obowiązujące wersje, dostępne są pod adresem internetowym: https://www.wada-ama.org/en/resources/world-anti-doping-code-and-international-standards/world-anti-doping-code [dostęp: 2.03.2026].
[11] European Data Protection Board, 'Recommendations 1/2025 on the 2027 WADA World Anti-Doping Code' https://www.edpb.europa.eu/system/files/2025-02/edpb_recommendations_202501_wada_2027_world_anti-doping_code_en.pdf [dostęp: 2.03.2026].
[12] WADA, '2027 Code and International Standards' https://www.wada-ama.org/en/what-we-do/world-anti-doping-code/2027-code-and-international-standards [dostęp: 2.03.2026].

zmodyfikowanego WADC, która ukazała się w listopadzie 2025 r.[13], uzyskała poparcie na konferencji w *Busan*[14] i wejdzie w życie w 2027 r.[15] Istotne jest porównanie obydwu wersji Kodeksu, ponieważ zawiera ona istotne zmiany w zakresie ochrony danych osobowych zawodników. Zasady publikowania danych sportowców może także doprecyzowywać prawo krajowe. Przykładowo, Polska Agencja Antydopingowa („POLADA") wydaje swoje przepisy[16], inspirowane WADC, które stosuje się do polskich związków sportowych i ich członków. Podobnie sytuacja wygląda we Francji[17] i Szwajcarii[18].

Art. 14.3 WADC 2021 stanowił, że organizacja antydopingowa odpowiedzialna za zarządzanie wynikami w danej sprawie ma obowiązek podać do publicznej wiadomości tożsamość każdego zawodnika lub innej osoby powiadomionej o możliwym naruszeniu przepisów antydopingowych, substancję zabronioną lub metodę zabronioną, charakter naruszenia oraz nałożone konsekwencje. Ujawnienie tych danych może także mieć miejsce na etapie postępowania antydopingowego, po pozytywnym wyniku testu antydopingowego u sportowca. W tej sytuacji nie jest to jednak obowiązkowe, a organizacja antydopingowa ma w tym zakresie dyskrecję zgodnie z Art. 14.3.1. Art. 14.3.4 pozwala także na podanie do wiadomości publicznej także informacji o tym, że nałożone kary dopingowe zostały zaskarżone, jeśli okaże się, że zawodnik nie stosował dopingu; w takiej sytuacji jednak decyzja o podaniu danych do wiadomości publicznej jest dobrowolna i należy do zawodnika. Zgodnie z Art. 14.3.7, obowiązek podania do wiadomości publicznej nie ma zastosowania, jeżeli zawodnik (a także inna osoba, której udowodniono naruszenie przepisów antydopingowych) jest osobą nieletnią, osobą chronioną lub zawodnikiem uprawiającym sport rekreacyjnie. Dobrowolne podawanie do wiadomości publicznej informacji o sprawach dotyczących takich osób musi być także proporcjonalne do faktów i okoliczności sprawy. Regulacja WADC pokazuje, że obowiązek podawania danych o sankcjach antydopingowych nie jest absolutny. Może być modyfikowany np. ze

[13] WADA, Najnowsza wersja kodeksu antydopingowego (grudzień 2025) https://www.wada-ama.org/sites/default/files/2025-11/Redline%20-%202021%20Code%20-%202027%20Code%28Final%20Draft%29.pdf [dostęp: 2.03.2026].

[14] Rada Europy, *World anti-doping code 2027 and international standards adopted in Busan* (2025) https://www.coe.int/en/web/portal/-/world-anti-doping-code-2027-and-international-standards-adopted-in-busan [dostęp: 2.03.2026].

[15] *Ibidem*.

[16] POLADA, Przepisy Antydopingowe Polskiej Agencji Antydopingowej (2021) https://antydoping.pl/wp-content/uploads/2021/06/Przepisy-Antydopingowe-POLADA-2021-wersja-1.3..pdf [dostęp: 2.03.2026].

[17] Agence française de lutte contre le dopage („AFDL") (Francuska Agencja Antydopingowa), Decyzje w sprawach antydopingowych, https://www.aflд.fr/decisions_disciplinaires/ [dostęp: 2.03.2026].

[18] Swiss Sport Integrity (Szwajcarska Fundacja ds. Integralności w Sporcie), Lista zawieszonych sportowców, https://www.sportintegrity.ch/en/anti-doping/laws/suspended-athletes [dostęp: 2.03.2026].

względu na wiek lub inne cechy zawodnika. Co więcej, w niektórych przypadkach, podanie danych do wiadomości publicznej nie jest obligatoryjne i zależy od decyzji organizacji sportowej lub samego sportowca.

WADC samo w sobie zawiera postanowienie odnoszące się bezpośrednio do ochrony danych osobowych sportowców. Zgodnie z Art. 14.6 WADC, organizacja antydopingowa może gromadzić, przechowywać, przetwarzać lub ujawniać informacje osobowe dotyczące zawodników i innych osób w sytuacjach, gdy jest to konieczne i właściwe do prowadzenia działań zwalczających doping „zgodnie z Kodeksem, standardami międzynarodowymi, oraz obowiązującym prawem" [podkreślenie własne]. WADC 2027 wprowadza istotne zmiany dotyczące publikacji danych zawodników oraz ochrony ich danych osobowych. Art. 14.3.2 wskazuje, że dane zawodników skazanych za używanie dopingu mają zostać opublikowane „z zastrzeżeniem postanowień artykułu 14.3.3 i obowiązujących przepisów prawa"[19], a więc obowiązek publikacji nie jest już bezwzględny, a uzależniony od przepisów międzynarodowych lub krajowych regulujących sytuację zawodników. Ma to istotne znaczenie dla ustalenia relacji między prawem ochrony danych, regulowanym na poziomie unijnym i częściowo na poziomie krajowym, a przepisami WADC, stosowanymi międzynarodowo, przez krajowe i ponadnarodowe organizacje sportowe.

2. RELEWANTNE PRAWO UE

Kwestia ochrony danych osobowych regulowana jest w prawie pierwotnym UE. Zgodnie z Art. 16 TFUE, który został wprowadzony do prawa pierwotnego UE na podstawie Traktatu z Lizbony[20], każda osoba ma prawo do ochrony dotyczących jej danych osobowych. Art. 16(2) TFUE jest podstawą prawną do wydania aktów prawnych regulujących ochronę danych osobowych. Omówieniu zasad i przepisów RODO poświęcona zostanie dalsza część artykułu.

Istotne dla sprawy postanowienia dotyczą także prawa sportowego. Zgodnie z Art. 165(3) TFUE, Unia i Państwa Członkowskie sprzyjają współpracy z państwami trzecimi oraz z kompetentnymi organizacjami międzynarodowymi w dziedzinie edukacji i sportu, zwłaszcza z Radą Europy. Co istotne, zgodnie z Art. 6(e) TFUE, który opisuje kompetencje pomocnicze UE, Unia może prowadzić działania mające na celu wspieranie, koordynowanie lub uzupełnianie działań Państw Członkowskich

[19] WADA, Światowy Kodeks Antydopingowy, art. 14.3.2, org. "subject to Art. 14.3.3 and applicable laws".
[20] H. Kranenborg, *Article 2. Material scope* [w:] *The EU General Data Protection Regulation (GDPR),* C. Kuner (red.), L.A. Bygrave (red.), D.C. Docksey (red.), Oxford 2020, s. 63.

w zakresie edukacji, kształcenia zawodowego, młodzieży i sportu. Art. 165 TFUE mógłby prima facie wskazywać na „specjalny" status sportu w prawie UE[21], dzięki któremu pewne przepisy prawa unijnego (np. prawo konkurencji) nie znajdowałyby do niego zastosowania. Takiego podejścia nie zaakceptował jednak TSUE, gdyż zagrażałoby to jednolitości stosowania prawa UE i umożliwiłoby zbyt prostą drogę do jego stosowania, także w sytuacjach, gdy specjalny charakter działalności sportowej nie odgrywałby żadnej roli. Przepisy prawa UE należy więc stosować także w sprawach sportowych[22].

Art. 165 TFUE stał się przedmiotem rozważań TSUE szczególnie w sprawach dotyczących rynku wewnętrznego, wolności przepływu osób oraz zasad konkurencji[23]. W świetle wyroków TSUE zapadłych w sprawach *European Superleague Comapny* („*ESL"*)[24] oraz *Royal Antwerp*[25], Art. 165 TFUE nie może stanowić podstawy argumentu prawnego o stosowaniu bądź niestosowaniu prawa UE w dziedzinie sportu[26]. Takie stanowisko jest zgodne z linią orzeczniczą zapoczątkowaną już w sprawie *Bosman*[27], gdzie TSUE wskazał, że przepisy o swobodnym przepływie pracowników i usług mogą zostać ograniczone regulacjami organizacji sportowych. Jednakże, „ograniczenie zakresu stosowania omawianych przepisów powinno być zawężone do jego celu. Nie można więc powoływać się na nie w celu wyłączenia wszelkiej działalności sportowej z zakresu stosowania traktatu"[28]. W ten sposób TSUE argumentuje, że nie można sportu wyłączyć *a priori* z zakresu zastosowania prawa UE, a wyłączenie stosowania przepisów unijnych powinni być niezbędne oraz uzasadnione konkretnym celem związanym ze specyfiką działalności sportowej. Jak zauważa A. Villanueva, podejście TSUE do wyłączenia sportu spod zasad prawa UE jest co do zasady zgodne ze stanowiskiem, jakie przyjmuje wobec innych dziedzin, które także mają „specjalny" status w świetle traktatów, np. bezpieczeństwa narodowego[29]. Stephen

[21] Wyrok TS z dnia 21 grudnia 2023 r., C-124/21, LEX nr 3688832; A. Villanueva, *Accounting for the Specificities of Sport in EU Law: Old and New Directions in the 21 December 2023 Judgments* "The International Sports Law Journal", 2024, nr 23(4), s. 424; S. Weatherill, *The EU as a Sports Regulator* [w:] *Handbook on International Sports Law,* J. Nafziger (red.), R. Gauthier (red.), "Cheltenham", 2022, s. 132.

[22] S. Weatherill, *The Impact of the Rulings of 21 December 2023 on the Structure of EU Sports Law,* "The International Sports Law Journal" 2024, nr 23(4), s. 410.

[23] S. Weatherill, *The Influence of EU Law on Sports Governance* [w:] *Principles and Practice in EU Sports Law*, S. Weatherill (red.), Oxford, 2017, s. 246.

[24] Opinia Rzecznika Generalnego z dnia 15 grudnia 2022 r., C-333/21, LEX nr 3442693.

[25] Wyrok TS z dnia 21 grudnia 2023 r., C-680/21, LEX nr 3689878.

[26] A. Villanueva, *Accounting for… op. cit.*, s. 423.

[27] Wyrok TS z dnia 15 grudnia1995 r., C-415/93, ECR 1995, nr 12, poz. I-4921.

[28] *Ibidem*, para. 76.

[29] A. Villanueva, *Accounting for… op. cit.,* s. 423. W zakresie zastosowania przepisów ochrony danych osobowych oraz Karty Praw Podstawowych w dziedzinie bezpieczeństwa, zob. wyrok TS z dnia 6 października 2020 r., C-511/18, LEX nr 3095381.

Weatherill zauważa, że niedawne wyroki TSUE: *ESL*, *Royal Antwerp*, i *International Skating Union*[30] mogą zmienić postrzeganie znaczenia Art. 165 TFUE dla europejskiego sportu[31], ponieważ TSUE zmarginalizował w nich znaczenie Art. 165 TFUE dla rozstrzygnięć spraw w zakresie prawa sportowego[32]. Chociaż nie zaprzeczył całkowicie, że sport sam w sobie posiada pewne charakterystyczne cechy, to sam w sobie nie jest „specjalny"[33]. Można więc zaobserwować stopniowe zawężanie autonomii organizacji sportowych i włączenie zasad prawa sportowego w zakres stosowania prawa UE[34]. Podsumowując, chociaż UE nie ma kompetencji do regulowania sportu (zasad organizacji zawodów sportowych, reguł rywalizacji etc.), nie zwalnia to związków sportowych od przestrzegania przepisów unijnych obowiązujących na rynku wewnętrznym. Ostatnio, TSUE zawęża ewentualne wyjątki od tej zasady.

Najistotniejszym standardem wypracowanym w prawie wtórnym UE jest RODO, które weszło w życie w 2018 r. i od tamtego czasu wyznacza niezmiennie standard ochrony danych osobowych obywateli Unii na jej terytorium, a czasem i poza[35]. Podstawą prawną RODO jest Art. 16 TFUE, a celem – przyznanie osobom fizycznym większej kontroli nad ich danymi osobowymi oraz wyższego poziomu ochrony ich danych[36]. Jako rozporządzenie, którego implementacja do przepisów krajowych nie jest konieczna, RODO ustanowiło także jednolity standard ochrony danych na terenie całej Unii. RODO zastąpiło obowiązującą poprzednio Dyrektywę 95/46 („Dyrektywa")[37], która przyznawała Państwom Członkowskim większą swobodę w kształtowaniu przepisów ochrony danych osobowych[38]. RODO wprowadziło „złoty standard" ochrony danych osobowych[39]. Z drugiej strony, bywa ono

[30] Wyrok TS z dnia 21 grudnia 2023 r., C-124/21, LEX nr 3688832.
[31] S. Weatherill, *The Impact of the Rulings of 21 December 2023 on the Structure of EU Sports Law* "The International Sports Law Journal" 2024, nr. 23(4), s. 415.
[32] *Ibidem*, s. 410.
[33] J. Zgliński, *Can EU competition law save sports governance*? "The International Sports Law Journal" 2024, nr. 23(4) s. 476.
[34] Coraz częściej można zaobserwować, że TSUE dąży do poddania działania organizacji sportowych zasadom UE, kwestionując ich bezwzględną autonomię. Miało to miejsce w zakresie zasad konkurencji i działań mających znaczenie gospodarcze (por. przywołane wyroki C-680/21, C-333/21), ale także w zakresie rozwiązywania sporów sportowych, por. Wyrok TS z 1 sierpnia 2025 r., C-600/23, LEX nr 3895721. Kolejną okazją do orzeczenia o są połączone sprawy C-424/24 oraz C-425/24. Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24. Wyroku można spodziewać się w 2026 r.
[35] Zob. zakres terytorialny stosowania RODO, Art. 2.
[36] RODO, Art. 1 ust. 2, motyw 7.
[37] 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 („Dyrektywa").
[38] RODO, Motyw 10.
[39] A. Mantelero, *The future of data protection: Gold standard vs. global standard*, "Computer Law & Security Review" 2021 nr 4.

krytykowane za niejasne i trudne do wdrożenia przepisy, co obciąża przedsiębiorstwa i generuje poważne koszty dla biznesu[40]. Mając na uwadze obciążenie finansowe i organizacyjne podmiotów gospodarczych, wywołane przez RODO, prawodawca unijny zapowiedział jego deregulację[41], jednak jej zakres, a tym samym faktyczny wpływ na sytuację przedsiębiorców, pozostaje na razie niepewny (tak samo jak fakt, czy faktycznie zostanie ona urzeczywistniona w praktyce)[42].

Dokładne zasady dotyczące sposobu publikowania danych zawodników ukaranych za doping sprecyzowane są przez przepisy krajowe[43]. Przykładowo, ustawa o zwalczaniu dopingu w sporcie[44] bezpośrednio wyłącza możliwość zastosowania Art. 18 RODO, który ustanawia prawo do ograniczenia przetwarzania (osoba, której dane dotyczą, może złożyć żądanie ograniczenia przetwarzania). Na marginesie, pokazuje to założenie polskiego prawodawcy, że co do zasady RODO znajduje zastosowanie do działań antydopingowych[45]. Dla porównania, w Austrii[46] dla celów spraw związanych z kontrolą antydopingową, do życia powołano NADA: spółkę z o.o. o charakterze spółki użyteczności publicznej. Zgodnie z austriacką federalną ustawa antydopingową („ADBG") NADA przetwarza dane osobowe jako administrator w rozumieniu RODO w związku z przeprowadzanymi czynnościami w zakresie zwalczania dopingu i wykonywania swoich obowiązków zgodnie z ADBG.

[40] O trudnościach, z którymi mierzą się przedsiębiorcy wdrażający RODO zob. m.in. I*T Governance* (*Organization*). Privacy Team. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. Fourth edition. Ely, Cambridgeshire, 2020: IT Governance Publishing. RODO jest także poddane krytyce w reporcie Draghiego, który stał się jednym z przyczynków do deregulacji i upraszczania unijnych przepisów, zob. M. Draghi, *The future of European competitiveness Part B | In-depth analysis and recommendations* Bruksela, 2024, s. 79 i n.

[41] Komisja Europejska, *Data Protection* https://commission.europa.eu/law/law-topic/data-protection_en#simplifying-compliance-with-the-gdpr-through-reduced-record-keeping-obligations [dostęp: 2.03.2026]. Deregulacja przepisów dot. ochrony danych osobowych jest częścią szerszej strategii uproszczenia i deregulacji przepisów dot. rynku cyfrowego, która obejmuje także zmiany w zakresie AI Act, CSDRR i innych, zob. Komisja Europejska, *Digital Omnibus Deregulation Proposal* https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal [dostęp: 2.03.2026].

[42] Niniejsza praca analizuje przepisy RODO obowiązujące na dzień 1 lutego 2026 r.

[43] B. van der Sloot, M. Paun, R. Leenes, P. McNally, P. Ypma *Anti-Doping & Data Protection An evaluation of the anti-doping laws and practices in the EU Member States in light of the General Data Protection Regulation* Luxembourg, 2017, s. 19.

[44] Ustawa z dnia 21 kwietnia 2017 r. o zwalczaniu dopingu w sporcie (t.j. Dz. U. z 2022 r. poz. 1258).

[45] O. Rudak, *Czy ujawnienie danych sportowca stosującego doping narusza RODO?* „Lege Artis", 2023.

[46] Austria została wykorzystana jako przykład, ponieważ obydwie sprawy omówione w artykule, tj. C-474/24 oraz C-115/22, pochodzą właśnie z tego kraju.

3. ZASTOSOWANIE RODO DO PRZEPISÓW ANTYDOPINGOWYCH REGULUJĄCYCH UJAWNIANIE SANKCJI NAŁOŻONYCH NA SPORTOWCÓW ZA NARUSZENIE PRZEPISÓW ANTYDOPINGOWYCH

Zastosowanie RODO do przepisów antydopingowych nie jest oczywiste. Dowodzą tego sprawy C-115/22 oraz C-474/24. Są one o tyle interesujące, że na podobne pytania dotyczące zastosowania RODO do danych osobowych sportowców, związanych z badaniami dopingowymi, rzecznicy udzielili zupełnie innych odpowiedzi.

Pierwsza sprawa dotyczyła austriackiej zawodowej lekkoatletki SO. Austriacka Komisja Antydopingowa *Österreichische Anti-Doping Rechtskommission* („ÖADR") stwierdziła, że SO stosowała substancję zabronioną i nałożyła na nią sankcję obejmującą publikację treści kary w internecie. SO odwołała się od niej, argumentując, że jest ona niezgodna z RODO. ÖADR odmówiła, powołując się na para.21 ust. 3 ADBG, zgodnie z którym musi informować opinię publiczną o decyzjach podjętych w postępowaniach antydopingowych, podając również dane osobowe zawieszonych sportowców. SO odwołała się do Austriackiej Niezależnej Komisji Arbitrażowej (*Unabhängige Schiedskommission*, „USK"), ponieważ nie chciała, aby opinia publiczna mogła zidentyfikować ją jako osobę objętą postępowaniem. W tej sprawie, TSUE odmówiło udzielenia odpowiedzi na pytania, uznając że pytający organ nie jest „sądem lub trybunałem", a więc nie jest uprawniony do zadawania pytań prejudycjalnych z Art. 267 TFUE. Rzecznik T. Ćapeta[47] uznała, że USK może być do nich zaliczony i udzieliła odpowiedzi na pytania merytoryczne.

W drugiej sprawie, Austriacki *Bundesverwaltungsgericht* (federalny sąd administracyjny, „BGH") skierował do TSUE pytanie, czy przetwarzanie danych osobowych (takich jak nazwisko, dyscyplina sportu, naruszenie przepisów antydopingowych, kara oraz początek i koniec jej trwania) oraz ich publikacja na stronie internetowej austriackiej agencji antydopingowej oraz w oficjalnych komunikatach prasowych są objęte zakresem stosowania RODO. Na wypadek odpowiedzi twierdzącej, BGH zadał także pytanie, czy informacja o tym, że dana osoba dopuściła się określonego naruszenia antydopingowego i z powodu tego naruszenia została wyłączona w związku z dyskwalifikacją z udziału w zawodach, stanowią „dane dotyczące zdrowia" w rozumieniu Art. 9 RODO oraz, czy przepisy RODO stoi na przeszkodzie uregulowaniu krajowemu przewidujemy publikację nazwisk osób, których dotyczy orzeczenie wydane przez ÖADR lub USK okresu dyskwalifikacji oraz przyczyn

[47] Opinia Rzecznik Generalnej TS Tamary Ćapety w sprawie C-115/22.

dla zastosowania tego środka. Sąd zapytał także, czy zasady określone w Art. 5(1)(a) i 5(1)(c) RODO wymagają, w każdym wypadku, dokonania wyważenia interesów osobistych danej osoby dotkniętej publikacją i interesu społeczeństwa w uzyskaniu informacji dotyczącej naruszenia antydopingowego popełnionego przez sportowca w każdym wypadku[48].

Rozważając kwestię zastosowania przepisów RODO do publikacji danych w sprawach antydopingowych, doszli do przeciwnych wniosków. W sprawie C-115/22, rzecznik generalna zakwestionowała (mimo, że USK nie zadało na ten temat wyraźnego pytania) fakt możliwości zastosowania przepisów RODO do przepisów prawa antydopingowego[49]. Wskazała, że "trudno (...) ustalić konieczny związek [przepisów prawa antydopingowego] z prawem Unii, co pozwoliłoby na uznanie okoliczności niniejszej sprawy za działalność państwa członkowskiego wchodzącą w zakres stosowania prawa Unii"[50]. W konsekwencji, RODO nie powinno stosować się w przedstawionej sprawie. Z drugiej strony, rzecznik Dean Spielmann w sprawie C-474/24 doszedł do wniosków, że przetwarzanie danych w celach badan antydopingowych mieści się w zakresie zastosowania RODO[51].

3.1. ZAKRES ART. 2(2)(A) RODO

Rzecznik Spielmann zaproponował interpretację, zgodnie z którą, w świetle Art. 16(2) zdanie pierwsze TFUE i Art. 2(2)(a) RODO, przetwarzanie danych osobowych na podstawie krajowych przepisów antydopingowych, polegające na publikacji nazwisk danych sportowców, informacji o uprawianej dyscyplinie sportu, popełnionym naruszeniu przepisów antydopingowych i nałożonej karze oraz dat początku i końca jej obowiązywania, nie może zostać uznane za dokonywane w ramach „działalności nieobjętej zakresem prawa Unii" w rozumieniu Art. 2(2)(a) RODO[52]. Rzecznik wskazał, że wszystkie wyjątki od zasad ogólnych powinny być interpretowane wąsko, zgodnie z generalną zasadą interpretacji prawa *exceptiones non sunt extendae*. Tym samym, RODO należy stosować do ujawniania danych sportowców i powiązanych informacji dotyczących dopingu.

Warto dokładniej pochylić się nad przywołanym przepisem. Zgodnie z Art. 2(2)(a) RODO, który określa zakres stosowania rozporządzenia, RODO nie

[48] OGH zadał do TSUE więcej pytań, które dotyczyły jednak Art. 10 RODO i w związku z tym pozostają poza zakresem niniejszego artykułu.
[49] Opinia Rzecznik Generalnej TS Tamary Ćapety w sprawie C-115/22, para. 83 i n.
[50] *Ibidem*, para. 90.
[51] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para. 60.
[52] *Ibidem*.

stosuje się do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa Unii. Jako przykłady podaje się najczęściej działalność dotyczącą bezpieczeństwa narodowego, działania związane ze zwalczaniem przestępczości oraz działania państw członkowskich w związku z wdrażaniem wspólnej polityki zagranicznej i bezpieczeństwa wewnętrznego UE[53]. W zakresie działalności organizacji sportowych, sytuacja nie jest tak jednoznaczna. Jak podkreślono na wstępie artykułu, kompetencje UE w zakresie regulacji sportu są ograniczone do działań pomocniczych. Dodatkowo, Art. 165(3) TFUE przewiduje, że Unia współpracuje z organizacjami międzynarodowymi w zakresie sportu – do takich niewątpliwie zalicza się WADA. W związku z tym odpowiedź pytanie, czy prawo UE może wpływać na stosowanie stanowionego przez nią prawa, przede wszystkim WADC, nie jest wcale oczywista.

Rzecznik argumentował także, że Art. 2(2)(a) RODO ma na celu wyłączenie z zakresu stosowania rozporządzenia przetwarzania danych osobowych w ramach działalności „mającej na celu ochronę bezpieczeństwa narodowego lub działalności, która może zostać zaliczona do tej samej kategorii"[54]. Opinia Rzecznika przywołuje w tym zakresie wyrok TSUE wydany w sprawie *Latvijas Republikas Saeima*[55], ale rozumowanie Trybunału w tamtej sprawie nie powinno zostać *mutatis mutandis* stosowane do sprawy C-474/24. Przywołana sprawa dotyczyła przetwarzania danych dot. wykroczeń drogowych, Trybunał orzekł, że fakt, iż dana „działalność jest właściwa państwu lub organowi publicznemu, nie wystarcza, aby wyjątek ten mógł być automatycznie stosowany". W wyroku *Demokratichna Bulgaria*[56] TSUE musiał natomiast udzielić odpowiedzi na pytanie, czy z zakresu stosowania RODO wyłączone jest przetwarzanie danych osobowych w kontekście organizacji wyborów w państwie członkowskim UE. Trybunał uznał, że wyjątek z Art. 2(2)(a) RODO należy stosować jedynie, gdy dane przetwarzane są w kontekście działalności mającej na celu „ochronę podstawowych funkcji państwa i podstawowych interesów społeczeństwa"[57]. Zdaniem TSUE, organizacja wyborów do takich działań nie należy, w związku z czym wyłączenie nie znajduje zastosowania.[58] W podobnym tonie TSUE wypowiedział się w wyroku *Land Hessen*[59], który dotyczył żądania dostępu do danych osobowych, zarejestrowanych przez komisję parlamentarną w ramach rozpatrywania petycji. Osoba, której dane dotyczyły, powołała się przy tym na RODO, a sąd krajowy miał

[53] H. Kranenborg, *Article 2. Material… op. cit.,* s. 69-71; RODO, motyw 16, motyw 19.
[54] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para. 40.
[55] Wyrok TS z dnia 22 czerwca 2021 r., C-439/19, LEX nr 3189121, para. 67.
[56] Wyrok TS dnia z 20 października 2022 r., C-306/21, LEX nr 3419660.
[57] *Ibidem*, para. 40.
[58] *Ibidem*, para. 41-42.
[59] Wyrok TS dnia z 9 lipca 2020 r., C-272/19, LEX nr 3027775.

rozstrzygnąć, czy zbieranie danych dla celów postępowania w sprawie petycji, które stanowi działalność parlamentarną, jest objęte zakresem zastosowania RODO. Wyroki te dotyczą więc sytuacji, które faktycznie dotykają kwestii bezpieczeństwa lub funkcjonowania państwa, w odróżnieniu od kwestii związanych z dopingiem.

W przywołanych wyrokach TSUE uznaje, że Art. 2(2) RODO odpowiada Art. 3(2) Dyrektywy[60]. Niemniej, Art. 2(2)(a) RODO i Art. 3(2) tiret 1 Dyrektywy nie miały tego samego brzmienia. Art. 3(2) tiret 1 Dyrektywy stanowił jednoznacznie, że nie ma ona zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego". Jest to znacznie bardziej dokładny, precyzyjny przepis, który TSUE faktycznie mogło zinterpretować jako zamkniętą listę wyjątków. O podobnej precyzji nie można mówić w odniesieniu do Art. 2 RODO.

Ponadto, interpretacji tych przepisów jako identycznych i mających taki sam zakres nie sprzyja wykładnia historyczna. Oryginalna propozycja legislacyjna Komisji Europejskiej dotycząca RODO przewidywała, że nie znajdzie ono zastosowania „w ramach działalności wykraczającej poza zakres prawa Unii, w szczególności w odniesieniu do bezpieczeństwa narodowego" (art. 2(2)(a)) oraz przy przetwarzaniu danych „przez właściwe organy w celu zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania lub wykonywania kar karnych" (art. 2(2)(e)[61]. Obecnie, Art. 2 RODO stanowi, że RODO nie stosuje się „w ramach działalności nieobjętej zakresem prawa Unii". Jak widać, ustawodawca unijny dokonał wyraźnej zmiany, polegającej na usunięciu fragmentu „w szczególności w odniesieniu do bezpieczeństwa narodowego",[62] oraz wyraźnym oddzieleniu od siebie działalność pozostającą poza prawem UE oraz działalności prowadzonej w celu zapobiegania przestępstwom. Argumentując, że RODO nie może mieć węższego

[60] *Ibidem*, para. 69.

[61] Komisja Europejska, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC00 [dostęp: 2.03.2026].

[62] Parlament Europejski, *Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))* https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52014AP0212 [dostęp: 2.03.2026].

zakresu niż dyrektywa, TSUE pomija ten szczegół procedury legislacyjnej. Trudno jest jednak uznać, że ta zmiana w brzmieniu przepisu miałyby pozostać bez wpływu na znaczenie oraz praktyczne skutki regulacji. Przeciwnie, skoro unijny prawodawca zdecydował się zmienić sformułowanie zawarte w dyrektywie i zastąpić szerokim Art. 2(2)(a) RODO, to nie można mu nadać tego samego znaczenia, co przepisom dyrektywy.

Nawet uznając, że w kontekście działalności państwa Art. 2(2)(a) RODO i Art. 3(2) tiret. 1 Dyrektywy mają tożsame zakresy zastosowania, nie jest to przesadzone w kontekście działań antydopingowych. Przywołane wcześniej wyroki TSUE interpretujące RODO w świetle Dyrektywy dotyczyły sytuacji, gdy dane przetwarzały organy publiczne. Wówczas nie było jasne, czy ich działanie pozostaje w zakresie działania związanego z bezpieczeństwem narodowym lub innym działaniem dotyczącym istotnych funkcji państwa, również wyłączonym z zakresu stosowania prawa UE. Sprawa C-474/24 jest o tyle nieporównywalna, że dotyczy przetwarzania danych co prawda przez organ publiczny, ale działający w sferze regulowanej na poziomie międzynarodowym, i w zakresie, w którym Unia nie posiada kompetencji legislacyjnych, a jedynie pomocnicze. Doktryna podobnie zauważa, że w dziedzinach wymienionych w Art. 6 TFUE „Unia ma kompetencje tylko do prowadzenia działań mających na celu wspieranie, koordynowanie lub uzupełnianie aktywności państw członkowskich (...) Brak regulacji szczególnej w określonych obszarach działania państw członkowskich w prawie pierwotnym skutkuje więc tym, że w tych obszarach Unia nie może podejmować działań unifikacyjnych, a tym samym nie powinno znajdować zastosowania RODO”[63]. Sprawy związane z dopingiem, regulowanym międzynarodowo, można więc odróżnić od poprzednich spraw zapadłych na gruncie Art. 2(2)(a).

3.2. ARGUMENTY ZA STOSOWANIEM RODO DO PRZETWARZANIA DANYCH RODO I ART. 3(2) TIRET. 1 DYREKTYWY

Rozważania dotyczące Art. 2(2)(a) RODO nie dają jasnej i przekonującej odpowiedzi na pytanie, czy RODO należy stosować do danych przetwarzanych w kontekście badań antydopingowych. Na potwierdzenie tej tezy można znaleźć jednak inne argumenty, wynikające z wykładni strukturalnej i funkcjonalnej. Motyw 112 RODO stanowi, że „wyjątki (...) powinny mieć w szczególności zastosowanie do przekazywania danych wymaganego i niezbędnego z uwagi na ważne względy

[63] P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz,* wyd. 2, P. Litwiński (red.), Warszawa 2025, Artykuł 2, nb. 12.

interesu publicznego, na przykład do (...) w celu zmniejszenia lub wyeliminowania dopingu w sporcie”[64], co wskazywałoby na to, że RODO znajduje zastosowanie. Argumentuje się też, że Art. 16 TFUE, który wprowadzono dopiero traktatem z Lizbony, „stał się furtką dającą UE możliwość zmiany takiego stanu rzeczy poprzez ustanowienie jednolitych przepisów w sprawach z zakresu ochrony osób fizycznych w odniesieniu do przetwarzania ich danych osobowych oraz swobodnego przepływu takich danych również w obszarach objętych kompetencjami koordynacyjnymi”[65]. W efekcie, należy go stosować „w całym spektrum działania UE”[66]. Tutaj szersze zastosowanie wynika jednak ze zmiany podstawy prawnej, a nie z nawiązania do Dyrektywy 95/64.

Jako kolejny argument, że RODO powinno stosować się do przetwarzania danych w celach antydopingowych, można wymienić faktyczne działania podejmowane przez instytucje unijne w zakresie walki z dopingiem. Komisja i państwa członkowskie podejmują działania mające na celu m. in. zapewnienie zgodności wszystkich przepisów i procedur związanych z nowym WADC z prawem UE[67]. Na arenie międzynarodowej, Komisja współpracuje z WADA oraz Radą Europy[68]. Są to jednak działania wspierające, nieprowadzące do wydania osobnych konkretnych aktów prawnych. Niemniej, jeśli uznać, że jakikolwiek sposób działania Unii wystarcza, aby dana sfera została objęta prawem ochrony danych, to będzie to wystarczające. Inni zauważają także, że TSUE w sprawie *Meca-Medina*[69] TSUE zastosował prawo unijne do przepisów antydopingowych[70], niemniej zdaniem autorki sytuacje te nie są porównywalne. W *Meca-Medina* przedmiotem zainteresowania były zasady konkurencji uregulowane bezpośrednio w Traktatach oraz swoboda świadczenia usług, również znajdująca umocowanie w TFUE. Na koniec, możliwy jest także argument, że sankcje za naruszenie przepisów antydopingowych mają walor ekonomiczny[71],

[64] Por. bardzo słuszna obserwacja poczyniona przez Jana Exnera, *Sports arbitration, doping and the GDPR: Tightening the judicial independence of non-judicial bodies in NADA and Others*, “Common Market Law Review” 2025, 62(3), s. 934. Argument o motywie 112 nie pojawia się natomiast w Opinii Rzecznika.

[65] P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz,* wyd. 2, P. Litwiński (red.), Warszawa 2025, Artykuł 2, nb 12.

[66] *Ibidem.*

[67] Komisja Euorpejska, *Anti-doping*, https://sport.ec.europa.eu/policies/sport-and-integrity/anti-doping [dostęp: 2.03.2026]

[68] Ibidem; zgodnie z art. 165(3) TFUE.

[69] Wyrok TS z dnia 18 lipca 2006 r., C-519/04 P, ZOTSiS 2006, nr 7B, poz. I-6991.

[70] J. Exner, *Sports arbitration, doping and the GDPR: Tightening the judicial independence of non-judicial bodies in NADA and Others*, “Common Market Law Review”, 2025, 62(3), s. 934.

[71] Exner J., *Putting Athletes in the Digital Pillory: Opinion of AG Spielmann in NADA Austria (C-474/24)*, EU Law Live, 30 September 2025.

a stosowanie przepisów unijnych do działań sportowych, które mają wymiar gospodarczy, jest akceptowane i utrwalone w orzecznictwie TSUE[72]. Stosowanie RODO do ochrony danych zawodników w procedurach antydopingowych nie jest porównywalne, i stanowi nowe zagadnienie postawione przed TSUE.

Twierdzenie, że RODO znajduje zastosowanie do przetwarzania oraz publikowania danych sportowców w sprawach antydopingowych, ma poparcie także w faktycznej praktyce krajowych organów antydopingowych oraz prawie krajowym. Jak już wspomniano, polska ustawa o zwalczaniu dopingu w sporcie wydaje się bezpośrednio zakładać, że RODO co do zasady znajduje do niej zastosowanie. Podobnie sytuacja przedstawia się we Włoszech, gdzie na stronie NADO Italia (włoskiej agencji antydopingowej) można znaleźć bezpośrednie odniesienia do obowiązków nałożonych przepisami RODO[73]. Podsumowując, stosowanie RODO do danych sportowców skazanych za naruszenia przepisów antydopingowych, chociaż nieoczywiste, często pojawia się w praktyce organów sportowych, a także zakłada je samo RODO.

4. DANE SPORTOWCÓW DOTYCZĄCE KAR ZA STOSOWANIE DOPINGU JAKO „DANE DOTYCZĄCE ZDROWIA"

Przyjmując jednak, że RODO znajduje zastosowanie do działań organizacji sportowych na terenie Unii, należy rozstrzygnąć, czy publikowane dane mogą zostać uznane za dane dotyczące zdrowia[74]. Dane dotyczące zdrowia to jedna z podkategorii danych wrażliwych, które obejmuje dane ujawniające np. pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, orientację seksualną[75]. Przetwarzanie tych danych jest co do zasady zabronione, ale Art. 9(2) RODO przewiduje liczne wyjątki od tej zasady. Do wyjątków uzasadniających przetwarzanie tych danych należą m. in. ochrona zdrowia publicznego, profilaktyka zdrowotna, wypełnianie praw i obowiązków przez osobę, której dane dotyczą oraz zgoda zainteresowanej osoby. W przypadku przetwarzania, warunki te byłyby spełnione m. in. na podstawie Art. 9(2)(g), zgodnie z którym przetwarzanie jest dopuszczalne, jeśli jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego. Niemniej, i ten artykuł obarczony jest dalszymi warunkami co do przetwarzania, np. przetwarzanie musi być proporcjonalne i nie

[72] S. Weatherill, *The EU as a Sports Regulator* [w:] *Handbook on International Sports Law,* J. Nafziger (red.), R. Gauthier (red.), Cheltenham, 2022, s. 112-123.
[73] NADO Italia, Przetwarzanie danych osobowych zawodników, https://www.nadoitalia.it/en/athletes/rights-and-responsibilities/processing-of-personal-data.html [dostęp: 2.03.2026].
[74] RODO, Art. 4 pkt 1.
[75] Ibidem, Art. 9 ust. 1.

naruszać istoty praw osoby, której dane są przetwarzane[76]. Jak widać, znalezienie się w reżimie danych wrażliwych niesie za sobą istotne konsekwencje.

Z propozycją, aby dane ujawniane przez austriackie organy traktować jako dane dotyczące zdrowia, nie zgodziła się Rzecznik Ćapeta. Zwróciła uwagę, że aby uznać dane za dotyczące zdrowia, muszą one spełniać dwa warunki: „muszą dotyczyć zdrowia fizycznego lub psychicznego osoby fizycznej oraz ujawniać informacje na temat stanu zdrowia osoby fizycznej"[77]. Rzecznik uznała, że stosowania substancji zabronionych przez prawo antydopingowe nie mówi jeszcze nic o stanie zdrowia danej osoby, wobec czego nie należą do tej kategorii[78].

Rzecznik Spielmann doszedł do przeciwnych wniosków[79]. Jego zdaniem, pojęcie „danych dotyczących zdrowia" należy interpretować szeroko[80], zgodnie z orzecznictwem. W sprawie *Lindenapotheke* TSUE uznał, za dane dotyczące zdrowia informacje o kupowanych produktów leczniczych, które pozwalały na wyciągnięcie wniosków co do stanu zdrowia zidentyfikowanej lub możliwej do zidentyfikowania osoby[81]. Ponadto, danymi wrażliwymi są też dane mogące pośrednio ujawniać orientację seksualną konkretnej osoby[82]. *Per analogiam*, za dane szczególnych kategorii należy uznać dane pośrednio ujawniające wrażliwą i chronioną cechę charakterystyczną (tj. zdrowie, orientację seksualną, pochodzenie etniczne etc.). Podobnie TSUE wypowiadał się w orzecznictwie wydanym na podstawie Art. 8 Dyrektywy 95/64[83].

Orzecznictwo do „danych dotyczących zdrowia" zalicza dane, które powstały w kontekście medycznym (dokumentacja medyczna, recepty etc.), jak również dane, które powstały poza nim, ale bezpośrednio/pośrednio ujawniają stan zdrowia możliwej do zidentyfikowania osoby. Wobec tego, aby odpowiedzieć na pytanie, czy informację o przyjmowanych przez zawodnika środkach dopingowych można uznać za wrażliwą, kluczowe jest stwierdzenie, czy między tymi środkami a stanem zdrowia istnieje wystarczający związek pośredni. Zdaniem Rzecznika, najistotniejsze jest rozstrzygnięcie, „czy na podstawie odnośnych danych można sformułować wnioski co do stanu zdrowia danej osoby, czy to chorobowego"[84]. W jego opinii, jest to możliwe, o ile ujawnione dane obejmują wzmiankę zabronionej substancji, którą przyjmował

[76] Ibidem, Art. 9 ust. 2 lit. g zdanie 2.
[77] Opinia Rzecznik Generalnej TS Tamary Ćapety w sprawie C-115/22, para.97.
[78] *Ibidem*.
[79] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para.82.
[80] *Ibidem*, para. 65, zob. Wyrok TS z dnia 4 października 2024 r., C-21/23, LEX nr 3783145.
[81] Wyrok TS z dnia 4 października 2024 r., C-21/23, LEX nr 3783145, para.78.
[82] Wyrok TS z dnia 1 sierpnia 2022 r., C-184/20, LEX nr 3371971, para. 125-127.
[83] Wyrok TS z dnia 6 listopada 2003 r., C-101/01, LEX nr 192425, para. 50.
[84] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para. 69.

dany sportowiec[85]. Informacja o przyjmowaniu substancji zabronionej sama w sobie nie jest jeszcze informacją dotyczącą zdrowia. Jednak, w połączeniu z innymi ujawnionymi danymi, poprzez dedukcję i rozumowanie, może ujawniać informacje o stanie zdrowia danej osoby.

Niemniej, jeśli chodzi o objęcie tym pojęciem danych dotyczących przyjmowanego przez sportowców dopingu, wypada zgodzić się z Rzecznik Ćapetą, że nie jest to uzasadnione. Argumentacja Rzecznika Spielmanna nie przekonuje i w pewnych przypadkach może okazać się nietrafiona. Np. strona internetowa POLADA podaje jako informacje naruszony przepis oraz nazwę zabronionej substancji, która była przyjmowana przez zawieszonego sportowca[86]. Te nazwy dotyczą często substancji, które nie należą do leków, suplementów etc. (zakazane są np. narkotyki, takie jak kokaina i amfetamina) lub których przyjmowanie jest nielegalne, ale występują one również naturalnie w organizmie, np. testosteron. Trudno uznać, że sama nazwa substancji, bez znajomości częstotliwości oraz okresu jej przyjmowania, a także bez wiedzy o innych przyjmowanych lekach i chorobach danej osoby, może ujawnić informacje jej/jego stanie zdrowia. Dodatkowo, obecnie stosowane testy dopingowe są niezwykle czułe i mogą wykrywać nawet mikroskopijne ilości dopingu, których wpływ na zdrowie zawodnika jest znikomy. Można zgodzić się z Rzecznikiem Generalnym, że walka z dopingiem ma aspekty zdrowotne[87], a jednym z kryterium zakazania substancji jest jej negatywny wpływ na zdrowie[88], ale nie oznacza, że informacje o branym dopingu są w stanie ujawnić informacje o stanie zdrowia danej osoby.

Można też zauważyć, że WADA przewiduje wyłączenia w celach terapeutycznych (*therapeutic use exemptions*, „TUEs"), dzięki którym sportowcy, którzy przyjmują substancję *prima facie* zakazaną, ale niezbędną ze względu na ich stan zdrowia, nie zostaną ukarani za doping[89]. Informacje o tym, jakie TUEs odnoszą się do danego sportowca, faktycznie mogłyby ujawniać jego stan zdrowia; taka sytuacja nie ma jednak miejsca w przypadku zwyczajnego dopingu.

Podsumowując, dane ujawniające kary antydopingowe, a także ujawniające stosowaną przez danego sportowca zakazanej substancji, nie powinny być traktowane jako dane dotyczące zdrowia w rozumieniu Art. 4(15) RODO.

---

[85] *Ibidem*, para. 75-81.

[86] POLADA, *Przypadki naruszenia przepisów* https://antydoping.pl/kontrole/przypadki-naruszenia-przepisow/ [dostęp: 2.03.2026].

[87] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para. 76.

[88] Art. 4.3.1.2. WADC.

[89] WADA, *Therapeutic Use Exemptions* (Wyłączenia w celu terapeutycznym), https://www.wada-ama.org/en/athletes-support-personnel/therapeutic-use-exemptions-tues [dostęp: 2.03.2026].

5. MOŻLIWOŚĆ PUBLIKOWANIA DANYCH OSOBOWYCH SPORTOWCÓW, NA KTÓRYCH NAŁOŻONO SANKCJE DOPINGOWE, W ŚWIETLE RODO

Zdaniem Rzecznika Spielmanna, Art. 5(1)(a) i (c.) oraz Art. 6(3) RODO stoją one na przeszkodzie nałożonym na krajowe organy antydopingowe obowiązkowi publikowania danych osobowych sportowców ukaranych za naruszenie przepisów antydopingowych, jeżeli, biorąc pod uwagę szczególne okoliczności sprawy, wymóg proporcjonalności nie został lub przestał być spełniony, w szczególności w odniesieniu do zakresu i czasu trwania publikacji, czego ustalenie należy do sądu odsyłającego[90]. Nadto, Art. 5 i 6 RODO ustanawiają wymóg, aby administrator przed przetwarzaniem danych dokonał w każdym indywidualnym przypadku wyważenia wchodzących w grę interesów, jeżeli jest ono konieczne do przetwarzania danych osobowych zgodnie z RODO[91]. Rzecznik przypomniał z jednej strony, że nadrzędnym celem RODO jest zagwarantowanie praw fundamentalnych zawartych w Art. 8(1) i Art. 7 Karty. Z drugiej strony, publikacja danych może być uzasadniona, jeśli służy celowi leżącemu w interesie publicznym i jest proporcjonalna do zamierzonego uzasadnionego celu. Rzecznik nie zgodził się ze stwierdzeniem, jakoby publikacja wszystkich danych, w tym nazwy substancji zabronionej, były odpowiednie i uzasadnione z perspektywy interesu publicznego. Rzecznik wyraził także wątpliwość, czy w każdym przypadku publikacja nazwiska sportowca jest niezbędna z perspektywy prewencyjnej funkcji publikacji[92].

Z kolei Rzecznik Ćapeta uznała, że nałożony przez prawo obowiązek publikowania przez organ antydopingowy informacji o naruszeniu obowiązujących przepisów antydopingowych przez sportowca zawodowego na ogólnodostępnej stronie internetowej jest adekwatny i konieczny, a więc zgodny z Art. 5(1)(c) oraz Art. 6(3) RODO[93]. W omawianej sprawie, przetwarzanie danych odbywa się na podstawie ustawy, a więc musi spełniać wymogi z Art. 6(3) RODO, tj. służyć realizacji celu leżącego w interesie publicznym oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu[94]. Rzecznik słusznie zauważyła, że równowagę między dwoma sprzecznymi wartościami, interesem publicznym a prywatnością zawodnika, zostały wykonane przez krajowego prawodawcę[95]. Tym bardziej decyzja, czy w konkretnej sprawie dane sportowca powinny być opublikowane, czy nie, nie powinna być

[90] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para. 179.
[91] *Ibidem*, para. 180.
[92] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para.154.
[93] Opinia Rzecznik Generalnej TS Tamary Ćapety w sprawie C-115/22, para. 171-172.
[94] *Ibidem*, para. 134.
[95] *Ibidem*, para. 139.

pozostawiona organowi antydopingowego, który nie jest politycznie odpowiedzialny. Dyskrecja z jego strony mogłaby prowadzić do prób nadużyć, a także poczucia, że zawodnicy nie są traktowani jednakowo[96]. Rzecznik zgodziła się, że publikowanie danych osobowych sportowców jest uzasadnione w świetle interesu publicznego: ochrony integralności sportu, zapobiegania obchodzeniu zawieszenia przez sportowców, oraz prewencji poprzez odstraszanie innych zawodników od przyjmowania dopingu[97].

Rzecznik wzięła pod uwagę istotną okoliczność, że dane publikowane są w internecie, gdzie są one w prosty sposób dostępne dla każdego użytkownika, przez co ingerencja w prywatność jest bardziej dotkliwa niż w przypadku publikacji offline[98]. Co do zasady, wypada zgodzić się z tym argumentem; publikacja online oznacza, że każdy mający dostęp do internetu może trafić na zamieszczone w nim informacje. Niemniej, jak zauważyła Rzecznik, publikacja internetowa jest dzisiaj najbardziej powszechnym i – w gruncie rzeczy – jedynym pewnym sposobem informacji społeczeństwa[99]. Ponadto, nie jest argumentem przeciwko fakt, że internet zapewnia dostęp do informacji każdemu – taki jest przecież cel publikacji danych, aby każdy miał do nich dostęp[100]. Gdyby dostęp do informacji o karach za doping był ograniczony do niewielkiej grupy odbiorców, sankcja ta byłaby znacznie mniej dotkliwa i nie realizowałaby w równym stopniu swojego prewencyjnego i odstraszającego charakteru[101].

Obydwie opinie zawierają celne uwagi, ale nie jest pożądane, aby TSUE zaaprobowało którąkolwiek z nich w całości. W praktyce, opinia Rzecznika Spielmanna mogłaby prowadzić do faktycznej arbitralności i nieprzewidywalności w publikowaniu danych sportowców. Ważenie sprzecznych ze sobą interesów nie jest zadaniem łatwym i w zależności od tego, kto podejmuje decyzję, może przynosić różne rezultaty. Jeśli administrator w każdym przypadku ma dokonywać indywidualnego ważenia interesów, może to prowadzić do sytuacji, gdy publikacja danych uzależniona jest nie tylko od powagi zawinienia czy długości wykluczenia z zawodów, ale też od tego, czy sportowiec jest znany lub które on lub jego drużyna ma miejsce w rankingu światowym.

[96] W przypadku tej obserwacji, Rzecznik słusznie zgodziła się z uwagami przedstawionymi przez WADA, *ibidem,* para. 140.
[97] *Ibidem* para. 148 i n.
[98] Opinia nr 4/2009 Grupy Roboczej Art. 29, 2009 s. 17, pkt 3.6.2, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp162_en.pdf [dostęp: 2.03.2026].
[99] Opinia Rzecznik Generalnej TS Tamary Ćapety w sprawie C-115/22, para. 169.
[100] *Ibidem*.
[101] *Ibidem*, para. 170.

6. MODEL OCHRONY DANYCH OSOBOWYCH SPORTOWCÓW UWZGLĘDNIAJĄCY SPECYFIKĘ PRAWA SPORTOWEGO

Niezależnie od tego, czy dane osobowe przetwarzane w związku ze zwalczaniem dopingu objęte są RODO, czy też nie, nie ulega wątpliwości, że ich przetwarzanie powinno podlegać regulacji. W związku z tym, wypracowanie modelu ochrony danych osobowych sportowców, który uwzględnia ich interesy, a jednocześnie odpowiada potrzebom świata sportowego, jest jak najbardziej aktualne.

Dla wypracowania adekwatnego modelu istotne jest wzięcie pod uwagę zarówno głównych interesów indywidualnych sportowców, jak i naczelnych zasad WADC. Interes sportowców dobrze oddają naczelne zasady prawa ochrony danych osobowych. Zgodnie z Art. 7 RODO, jest to m. in. zasada minimalizacji danych. Zgodnie z nią, przetwarzane dane muszą być adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do określonych celów przetwarzania. Z perspektywy indywidualnego sportowca, w grę wchodzić może także niechęć przed podaniem ich danych do publicznej wiadomości ze względu na możliwą reakcję społeczną. Informacja o braniu dopingu przez sportowca przerywa karierę – może nawet ją zakończyć – i często oznacza też utratę sponsorów, partnerstw, oraz popularności. Może ona także narażać sportowców na negatywną reakcję ze strony fanów i otoczenia. W związku z tym, sportowcy mogą nie chcieć, aby ich dane podawać do publicznej wiadomości. Będzie to istotne szczególnie w przypadku sportowców, którzy są mniej znani i rozpoznawani w kraju lub międzynarodowo, i o których testach dopingowych nie informują media.

Niemniej, istotne interesy przedstawia także model regulowania walki z dopingiem, który regulowany jest na poziomie międzynarodowym. Doping to znaczący problem w sporcie, zagrażający zdrowiu zawodników i duchowi rywalizacji sportowej. Dla zapewnienia jego skutecznego zwalczania, można argumentować, że publikacja przynajmniej części danych zawodników decydujących się na doping jest wskazana i wskazuje na penalny charakter sankcji antydopingowych. Wynik ważenia przeciwstawnych interesów zależy od tego, czy dane oprzyjmowanym dopingu zostaną uznane za „dane dotyczące zdrowia”[102].

Odrzucić należy propozycję Rzecznika Spielmanna, żeby organy krajowe każdorazowo analizowały proporcjonalność ujawnienia danych zawodnika w konkretnej sprawie. Ocena proporcjonalności publikacji wymaga zbilansowania dwóch przeciwstawnych interesów i jako taka pozostaje ocenna. Potrzebny byłby specjalny

[102] Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24, para. 162 i przedstawione tam uwagi i założenia.

test proporcjonalności wypracowany w orzecznictwie lub chociaż wskazówki, jakie czynniki powinny być brane pod uwagę przez organ krajowy dokonujący oceny, żeby ocena ta nie była zupełnie uznaniowa i nie prowadziła do nieuzasadnionego zróżnicowanego traktowania sportowców. Ponadto, taka sytuacja generuje większą niepewność prawną niż sytuacja, w której jedyne, wąsko zakreślone wyjątki od obowiązku publikacji, zawiera WADC.

Konkludując, pewien zakres danych sportowców, którzy łamią przepisy poprzez stosowanie dopingu, może być dostępny publicznie dostępny. Ten dostęp do danych nie będzie nieproporcjonalny; uwzględnia to nie tylko interes publiczny, ale również powoduje, że sankcja za stosowanie dopingu będzie miała dodatkowy wymiar odstraszający. Niemniej, aktualnie publikowany i dostępny w internecie zakres danych nie jest konieczny do osiągnięcia tych celów, a więc pozostaje niezgodny z przepisami. Prawodawca powinien jasno wskazać, publikacja których danych jest rzeczywiście konieczna i adekwatna do osiągnięcia celu, a których wynika jedynie z utartej praktyki.

Podnoszona niezgodność przepisów unijnych z WADC nie musi jednak w przyszłości stanowić problemu, a to ze względu na zmianę kodeksu. WADC 2027 *explicite* uwzględnia stosowanie prawa krajowego do zasad ochrony zawodników, a więc ewentualna niezgodność zasad WADC z RODO i prawem krajowym wydanym z jego inspiracji przestanie być problemem. Jednocześnie, na poziomie unijnym da się zaobserwować tendencję do deregulacji i rozluźniania zasad ochrony danych osobowych pod hasłem ich uproszczenia. Cyfrowy Omnibus[103] zaproponowany przez Komisję Europejską w listopadzie 2025 r. wprowadza wiele zmian w tym zakresie. Jak zauważa wielu badaczy, dążenie do uproszczenia przepisów i odciążenia przedsiębiorców może prowadzić do znacznego osłabienia standardów ochrony danych osobowych. Powstaje więc pytanie, czy obniżenie standardu ochrony danych nie spowodowałoby, że publikacja danych sportowców skazanych za doping zostałaby uznana za zgodną z RODO oraz uzasadnioną ze względu na interes publiczny. Jeśli obniżyć standard ochrony danych osobowych, to balans interesu publicznego i indywidualnego prawa do ochrony danych może przechylić się w drugą stronę.

PODSUMOWANIE

Rozpatrywana przez TSUE sprawa jest nieoczywista na wielu płaszczyznach. Samo stosowanie RODO do przepisów antydopingowych, z których duża część regulacji pochodzi od prywatnych organizacji międzynarodowych, budzi wątpliwość

[103] Komisja Europejska, *Digital Omnibus Regulation Proposal…*, *op.cit.*

co do możliwości i zakresu wpływu możliwego wpływu na nie przez prawo UE. O ile z perspektywy Trybunału i prawa unijnego może to być pożądane, nie musi tak być z perspektywy prawa sportowego oraz międzynarodowych organizacji sportowych[104]. Dlatego też, jeśli TSUE podzieli opinię Rzecznika, sprawa C-474/24 może stać się precedensem wzmacniającym ochronę danych osobowych sportowców i wpłynąć na zakres ochrony sportowców i publikowania ich danych. W ten sposób, prawo ochrony danych osobowych wpływa na kolejne dziedziny, także te regulowane na poziomie globalnym, przywodząc na myśl tezę o działającym „efekcie Brukseli"[105].

Z entuzjazmem należy też oceniać WADC 2027, który w większym stopniu uwzględnia przepisy krajowe dotyczące ochrony danych osobowych sportowców. Co więcej, jeśli poziom ochrony danych w prawie unijnym faktycznie się obniży, być może zasady publikowania danych sportowców skazanych za doping nie będą musiały być już tak restrykcyjne, aby pozostawać w zgodzie z prawem unijnym.

BIBLIOGRAFIA

LITERATURA

Barta P., Kawecki M., Litwiński P. [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz,* P. Litwiński (red.), wyd. 2, Warszawa 2025.

Bradford A.H., *The Brussels Effect: How the European Union Rules the World* 2020 Oxford 2020.

Exner J., *Sports arbitration, doping and the GDPR: Tightening the judicial independence of non-judicial bodies in NADA and Others,* "Common Market Law Review" 2025, nr 62(3).

Draghi M., *The future of European competitiveness Part B | In-depth analysis and recommendations,* Bruksela 2024.

Kranenborg H. [w:] *The EU General Data Protection Regulation (GDPR),* C. Kuner (red.), L.A. Bygrave (red.), C. Docksey (red.), Oxford 2020.

IT Governance (Organization). Privacy Team, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide.* Fourth edition. Ely, Cambridgeshire: IT Governance Publishing, 2020.

[104] Por. przywoływany wcześniej wyrok w sprawie *RFC Seraing* dotyczący relacji prawa unijnego oraz arbitrażu sportowego administrowanego przez Sportowy Sąd Arbitrażowy („CAS") oraz wywołaną przez niego reakcję, np. stanowisko ICAS z 1 sierpnia 2025 r., https://www.tas-cas.org/generated/assets/lists/dceab111-07bc-435f-b5f9-de88eff9db72/ICAS_statement_CJEU_Seraing_ENG.pdf [dostęp: 2.03.2026]

[105] Sformułowanie „efekt Brukseli" (ang. *Brussels effect*) pochodzi i zostało spopularyzowane przez publikacje A.H. Bradford, *The Brussels Effect: How the European Union Rules the World* Oxford, 2022 i odnosi się do procesu rozprzestrzeniania się unijnych standardów regulacyjnych poza państwa UE. Zob. S. Weatherill, *The EU as a Sports Regulator…*, *op. cit.*, s. 137.

Mantelero A., *The future of data protection: Gold standard vs. global standard', "*Computer Law & Security Review" 2021, nr 4.

Rudak, O. *Czy ujawnienie danych sportowca stosującego doping narusza RODO? „*Lege Artis" 2023.

Villanueva A, *Accounting for the Specificities of Sport in EU Law: Old and New Directions in the 21 December 2023 Judgments* "The International Sports Law Journal" 2024, nr. 23(4).

van der Sloot B., Paun M., Leenes R., McNally P., Ypma P. *Anti-Doping & Data Protection. An evaluation of the anti-doping laws and practices in the EU Member States in light of the General Data Protection Regulation* Luksemburg 2017.

Weatherill S., *The Impact of the Rulings of 21 December 2023 on the Structure of EU Sports Law,* "The International Sports Law Journal" 2023, nr. 23(4).

Weatherill S., *The Influence of EU Law on Sports Governance* [w:] *Principles and Practice in EU Sports Law* S. Weatherill (red.), Oxford 2017.

S. Weatherill, *The EU as a Sports Regulator* [w:] *Handbook on International Sports Law,* J. Nafziger (red.), R. Gauthier (red.), Cheltenham 2022.

Zgliński J., *Can EU competition law save sports governance?,* "The International Sports Law Journal" 2023, nr. 23(4).

AKTY PRAWNE

Karta praw podstawowych Unii Europejskiej (Dz.U. C 202 z 7.06.2016, pp. 389-405).

Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana), Dz.U. C 202 z 7.06.2016, pp. 1–388.

Konwencja Antydopingowa Rady Europy, 1989 r.

Międzynarodowa Konwencja UNESCO przeciwko dopingowi w sporcie, 2005 r.

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) (Tekst mający znaczenie dla EOG).

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.

Ustawa z dnia 21 kwietnia 2017 r. o zwalczaniu dopingu w sporcie (t.j. Dz. U. z 2022 r. poz. 1258).

Ustawa antydopingowa (ADBG) (Anti-Doping-Bundesgesetz) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011421 [dostęp: 2.03.2026].

Światowy Kodeks Antydopingowy, wersja uchwalona w 2019 r.

Światowy Kodeks Antydopingowy, wersja uchwalona w 2025 r.

POLADA, Przepisy Antydopingowe Polskiej Agencji Antydopingowej (2021).

ORZECZNICTWO

Wyrok TS z dnia 18 lipca 2006 r., C-519/04 P, ZOTSiS 2006.

Wyrok TS z dnia 15 grudnia 1995 r., C-415/93, ECR 1995.

Wyrok TS z dnia 6 października 2020 r., C-511/18, LEX nr 3095381.

Wyrok TS z dnia 9 lipca 2020 r., C-272/19, LEX nr 3189121.

Wyrok TS z dnia 21 grudnia 2023 r., C-124/21 P, LEX nr 3688832.

Wyrok TS z dnia 21 grudnia 2023 r., C-333/21, LEX nr 3688831.

Wyrok TS z dnia 2 marca 2023 r., C-31/21, LEX nr 3500707.

Opinia Rzecznika Generalnego TS Deana Spielmanna w sprawie C-424/24.

Opinia Rzecznik Generalnej TS Tamary Ćapety w sprawie C-115/22.

INNE PUBLIKACJE

Agence française de lutte contre le dopage (AFDL) (Francuska Agencja Antydopingowa), Decyzje w sprawach antydopingowych https://www.afld.fr/decisions_disciplinaires/ [dostęp: 2.03.2026].

Exner J., *Putting Athletes in the Digital Pillory: Opinion of AG Spielmann in NADA Austria (C-474/24)* EU Law Live https://eulawlive.com/op-ed-putting-athletes-in-the-digital-pillory-opinion-of-ag-spielmann-in-nada-austria-c-474-24 [dostęp: 2.03.2026].

Komisja Europejska, *Data Protection*, https://commission.europa.eu/law/law-topic/data-protection_en#simplifying-compliance-with-the-gdpr-through-reduced-record-keeping-obligations [dostęp: 2.03.2026].

Komisja Europejska, *Digital Omnibus Regulation Proposal* https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal [dostęp: 2.03.2026].

Rada Europy, *World anti-doping code 2027 and international standards adopted in Busan* 2025

https://www.coe.int/en/web/portal/-/world-anti-doping-code-2027-and-international-standards-adopted-in-busan [dostęp: 2.03.2026].

ICAS, Stanowisko ICAS z 1 sierpnia 2025 r., https://www.tas-cas.org/generated/assets/lists/dceab111-07bc-435f-b5f9-de88eff9db72/ICAS_statement_CJEU_Seraing_ENG.pdf [dostęp: 2.03.2026].

Grupa Robocza Art. 29, Opinia nr 4/2009 Grupy Roboczej Art. 29 (Druga opinia 4/2009 w sprawie międzynarodowego standardu ochrony prywatności i danych osobowych Światowej Agencji Antydopingowej (WADA), powiązanych przepisów kodeksu WADA oraz innych kwestii związanych z ochroną prywatności w kontekście walki z dopingiem w sporcie prowadzonej przez WADA i (krajowe) organizacje antydopingowe), 2009 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp162_en.pdf [dostęp: 2.03.2026].

European Data Protection Board, *Recommendations 1/2025 on the 2027 WADA World Anti-Doping Code,* 2025) https://www.edpb.europa.eu/system/files/2025-02/edpb_recommendations_202501_wada_2027_world_anti-doping_code_en.pdf [dostęp: 2.03.2026].

NADO Italia, Przetwarzanie danych osobowych zawodników https://www.nadoitalia.it/en/athletes/rights-and-responsibilities/processing-of-personal-data.html [dostęp: 2.03.2026].

POLADA, *Przypadki naruszenia przepisów* https://antydoping.pl/kontrole/przypadki-naruszenia-przepisow/ [dostęp: 2.03.2026].

Swiss Sport Integrity (Szwajcarska Fundacja ds. Integralności w Sporcie), Lista zawieszonych sportowców,

https://www.sportintegrity.ch/en/anti-doping/laws/suspended-athletes [dostęp: 2.03.2026].

WADA, *Therapeutic Use Exemptions* (Wyłączenia w celu terapeutycznym) https://www.wada-ama.org/en/athletes-support-personnel/therapeutic-use-exemptions-tues [dostęp: 2.03.2026].

DATA PROTECTION ON THE STADIUM: GDPR AND THE PROTECTION OF PERSONAL DATA OF ATHLETES IN ANTI-DOPING CASES

Summary: EU data protection law permeates many areas of social life, exerting an influence on them. The article analyses the preliminary questions referred to the CJEU, considering where the line lies between the protection of athletes and the public interest, as well as the need to ensure the integrity of sport. It discusses the scope and status of athletes' data that are publicly available, particularly in cases involving breaches of anti-doping rules. The article also assesses the compatibility of current solutions with the requirements of EU law, referring to the Opinions of the Advocate General in Cases C-474/24 and C-115/22. It further proposes a model for the publication of data that balances the public interest in transparency in sport with athletes' rights to privacy and data protection

Keywords: GDPR; sports law; anti-doping law; protection of athletes; CJEU.

mgr **Kinga Parchem**
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej, Uniwersytet Wrocławski
parchemkinga@gmail.com
https://orcid.org/0009-0009-4275-0559

EUROPEJSKA PRZESTRZEŃ DANYCH O ZDROWIU (EHDS) A DYREKTYWA NIS 2 – WYZWANIA W ZAKRESIE CYBERBEZPIECZEŃSTWA DANYCH ZDROWOTNYCH

Streszczenie: Europejska Przestrzeń Danych o Zdrowiu (ang. *European Health Data Space*, dalej: EHDS) jest jednym z projektów Unii Europejskiej w ramach strategii budowy wspólnego rynku danych. Jej celem jest stworzenie bezpiecznego i interoperacyjnego środowiska umożliwiającego przetwarzanie oraz wtórne wykorzystanie danych zdrowotnych w całej Unii Europejskiej. Z uwagi na szczególny charakter tych danych, zapewnienie odpowiedniego poziomu cyberbezpieczeństwa stanowi jedno z głównych wyzwań prawnych i organizacyjnych wdrażania EHDS. W tym kontekście znaczenie zyskuje dyrektywa Unii Europejskiej 2022/2555 (dalej w tekście: NIS 2), która ustanawia wspólne ramy dla wysokiego poziomu bezpieczeństwa sieci i informacji w Unii Europejskiej. Dyrektywa rozszerza zakres regulacji na sektor ochrony zdrowia oraz nakłada na określone podmioty obowiązki w zakresie zarządzania ryzykiem, reagowania na incydenty i wdrażania środków technicznych oraz organizacyjnych. Wprowadzone rozwiązania mogą mieć zastosowanie do podmiotów uczestniczących w funkcjonowaniu EHDS, w tym organów odpowiedzialnych za dostęp do danych oraz instytucji przetwarzających dane zdrowotne w celach badawczych i analitycznych. Opracowanie rozdziału podejmuje analizę relacji pomiędzy EHDS a przepisami dyrektywy NIS 2 w kontekście budowy jednolitego standardu cyberbezpieczeństwa w sektorze danych zdrowotnych. Przedmiotem rozważań jest również problem harmonizacji przepisów krajowych w świetle NIS 2 oraz wpływ tej dyrektywy na kształtowanie praktyk bezpieczeństwa w infrastrukturze cyfrowej służącej do udostępniania i wtórnego wykorzystania danych zdrowotnych

Słowa kluczowe: Europejska Przestrzeń Danych o Zdrowiu (EHDS); NIS 2; cyberbezpieczeństwo; dane zdrowotne; wtórne wykorzystanie danych; prawo Unii Europejskiej.

WPROWADZENIE

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia („EHDS", „Rozporządzenie EHDS") to inicjatywa Unii Europejskiej mająca na celu stworzenie wspólnego rynku danych zdrowotnych poprzez bezpieczne i interoperacyjne środowisko wymiany informacji medycznych. EHDS przewiduje zarówno pierwotne wykorzystanie danych (dla opieki nad pacjentem), jak i wtórne wykorzystanie danych (dla badań naukowych, polityk zdrowotnych) na poziomie całej Unii Europejskiej[1]. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 („NIS 2") ustanawia z kolei ogólne ramy wysokiego poziomu bezpieczeństwa sieci i informacji w Unii Europejskiej, obejmując rozszerzony zakres sektorów, w tym sektor opieki zdrowotnej[2]. NIS 2 zastąpiła poprzednią dyrektywę NIS z 2016 r., wprowadzając jednolite wymagania cyberbezpieczeństwa dla szerokiego katalogu podmiotów kluczowych i ważnych we wszystkich państwach członkowskich.

Incydenty cybernetyczne w sektorze zdrowotnym mogą nie tylko naruszać prywatność pacjentów, ale wręcz zagrażać ich życiu i zdrowiu poprzez zakłócenie ciągłości opieki. W ostatnich latach obserwuje się wzrost ataków na infrastrukturę medyczną. W Polsce liczba incydentów w placówkach zdrowia wzrosła z 150 w 2021 r. do 1028 w 2024 r., a tylko w okresie styczeń - sierpień 2025 r. odnotowano 946 zdarzeń, więcej niż w całym 2023 r.[3]. Incydent w postaci ataku *ransomware* z maja 2021 r. na irlandzką służbę zdrowia („HSE"), który sparaliżował systemy informatyczne szpitali w całym kraju, czy marcowy cyberatak na szpital MSWiA w Krakowie w 2025 r., skutkujący czasowym wstrzymaniem działania systemu dokumentacji medycznej, unaoczniają skalę zagrożeń. Rozporządzenie EHDS, zostało pomyślane jako instrument integrujący dotychczas rozproszone mechanizmy obrotu danymi zdrowotnymi, w tym infrastrukturę MyHealth@EU dla pierwotnego użycia danych i HealthData@EU dla ich wtórnego wykorzystania. Nie ulega jednak wątpliwości, że powodzenie tej konstrukcji jest zależne od zapewnienia wysokiego poziomu cyberbezpieczeństwa.

W literaturze trafnie akcentuje się, że projekt EHDS od początku był obciążony napięciem pomiędzy ambicją szerokiego udostępniania danych a koniecznością

[1] European Commission, *European Health Data Space Regulation (EHDS). EC – Health – eHealth, Digital Health and Care* https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en [dostęp: 2.03.2026].

[2] KLM Law Poland, *What obligations does the NIS 2 Directive impose on the healthcare sector?* https://www.lexology.com/library/detail.aspx?g=5fab2347-45be-4378-beac-91c9f958abb1 [dostęp: 2.03.2026].

[3] M. Kośla, *Cyberataki na szpitale biją rekordy. Prawie 1000 incydentów w 2025 roku. Dlaczego to zagraża życiu pacjentów?* https://politykazdrowotna.com/artykul/cyberataki-na-szpitale-n2043097 [dostęp: 2.03.2026].

zachowania rygorystycznych gwarancji bezpieczeństwa. Robin van Kessel, Madeleine Haig i Elias Mossialos zwracają uwagę, że w pierwotnej konstrukcji EHDS zagadnienie cyberbezpieczeństwa pozostawało rozwinięte jedynie marginalnie, mimo że sektor ochrony zdrowia należy do najbardziej narażonych na incydenty cyfrowe i skutki tych incydentów wykraczają poza sferę czysto majątkową czy reputacyjną[4]. Z kolei Wenkai Li i Paul Quinn wskazują, że EHDS należy rozumieć jako jakościowe rozszerzenie prawa do przenoszalności danych, ale rozszerzenie to nie usuwa wszystkich wątpliwości na styku prawa ochrony danych, interoperacyjności i dopuszczalnych celów przetwarzania[5].

Z perspektywy dogmatycznej nie jest zatem wystarczające proste zestawienie EHDS z dyrektywą NIS 2. Konieczne jest ustalenie, w jakim zakresie oba akty pozostają względem siebie komplementarne, a w jakim nakładają na uczestników systemu zdrowotnego równoległe lub skumulowane obowiązki. Dlatego analizie poddano relacje między rozporządzeniem EHDS a wymogami dyrektywy NIS 2 w kontekście budowy jednolitych standardów cyberbezpieczeństwa dla danych zdrowotnych w Unii Europejskiej. Punktem wyjścia wydaje się być wyraźne doprecyzowanie dwóch pojęć, które w dyskursie dotyczącym EHDS bywają używane w sposób zbyt intuicyjny, a mianowicie: „cyberbezpieczeństwa" oraz „danych dotyczących zdrowia". W prawie Unii Europejskiej cyberbezpieczeństwo posiada legalną definicję zawartą w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych i uchylającego rozporządzenie (UE) nr 526/2013[6], zgodnie z którą oznacza ono: „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów i innych osób przed zagrożeniami cybernetycznymi". Definicja ta ma charakter funkcjonalny i celowy, ponieważ obejmuje zdolność instytucjonalną do zapobiegania incydentom, ich wykrywania, raportowania i odtwarzania funkcji systemów po zakłóceniu. W kontekście sektora zdrowotnego oznacza to, że cyberbezpieczeństwo musi być rozumiane jednocześnie jako: (i) poufność danych pacjentów, (ii) integralność dokumentacji medycznej i systemów diagnostycznych, (iii) dostępność i ciągłość świadczenia usług

[4] R. van Kessel, M. Haig, E. Mossialos, *Strengthening Cybersecurity for Patient Data Protection in Europe*, "Journal of Medical Internet Research", 25, 2023, s. 1-3.

[5] W. Li, P. Quinn, *The European Health Data Space: An expanded right to data portability?*, "Computer Law & Security Review" 52, 2024, s. 1, 12-15.

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm.), s. 15.

zdrowotnych. Ten ostatni wymiar jest w sektorze zdrowia szczególnie tkliwy, ponieważ zakłócenie działania systemu informatycznego szpitala może bezpośrednio zagrozić życiu i zdrowiu pacjentów, co odróżnia ten sektor od większości innych obszarów infrastruktury krytycznej. Doniosłość tego rozróżnienia potwierdza doktryna. Biasin, Yaşar i Kamenjašević trafnie wskazują, że pojęcie cyberbezpieczeństwa na gruncie prawa unijnego łączy komponent techniczny z komponentem organizacyjnym i zarządczym, a ryzyko fragmentacji regulacyjnej wynika właśnie z niedoszacowania wymiaru instytucjonalnego w stosunku do wymiaru technicznego[7]. Dane dotyczące zdrowia mają natomiast w prawie europejskim status danych szczególnej kategorii. Wynika to z art. 9 ust. 1 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 („RODO"), który co do zasady zakazuje przetwarzania danych ujawniających stan zdrowia, chyba że zachodzi jedna z przesłanek legalizujących wskazanych w art. 9 ust. 2 tego aktu. Szczególny status tej kategorii jest uzasadniony zarówno intensywnością ingerencji w sferę prywatności, jak i ryzykiem dyskryminacji, stygmatyzacji oraz nieodwracalnych konsekwencji społecznych lub zawodowych dla osoby, której dane dotyczą. W realiach sektora zdrowia do ochrony prywatności dołącza jeszcze drugi wymiar, tj. naruszenie bezpieczeństwa danych medycznych, które może zakłócić proces diagnostyczny, leczenie, dystrybucję leków czy funkcjonowanie oddziałów ratunkowych. W tym znaczeniu ochrona danych zdrowotnych ma charakter jednocześnie osobowy i systemowy.

Nieprzypadkowo zatem EHDS opiera się na konstrukcji zaufanego środowiska wymiany danych, a prawodawca unijny odchodzi od prostego modelu, który można sprowadzić do „udostępnienia pliku" na rzecz modelu kontrolowanego dostępu, prowadzonego w bezpiecznych środowiskach przetwarzania. Richard Rak trafnie wskazuje, że problem prawny nie sprowadza się wyłącznie do pytania, czy dane mają zostać zanonimizowane albo spseudonimizowane, lecz dotyczy także tego, czy sposób ich udostępnienia pozostaje zgodny z zasadą minimalizacji, ograniczenia celu i odpowiednich zabezpieczeń organizacyjnych, bez których wtórne wykorzystywanie danych w ramach EHDS może prowadzić do fragmentacji praktyk i wzrostu ryzyka dla osób, których dane dotyczą[8].

---

[7] E. Biasin, B. Yaşar, E. Kamenjašević, *New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act*, "Law, Technology and Humans" 5(2), 2023, s. 49-51.

[8] R. Rak, *Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)*, "European Journal of Risk Regulation", 15(4), 2024, s. 928-931. DOI: https://doi.org/10.1017/err.2024.67.

1. EUROPEJSKA PRZESTRZEŃ DANYCH O ZDROWIU – ZAŁOŻENIA I STATUS PRAWNY

EHDS jest projektem w ramach unijnej strategii danych, tworząc pierwszą wspólną przestrzeń danych dedykowaną sektorowi zdrowia. Celem rozporządzenia EHDS jest ustanowienie zharmonizowanych zasad korzystania z danych zdrowotnych i ich wymiany transgranicznej, z korzyścią dla pacjentów, systemów ochrony zdrowia, badań i innowacji. Rozporządzenie pozwoli pacjentom na dostęp do własnej dokumentacji medycznej i kontrolę nad nią (w tym udostępnianie lekarzom, także za granicą), a jednocześnie stworzy podstawy prawne dla udostępniania zanonimizowanych danych w celach wtórnych (np. prace badawcze, tworzenie nowych terapii). Projekt rozporządzenia EHDS został przedstawiony przez Komisję Europejską w marcu 2022 r. i po negocjacjach został formalnie przyjęty na początku 2025 r. Akt opublikowano w Dzienniku Urzędowym Unii Europejskiej 5 marca 2025 r., a Rozporządzenie (UE) 2025/327 ustanawiające EHDS weszło w życie 26 marca 2025 r. Zastosowanie większości przepisów będzie jednak odroczone w czasie. Rozporządzenie przewiduje kilkuletni okres przejściowy na wdrożenie rozwiązań technicznych i organizacyjnych. Obowiązki będą stopniowo wchodzić w życie, tj. po dwóch latach od wejścia w życie zaczną funkcjonować instytucje i mechanizmy przewidziane dla pierwotnego wykorzystania danych, zaś przepisy dotyczące wtórnego wykorzystania danych znajdą pełne zastosowanie po czterech latach, z pewnymi wyjątkami wydłużonymi do sześciu lat dla najwrażliwszych kategorii informacji (m.in. dane genomiczne czy z badań klinicznych). Tak długi horyzont czasowy wynika z kompleksowości projektu EHDS, tj. implementacja będzie stopniowa i wymaga licznych aktów wykonawczych oraz dostosowania infrastruktury w państwach członkowskich. Rozporządzenie opiera się na trzech filarach: (1) wzmocnienie praw pacjentów poprzez zapewnienie im pełnego dostępu do elektronicznych danych zdrowotnych i kontroli nad nimi (w tym prawo wprowadzania ograniczeń dostępu, korygowania informacji, a nawet całkowitego *opt-out* z systemu wymiany danych); (2) rozwój jednolitego rynku usług e-zdrowia poprzez ustanowienie europejskich standardów interoperacyjności dla systemów elektronicznej dokumentacji medycznej („EHR") i aplikacji zdrowotnych, tak aby dane mogły płynnie przepływać między systemami i państwami członkowskimi; (3) bezpieczne i efektywne wtórne wykorzystanie danych zdrowotnych, dzięki stworzeniu mechanizmów prawnych i technicznych umożliwiających udostępnianie zanonimizowanych lub pseudonimizowanych danych do celów badań naukowych, innowacji, ochrony zdrowia publicznego czy

tworzenia polityk, przy zachowaniu gwarancji ochrony prywatności[9]. Każde państwo członkowskie będzie zobowiązane wyznaczyć instytucje wspierające funkcjonowanie EHDS. Dla pierwotnego wykorzystania danych państwa muszą powołać organ ds. cyfrowego zdrowia (ang. *digital health authority*), który będzie koordynować wymianę danych (np. poprzez infrastrukturę MyHealth@EU dla e-recept, kart informacyjnych, wyników badań). Dla wtórnego wykorzystania danych każde państwo musi ustanowić tzw. organ dostępu do danych zdrowotnych (ang. *Health Data Access Body*, „HDAB") jego zadaniem będzie wydawanie zezwoleń na dostęp do danych dla celów wtórnych i udostępnianie tych danych uprawnionym podmiotom. Termin wyznaczenia HDAB oscyluje na dwa lata od wejścia w życie rozporządzenia, a organ powinien osiągnąć pełną operacyjność w ciągu czterech lat. W strukturze europejskiej przewidziano utworzenie Rady EHDS z przedstawicielami wszystkich państw (organów cyfrowego zdrowia i HDAB), koordynującej jednolite stosowanie przepisów i wymianę dobrych praktyk w całej Unii Europejskiej. Ze względu na szczególnie wrażliwy charakter danych medycznych, rozporządzenie EHDS opiera się na istniejących przepisach horyzontalnych, tj. m.in. na RODO, rozporządzenie w sprawie europejskiego zarządzania danymi („DGA")[10] oraz dyrektywie NIS 2, które zawierają pewne wymogi dotyczące ochrony danych i bezpieczeństwa w sektorze zdrowia. Jednocześnie jednak EHDS wprowadza dodatkowe, sektorowo ukierunkowane środki uwzględniające dane o zdrowiu. Przykładowo, dane udostępniane do celów wtórnych będą mogły być przetwarzane wyłącznie w zamkniętych, bezpiecznych środowiskach informatycznych zapewnianych przez organy dostępu do danych, spełniających ściśle określone standardy cyberbezpieczeństwa. Rozporządzenie wymaga też certyfikacji i zgodności z normami bezpieczeństwa dla systemów EHR i tzw. *wellness applications*, zanim zostaną one wprowadzone na rynek.

Z perspektywy prawnej kluczowe znaczenie ma relacja między pojęciem *trusted environment* (bezpiecznego środowiska przetwarzania) w rozumieniu art. 73 rozporządzenia EHDS a ogólnymi wymogami zarządzania ryzykiem wynikającymi z art. 21 dyrektywy NIS 2. Artykuł 73 EHDS nakłada na organy dostępu do danych zdrowotnych obowiązek udostępniania danych w środowiskach zapewniających, że dane nie opuszczają kontrolowanej infrastruktury w formie umożliwiającej identyfikację osób fizycznych. Oznacza to w praktyce konieczność stosowania mechanizmów

[9] European Commission, *European Health Data Space Regulation (EHDS). EC – Health – eHealth, Digital Health and Care* https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en [dostęp: 2.03.2026].

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz. U. UE. L. z 2022 r. Nr 152, str. 1 z późn. zm.)

takich jak szyfrowanie end-to-end, kontrola dostępu oparta na rolach (ang. *role-based access control*), pełny audyt operacji na danych oraz systemy zapobiegające wyciekowi informacji (ang. *data loss prevention*). Wymogi te nie są tożsame z obowiązkami wynikającymi z art. 21 NIS 2, który koncentruje się na ryzyku incydentów dla sieci i systemów informacyjnych, a nie na kontroli przepływu danych *per se*. Oznacza to, że podmioty uczestniczące w EHDS muszą spełnić łącznie oba zestawy wymagań: ogólny standard odporności cybernetycznej z NIS 2 oraz sektorowy standard kontroli dostępu i izolacji danych z EHDS. W tym znaczeniu EHDS nie zastępuje dyrektywy NIS 2, lecz nakłada na te same podmioty dodatkową warstwę obowiązków sektorowych, czego konsekwencją jest skumulowanie, a nie zharmonizowanie wymogów. W efekcie EHDS tworzy zaufane środowisko przetwarzania informacji zdrowotnych, co stanowi warunek niezbędny, by obywatele i podmioty medyczne chciały dzielić się danymi na skalę ogólnounijną[11]. Jednocześnie wprowadza dodatkowe, sektorowo ukierunkowane środki uwzględniające dane o zdrowiu. Przykładowo, dane udostępniane do celów wtórnych będą mogły być przetwarzane wyłącznie w zamkniętych, bezpiecznych środowiskach informatycznych zapewnianych przez organy dostępu do danych, spełniających ściśle określone standardy cyberbezpieczeństwa. Rozporządzenie wymaga też certyfikacji i zgodności z normami bezpieczeństwa dla systemów EHR i tzw. *wellness applications*, zanim zostaną one wprowadzone na rynek. Ma to zagwarantować spełnienie minimalnych wymagań z zakresu interoperacyjności i ochrony danych. EHDS należy zatem odczytywać nie jako regulację autonomiczną, lecz jako akt osadzony w szerszym systemie prawa danych. Hussein i współautorzy zauważają, że architektura EHDS została zbudowana na fundamencie RODO, aktu o zarządzaniu danymi, aktu w sprawie danych, przepisów o wyrobach medycznych, a także dyrektywy NIS 2 i AI Act, co oznacza, że efektywne wdrożenie EHDS wymaga równoczesnego zapewnienia interoperacyjności technicznej, zgodności semantycznej, przejrzystości procesów dostępu oraz bezpieczeństwa organizacyjnego[12]. Takie ujęcie zasługuje na aprobatę, ponieważ sektor zdrowia nie funkcjonuje w izolacji od systemów sztucznej inteligencji, chmury obliczeniowej, czy oprogramowania wspomagającego decyzje kliniczne. Zabezpieczenia przewidziane przez EHDS mają charakter wyraźnie sektorowy. Należą do nich w szczególności: wymóg stosowania bezpiecznych środowisk przetwarzania dla wtórnego użycia danych; wymogi interoperacyjności i zgodności dla systemów EHR; szczególna pozycja organów dostępu

[11] R. Rak, *Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)*, "European Journal of Risk Regulation", 15(4), 2024, s. 928-931. DOI: https://doi.org/10.1017/err.2024.67.

[12] R. Hussein, A. Gyrard, S. Abedian, *Interoperability Framework of the European Health Data Space for the Secondary Use of Data*, "Journal of Medical Internet Research", 27, 2025, s. 2-4.

do danych zdrowotnych; ograniczenie katalogu celów wtórnego wykorzystania; mechanizmy kontroli dostępu i identyfikowalności operacji wykonywanych na danych; a także instrumenty nadzorcze i sankcyjne wobec użytkowników danych lub posiadaczy danych naruszających obowiązki wynikające z rozporządzenia. W tym sensie EHDS nie zastępuje NIS 2, lecz doszczegóławia bezpieczeństwo w tych punktach, w których ogólne wymogi cyberbezpieczeństwa muszą zostać przystosowane do wyjątkowo wrażliwego charakteru danych zdrowotnych.

Na szczególną uwagę zasługuje też powiązanie EHDS z problematyką certyfikacji i bezpieczeństwa produktów cyfrowych używanych w ochronie zdrowia. Federica Casarosa trafnie zwraca uwagę, że model oparty na certyfikacji systemów EHR (*Electronic Health Records*) i aplikacji interoperacyjnych może wzmacniać zaufanie do obrotu danymi, ale tylko pod warunkiem, że kryteria zgodności będą obejmowały nie jedynie interoperacyjność formalną, lecz również realne wymagania cyberbezpieczeństwa i aktualności produktów przez cały okres ich używania[13].

2. DYREKTYWA NIS 2 I JEJ ZNACZENIE DLA SEKTORA OCHRONY ZDROWIA

Dyrektywa NIS 2 obejmuje szerokie spektrum sektorów kluczowych dla funkcjonowania społeczeństwa i gospodarki. W miejsce dawnej klasyfikacji operatorów usług kluczowych i dostawców usług cyfrowych, dyrektywa NIS 2 wprowadza kategorie sektorów o wysokiej krytyczności oraz innych sektorów krytycznych. Ochrona zdrowia została *expressis verbis* uznana za sektor o wysokiej krytyczności (obok m.in. energetyki, transportu, bankowości), co oznacza objęcie podmiotów działających w tym obszarze surowszymi wymogami bezpieczeństwa i nadzorem. W praktyce dyrektywa dotyczy nie tylko szpitali. Jako podmioty kluczowe traktowani będą również producenci farmaceutyków, laboratoria, a nawet podmioty prowadzące badania naukowe w dziedzinie zdrowia. Należy jednak zaznaczyć, że już wcześniejsza dyrektywa 2016/1148 obejmowała ochronę zdrowia w ramach operatorów usług kluczowych. NIS 2 nie tyle definiuje na nowo sektora zdrowia jako obszaru krytycznego, ile znacząco wzmacnia obowiązki, rozszerza krąg podmiotów i harmonizuje reżim nadzorczy. Kryterium formalnym podlegania dyrektywy NIS 2 jest co do zasady skala organizacji (co najmniej 50 pracowników lub obrót powyżej 10 mln Euro). Państwa członkowskie mają obowiązek objąć wymogami także mniejsze jednostki, jeśli są istotne systemowo. Dyrektywa NIS 2 nakłada na podmioty z sektora zdrowotnego (podobnie jak na inne podmioty krytyczne) rozbudowane obowiązki w zakresie

[13] F. Casarosa, *European Health Data Space – Is the Proposed Certification System Effective against Cyber Threats?*, "European Journal of Risk Regulation", 15(4), 2024, s. 939-945.

wdrożenia środków technicznych i organizacyjnych służących zarządzaniu ryzykiem cyberbezpieczeństwa (art. 21 NIS 2). Podejście jest zorientowane na ryzyko. Przepisy nie wskazują konkretnych technologii, które miałyby zastosowanie, lecz zobowiązują organizacje do przeprowadzenia własnej analizy ryzyka i zastosowania odpowiednich środków proporcjonalnych do zidentyfikowanych zagrożeń. Dyrektywa enumeratywnie wymienia obszary, które taka analiza i środki powinny obejmować, to jest między innymi: polityki bezpieczeństwa informacji i procedury, zarządzanie zasobami ludzkimi - świadomość pracowników i szkolenia z cyberbezpieczeństwa, kontrola dostępu i uprawnień (czynnik ludzki jest często najsłabszym ogniwem bezpieczeństwa); środki techniczne - zabezpieczenia systemów i sieci (zapory, systemy wykrywania włamań, szyfrowanie danych w spoczynku i w tranzycie), bezpieczeństwo łańcucha dostaw (weryfikacja dostawców technologii pod kątem podatności, zgodności z normami), zabezpieczenie kanałów komunikacji (w tym komunikacji głosowej i tekstowej) oraz planów awaryjnych na wypadek incydentu; zarządzanie ciągłością działania - opracowanie planów reagowania na incydenty i utrzymania (lub szybkiego wznowienia) krytycznych usług zdrowotnych w przypadku cyberataku; regularne tworzenie kopii zapasowych i testowanie ich odtwarzania. Analiza incydentów i uczenie się na błędach w tym mechanizmy raportowania wewnętrznego incydentów, przeglądy poawaryjne i wdrażanie ulepszeń mając zapobiegać atakom.

W ocenie Schmitz-Berndt[14], problemem praktycznym może być ocena, czy dany incydent rzeczywiście spełnia kryteria znaczącego wpływu na usługę kluczową, co warunkuje obowiązek raportowy. NIS 2 wprowadza zatem wymóg wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z uznanymi standardami (jak ISO/IEC 27001). Celem NIS 2 jest ustanowienie jednolitego systemu notyfikacji incydentów cyberbezpieczeństwa. Podmioty kluczowe takie jak szpitale będą musiały zgłaszać poważne incydenty właściwym organom lub Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego („CSIRT") najpóźniej w ciągu 24 godzin od wykrycia (informacja wstępna), a pełny raport incydentalny w ciągu 72 godzin. Dodatkowo wymagane może być przekazanie w terminie do miesiąca końcowego raportu z analizą incydentu i podjętymi działaniami naprawczymi. Ma to prowadzić nie tylko do szybkiej reakcji (mobilizacja pomocy, ostrzeżenie innych), ale też do gromadzenia wiedzy o zagrożeniach i trendach. W kontekście danych zdrowotnych obowiązek notyfikacji incydentów wynikający z dyrektywy NIS 2 krzyżuje się z już istniejącym obowiązkiem zgłaszania naruszeń ochrony danych osobowych na gruncie art. 33 RODO. Zbieg ten wymaga szczegółowej analizy, ponieważ oba

[14] S. Schmitz-Berndt, *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, "Journal of Cybersecurity" 9(1), 2023, s. 2.

reżimy posługują się odmiennymi progami istotności, różnymi adresatami notyfikacji oraz odrębnymi terminami. Na gruncie art. 33 RODO podmiot przetwarzający dane zobowiązany jest zgłosić naruszenie do organu nadzorczego (w Polsce: Prezesa Urzędu Ochrony Danych Osobowych, „Prezes UODO") „w miarę możliwości, nie później niż w terminie 72 godzin" od chwili stwierdzenia naruszenia, jeżeli jest prawdopodobne, że naruszenie to spowoduje ryzyko naruszenia praw lub wolności osób fizycznych. Na gruncie art. 23 ust. 1 dyrektywy NIS 2 podmiot kluczowy lub ważny jest natomiast zobowiązany do przesłania wczesnego ostrzeżenia do właściwego CSIRT lub organu właściwego w ciągu 24 godzin od powzięcia wiadomości o istotnym incydencie, a następnie pełnego zgłoszenia w ciągu 72 godzin. Progi te są zatem liczone od różnych zdarzeń (stwierdzenie naruszenia na gruncie RODO vs. powzięcie wiadomości o incydencie na gruncie NIS 2) i kierowane do różnych organów. Jak słusznie wskazuje Schmitz-Berndt, ustalenie, czy dany incydent „znacząco wpływa" na świadczenie usługi kluczowej w rozumieniu NIS 2, jest zadaniem znacznie trudniejszym niż ocena ryzyka naruszenia praw jednostki w reżimie RODO, ponieważ wymaga uwzględnienia m.in. liczby dotkniętych użytkowników, czasu trwania zakłócenia oraz zasięgu geograficznego - kryteriów, które Komisja Europejska doprecyzowuje w aktach wykonawczych[15]. W praktyce oznacza to, że podmiot leczniczy, który stał się ofiarą ataku typu ransomware blokującego dostęp do elektronicznych kart pacjentów, musi niemal równocześnie: (i) ocenić ryzyko naruszenia praw pacjentów i zdecydować o notyfikacji do Prezesa UODO; (ii) ocenić, czy incydent spełnia kryteria istotności z NIS 2 i przesłać wczesne ostrzeżenie do CSIRT CeZ; (iii) rozważyć, czy konieczne jest poinformowanie samych pacjentów na podstawie art. 34 RODO. Właśnie dlatego organizacje medyczne powinny konstruować jednolite, zintegrowane procedury reagowania na incydenty, które obejmują jednocześnie ścieżkę ochrony danych i ścieżkę cyberbezpieczeństwa, a nie dwa odrębne, niekompatybilne tryby postępowania. Egzemplifikacją konsekwencji braku takich procedur jest sprawa Szpitala Powiatowego we Wrześni, który został ukarany przez Prezesa UODO karą pieniężną za opóźnienie zgłoszenia wycieku danych medycznych pacjentki. Personel nie powiadomił na czas organu nadzorczego[16], co uznano za naruszenie obowiązków z art. 33 RODO. Dyrektywa NIS 2 wprowadza w analogicznych sytuacjach dodatkowy reżim raportowania do struktur cyberbezpieczeństwa, co z jednej strony wzmacnia ochronę systemową, z drugiej zaś znacząco zwiększa ciężar administracyjny podmiotów leczniczych w sytuacjach kryzysowych.Dyrektywa NIS 2 wzmacnia kompetencje organów krajowych ds. cyberbezpieczeństwa w zakresie

[15] *Ibidem*, s. 3-7.
[16] Decyzja Prezesa UODO z dnia 26 listopada 2024 r., DKN.5131.6.2024, LEX nr 3790660.

nadzoru nad podmiotami kluczowymi i ważnymi. W polskim porządku prawnym, na gruncie znowelizowanej ustawy o u.k.s.c., konieczne jest rozróżnienie dwóch odrębnych funkcji. Po pierwsze, funkcję organu właściwego ds. cyberbezpieczeństwa dla sektora ochrony zdrowia pełni minister właściwy do spraw zdrowia (art. 41 pkt 5 ustawy o u.k.s.c. w dotychczasowym brzmieniu; dla podsektora produkcji wyrobów medycznych - art. 41 pkt 9g w brzmieniu nadanym nowelizacją z 2026 r.), który jest uprawniony do sprawowania nadzoru, wydawania decyzji administracyjnych i nakładania kar. Po drugie, funkcję CSIRT sektorowego dla podmiotów z sektora zdrowia pełni CSIRT CeZ, działający w strukturach Centrum e-Zdrowia. Jest to organ o kompetencjach operacyjnych i doradczych (obsługa incydentów, ostrzeganie, koordynacja), a nie nadzorczych w rozumieniu administracyjnoprawnym. Pomieszanie tych dwóch funkcji prowadzi do istotnych błędów w rozumieniu systemu odpowiedzialności za cyberbezpieczeństwo sektora zdrowotnego. Rolę koordynacyjną na poziomie krajowym pełni natomiast Pełnomocnik Rządu ds. Cyberbezpieczeństwa. Swoistym *novum* jest nałożenie osobistej odpowiedzialności członków kierownictwa za przestrzeganie wymogów cyberbezpieczeństwa. Kadra zarządzająca będzie miała obowiązek podjąć się specjalistycznych szkoleń, a za zaniedbania w nadzorze nad bezpieczeństwem obwarowane będą sankcjami. Dyrektywa NIS 2 wprowadza kary administracyjne za nieprzestrzeganie przepisów dla podmiotów kluczowych. Maksymalna wysokość kary to co najmniej 10 milionów euro lub 2% całkowitego rocznego światowego obrotu. Warto również zaznaczyć, że w praktyce incydent w sektorze zdrowia często uruchamia równolegle obowiązki wynikające z co najmniej trzech reżimów prawnych: RODO, NIS 2 oraz przepisów sektorowych dotyczących dokumentacji medycznej i ciągłości udzielania świadczeń. Wyciek danych pacjentów, zaszyfrowanie bazy przez ransomware lub zakłócenie pracy systemu laboratoryjnego może jednocześnie stanowić naruszenie ochrony danych osobowych, istotny incydent cyberbezpieczeństwa oraz zdarzenie zagrażające ciągłości działalności leczniczej. Właśnie dlatego organizacje medyczne powinny konstruować jednolite procedury reagowania, a nie odrębne, niekompatybilne ścieżki dla ochrony danych i dla cyberbezpieczeństwa.

Zasadniczym aktem implementującym dyrektywę NIS 2 do polskiego porządku prawnego jest ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. z 2026 r. poz. 252). Regulacja ta w sposób szczególny zajęła sektor ochrony zdrowia, wprowadzając mechanizmy, które wymagają szerszego komentarza w kontekście przetwarzania danych zdrowotnych.

Znowelizowany art. 5 ust. 8 u.k.s.c.[17] przesądza, że podmiot leczniczy w rozumieniu art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2026 r. poz. 156), który nie jest przedsiębiorcą, zalicza się do podmiotów ważnych, jeżeli zatrudnia od 50 do 249 osób, albo do podmiotów kluczowych, gdy zatrudnia co najmniej 250 osób. Ustawodawca odszedł tym samym z dotychczasowego modelu wyznaczania operatorów usług kluczowych w drodze indywidualnych decyzji administracyjnych na rzecz mechanizmu samookreślenia opartego na obiektywnym kryterium zatrudnienia. Z perspektywy ochrony danych zdrowotnych doniosłość tej zmiany trudno przecenić. Oznacza ona, że każdy szpital wielooddziałowy, a więc podmiot przetwarzający z natury rzeczy szczególnie wrażliwe dane jest z mocy prawa objęty pełnym reżimem ustawy o u.k.s.c., bez względu na to, czy organ właściwy podjął w jego sprawie jakiekolwiek działania.

Istotę regulacji materialnoprawnej stanowi art. 8 u.k.s.c. w brzmieniu nadanym nowelizacją. Przepis ten nakłada na podmioty kluczowe i ważne obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi. Katalog wymaganych środków technicznych i organizacyjnych jest rozbudowany i precyzyjny: obejmuje polityki szacowania ryzyka i bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne (art. 8 ust. 1 pkt 2 lit. a u.k.s.c.), bezpieczeństwo i ciągłość łańcucha dostaw produktów oraz usług ICT z uwzględnieniem relacji z bezpośrednimi dostawcami sprzętu i oprogramowania (art. 8 ust. 1 pkt 2 lit. e u.k.s.c.), wdrożenie i testowanie planów ciągłości działania oraz planów odtworzenia po zdarzeniu powodującym straty przekraczające możliwości samodzielnej odbudowy przez podmiot (art. 8 ust. 1 pkt 2 lit. f u.k.s.c.), monitorowanie systemu informacyjnego w trybie ciągłym (lit. g u.k.s.c.), polityki i procedury stosowania kryptografii, w tym szyfrowania (art. 8 ust. 1 pkt 2 lit. k u.k.s.c.), stosowanie bezpiecznych środków komunikacji z uwierzytelnianiem wieloskładnikowym (art. 8 ust. 1 pkt 2 lit. l u.k.s.c.) oraz polityki kontroli dostępu (lit. n u.k.s.c.). Dopełnieniem jest art. 8 ust. 2 u.k.s.c., zobowiązujący podmiot do uwzględnienia przy wdrażaniu środków dotyczących łańcucha dostaw wyników skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę Współpracy, o której mowa w art. 22 ust. 1 dyrektywy NIS 2, co spaja regulację krajową z mechanizmami unijnymi.

Artykuł 8c ust. 1 u.k.s.c. ustanawia zaś zasadę osobistej odpowiedzialności kierownika podmiotu kluczowego lub ważnego za wykonywanie obowiązków cyberbezpieczeństwa, przy czym, co ustawodawca zaznacza w ust. 3 tego artykułu,

[17] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.) („u.k.s.c.").

odpowiedzialność ta nie wygasa z chwilą powierzenia zadań innej osobie. W przypadku organu wieloosobowego, gdy nie wskazano osoby odpowiedzialnej, odpowiadają wszyscy jego członkowie solidarnie (art. 8c ust. 2 u.k.s.c.). Artykuł 8d u.k.s.c. uszczegóławia zakres tej odpowiedzialności: kierownik podejmuje decyzje dotyczące przygotowania, wdrażania i nadzoru systemu zarządzania bezpieczeństwem informacji (art. 8d pkt 1 u.k.s.c.), planuje adekwatne środki finansowe na realizację obowiązków (art. 8d pkt 2 u.k.s.c.), przydziela zadania z zakresu cyberbezpieczeństwa i nadzoruje ich wykonanie (art. 8d pkt 3 u.k.s.c.) oraz zapewnia, że personel jest świadomy obowiązków i zna wewnętrzne regulacje (art. 8d pkt 4 u.k.s.c.). Dla zarządów i dyrektorów podmiotów leczniczych oznacza to radykalną zmianę pozycji prawnej: cyberbezpieczeństwo przestaje być sprawą działu IT, stając się elementem osobistej odpowiedzialności kierownictwa – analogiczną do odpowiedzialności za zapewnienie zgodności z RODO, wynikającej z art. 5 ust. 2 RODO w zw. z art. 24 RODO. Artykuł 8e u.k.s.c. uzupełnia ten mechanizm, wprowadzając obowiązek corocznego szkolenia kierownika podmiotu w zakresie obowiązków cyberbezpieczeństwa, udokumentowanego stosownym zaświadczeniem.

Odrębnego omówienia wymaga art. 10 u.k.s.c. regulujący dokumentację bezpieczeństwa systemu informacyjnego. Przepis ten nakłada na podmioty lecznicze obowiązek opracowania, stosowania i aktualizowania dokumentacji normatywnej, na którą składają się: dokumentacja systemu zarządzania bezpieczeństwem informacji, dokumentacja ochrony infrastruktury obejmująca ocenę aktualnego stanu ochrony, szacowanie ryzyka dla obiektów infrastruktury i plan postępowania z ryzykiem (art. 10 ust. 3 pkt 2 lit. b-d u.k.s.c.), a także dokumentacja systemu zarządzania ciągłością działania (art. 10 ust. 3 pkt 3 u.k.s.c.). Dokumentacja przechowywana jest przez co najmniej dwa lata od jej wycofania z użytkowania lub zakończenia świadczenia usługi. Jej znaczenie wykracza poza wymogi u.k.s.c.: stanowi materialne odzwierciedlenie zasady rozliczalności z art. 5 ust. 2 RODO i może być kluczowym dowodem w postępowaniach nadzorczych prowadzonych zarówno przez organ właściwy ds. cyberbezpieczeństwa, jak i przez Prezesa UODO. Warto nadmienić, że art. 8a u.k.s.c. legitymuje Radę Ministrów do wydania rozporządzenia określającego, odrębnie dla poszczególnych rodzajów działalności podmiotów kluczowych i ważnych, szczegółowych wymagań dla systemu zarządzania bezpieczeństwem informacji, z uwzględnieniem rekomendacji ENISA. Przepis ten może w przyszłości stanowić podstawę do opracowania sektorowych standardów cyberbezpieczeństwa adresowanych wprost podmiotom leczniczym, co byłoby szczególnie istotne w kontekście infrastruktury tworzonej na potrzeby rozporządzenia EHDS. Organem właściwym ds. cyberbezpieczeństwa dla podsektora produkcji wyrobów medycznych i wyrobów

medycznych do diagnostyki *in vitro* jest minister właściwy do spraw zdrowia (art. 41 pkt 9g u.k.s.c.), co potwierdza rolę tego organu jako centralnego regulatora sektora w obszarze cyberbezpieczeństwa.

3. RELACJA MIĘDZY EHDS A NIS 2

EHDS i NIS 2 działają na odrębnych płaszczyznach, ale ich zakresy nakładają się w obszarze cyberbezpieczeństwa infrastruktury zdrowotnej. NIS 2 to regulacja horyzontalna, która ustanawia wspólne wymogi bezpieczeństwa dla wszystkich kluczowych sektorów (w tym zdrowia) i tworzy ogólnounijny minimalny standard odporności cyfrowej. EHDS natomiast jest regulacją sektorową, skupioną na specyfice przetwarzania danych zdrowotnych i zapewniającą podstawy prawne dla udostępniania tych danych. Obie inicjatywy wzajemnie się uzupełniają: EHDS wymaga bezpiecznych systemów i zaufania użytkowników, co gwarantować mają wymogi NIS 2; z kolei NIS 2 wskazuje cele i środki bezpieczeństwa, które w sektorze zdrowotnym muszą zostać wdrożone po to, aby projekt wymiany danych jak EHDS mógł funkcjonować bez narażania pacjentów i zaufania do organów publicznych działających w tym sektorze. Już w fazie projektowania EHDS uwzględniono kontekst istniejących regulacji. EHDS czerpie z RODO, DGA, Data Act i dyrektywy NIS te akty prawne zapewniają podstawowe zasady, do których zaliczyć można ochronę danych osobowych czy minimalne środki bezpieczeństwa, które również odnoszą się do sektora zdrowia. Rozporządzenie EHDS pozostaje spójne z NIS 2 i innymi aktami. W praktyce może oznaczać to, że podmioty uczestniczące w EHDS będą podlegać zarówno wymaganiom sektorowym EHDS, jak i ogólnym obowiązkom przewidzianym w NIS 2. W kontekście danych zdrowotnych funkcjonują także inne akty horyzontalne, które mają wpływ na bezpieczeństwo ich przetwarzania. Poza NIS 2 i RODO warto wspomnieć Akt o cyberodporności („CRA")[18] rozporządzenie ustanawiające wymogi cyberbezpieczeństwa dla urządzeń i oprogramowania (co obejmie m.in. wyroby medyczne IoT i aplikacje zdrowotne). Dyrektywa CER[19] o odporności podmiotów krytycznych z kolei uzupełnia NIS 2 o aspekty fizycznej infrastruktury, który wymaga, by szpitale jako podmioty krytyczne posiadały plany ciągłości działania obejmujące również scenariusze awarii technicznej czy braku zasilania.

[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm.).

[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. U. UE. L. z 2022 r. Nr 333).

Regulacje sektorowe w ochronie zdrowia obejmują natomiast m.in. przepisy o tajemnicy medycznej, krajowe standardy teleinformatyczne czy wytyczne sieci e-zdrowia (*eHealth Network*) dotyczące c wymiany e-recept. Wszystkie te akty muszą być stosowane spójnie. Zwraca się uwagę, że propozycja EHDS nie zapewnia jeszcze wystarczających środków dla utworzenia odpornego i bezpiecznego środowiska cyfrowego – co rodzi obawy co do bezpieczeństwa pacjentów[20]. EHDS będzie rozporządzeniem bezpośrednio obowiązującym, które nie deroguje jednak obowiązków wynikających z NIS 2 czy RODO. W sytuacji, gdy badacz uzyska dostęp do danych w ramach EHDS, organ dostępu do danych będzie musiał zapewnić, że dostęp ten odbywa się w zgodzie z zasadami bezpieczeństwa (kontrola tożsamości, monitoring operacji na danych, zabezpieczenie przed wyniesieniem danych poza środowisko) co wynika z przepisów EHDS, ale wpisuje się również w ogólne obowiązki zapewnienia poufności i integralności systemów zgodnie z NIS 2 i RODO (art. 32 RODO). Jak zauważają Li i Quinn[21], EHDS znacząco rozszerza prawo do przenoszalności danych zawarte już w RODO, zwłaszcza dla danych w EHR przez narzucenie interoperacyjnych formatów i wspólnych standardów technicznych. Podsumowując, w EHDS zasadniczym przedmiotem regulacji jest dopuszczalność i organizacja udostępniania danych, a więc pytanie: „komu, w jakim celu i w jakiej formie dane zdrowotne mogą zostać udostępnione". W dyrektywie NIS 2 natomiast centralne pytanie brzmi: „jak podmiot ma zorganizować swoje sieci i systemy oraz procedury, aby ryzyko incydentu ograniczyć do poziomu akceptowalnego i zapewnić zdolność szybkiej reakcji?". To rozróżnienie jest istotne także metodologicznie. Błąd interpretacyjny polegałby na oczekiwaniu, że EHDS samodzielnie rozstrzygnie kwestie typowe dla cyberbezpieczeństwa infrastrukturalnego, albo odwrotnie że NIS 2 rozstrzygnie dopuszczalność wtórnego wykorzystania danych zdrowotnych.

Z doktrynalnego punktu widzenia trafna jest teza, iż EHDS stanowi *lex specialis* względem ogólnych zasad obrotu danymi zdrowotnymi, lecz nie względem całego reżimu cyberbezpieczeństwa. To zaś oznacza konieczność stosowania wykładni systemowej i funkcjonalnej. Normy EHDS należy interpretować w świetle obowiązków bezpieczeństwa wynikających z NIS 2 i RODO, natomiast obowiązki z NIS 2 z uwzględnieniem tego, że w sektorze zdrowia skutek incydentu ocenia się również przez pryzmat bezpieczeństwa pacjenta i ochrony praw podstawowych. Tak rozumiana wykładnia sprzyja spójności prawa i przeciwdziała sztucznemu rozdzielaniu zagadnień ochrony danych i cyberbezpieczeństwa.

[20] R. van Kessel, M. Haig, E. Mossialos, *Strengthening Cybersecurity for Patient Data Protection in Europe*, "Journal of Medical Internet Research", 25, 2023.
[21] W. Li, P. Quinn, *The European Health Data Space: An expanded right to data portability?*, "Computer Law & Security Review" 52, 2024.

4. HARMONIZACJA PRZEPISÓW KRAJOWYCH I WDROŻENIE W POLSCE

Termin implementacji dyrektywy NIS 2 upłynął 17 października 2024 r., jednak wiele państw w tym Polska, nie zdążyło uchwalić stosownych aktów prawnych. W Polsce wdrożenie NIS 2 następuje poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r.

Znowelizowana u.k.s.c.[22] zakłada rozszerzenie katalogu podmiotów objętych systemem cyberbezpieczeństwa. Sektor ochrony zdrowia ma być ujęty w kategorii podmiotów kluczowych. W praktyce oznacza to, że każda większa placówka medyczna (szpital, duża przychodnia, sieć laboratoriów diagnostycznych) zostanie z mocy ustawy uznana za operatora usługi kluczowej bez potrzeby wydawania decyzji administracyjnej (jak miało to miejsce na mocy NIS 1). Podmioty będą musiały same dokonać samoidentyfikacji i zgłosić się do rejestru prowadzonego przez właściwe organy. Obowiązki wynikające z ustawy będą obowiązywać także niektórych dostawców dla podmiotów kluczowych (m.in. przedsiębiorstwa informatyczne obsługujące szpitale mogą podlegać wymogom w zakresie bezpieczeństwa łańcucha dostaw). Definicja usługi kluczowej w sektorze zdrowia może obejmować świadczenia z zakresu opieki medycznej wymagające systemów teleinformatycznych. Dostosowanie do NIS 2 wiąże się z obciążeniem organizacyjnym dla wielu placówek. Świadomość w zakresie cyberzagrożeń i poziom zabezpieczeń w polskich szpitalach dotąd bywały niewystarczające. Wielu podmiotom brakuje procedur reagowania na incydenty, a analiza ryzyka ma często charakter marginalny. Wskazują na to kary, które UODO nakłada na jednostki medyczne za zaniedbania w zabezpieczeniu danych. Sprawa NZOZu w Pyskowicach, który został ukarany niemal 33 tys. zł za nieprzeprowadzenie rzetelnej analizy ryzyka i brak zabezpieczeń dokumentacji medycznej. W efekcie czego doszło do naruszenia danych ośmiu pacjentów (kartoteki zostały skradzione wraz z laptopem lekarza podczas wizyty domowej z jego samochodu). Dopiero po incydencie placówka wdrożyła właściwe procedury transportu i przechowywania dokumentacji (szyfrowane teczki, szkolenia personelu). Przykład ten ilustruje lukę pomiędzy teorią a praktyką w przystosowaniu placówek medycznych do wymogów bezpieczeństwa.

Równolegle Polska uczestniczy w działaniach przygotowawczych związanych z EHDS, w tym w projektach dotyczących rozwoju interoperacyjności, transgranicznej wymiany danych i przygotowania infrastruktury dla praw pacjentów oraz wtórnego wykorzystywania danych. Oznacza to, że krajowy proces wdrażania musi być oceniany dwutorowo: z jednej strony przez pryzmat zgodności z NIS 2

[22] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.)

i krajową ustawą o cyberbezpieczeństwie, z drugiej zaś przez zdolność organizacyjną do utworzenia instytucji właściwych dla EHDS oraz bezpiecznych środowisk udostępniania danych.

5. CYBERBEZPIECZEŃSTWO DANYCH ZDROWOTNYCH – ORGANY WŁAŚCIWE I PRZYKŁADY INCYDENTÓW

Na poziomie Unii po stronie cyberbezpieczeństwa zasadniczą rolę odgrywają ENISA, sieć CSIRT oraz mechanizmy współpracy przewidziane w dyrektywie NIS 2. Ich zadaniem jest nie tylko koordynacja działań w razie incydentów, lecz również budowanie wspólnej kultury zarządzania ryzykiem, opracowywanie dobrych praktyk i wzmacnianie odporności sektorów krytycznych. Po stronie EHDS funkcjonować mają z kolei organy właściwe dla zdrowia cyfrowego, organy dostępu do danych zdrowotnych oraz rada EHDS (*EHDS Board*), odpowiedzialna za koordynację stosowania rozporządzenia i wymianę doświadczeń pomiędzy państwami członkowskimi.

Na poziomie krajowym konieczne jest zapewnienie realnej współpracy między organami ochrony danych, organami właściwymi w sprawach cyberbezpieczeństwa oraz instytucjami sektora zdrowia. W polskich warunkach szczególnie istotna jest rola Centrum e-Zdrowia, które – obok funkcji systemowych i operacyjnych – pełni także rolę podmiotu wspierającego bezpieczeństwo cyfrowe sektora zdrowotnego, w tym przez działania CSIRT CeZ, ostrzeganie o zagrożeniach i rozwijanie praktyk cyberhigieny. W ujęciu *de lege lata* i *de lege ferenda* ważne jest jednak, aby wdrożenie EHDS nie doprowadziło do rozproszenia kompetencji, lecz do ich czytelnego skoordynowania. Sektor ochrony zdrowia stał się jednym z głównych celów cyberprzestępców. Jak wskazano, liczba ataków na placówki medyczne rośnie wykładniczo z roku na rok. Ataki te obejmują zarówno próby wyłudzenia danych (phishing skierowany do personelu, ataki socjotechniczne), malware (w tym ransomware szyfrujące bazy danych szpitalnych), jak i włamania mające na celu kradzież wrażliwych informacji medycznych. Cyberataki na infrastrukturę zdrowotną mogą mieć dramatyczne skutki. W wymiarze ochrony danych naruszenie poufności dokumentacji medycznej pacjentów (ujawnienie diagnoz, historii chorób) godzi w prywatność i może prowadzić do dyskryminacji, stygmatyzacji lub trwałych szkód w sferze społecznej i zawodowej osoby, której dane dotyczą. Jednak równie groźne są skutki operacyjne: sparaliżowanie działania szpitala czy przychodni. Atak ransomware na irlandzki HSE w 2021 r. spowodował wyłączenie systemów IT w całej służbie zdrowia. Odwołano tysiące wizyt, wstrzymano planowe zabiegi, a personel musiał przejść na dokumentację papierową. Odzyskanie pełnej sprawności zajęło wiele tygodni, a analiza wykazała szereg

nieprawidłowości, m.in. brak szybkiej reakcji na sygnały włamania. W Polsce głośny cyberatak na szpital MSWiA w Krakowie unieruchomił główny system informatyczny placówki. Wdrożono tryb awaryjny pracy, czasowo wstrzymano przyjęcia na oddziale, a dyrekcja z niepokojem monitorowała, czy nie doszło do wycieku wrażliwych danych pacjentów. Szybka interwencja służb pozwoliła ograniczyć skutki ataku. Pacjenci są bezpośrednio zagrożeni. Zawieszenie systemów rejestracji, brak dostępu do elektronicznych kart pacjenta czy wyników badań może opóźnić diagnostykę i leczenie, stanowiąc realne niebezpieczeństwo dla zdrowia i życia. Dyrektywa NIS 2 ma na celu zapobieganie powyższym sytuacjom bądź minimalizowanie ich skutków. Wprowadzenie obowiązkowych mechanizmów (jak kopie zapasowe i ćwiczenia ich odtwarzania, segmentacja sieci w szpitalach, szyfrowanie danych wrażliwych, wieloczynnikowe uwierzytelnianie dla personelu) powinno utrudnić atakującym zadanie. Również obowiązek zgłaszania incydentu w ciągu 24 godzin spowoduje, że placówki nie będą mogły być opieszałe co do czynności zgłaszania naruszeń. Każdy poważny incydent stanie się sygnałem alarmowym dla systemu ochrony zdrowia, co umożliwi szybszą reakcję i wymianę informacji o zagrożeniu. Standaryzacja podejścia do bezpieczeństwa przejawiająca się w wymóg posiadania planu reagowania na incydent i wyznaczenia osoby odpowiedzialnej, oznacza, że nawet mniejsze podmioty medyczne będą musiały przygotować się na ewentualny atak. To zaś zwiększa ogólną odporność systemu. Atakujący napotkają bardziej wyrównany poziom zabezpieczeń we wszystkich państwach członkowskich. Dyrektywa NIS 2 akcentuje wyraźnie bezpieczeństwo łańcucha dostaw, co w praktyce wymusi na dostawcach oprogramowania dla sektora zdrowia uzyskania certyfikacji i podniesienia jakości swoich produktów (między innymi producent systemu szpitalnego będzie musiał zapewnić regularne aktualizacje eliminujące podatności, inaczej placówka nie będzie mogła współpracować z takim podmiotem bez narażenia się na zarzut niespełnienia wymogów NIS 2, co może mieć wpływ na przebieg postępowania o zamówienie publiczne).

PODSUMOWANIE

Analiza relacji pomiędzy Europejską Przestrzenią Danych o Zdrowiu a dyrektywą NIS 2 prowadzi do wniosku, że skuteczna realizacja założeń rozporządzenia EHDS jest uzależniona od zapewnienia wysokiego poziomu cyberbezpieczeństwa infrastruktury przetwarzającej dane zdrowotne. Rozporządzenie EHDS tworzy ramy prawne dla transgranicznego udostępniania i wtórnego wykorzystania danych medycznych, jednak nie ustanawia samodzielnego i wyczerpującego systemu ochrony

infrastruktury cyfrowej. Funkcję tę pełni dyrektywa NIS 2 jako akt horyzontalny wyznaczający minimalne standardy odporności systemów teleinformatycznych w sektorach o wysokiej krytyczności, w tym w ochronie zdrowia.

Dyrektywa NIS 2 znacząco wzmacnia obowiązki podmiotów przetwarzających dane zdrowotne poprzez wprowadzenie podejścia opartego na analizie ryzyka, obowiązków raportowania incydentów oraz wymogów w zakresie zarządzania ciągłością działania. Obowiązki te mają bezpośrednie zastosowanie do podmiotów uczestniczących w funkcjonowaniu EHDS, w szczególności organów dostępu do danych zdrowotnych oraz instytucji korzystających z danych w ramach wtórnego wykorzystania. W praktyce oznacza to konieczność wdrożenia spójnych systemów zarządzania bezpieczeństwem informacji, uwzględniających zarówno wymogi sektorowe EHDS, jak i horyzontalne obowiązki wynikające z NIS 2 oraz RODO.

Przeprowadzona analiza wskazuje również na istotne wyzwania implementacyjne na poziomie krajowym. Opóźnienia we wdrażaniu dyrektywy NIS 2 oraz zróżnicowany poziom dojrzałości organizacyjnej i technicznej podmiotów ochrony zdrowia mogą prowadzić do fragmentarycznego stosowania standardów cyberbezpieczeństwa. Zjawisko to stanowi realne zagrożenie dla jednolitego funkcjonowania EHDS oraz dla równego poziomu ochrony danych zdrowotnych w państwach członkowskich.

W świetle rosnącej liczby incydentów cyberbezpieczeństwa w sektorze ochrony zdrowia należy przyjąć, że ryzyka te mają charakter systemowy i bezpośrednio wpływają na bezpieczeństwo pacjentów oraz ciągłość świadczenia usług zdrowotnych. W tym kontekście dyrektywa NIS 2 należy ocenić jako niezbędny element architektury prawnej wspierającej EHDS. Skuteczność obu regulacji będzie jednak zależeć od faktycznego wdrożenia obowiązków po stronie podmiotów publicznych i prywatnych oraz od zapewnienia skutecznego nadzoru na poziomie krajowym.

BIBLIOGRAFIA

LITERATURA

Biasin E., Yaşar B., Kamenjašević E., *New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act*, "Law, Technology and Humans" 5(2), 2023.

Casarosa, F., *European Health Data Space – Is the Proposed Certification System Effective against Cyber Threats?*, "European Journal of Risk Regulation", 15(4), 2024

Li W., Quinn P., *The European Health Data Space: An expanded right to data portability?*, "Computer Law & Security Review" 52, 2024.

Schmitz-Berndt, S. *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, "Journal of Cybersecurity" 9(1), 2023.

van Kessel R., Haig M., Mossialos E., *Strengthening Cybersecurity for Patient Data Protection in Europe*, "Journal of Medical Internet Research", 25, 2023.

Rak R., *Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)*, "European Journal of Risk Regulation", 15(4), 2024. DOI: https://doi.org/10.1017/err.2024.67.

Hussein R., Gyrard A., Abedian S., *Interoperability Framework of the European Health Data Space for the Secondary Use of Data*, "Journal of Medical Internet Research", 27, 2025.

AKTY PRAWNE

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 (RODO) (Dz.Urz. UE L 119 z 4.05.2016 r., s. 1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847 (Dz. U. UE. L. z 2025 r. poz. 327).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80 z późn. zm.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. U. UE. L. z 2022 r. Nr 333).

Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. z 2026 r. poz. 252)

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20).

ORZECZNICTWO

Decyzja Prezesa UODO z dnia 26 listopada 2024 r., DKN.5131.6.2024, LEX nr 3790660.

INNE PUBLIKACJE

European Commission, *European Health Data Space Regulation (EHDS). EC – Health – eHealth, Digital Health and Care* https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en [dostęp: 2.03.2026].

KLM Law Poland, *What obligations does the NIS 2 Directive impose on the healthcare sector?* https://www.lexology.com/library/detail.aspx?g=5fab2347-45be-4378-beac-91c9f958abb1 [dostęp: 2.03.2026].

Kośla M., *Cyberataki na szpitale biją rekordy. Prawie 1000 incydentów w 2025 roku. Dlaczego to zagraża życiu pacjentów?* https://politykazdrowotna.com/artykul/cyberataki-na-szpitale-n2043097 [dostęp: 2.03.2026].

EUROPEAN HEALTH DATA SPACE (EHDS) AND THE NIS 2 DIRECTIVE – CHALLENGES IN THE CYBERSECURITY OF HEALTH DATA

Summary: The European Health Data Space (EHDS) constitutes a key element of the European Union's strategy to develop a common data market by enabling the secure exchange and secondary use of health data across Member States. Given the sensitive nature of health data, the establishment of an adequate level of cybersecurity represents one of the central legal and organizational challenges associated with the implementation of the EHDS framework. In this context, Directive (EU) 2022/2555 (NIS 2) plays a significant role by introducing a harmonized framework for ensuring a high level of network and information security within the European Union. The Directive extends cybersecurity obligations to the healthcare sector and imposes requirements concerning risk management, incident reporting, and the implementation of appropriate technical and organizational measures. These obligations are of particular relevance to entities involved in the functioning of the EHDS, including data access bodies and institutions processing health data for research and analytical purposes. The chapter examines the relationship between the EHDS regulatory framework and the provisions of the NIS 2 Directive, focusing on the development of coherent cybersecurity standards for the health data ecosystem. It also addresses challenges related to the harmonization of national legal frameworks under NIS 2 and assesses the Directive's impact on cybersecurity practices within digital infrastructures supporting the sharing and secondary use of health data.

Keywords: European Health Data Space; EHDS; NIS 2; cybersecurity; health data; secondary use of data; European Union law.

Michał Zawada
Uniwersytet Mikołaja Kopernika w Toruniu
e-mail: zawadamichal01@gmail.com
https://orcid.org/0000-0001-9892-396X

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA WOBEC PROJEKTU NOWELIZACJI W KONTEKŚCIE FUNKCJONOWANIA SZPITALI NA TLE UNIJNYCH DYREKTYW ORAZ USTAW OBOWIĄZUJĄCYCH W WYBRANYCH PAŃSTWACH CZŁONKOWSKICH UE

Streszczenie: 21 października 2025 r. Rada Ministrów przyjęła projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Stanowi on odpowiedź na rosnącą skalę zagrożeń w cyberprzestrzeni, zwłaszcza w związku z obecną sytuacją geopolityczną, a także wpisuje się w szerszy proces budowy odporności państwa na zagrożenia w cyberprzestrzeni oraz implementację unijnych dyrektyw dotyczących bezpieczeństwa sieci i informacji. Do kluczowych rozwiązań należy m.in. rozszerzenie katalogu podmiotów zobowiązanych do zapewnienia bezpieczeństwa cyfrowego. Skutkuje to wszystko zwiększeniem odpowiedzialności osób zarządzających instytucjami i przedsiębiorstwami objętymi u.k.s.c.. Łączy się to jednocześnie z utworzeniem krajowego planu reagowania na poważne incydenty, który będzie określał zasady współpracy oraz procedury postępowania w sytuacjach zagrożenia dla kluczowych usług publicznych i gospodarczych, np. elektrowni czy szpitali. Warto przy tym zwrócić uwagę na wpływ potencjalnej ustawy na funkcjonowanie tych ostatnich i innych ośrodków ochrony zdrowia, w szczególności pod względem finansowym. Celem niniejszego rozdziału jest ocena głównych założeń wskazanego projektu ustawy, przy czym zostanie dokonane porównanie do rozwiązań prawnych w tej materii ustawowej, które występują w innych państwach Unii Europejskiej. Ponadto podjęta zostanie próba odpowiedzi na pytania dotyczące wpływu tej nowelizacji na funkcjonowanie szpitali i innych ośrodków ochrony zdrowia.

Słowa kluczowe: krajowy system cyberbezpieczeństwa; NIS 2; CSIRT; ochrona zdrowia.

WPROWADZENIE

21 października 2025 r. Rada Ministrów przyjęła projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa („u.k.s.c.") oraz niektórych innych ustaw[1], który wpłynął do Sejmu 7 listopada b.r. Został on opracowany z inicjatywy Ministra Cyfryzacji i stanowi odpowiedź na rosnącą skalę zagrożeń w cyberprzestrzeni, zwłaszcza w związku z obecną sytuacją geopolityczną. Objawiają się one coraz to bardziej rosnącą liczbą cyberataków, co stanowi bezpośrednią przesłankę dla wzmocnienia krajowego systemu cyberbezpieczeństwa. Według danych CSIRT NASK[2] liczba zgłoszonych incydentów wzrosła z ponad 39 tys. w 2022 r., do ponad 75 tys. w 2023 r., osiągając ponad 103 tys. przypadków w 2024 r. Dane te wskazują na ponad dwukrotny wzrost w ciągu dwóch lat, co dowodzi narastającej presji na infrastrukturę cyfrową państwa oraz konieczności modernizacji instrumentów prawnych i organizacyjnych.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa[3] wpisuje się w szerszy proces budowy odporności państwa na zagrożenia w cyberprzestrzeni oraz implementację unijnych dyrektyw dotyczących bezpieczeństwa sieci i informacji („NIS 2", dyrektywa NIS 2)[4]. Zwiększenie kompetencji instytucjonalnych, rozszerzenie zakresu odpowiedzialności oraz wdrożenie nowych narzędzi informatycznych ma więc umożliwić skuteczniejsze przeciwdziałanie atakom cyfrowym i ograniczenie ich skutków dla funkcjonowania gospodarki oraz administracji publicznej.

Do kluczowych rozwiązań należy m.in. rozszerzenie katalogu podmiotów zobowiązanych do zapewnienia bezpieczeństwa cyfrowego. Oprócz dotychczasowych sektorów (energia, transport, zdrowie czy bankowość), obowiązki te mają objąć również nowe obszary, w tym m.in. gospodarkę wodno-ściekową, gospodarkę odpadami, produkcję i dystrybucję chemikaliów oraz żywności, sektor pocztowy, a nawet przestrzeń kosmiczną. Ponadto przewiduje się wzmocnienie infrastruktury technicznej i organizacyjnej, poprzez umożliwienie inwestycji w nowoczesny sprzęt, oprogramowanie oraz zwiększenie finansowania kadr IT. Na uwagę zasługuje również

[1] Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk sejmowy nr 1955, Warszawa, 7 listopada 2025 r.) [dalej również jako: projekt ustawy, projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (u.k.s.c.)].

[2] Według art. 2 pkt 3 u.k.s.c., jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

[3] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.) (dalej również jako: u.k.s.c.).

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80 z późn. zm.).

potencjalne tworzenie sektorowych zespołów reagowania na incydenty cyberbezpieczeństwa (CSIRT sektorowych), odpowiedzialnych za szybkie reagowanie i wymianę informacji o zagrożeniach w poszczególnych dziedzinach gospodarki.

Skutkuje to wszystko zwiększeniem odpowiedzialności osób zarządzających instytucjami i przedsiębiorstwami objętymi u.k.s.c. Kierownictwo poszczególnych jednostek ma ponosić osobistą odpowiedzialność za realizację obowiązków w zakresie bezpieczeństwa informatycznego, w tym za ewentualne zaniedbania. Łączy się to jednocześnie z utworzeniem krajowego planu reagowania na poważne incydenty, który będzie określał zasady współpracy oraz procedury postępowania w sytuacjach zagrożenia dla kluczowych usług publicznych i gospodarczych, np. elektrowni czy szpitali. Warto przy tym zwrócić uwagę na wpływ potencjalnej ustawy na funkcjonowanie tych ostatnich i innych ośrodków ochrony zdrowia, w szczególności pod względem finansowym.

Celem niniejszego rozdziału jest ocena głównych założeń wskazanego projektu ustawy, przy czym zostanie dokonane porównanie do rozwiązań prawnych w tej materii ustawowej, które występują w innych państwach Unii Europejskiej. Ponadto podjęta zostanie próba odpowiedzi na pytania dotyczące wpływu tej nowelizacji na funkcjonowanie szpitali i innych ośrodków ochrony zdrowia, zwłaszcza w aspekcie finansowym. W ramach przeprowadzonych badań wykorzystano metodę dogmatyczno-prawną oraz metodę prawnoporównawczą.

1. POJĘCIE KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Jeśli chodzi o to, czym tak naprawdę jest krajowy system cyberbezpieczeństwa, wyjaśnił to pojęcie polski ustawodawca. Co prawda, według art. 3 u.k.s.c. omawiany system nie jest zdefiniowany wprost, lecz uregulowany jest cel jego funkcjonowania. Jest to bowiem zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

W przypadku tej ostatniej kwestii, mamy do czynienia wówczas, gdy podejmowane są czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu, a więc zdarzenia, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo (art. 2 pkt 5 i 10 u.k.s.c.). W zależności od konsekwencji, jakie niesie za sobą dane zdarzenie, klasyfikuje się incydenty na krytyczny, poważny, istotny czy też w podmiocie publicznym (art. 2 pkt 6-9 u.k.s.c.).

W literaturze natomiast, owy system rozumie się jako integralną część krajowego systemu bezpieczeństwa oraz europejskiego systemu bezpieczeństwa sieci i systemów informacyjnych, wyodrębnioną w celu efektywnego (sprawnego, niezakłóconego) wykonywania zadań publicznych, usług kluczowych i usług cyfrowych poprzez ustalanie strategii i jej realizację, w której podmioty objęte systemem wypełniają przypisane im dla ochrony interesu publicznego obowiązki ustawowe[5]. Oprócz tego, uważa się również, że „systemowość" u.k.s.c. można odnieść do pojęcia systemu znanego z prawa administracyjnego. Użycie terminu „system" wskazuje, że regulacja ta ma charakter kompleksowy i zupełny obejmuje całość instytucji, procedur, organów i instrumentów odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni. Choć ustawa zakłada pełność tego systemu, należy pamiętać, że jego funkcjonowanie opiera się również na powiązaniach z regulacjami spoza samej ustawy. W praktyce oznacza to, że krajowy system cyberbezpieczeństwa, mimo swojej wewnętrznej spójności, korzysta także z rozwiązań właściwych innym podsystemom prawa[6].

Istotne jest przy tym jednak jak należy rozumieć samo pojęcie cyberbezpieczeństwa. Według definicji legalnej z art. 2 pkt 4 u.k.s.c., jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Nieco inaczej zdefiniował to pojęcie unijny prawodawca, gdyż według dyrektywy NIS 2, która odsyła nas do art. 2 pkt 1 rozporządzenia UE z 2019 r. w sprawie ENISA[7].

Zgodnie z tym aktem prawnym „cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami. W literaturze natomiast za pojęcie cyberbezpieczeństwa rozumie się ogół technik, procesów i praktyk realizowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem do cybernetycznej przestrzeni przetwarzania informacji np. w sieciach teleinformatycznych[8].

---

[5] G. Szpor [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, Warszawa 2019, art. 3.

[6] D. Tyrawa, *Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane*, „International Journal of Legal Studies" 2023, nr 1(13), s. 20.

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm.) (dalej również jako: rozporządzenie ENISA).

[8] D. Adamiec et al., *Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja)*, „Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu" 2021, nr 3(71), s. 281.

Za sprawą nowego projektu ustawy, obecna definicja legalna w polskiej ustawie ma zostać zastąpiona w sposób dosłowny definicją ze wspomnianego rozporządzenia. Ma to ścisły związek z wdrożeniem do krajowego porządku prawnego dyrektywy unijnej NIS 2, co zakłada ten właśnie projekt. Wyróżniono również przy tym niektóre pojęcia, których dodanie do u.k.s.c. przewiduje się za sprawą możliwej nowelizacji. Na uwagę zasługuje definicja legalna cyberzagrożenia, która ma być dołączona w formie art. 2 pkt 4a u.k.s.c. Zjawisko to ma oznaczać wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób, a więc należy rozumieć to w taki sposób, w jaki jest to uregulowane w art. 2 pkt 8 wspomnianego wcześniej rozporządzenia z 2019 r.

Polski ustawodawca tłumaczy wprowadzenie takiego rozwiązania tym, że „jest to definicja szeroka, która obejmuje całe spektrum zagrożeń, w tym także zagrożenia o charakterze fizycznym i środowiskowym. Pokazując to na całkiem realnym przykładzie - zdarza się czasem, że serwerownia jest w pomieszczeniu, które nie jest zamknięte i dostęp fizyczny mają do niej wszyscy - pracownicy czy interesariusze podmiotu. Jest to niewątpliwe cyberzagrożenie - każdy może uzyskać dostęp i chociażby wyjąć okablowanie lub przeprowadzić atak *man in the middle*"[9].

Ten ostatni ze zwrotów, którym posługuje się ustawodawca w uzasadnieniu projektu, oznacza typ ataku, który polega na podsłuchiwaniu wymiany danych pomiędzy stronami komunikacji. Po usytuowaniu się w „środek" transferu między użytkownikiem a aplikacją, atakujący podszywa się pod jedną ze stron, co sprawia wrażenie zwyczajnej wymiany informacji. Umożliwia to osobie atakującej przechwycenie informacji i danych od dowolnej ze stron[10]. Jest to o tyle trudne do wykrycia, ponieważ strona atakowana nie zauważa niczego niepokojącego ani nadzwyczajnego w danej konwersacji.

Dodatkowo, projektodawca wyróżnia pojęcia potencjalnego zdarzenia dla cyberbezpieczeństwa, a także poważnego cyberzagrożenia (możliwy art. 2 pkt 11f i 11g u.k.s.c.). Pierwsze z nich należy rozumieć jako zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, które jednak nie wystąpiło lub któremu udało się zapobiec. Polski ustawodawca był zobowiązany do wprowadzenia tej definicji z tego względu, że występuje ona w dyrektywie NIS 2, a w dodatku państwa członkowskie UE składają sprawozdania z liczby zgłoszonych potencjalnych zdarzeń dla cyberbezpieczeństwa.

[9] Uzasadnienie rządowego projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk sejmowy nr 1955, Warszawa, 7 listopada 2025 r.), s. 10.
[10] E. Belka, *Deanonimizacja użytkowników sieci Tor*, „Cybersecurity & Cybercrime" 2021, nr. 1(1), s. 122.

W samej możliwości zaś zgłoszeń tego rodzaju zdarzeń chodzi o to, aby móc wyciągnąć informacje z tego rodzaju sytuacji, które nie doprowadziły do strat, ale wyciągnięte z nich wnioski mogą pozwolić na zabezpieczenie się przed innymi incydentami[11]. Drugie natomiast to cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników tych systemów przez wywołanie poważnej szkody materialnej lub niematerialnej. Ustawodawca uzasadnia wprowadzenie tejże kwalifikowanej postaci cyberzagrożenia ze względu na to, że jego zaistnienie będzie powodowało obowiązek poinformowania o środkach, które mogą podjąć użytkownicy podmiotów kluczowych i podmiotów ważnych celem zabezpieczenia się przed jego skutkami[12].

Pojęcie cyberbezpieczeństwa, analizowane na gruncie przywołanych definicji, ukazuje istotne rozbieżności pomiędzy podejściem ustawodawcy krajowego, unijnego oraz ujęciami doktrynalnymi. Z powyższego porównania definicji wynika, że cyberbezpieczeństwo jest pojęciem wielowymiarowym, obejmującym zarówno elementy techniczne, organizacyjne, jak i ochronę społeczeństwa. Tę ostatnią kwestię szczególnie podkreśla D. Tyrawa, ponieważ według niego zasadniczym i głównym dobrem, które ma być chronione przed cyberatakami, jest człowiek, a dokładniej jego życie i zdrowie[13]. Jak dobrze wiadomo, są to oczywiście najwyższe wartości w hierarchii ważnych dla nas, o ile nie najważniejsze. Mimo to, różnice w pojedynczych definicjach, które zostały przytoczone powyżej, nie mają charakteru sprzecznego, lecz komplementarny.

Prawo krajowe koncentruje się na odporności systemu, prawo unijne na działaniach ochronnych w szerszym kontekście, natomiast doktryna na praktycznym wymiarze procesów bezpieczeństwa. Zestawienie tych stanowisk prowadzi do wniosku, że prawidłowe rozumienie cyberbezpieczeństwa wymaga integracji wszystkich trzech perspektyw, co poniekąd może się stać wskutek wspominanego projektu ustawy. Wydaje się być to bowiem niezbędne dla tworzenia skutecznych regulacji i rozwiązań instytucjonalnych w ramach u.k.s.c.

2. ODDZIAŁYWANIE NA OŚRODKI OCHRONY ZDROWIA

Jeśli chodzi o podmioty objęte krajowym systemem cyberbezpieczeństwa, to już obecnie obowiązuje szeroki ich katalog w art. 4 u.k.s.c., a w związku z ww. projektem ustawy ma on zostać zmieniony. Zmiana ma dotyczyć operatorów usług kluczowych

[11] Uzasadnienie… *op.cit.*, s. 20.
[12] *Ibidem*.
[13] D. Tyrawa, *Krajowy system… op.cit.*, s. 18.

i dostawców usług cyfrowych z art. 4 pkt 1 i 2 u.k.s.c. Projekt przewiduje bowiem wprowadzanie dwóch głównych kategorii podmiotów: podmioty kluczowe oraz podmioty ważne. Podział ten opiera się na kryteriach wskazanych w NIS 2, czyli wielkość organizacji, sektor działalności czy też znaczenie dla funkcjonowania państwa i społeczeństwa.

Wśród podmiotów kluczowych możemy wymienić m.in. operatorów infrastruktury krytycznej, duże przedsiębiorstwa z sektorów takich jak właśnie zdrowie, energetyka, transport, bankowość czy w końcu administrację publiczną. Podmioty ważne to z kolei średnie przedsiębiorstwa działające w tych samych sektorach lub inne podmioty, które, pomimo mniejszej wagi, mają istotne znaczenie dla bezpieczeństwa cyfrowego kraju.

Wiąże się to z obowiązkiem stosowania środków zarządzania ryzykiem w cyberbezpieczeństwie w sektorze ochrony zdrowia, które zostaną ustanowione w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez podmioty do prowadzenia działalności lub świadczenia usług medycznych oraz w celu zapobiegania wpływowi incydentów na odbiorców tych usług bądź minimalizowania takiego wpływu. Oceniając proporcjonalność tych środków, należycie uwzględnia się stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze (art. 21 ust. 1 dyrektywy NIS 2).

Polski ustawodawca wymienił te środki w art. 1 pkt 16 projektu nowelizacji u.k.s.c., który nadaje nowe brzmienie art. 8 u.k.s.c. ze względu na art. 21 dyrektywy NIS 2. Zgodnie z art. 8 ust. 1 pkt 1 i 2 u.k.s.c. podmioty kluczowe oraz podmioty ważne będą miały wdrożyć system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem, a także wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze. Są to w szczególności:

a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu,

d) bezpieczeństwo zasobów ludzkich,

e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT[14], od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,

f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,

g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,

h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,

i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,

j) podstawowe zasady cyberhigieny,

k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,

l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,

m) zarządzanie aktywami,

n) polityki kontroli dostępu.

Ponadto, na podstawie art. 8 ust. 1 pkt 3-5 u.k.s.c. po nowelizacji, podmioty te mają być zobowiązane do zbierania informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi, zarządzania incydentami, a także stosowania

[14] Polski ustawodawca w projekcie ustawy o nowelizacji u.k.s.c. zakłada dodanie do niej w art. 2 pkt 11k-11m definicji legalnych produktu, procesu i usługi ICT. Zgodnie z tymi przepisami rozumie się je według art. 2 pkt 12-14 wspomnianego wcześniej rozporządzenia 2019/881 (ENISA). Stanowi ono, że: 12) „produkt ICT" oznacza element lub grupę elementów sieci lub systemów informatycznych; 13) „usługa ICT" oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych; 14) „proces ICT" oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT.

środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:

a) stosowania mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,

b) regularnego przeprowadzania aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,

c) ochrony przed nieuprawnioną modyfikacją w systemie informacyjnym,

d) niezwłocznego podejmowania działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowego ograniczania ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, z uwzględnieniem konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

Jest to niewątpliwie bardzo szeroki katalog obowiązków, które przybędą ośrodkom ochrony zdrowia, lecz umieszczenie ich w kategorii podmiotów kluczowych jest całkowicie uzasadnione zdaniem niektórych autorów. W literaturze zwraca się bowiem uwagę na to, że dane medyczne są szczególnie podatne na zagrożenia cybernetyczne, w ostatnich latach szczególnie nasilone w obliczu wojny na Ukrainie. Domyślnym celem stał się system teleinformatyczny Elektronicznej Dokumentacji Medycznej („EDM"), który stanowi podstawowe narzędzie do gromadzenia i przechowywania danych w sektorze ochrony zdrowia.

Stwarza to zatem nowe wyzwania dla tego właśnie sektora i wymaga wzmożonych środków zarówno w celu ochrony EDM, jak i cyberbezpieczeństwa całej sieci szpitali i innych ośrodków ochrony zdrowia. Dowodem tego jest fakt, iż w samym 2023 r. polskie instytucje medyczne odnotowały 405 incydentów zagrożeń cybernetycznych, a najczęstszym typem ataku był *ransomware*[15]. Jest to szczególnie niebezpieczny atak złośliwym oprogramowaniem w modelu platformy cyfrowej - RaaS, w którym dostęp do usługi, czyli wirusa lub wykradzionych danych, jest relatywnie łatwy, tani i nie wymaga specjalistycznej wiedzy[16].

[15] M. Guziak, K. Ziarnik, *Przegląd naruszeń cyberbezpieczeństwa danych medycznych w polskim sektorze ochrony zdrowia w 2023 roku*, Rocznik Bezpieczeństwa Międzynarodowego 2024, vol. 18, nr 2, s. 109.
[16] M. Poniatowska-Jaksch, *Ransomware w sektorze ochrony zdrowia – przyczyny, konsekwencje*, „Kwartalnik Nauk o Przedsiębiorstwie" 2024, nr 4, s. 5.

Wobec tego decyzją Ministra Zdrowia (na podstawie art. 44 u.k.s.c.[17]) powołano 1 grudnia 2023 r. Zespół Reagowania na Incydenty Bezpieczeństwa (*Cyber Security Incident Response Team*), w celu realizacji zadań Sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego w sektorze ochrony zdrowia (CSiRT CeZ)[18]. Jeśli chodzi o najnowsze dane, to w 2025 r. w okresie od stycznia do czerwca CSIRT CeZ zarejestrował 792 incydenty, natomiast w analogicznym okresie w 2024 r. 470 incydentów, co potwierdza niestety rosnącą tendencję liczby zagrożeń w cyberprzestrzeni[19].

W obliczu wyzwań konieczne są skuteczne działania, aby zapewnić bezpieczeństwo danych pacjentów. Autorzy wskazują przy tym na znaczną rolę edukacji personelu w tym zakresie, która powinna odbywać się ich zdaniem w drodze współpracy pomiędzy instytucjami medycznymi i ekspertami ds. cyberbezpieczeństwa w celu zapewnienia skutecznej ochrony danych medycznych w erze rosnących zagrożeń cybernetycznych[20]. Jest to wyjątkowo istotne ze względu na bardzo dużą liczbę wrażliwych danych przechowywanych przez sektor ochrony zdrowia oraz niski poziom ich zabezpieczenia.

Ponadto konsekwencje takich ataków cybernetycznych mają wymiar społeczny ze względu na utratę dokumentacji, w tym danych osobowych pacjentów, co może mieć również skutki w sztuce medycznej, ale także i wymiar finansowy, gdyż koszty usuwania ataku niemal w połowie pokrywają podmioty ochrony zdrowia[21]. Mimo to, w ocenie Ministerstwa Zdrowia, obecnie występująca w podmiotach architektura usług w placówkach sektora ochrony zdrowia powoduje, że prawdopodobieństwo wystąpienia zdarzenia związanego z cyberbezpieczeństwem, mającego bezpośredni wpływ na stan zdrowia i życia pacjentów jest bardzo niskie[22].

---

[17] Zgodnie z art. 44 ust. 1 u.k.s.c., organ właściwy do spraw cyberbezpieczeństwa może ustanowić, zgodnie z odrębnymi przepisami, sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, odpowiedzialny w szczególności za: 1) przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów; 2) wspieranie operatorów usług kluczowych w wykonywaniu obowiązków określonych w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13 u.k.s.c.; 3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z obsługi incydentu; 4) współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych. Warto podkreślić przy tym, że organem właściwym ds. cyberbezpieczeństwa dla sektoru ochrony zdrowia jest minister właściwy ds. zdrowia, jak reguluje art. 41 pkt 5 u.k.s.c.

[18] Centrum e-Zdrowia, https://www.cez.gov.pl/pl/page/o-nas-0 (dostęp z dnia: 29 listopada 2025 r.).

[19] Odpowiedź na Interpelację nr 10455 z dnia 25 czerwca 2025 r. Pana Posła Piotra Górnikiewicza w sprawie zagrożeń wynikających z niedostatecznego poziomu cyberbezpieczeństwa w podmiotach wykonujących działalność leczniczą oraz działań podejmowanych przez Ministerstwo Zdrowia w celu jego poprawy, s. 4.

[20] M. Guziak, K. Ziarnik, *Przegląd naruszeń… op.cit.*, s. 109-110.

[21] M. Poniatowska-Jaksch, *Ransomware w sektorze ochrony zdrowia… op.cit.*, s. 5.

[22] Odpowiedź na Interpelację… *op. cit.*, s. 3.

3. NOWE OBOWIĄZKI A KONDYCJA FINANSOWA OŚRODKÓW OCHRONY ZDROWIA

W raporcie przygotowanym na temat wpływu projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa na szpitale wyraźnie podkreślony został aspekt finansowy[23]. Autorzy raportu wskazują, że przedstawiciele szpitali mają niską świadomość konsekwencji i skutków finansowych potencjalnego wejścia w życie nowelizacji u.k.s.c. dla prowadzenia działalności leczniczej. Z przeprowadzonej analizy szacowania kosztów związanych z koniecznością wymiany produktów i usług pochodzących od dostawców wysokiego ryzyka, w przypadku wydania decyzji administracyjnej w pełnym zakresie, wynika również, że łączna kwota dla jednego szpitala może wynieść 4,6 mln zł netto w pięcioletnim okresie, a dla wszystkich szpitali publicznych w Polsce może wynosić w ciągu pięciu lat 3,7 mld zł netto. Koszty zaś dla całego podsektora podmiotów leczniczych będą zdecydowanie wyższe ze względu na konieczność dokonania wydatków przez szpitale prywatne, które nie brały udziały we wskazanym badaniu[24].

Rozwiązania w tej sprawie ustawodawca upatruje w środkach z Krajowego Planu Odbudowy i Rozwoju. W uzasadnieniu projektu wskazuje się, że koszty wdrożenia nowych usług w ramach nowelizacji u.k.s.c. w latach 2025-2026 roku ponoszone będą w dużej części z dofinansowaniem z funduszy unijnych KPO, w ramach projektu S46-KPO, przy czym te wydatki rozwojowe są ujęte w przedstawionych tu kalkulacjach w latach 2025 i 2026[25]. Oprócz tego również Ministerstwo Zdrowia w kwietniu 2025 r. ogłosiło nabór do konkursu „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" ze środków KPO, przy czym na cyfrową transformację ochrony zdrowia przeznaczone zostanie ponad 3 mld zł i jest on skierowany do podmiotów leczniczych zakwalifikowanych do tzw. sieci szpitali[26].

Warto również wspomnieć w tym kontekście o analizie Oceny Skutków Regulacji, będącej załącznikiem do projektu ustawy, a konkretnie w zakresie przydzielania wsparcia finansowego dla administracji centralnej i rządowej oraz jednostek

[23] Raport pt. *Wpływ projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa na szpitale publiczne*, red. U. Szybowicz, I. Wochlik, Polskie Towarzystwo Koordynowanej Ochrony Zdrowia, Izba Gospodarcza Farmacja Polska, Fundacja AI LAW TECH i Federacja Przedsiębiorców Polskich, Warszawa, październik 2025, https://ptkoz.org/wp-content/uploads/2025/10/u.k.s.c.-a-szpitale-publiczne.pdf [dostęp: 2.03.2026].

[24] *Ibidem*, s. 1-2.

[25] Uzasadnienie… *op.cit.*, Ocena skutków regulacji u.k.s.c. 2.0 dla NASK-PIB w latach 2025–2035. Estymacja kosztów – Załącznik nr 3 do OSR, s. 20.

[26] Odpowiedź na Interpelację… *op. cit.*, s. 2.

samorządu terytorialnego, którym to ostatnim zresztą podlega znacząca większość szpitali w Polsce. Ujawnia ona bowiem znaczącą dysproporcję w rozdzieleniu środków. Ustawodawca zakłada przyznanie wsparcia finansowego w wysokości ok. 700 mln zł dla blisko 70 podmiotów administracji centralnej i rządowej, co przekłada się średnio na 10 mln zł na każdą z tych jednostek, natomiast dla 2500 j.s.t. ma zostać przeznaczone 1,5 mld zł, co oznacza średnio zaledwie ok. 600 tys. zł na jednostkę.

Taka różnica w finansowaniu, zdaniem Konfederacji Lewiatan, której uwaga dotyczy właśnie tej kwestii w uzasadnieniu projektu ustawy, nie tylko wprowadza nierówności, ale także może skutkować powstawaniem różnic w poziomie zabezpieczeń cybernetycznych między różnymi szczeblami administracji publicznej[27]. Ustawodawca jednak argumentuje to nowymi obowiązkami nałożonymi na administrację rządową, w tym m.in. stworzenia CSIRT sektorowych oraz pełnienia roli organów nadzorczych dla poszczególnych sektorów, z czym mają wiązać się dodatkowe koszty. Dodatkowo podkreśla, że „wiele obowiązków nakładanych na jednostki samorządu terytorialnego nie jest nowych", stąd powstała owa dysproporcja[28].

Mimo to, planowane jest uruchomienie czterech projektów dedykowanych dla wybranych grup podmiotów u.k.s.c., w tym właśnie dla jednostek sektora finansów publicznych. Według ustawodawcy aktualnie trwają prace do przygotowania naborów, z uwzględnieniem ich celu określonego w KPO i zwiększania odporności, a także przy udziale jednostki budżetowej, podległej ministrowi właściwemu do spraw informatyzacji, która posiada wieloletnie doświadczenie, wiedzę i kompetencje w zakresie udzielania różnego rodzaju wsparcia finansowego, czyli Centrum Projektów Polska Cyfrowa[29]. Wsparcie ma umożliwić wzmocnienie cyberbezpieczeństwa w obszarach organizacji, w szczególności procedur, kompetencji personelu oraz technologii. Zwrócić należy jednak uwagę na fakt, że „zgodnie z zasadami obowiązującymi w KPO podatek VAT stanowi koszt niekwalifikowany, wobec czego niezbędne jest zaangażowanie na ten cel własnych środków pochodzących z budżetu jednostki"[30].

Choć ustawodawca zakłada finansowanie znacznej części tych wydatków ze środków Krajowego Planu Odbudowy, trudno jednoznacznie ocenić, czy przewidziany poziom wsparcia okaże się wystarczający wobec rzeczywistych potrzeb podmiotów leczniczych. Dodatkowe wątpliwości budzi fakt, że nie przewidziano na odpowiednim poziomie bezpośredniego wsparcia z budżetu państwa, a dostęp do środków uzależniono od procedur konkursowych oraz inicjatywy dyrekcji szpitali

[27] Uzasadnienie… *op.cit.*, Tabela uwag zgłoszonych w ramach konsultacji publicznych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) cz. III, s. 140-141.
[28] *Ibidem*.
[29] Uzasadnienie… *op.cit.,* s. 107-108.
[30] *Ibidem*, Tabela uwag… *op.cit.*, s. 140-142.

w zakresie składania wniosków i ich pozytywnego rozpatrzenia. Należy zatem stwierdzić, że taki model finansowania może prowadzić do nierównomiernego dostępu do środków oraz opóźnień w realizacji niezbędnych inwestycji, takich jak wymiana infrastruktury czy przeszkolenie personelu. W konsekwencji podważa to efektywność systemowego wsparcia państwa w procesie wdrażania nowych obowiązków z zakresu cyberbezpieczeństwa, oczywiście w razie gdy ustawa ta wejdzie w życie.

4. PORÓWNANIE: ESTONIA I SZWECJA

Analizując zagraniczne modele zarządzania cyberbezpieczeństwem, zasadnym jest odwołanie się do doświadczeń wybranych państw regionu Morza Bałtyckiego, w szczególności Estonii oraz Szwecji, przy czym to właśnie przypadek estoński zasługuje na pogłębioną uwagę. W debacie publicznej oraz naukowej utrwaliły się bowiem pojęcia takie jak „wojna informacyjna", odnoszące się do praktyk rozpowszechniania dezinformacji i propagandy, jak również „wojna cybernetyczna" (*cyber war*), obejmująca działania polegające m.in. na nieuprawnionym dostępie do systemów informatycznych czy czasowym zakłócaniu funkcjonowania usług cyfrowych. Aktywności, które jeszcze niedawno były postrzegane przede wszystkim jako tymczasowe awarie lub problemy techniczne pozostające w gestii specjalistów IT, współcześnie coraz częściej ujmowane są w kategoriach praktyk o charakterze militarnym, elementów bezpieczeństwa narodowego oraz przejawów konfliktów międzypaństwowych, co nabiera szczególnego znaczenia w kontekście trwającej od kilku lat wojny w Ukrainie. W tym sensie Estonia stanowi jedno z kluczowych studiów przypadku ilustrujących nową interpretację bezpieczeństwa nowych technologii oraz danych.

W 2007 r. Estonia doświadczyła skoordynowanych cyberataków, które w późniejszym dyskursie zostały określone mianem „pierwszej wojny sieciowej". Ataki te, uznane przez władze estońskie za pierwszy przypadek cyfrowego ataku państwa na państwo, były wymierzone w system bankowy, media oraz infrastrukturę administracji publicznej, a ich sprawstwo zostało przypisane Federacji Rosyjskiej[31]. Narracja „Web War I" znalazła szeroki oddźwięk w międzynarodowych mediach, oddziałując zarówno na debaty akademickie, jak i polityczne oraz intensyfikując obawy związane z zagrożeniami cybernetycznymi[32]. Od tego momentu cyberwojna zaczęła być

[31] S. Shackelford, *Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks*, „Journal of Internet Law, Forthcoming" 2009, s. 1.

[32] Zob. S. Blank, *Web War I: Is Europe's First Information War a New Kind of War?*, „Comparative Strategy" 2008, nr 27(3), s. 227-247; R. Kaiser, *The birth of cyberwar*, „Political Geography" 2015, nr 46, s. 12; M.C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, „Yale Journal of International Law" 2011, s. 423.

postrzegana jako realne i narastające zagrożenie, zajmując coraz bardziej eksponowane miejsce w agendzie estońskiej polityki cyberbezpieczeństwa.

Pozycja Estonii jako jednego z liderów w obszarze cyfryzacji i cyberbezpieczeństwa została w znacznym stopniu ukształtowana w następstwie reakcji państwa właśnie na wydarzenia z 2007 r[33]. Incydenty te stały się impulsem do zasadniczej zmiany podejścia strategicznego, prowadząc do natychmiastowych i systematycznych inwestycji w zdolności cyberobronne, ustanowienia w Tallinie Centrum Doskonalenia NATO ds. Współpracy w Dziedzinie Cyberobrony (*NATO Cooperative Cyber Defence Centre of Excellence*, „CCDCOE")[34] oraz aktywnego zaangażowania Estonii w kształtowanie ram polityki cyberbezpieczeństwa na poziomie Unii Europejskiej[35].

Estonia od wielu lat wykazuje tendencję do pełnienia roli prekursora w zakresie cyfryzacji życia publicznego i społecznego. Była jednym z pierwszych państw na świecie, które na szeroką skalę włączyły technologie informatyczne do systemu edukacji[36], co przełożyło się na wysoki poziom kompetencji cyfrowych, rozwijanych w ramach licznych zdecentralizowanych inicjatyw oddolnych. Ponadto jako pierwsze państwo wdrożyła powszechnie stosowaną elektroniczną tożsamość, wykorzystywaną w niemal wszystkich usługach publicznych, w tym w procedurach głosowania[37]. Estonia przyjęła również pierwszą w Europie kompleksową, obejmującą cały

[33] CSS (Centre for Security Studies), *Estonia's National Cybersecurity and Cyberdefence Posture. Policy and Organizations*, ETH Zürich 2020, s. 17, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf [dostęp: 2.03.2026].

[34] Zob. M.R. Grimaila, *The Genesis of the NATO Cooperative Cyber Defense Centre of Excellence*, „ISSA Journal" 2018, nr 16(8), s. 22-26; C.N.J. Cath, L. Glorioso, M. Taddeo, *NATO CCD COE Workshop on 'Ethics and Policies for Cyber Warfare' – A Report*, [w:] M. Taddeo, L. Glorioso (red.) *Ethics and Policies for Cyber Operations. Philosophical Studies Series*, vol. 124, Springer, Cham 2017, s. 231-241.

[35] Zob. X. Gao, *Challenges and opportunities: Estonia's role in shaping EU cybersecurity policy*, [w:] A.-L. Högenauer, M. Mišík (red.), *Small States in EU Policy-Making: Strategies, Challenges, Opportunities*, Routledge, Abingdon-Nowy Jork 2024, s. 159-173.

[36] Chodzi tutaj przede wszystkim o program „Tiger Leap" (est. *Tiigrihüpe*), który został wprowadzony w latach 90. XX w.: Education Estonia, *How it all began? From Tiger Leap to digital society*, https://www.educationestonia.org/tiger-leap/ [dostęp: 2.03.2026]; e-Estonia, *e-Education and research*, https://e-estonia.com/solutions/e-education-and-research/education_system/ [dostęp: 2.03.2026]; CSS (Centre for Security Studies), *Estonia's National Cybersecurity… op.cit.*, s. 4 [dostęp: 2.03.2026].

[37] Zob. Republic of Estonia Information System Authority, *Electronic Identity eID*, https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/electronic-identity-eid [dostęp: 2.03.2026]; K. Valgur, *Kakskümmend aastat tagasi väljastati esimene ID-kaart* (*Twenty years ago, the first ID card was issued*) (dostępne w j. estońskim), Ärileht (28.01.2022 r.), https://arileht.delfi.ee/artikkel/95755585/kakskummend-aastat-tagasi-valjastati-esimene-id-kaart [dostęp: 2.03.2026]; A. Parsovs, *Solving the Estonian ID Card Crisis: the Legal Issues*, [w:] *ISCRAM 2020 Conference Proceedings - 17th International Conference on Information Systems for Crisis Response and Management*, Blacksburg, Virginia (USA), May 2020, s. 459–471; A. Parsovs, *Estonian Electronic Identity Card: Security Flaws in Key Management*, [w:] *SEC'20: Proceedings of the 29th USENIX Conference on Security Symposium*, August 12–14, 2020, USENIX Association, USA, s. 1785-1802.

aparat rządowy strategię cyberbezpieczeństwa oraz uruchomiła pierwszą na świecie tzw. „ambasadę danych"[38].

Rozbudowane ramy regulacyjne w obszarze cyberbezpieczeństwa zostały w Estonii ustanowione ustawą o cyberbezpieczeństwie z 2018 r.[39], nowelizowaną w 2022 r., która w najbliższym czasie zostanie uzupełniona o przepisy wynikające z dyrektywy NIS 2. W konsekwencji nie zachodzi potrzeba zasadniczej rekonstrukcji estońskiego porządku prawnego w celu transpozycji tej dyrektywy, gdyż obowiązująca ustawa oraz akty wykonawcze wydane na jej podstawie w dużej mierze regulują wymogi w sposób spójny z rozwiązaniami przewidzianymi w NIS 2.

Za opracowywanie i koordynację polityki cyberbezpieczeństwa oraz wdrażanie strategii w tym obszarze odpowiada w Estonii Ministerstwo Spraw Gospodarczych i Komunikacji. Do jego zadań należy również koordynacja współpracy pomiędzy organami administracji publicznej, pozostałymi interesariuszami oraz społeczeństwem. W realizację strategii zaangażowane są także inne resorty, w tym właściwe do spraw edukacji, sprawiedliwości, obrony, spraw wewnętrznych, spraw zagranicznych oraz finansów, a także wyspecjalizowane agencje rządowe. Wśród nich należy wymienić Urząd Nadzoru Technicznego (*Technical Surveillance Authority*, „TJA"), odpowiedzialny za promowanie bezpieczeństwa i wiarygodności sprzętu łączności elektronicznej oraz nadzór nad dostawcami usług certyfikacyjnych i usług znakowania czasu; Estońską Fundację Internetową (*Estonian Internet Foundation*, „EIS"), reprezentującą estońską społeczność internetową i zarządzającą domeną krajową .ee; Państwową Fundację Infokomunikacyjną (*State Infocommunication Foundation*, „RIKS"), zapewniającą jakość, ciągłość, bezpieczeństwo oraz efektywność kosztową

[38] Zob. Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems, Luxembourg, 20th of June 2017; Republic of Estonia, *Estonia to establish the world's first data embassy in Luxembourg*, (20.06.2017 r.) https://www.valitsus.ee/en/news/estonia-establishworlds-first-data-embassy-luxembourg [dostęp: 2.03.2026]; e-Estonia, e-Governance, https://e-estonia.com/solutions/e-governance/data-embassy/ [dostęp: 2.03.2026]; B. Sierzputowski, *The data embassy under public international law*, „International and Comparative Law Quarterly" 2019, nr 68(1), s. 225-242; N. Heller, *Estonia, the Digital Republic*, „The New Yorker" 2018, nr 1(1), s. 1-12; A. Hardy, *Digital innovation and shelter theory: exploring Estonia's e-Residency, Data Embassy, and cross-border e-governance initiatives*, „Journal of Baltic Studies" 2024, nr 55(4), s. 793-810; N. Robinson, L. Kask, R. Krimmer, *The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis*, [w:] *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV '19)*, Association for Computing Machinery, Nowy Jork 2019, s. 391-396; N. Robinson, K. Martin, *Distributed denial of government: the Estonian Data Embassy Initiative*, „Network Security" 2017, nr 9, s. 13-16; T. Kotka, I. Liiv, *Concept of Estonian Government Cloud and Data Embassies*, [w:] A. Kő, E. Francesconi (red.) *Electronic Government and the Information Systems Perspective. EGOVIS 2015. Lecture Notes in Computer Science*, vol. 9265. Springer, Cham 2015; V. Rashica, *Data Embassy in the European Union: The Digital Diplomacy*, [w:] D. Ramiro Troitiño (red.) *E-Governance in the European Union. Contributions to Political Science*, Springer, Cham 2024.

[39] Ustawa z 23 maja 2018 r. o bezpieczeństwie cybernetycznym [Cybersecurity Act (Küberturvalisuse seadus) of 23rd May 2018] (dalej również jako: estońska ustawa, ustawa o cyberbezpieczeństwie).

państwowych usług komunikacyjnych i infrastrukturalnych, w tym rządowej chmury obliczeniowej; a także *Enterprise Estonia* i *Startup Estonia*, wspierające rozwój przedsiębiorczości i innowacyjności[40].

Zarządzanie operacyjne działaniami związanymi z bezpieczeństwem informacji oraz obsługą incydentów cybernetycznych w estońskich sieciach komputerowych zostało powierzone Organowi ds. Systemu Informacyjnego, działającemu na podstawie art. 12 ustawy o cyberbezpieczeństwie. Do jego kluczowych zadań należy zapewnienie bezpieczeństwa wszystkich sieci i systemów informatycznych niezbędnych do funkcjonowania państwa. W ramach tej struktury funkcjonuje również zespół reagowania na incydenty komputerowe CERT-EE, który prowadzi stały monitoring estońskiej cyberprzestrzeni oraz podejmuje działania mające na celu zapobieganie i neutralizację incydentów cybernetycznych.

Na tle rozwiązań przyjętych w Estonii szwedzki model zarządzania cyberbezpieczeństwem cechuje się natomiast wyższym stopniem decentralizacji oraz proaktywnym podejściem regulacyjnym. Charakteryzuje się to podziałem kompetencji pomiędzy liczne organy i agencje rządowe, co może prowadzić do trudności w koordynacji działań[41]. W literaturze zauważa się, że Estonia konsekwentnie wykazuje ścisłą zgodność z celami Unii Europejskiej w zakresie cyberbezpieczeństwa, nierzadko pełniąc funkcję punktu odniesienia dla innych państw członkowskich w obszarze implementacji polityk oraz innowacji strategicznych[42]. Mimo to, Szwecja właśnie wraz z Niemcami jako pierwsze kraje UE opracowały swoje krajowe strategie cyberbezpieczeństwa, co miało miejsce w 2005 r, lecz Estonia dokonała tego zaledwie dwa lata później ze względu na wspomnianą serię cyberataków[43]. Z pewnością różnicę w pozycji na arenie międzynarodowej w przypadku cyberobrony ukazuje krótki okres pobytu Szwecji w szeregach państw NATO, do którego dołączyła dopiero w 2024 r. Narastające zagrożenie militarne oraz cybernetyczne ze strony Federacji Rosyjskiej skłoniło Szwecję do przystąpienia właśnie do Organizacji Traktatu Północnoatlantyckiego. Bez wątpienia stanowiło to zasadniczą zmianę w jej tradycyjnej polityce bezpieczeństwa ze względu na dotychczasową neutralność, dlatego też

[40] D. Adamiec et al., *Informacja na temat legislacji… op.cit.*, s. 293-294.
[41] Zob. A. Andreasson et al., *Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval*, „Cognition, Technology & Work" 2024, nr 26, s. 709-731; E. Rehnstam, W. Winquist, S. Hacks, *NIS 2 Directive in Sweden: A Report on the Readiness of Swedish Critical Infrastructure*, [w:] L. Horn Iwaya et al. (red.), *Secure IT Systems. 29th Nordic Conference, Nord Sec 2024. Lecture Notes in Computer Science*, Cham 2025, s. 176-195.
[42] S. Enescu, *A comparative study on European cybersecurity strategies*, „Redefining Community in Intercultural Context" 2020, nr 9(1), s. 281.
[43] *Ibidem*, s. 278.

Szwedzi potrzebują czasu, aby dorównać pod tym względem innym państwom basenu Morza Bałtyckiego, takich jak Finlandia czy Estonia.

PODSUMOWANIE

Przeprowadzona analiza projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa pozwala stwierdzić, że proponowana nowelizacja stanowi jeden z najbardziej kompleksowych etapów dostosowania polskiego porządku prawnego do wymogów dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555, a zarazem odpowiedź na dynamicznie narastające zagrożenia w cyberprzestrzeni, determinowane zarówno czynnikami technologicznymi, jak i aktualną sytuacją geopolityczną. Projekt ten wpisuje się w szerszą tendencję postrzegania cyberbezpieczeństwa nie wyłącznie jako zagadnienia technicznego, lecz jako elementu bezpieczeństwa publicznego, ochrony zdrowia, ciągłości działania państwa oraz ochrony praw podstawowych, w tym prawa do ochrony danych osobowych.

Z perspektywy systemowej nowelizacja u.k.s.c. wzmacnia model regulacyjny oparty na odpowiedzialności podmiotowej i zarządczej, co znajduje bezpośrednie odzwierciedlenie w rozwiązaniach przewidzianych w NIS 2. Rozszerzenie katalogu podmiotów objętych obowiązkami ustawowymi, wprowadzenie rozróżnienia na podmioty kluczowe i podmioty ważne, a także zwiększenie zakresu odpowiedzialności kierownictwa jednostek należy ocenić jako krok w kierunku realnego podniesienia poziomu odporności krajowej infrastruktury cyfrowej. Jednocześnie jednak rozwiązania te rodzą istotne wyzwania w ramach wdrożenia ich do praktyki, w szczególności dla sektorów o ograniczonych zasobach finansowych i kadrowych.

Szczególnie wyraźnie problem ten ujawnia się w odniesieniu do sektora ochrony zdrowia. Umieszczenie szpitali i innych podmiotów leczniczych w kategorii podmiotów kluczowych jest oczywiście w pełni uzasadnione ze względu na charakter przetwarzanych danych, znaczenie usług zdrowotnych dla bezpieczeństwa publicznego oraz rosnącą skalę cyberataków. Natomiast analiza skutków finansowych projektowanej nowelizacji wskazuje, że bez adekwatnych mechanizmów wsparcia w zakresie finansowym i organizacyjnym mogą prowadzić do nadmiernego obciążenia placówek medycznych, przy czym i bez tego jest to już doskonale widoczne. W tym kontekście zasadne wydaje się postulowanie uzupełnienia systemu u.k.s.c. o dedykowane instrumenty kompensacyjne lub programy wsparcia dla podmiotów leczniczych, analogicznie do rozwiązań funkcjonujących w niektórych państwach członkowskich UE.

Na tle rozwiązań krajowych szczególnie wartościowe wnioski płyną z analizy estońskiego modelu cyberbezpieczeństwa. Estonia, jako państwo o wysokim poziomie

cyfryzacji i długoletnim doświadczeniu w przeciwdziałaniu zagrożeniom cybernetycznym, wypracowała spójny, scentralizowany i efektywny system zarządzania cyberbezpieczeństwem, który w znacznej mierze antycypuje rozwiązania przewidziane w unijnych dyrektywach. Na uwagę zasługuje zwłaszcza konsekwentne powiązanie strategii cyberbezpieczeństwa z innymi strategiami sektorowymi, jasne przypisanie odpowiedzialności podmiotom świadczącym usługi cyfrowe, a także silna rola jednego organu koordynującego działania operacyjne (RIA i CERT-EE). Polski ustawodawca mógłby czerpać z tego modelu w szczególności w zakresie lepszej integracji planowania strategicznego, skuteczniejszej koordynacji pomiędzy sektorowymi CSIRT oraz większego nacisku na prewencję i edukację jako elementy systemowe, a nie wyłącznie uzupełniające.

Podsumowując, projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa należy ocenić jako krok konieczny i zasadniczo zgodny z kierunkiem wyznaczonym przez prawo unijne, w szczególności dyrektywę NIS 2. Jednocześnie jednak jego skuteczność będzie zależała nie tylko od formalnej implementacji nowych przepisów, lecz od ich praktycznego wdrożenia, zapewnienia odpowiednich środków finansowych i organizacyjnych oraz uwzględnienia specyfiki sektorów wrażliwych, w szczególności takich jak ochrona zdrowia. Doświadczenia estońskie pokazują, że trwała odporność cybernetyczna państwa nie wymaga rozbudowanych regulacji prawnych (estońska ustawa ma 29 paragrafów przy 94 artykułach dotychczasowej wersji polskiego aktu prawnego), lecz przede wszystkim spójnej wizji strategicznej, stabilnych struktur instytucjonalnych oraz długofalowych inwestycji w kompetencje i kulturę cyberbezpieczeństwa.

BIBLIOGRAFIA

LITERATURA

Adamiec D. et al., *Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja)*, „Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu" 2021, nr 3(71).

Andreasson A. et al., *Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval*, „Cognition, Technology & Work" 2024, nr 26, s. 709-731

Bederna Z., Rajnai Z., *Analysis of the cybersecurity ecosystem in the European Union*, „International Cybersecurity Law Review" 2022, Vol. 3.

Belka E., *Deanonimizacja użytkowników sieci Tor*, „Cybersecurity & Cybercrime" 2021, nr. 1(1).

Blank S., *Web War I: Is Europe's First Information War a New Kind of War?*, „Comparative Strategy" 2008, nr 27(3).

Cath C.N.J., Glorioso L., Taddeo M., *NATO CCD COE Workshop on 'Ethics and Policies for Cyber Warfare' – A Report*, [w:] M. Taddeo, L. Glorioso (red.) *Ethics and Policies for Cyber Operations. Philosophical Studies Series*, vol. 124, Springer, Cham 2017.

Crandall M., Allan C., *Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms*, „Contemporary Security Policy" 2015, nr 36(2).

Enescu S., *A comparative study on European cybersecurity strategies*, „Redefining Community in Intercultural Context" 2020, nr 9(1).

Gao X., *Challenges and opportunities: Estonia's role in shaping EU cybersecurity policy*, [w:] A.-L. Högenauer, M. Mišík (red.), *Small States in EU Policy-Making: Strategies, Challenges, Opportunities*, Routledge, Abingdon-Nowy Jork 2024.

Graca W., *Protection of Cyberspace in Poland and the Czech Republic – the Role of Secret Services*, „Modern Management Review" 2022, nr 27(1).

Grimaila M.R., *The Genesis of the NATO Cooperative Cyber Defense Centre of Excellence*, „ISSA Journal" 2018, nr 16(8).

Guziak M., Ziarnik K., *Przegląd naruszeń cyberbezpieczeństwa danych medycznych w polskim sektorze ochrony zdrowia w 2023 roku*, „Rocznik Bezpieczeństwa Międzynarodowego" 2024, vol. 18, nr 2.

Haataja S., *The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach*, „Law, Innovation and Technology" 2017, nr 9(2).

Hardy A., *Digital innovation and shelter theory: exploring Estonia's e-Residency, Data Embassy, and cross-border e-governance initiatives*, „Journal of Baltic Studies" 2024, nr 55(4).

Heller N., *Estonia, the Digital Republic*, „The New Yorker" 2018, nr 1(1).

Hybrid Threats: 2007 cyber attacks on Estonia, [w:] S. Aday et al., *Hybrid Threats. A Strategic Communications Perspective*., Riga: NATO Strategic Communications Centre of Excellence, 2019.

Jacuch A., *Comparative Analysis of Cybersecurity Strategies. European Union Strategy and Policies. Polish and Selected Countries Strategies*, „Online Journal Modelling the New Europe" 2021, No. 37.

Jayakumar S., *Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness With Three Case Studies on Estonia, Singapore, and the United States*, [w:] A.P. Shmid (red.), *Handbook of Terrorism Prevention and Preparedness*, Haga 2021.

Kaiser R., *The birth of cyberwar*, „Political Geography" 2015, nr 46.

Kattel R., Mergel I., *Estonia's digital transformation: Mission mystique and the hiding hand*, "UCL Institute for Innovation and Public Purpose Working Paper Series" (IIPP WP 2018-09), Londyn 2018.

Kianpour M., Earls Davis P. A., Windekilde I. M., *Digital sovereignty in practice: analyzing the EU's NIS 2 directive*, „International Journal of Information Security" 2025, nr 24(167).

Kotka T., Liiv I., *Concept of Estonian Government Cloud and Data Embassies*, [w:] A. Kő, E. Francesconi (red.) *Electronic Government and the Information Systems Perspective. EGOVIS 2015. Lecture Notes in Computer Science*, vol. 9265. Springer, Cham 2015.

Kun E., *Unpacking the NIS 2 Directive: Enhancing EU Cybersecurity for the Digital Age*, [w:] R. Gsenger (red.), *Digital Decade: How the EU Shapes Digitalisation Research*, M.T. Sekwenz.

Limba T. et al., *Cyber security management model for critical infrastructure*, „Entrepreneurship and Sustainability Issues" 2017, nr 4(4).

Makuch J., Guziak M., *Cyberbezpieczeństwo w sektorze ochrony zdrowia. Przypadek Polski na tle tendencji światowych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2020, vol. 14, nr 2.

Ottis R., *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective*, [w:] D. Remenyi (red.), *Proceedings of the 7th European Conference on Information Warfare and Security*, Plymouth 2008.

Parsovs A., *Estonian Electronic Identity Card: Security Flaws in Key Management*, [w:] *SEC'20: Proceedings of the 29th USENIX Conference on Security Symposium*, August 12–14, 2020, USENIX Association, USA.

Parsovs A., *Solving the Estonian ID Card Crisis: the Legal Issues*, [w:] *ISCRAM 2020 Conference Proceedings - 17th International Conference on Information Systems for Crisis Response and Management*, Blacksburg, Virginia (USA), May 2020.

Poniatowska-Jaksch M., *Ransomware w sektorze ochrony zdrowia – przyczyny, konsekwencje*, „Kwartalnik Nauk o Przedsiębiorstwie" 2024, nr 4.

Rashica V., *Data Embassy in the European Union: The Digital Diplomacy*, [w:] D. Ramiro Troitiño (red.) *E-Governance in the European Union. Contributions to Political Science*, Springer, Cham 2024.

Rehnstam E., Winquist W., Hacks S., *NIS 2 Directive in Sweden: A Report on the Readiness of Swedish Critical Infrastructure*, [w:] L. Horn Iwaya et al. (red.), *Secure IT Systems. 29th Nordic Conference, Nord Sec 2024. Lecture Notes in Computer Science*, Cham 2025.

Robinson N., Kask L., Krimmer R., *The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis*, [w:] *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV '19)*, Association for Computing Machinery, Nowy Jork 2019.

Robinson N., Martin K., *Distributed denial of government: the Estonian Data Embassy Initiative*, „Network Security" 2017, nr 9.

Shackelford S., *Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks*, „Journal of Internet Law, Forthcoming" 2009, s. 1-12.

Sierzputowski B., *The data embassy under public international law*, „International and Comparative Law Quarterly" 2019, nr 68(1).

Teichmann F., C*ybersecurity of critical infrastructure in europe: the NIS 2 directive in Focus*, „International Cybersecurity Law Review" 2025, Vol. 6.

Tvaronavičienė M. et al., *Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania*; „Insights into Regional Development" 2020, nr 2(4).

Tyrawa D., *Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane*, „International Journal of Legal Studies" 2023, nr 1(13).

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, K. Czaplicki (red.), A. Gryszczyńska, Warszawa 2019.

Waxman M.C., *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, „Yale Journal of International Law" 2011.

AKTY PRAWNE

Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems, Luxembourg, 20th of June 2017.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80 z późn. zm.)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm.).

Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk sejmowy nr 1955, Warszawa, 7 listopada 2025 r.)

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.).

Ustawa z 23 maja 2018 r. o bezpieczeństwie cybernetycznym [*Cybersecurity Act* (*Küberturvalisuse seadus*) *of 23rd May 2018*].

INNE PUBLIKACJE

CSS (Centre for Security Studies), *Estonia's National Cybersecurity and Cyberdefence Posture. Policy and Organizations*, ETH Zürich 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf [dostęp: 2.03.2026].

Education Estonia, *How it all began? From Tiger Leap to digital society*, https://www.educationestonia.org/tiger-leap/ [dostęp: 2.03.2026].

e-Estonia, *e-Education and research*, https://e-estonia.com/solutions/e-education-and-research/education_system/ [dostęp: 2.03.2026].

e-Estonia, e-Governance, https://e-estonia.com/solutions/e-governance/data-embassy/ [dostęp: 2.03.2026].

K. Valgur, *Kakskümmend aastat tagasi väljastati esimene ID-kaart* (*Twenty years ago, the first ID card was issued*) (dostępne w j. estońskim), Ärileht (28.01.2022 r.), https://arileht.delfi.ee/artikkel/95755585/kakskummend-aastat-tagasi-valjastati-esimene-id-kaart [dostęp: 2.03.2026].

Raport pt. Wpływ projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa na szpitale publiczne, red. U. Szybowicz, I. Wochlik, Polskie Towarzystwo Koordynowanej Ochrony Zdrowia, Izba Gospodarcza Farmacja Polska, Fundacja AI LAW TECH i Federacja Przedsiębiorców Polskich, Warszawa, październik 2025, https://ptkoz.org/wp-content/uploads/2025/10/u.k.s.c.-a-szpitale-publiczne.pdf [dostęp: 2.03.2026].

Republic of Estonia Information System Authority, *Electronic Identity eID*, https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/electronic-identity-eid [dostęp: 2.03.2026].

Republic of Estonia, *Estonia to establish the world's first data embassy in Luxembourg*, Republic of Estonia, 20.06.2017 r., https://www.valitsus.ee/en/news/estonia-establishworlds-first-data-embassy-luxembourg [dostęp: 2.03.2026].

THE NATIONAL CYBERSECURITY SYSTEM IN LIGHT OF THE DRAFT AMENDMENT IN THE CONTEXT OF HOSPITAL OPERATIONS AGAINST THE BACKGROUND OF EU DIRECTIVES AND THE LEGISLATION OF SELECTED EU MEMBER STATES

Summary: On 21 October 2025, the Council of Ministers adopted a draft act amending the Act on the National Cybersecurity System and certain other statutes. The proposal constitutes a response to the growing scale of threats in cyberspace, particularly in the context of the current geopolitical situation, and forms part of a broader process aimed at strengthening the State's resilience to cyber threats and implementing EU directives on network and information security. Key solutions include, inter alia, the extension of the catalogue of entities obliged to ensure digital security. These measures collectively enhance the accountability of managers of institutions and enterprises covered by the NCS. They are also linked to the creation of a national response plan for major incidents, which will define cooperation principles and procedures for situations that threaten essential public and economic services, such as power plants or hospitals. Particular attention should be paid to the potential impact of the proposed act on the functioning of the latter and other healthcare facilities, especially in financial terms. The purpose of this chapter is to assess the main assumptions of the draft act and to compare them with statutory solutions adopted in other EU Member States. In addition, the chapter seeks to address questions concerning the impact of the amendment on the operation of hospitals and other healthcare institutions.

Keywords: national cybersecurity system; NIS 2; CSIRT; healthcare system.

Wiktoria Grzesiuk
Uniwersytet SWPS w Warszawie
wi.grzesiuk@gmail.com
https://orcid.org/0009-0000-9931-5683

SKUTECZNOŚĆ PRAWA DO SPRZECIWU W ODNIESIENIU DO DANYCH WYWNIOSKOWANYCH PRZEZ WYJAŚNIALNĄ SZTUCZNĄ INTELIGENCJĘ

Streszczenie: Dynamiczna ewolucja systemów sztucznej inteligencji doprowadziła do upowszechnienia danych wywnioskowanych, generowanych w procesie predykcji algorytmicznej, a nie poprzez bezpośrednie pozyskiwanie informacji od osób fizycznych. Dane te, pomimo ich pośredniego charakteru, w sposób istotny kształtują sytuację prawną oraz ekonomiczną jednostek w kluczowych obszarach, takich jak rynek pracy. Skuteczność prawa do sprzeciwu, o którym mowa w art. 21 ust. 1 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 (Dz.U.UE.L. z 2016 r. Nr 119), opiera się na fundamencie przejrzystości operacji przetwarzania. Niemniej w przypadku modeli o charakterze *black-blox* założenie to staje się całkowicie iluzoryczne. Deficyt wglądu w proces wnioskowania oraz brak możliwości pozyskania informacji o znaczeniu poszczególnych zmiennych uniemożliwia podmiotowi danych wykazanie własnej „szczególnej sytuacji", co stanowi wymóg wynikający z treści przywołanego przepisu. Zjawisko to prowadzi do powstania radykalnej asymetrii informacyjnej, degradują instytucję prawa do sprzeciwu do wymiaru czysto fasadowego. Dodatkowe zagrożenie stanowi zjawisko halucynacji modeli generatywnych oraz wykorzystywanie przez nie zmiennych zastępczych, co może skutkować wystąpieniem dyskryminacji o charakterze pośrednim. W takich uwarunkowaniach ciężar dowodu w sposób faktyczny obciąża osobę fizyczną, która pozostaje pozbawiona instrumentów niezbędnych do zakwestionowania błędnych lub arbitralnych procesów wnioskowania. Przywrócenie pełnej skuteczności ochrony prawnej wymaga implementacji wyjaśnialnej sztucznej inteligencji, która pozwoli na rekonstrukcję przesłanek decyzyjnych oraz merytoryczną weryfikację rzetelności predykcji. W paradygmacie algorytmicznym wyjaśnialna sztuczna inteligencja nie stanowi jedynie fakultatywnego elementu transparentności, lecz jest warunkiem koniecznym dla urzeczywistnienia autonomii informacyjnej oraz sprawowania realnej kontroli nad własnymi danymi osobowymi.

Słowa kluczowe: dane wywnioskowane; ochrona danych osobowych; prawo do sprzeciwu; sztuczna inteligencja; RODO; przejrzystość algorytmiczna

WPROWADZENIE

Rozwój modeli predykcyjnych i generatywnych sztucznej inteligencji („AI"), w szczególności zaawansowanych modeli językowych, istotnie wpłynął na sposób tworzenia oraz wykorzystywania informacji o osobach fizycznych. W praktyce rekrutacyjnej i zarządzania zasobami ludzkimi pełnią funkcje analityczne, klasyfikacyjne i wspomagające decyzje[1]. Ich cechą wyróżniającą jest generowanie nowych informacji o jednostce w drodze algorytmicznego wnioskowania, niezależnie od jej aktywnego udziału w procesie przetwarzania. Podstawę stanowi analiza masowych zbiorów danych (*big data*) prowadzona z wykorzystaniem złożonych systemów obliczeniowych, co umożliwia formułowanie wniosków wykraczających poza treści pozyskane bezpośrednio od osób fizycznych. Informacje te, zdefiniowane w literaturze jako dane wywnioskowane (*inferred data*), nie stanowią prostego odzwierciedlenia rzeczywistości, lecz rezultat statystycznych przewidywań oraz wzorców wyuczonych przez model. W konsekwencji mogą obejmować cechy lub prognozy przypisywane osobie fizycznej, które nigdy nie zostały przez nią dobrowolnie ujawnione[2]. Ryzyko ulega spotęgowaniu w związku z intensyfikacją zastosowań systemów AI w sektorach wysokiego ryzyka, gdzie wynik predykcji wpływa na sytuację prawną lub faktyczną osoby, w tym na dostęp do zatrudnienia lub warunki wykonywania pracy[3].

Dodatkowy problem wynika z ograniczonej wykrywalności i weryfikowalności wniosków inferencyjnych. Trudność polega na ustaleniu, w jakim zakresie instrumenty ochrony danych osobowych pozwalają jednostce na realną kontrolę nad danymi wywnioskowanymi oraz na skuteczne zakwestionowanie ich przetwarzania. Na tym tle szczególne znaczenie zyskuje prawo do sprzeciwu, opisane w art. 21 ust. 1 ogólnego rozporządzenia o ochronie danych („RODO")[4], które inicjuje ponowne ważenie interesów stron w perspektywie indywidualnej sytuacji jednostki. Procedura wymaga jednak elementarnej wiedzy o tym, jakie dane podlegają przetwarzaniu,

[1] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Dz.U.UE.L. z 2024 r. poz. 1689), („AI Act"), motyw 57.

[2] M. Sakowska-Baryła, *2.2.7.7. Dane osobowe* [w:] *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

[3] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, *III.3.6. Prawo sprzeciwu oraz dalsze czynniki* [w:] *Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE*, 844/14/PL, WP 217, s. 50.

[4] 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 (Dz.U.UE.L. z 2016 r. Nr 119 z późn. zm.).

z jakich przesłanek powstała dana inferencja oraz jaką rolę odgrywa ona w procesie decyzyjnym.

Dalsze rozważania koncentrują się na ocenie materialnej wykonalności prawa do sprzeciwu w sytuacji, w której przedmiotem przetwarzania są dane wywnioskowane generowane przez AI. Zastosowanie znajduje metoda dogmatycznoprawna, uzupełniona analizą funkcjonalną uwzględniającą techniczne uwarunkowania powstawania inferencji, w tym nietransparentność modeli. Przyjęta teza zakłada silną korelację skuteczności prawa do sprzeciwu z możliwością uzasadnienia przesłanek inferencji. Realna wykonalność art. 21 ust. 1 RODO jest uzależniona od zastosowania technologii wyjaśnialnej AI (*Explainable Artificial Intelligence*, „XAI"), pozwalającej na identyfikację czynników decydujących o wyniku oraz rekonstrukcję podstaw wnioskowania. Bez technicznej możliwości zrozumienia, a w konsekwencji zakwestionowania procesu wnioskowania, prawo do sprzeciwu ulega degradacji do formy czysto nominalnej, pozbawionej realnej funkcji ochronnej. Wdrożenie rozwiązań XAI jawi się zatem jako warunek *sine qua non* przywrócenia rzeczywistej autonomii informacyjnej jednostki.

1. DANE WYWNIOSKOWANE JAKO KATEGORIA OCHRONY DANYCH

Dla dalszego wywodu kluczowe znaczenie posiada rozróżnienie danych wywnioskowanych od podstawowych kategorii funkcjonujących w doktrynie. Pierwszą z nich stanowią dane deklaratywne oparte na dobrowolnym i intencjonalnym udostępnieniu informacji przez osobę fizyczną, najczęściej w drodze bezpośrednich oświadczeń. Drugą grupę tworzą dane zaobserwowane będące rezultatem rejestracji behawioralnej aktywności jednostki, takiej jak historia lokalizacji i logi systemowe[5]. Z kolei dane wytworzone dzielą się na pochodne oraz wywnioskowane. Dane pochodne wynikają z relatywnie prostego przekształcenia danych pierwotnych, m.in. poprzez obliczenia lub klasyfikacje o stałej regule, bez elementu predykcji. Dane wywnioskowane stanowią natomiast rezultat wytworzenia dodatkowej treści, ponad zakres danych pierwotnych. Opierają się na statystycznym prawdopodobieństwie przypisanym przez model, w którego sposób wyznaczenia podmiot danych nie ma wglądu. W konsekwencji osoba, której dane dotyczą, zostaje pozbawiona naturalnego punktu odniesienia umożliwiającego zakwestionowanie prawdziwości takiej informacji. Ponadto zwiększa się potencjał ich oddziaływania na sytuację osoby[6].

[5] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym*, Warszawa 2018, s. 36-38.
[6] M. Gumularz, *1.1.1. Informacje przekazane przez odbiorcę usługi* [w:] *Akt o usługach cyfrowych. Komentarz*, M. Gumularz (red.), Warszawa 2024, art. 6.

Powyższy deficyt wymusza kwalifikację danych wywnioskowanych jako danych osobowych w rozumieniu art. 4 pkt 1 RODO. Z perspektywy systemowej rozstrzygające znaczenie ma tu bowiem nie samo źródło ani technika generowania, lecz możność powiązania informacji z osobą zidentyfikowaną lub możliwą do zidentyfikowania. Szeroką wykładnię pojęcia danych osobowych potwierdza orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej. W wyroku z 20 grudnia 2017 r. w sprawie Piotra Nowaka przeciwko *Data Protection Commissioner* (sygn. akt C-434/16)[7] wskazano, że związek informacji z osobą może wynikać nie tylko z samej treści, lecz również z celu bądź skutku przetwarzania, o ile umożliwia to ocenę osoby lub oddziałuje na jej sytuację. W rezultacie inferencje odnoszące się do cech indywidualnych, nawet przy ujęciu probabilistycznym, mogą spełniać przesłanki kwalifikacji jako dane osobowe. Ponadto kryterium identyfikowalności należy oceniać przez pryzmat „racjonalnie prawdopodobnych" środków w rozumieniu motywu 26 RODO. W wyroku z 19 października 2016 r. w sprawie Patryka Breyer'a przeciwko *Bundesrepublik Deutschland* (sygn. akt C-582/14)[8] TSUE przyjął, iż informacja może stanowić dane osobowe także wówczas, gdy identyfikacja wymaga zestawienia z danymi pozostającymi u podmiotu trzeciego, jeżeli dostęp do takich środków prawnych lub organizacyjnych pozostaje realny.

W praktyce kontrowersje budzą procesy inferencyjne dotyczące szczególnych kategorii danych osobowych, np. przekonań światopoglądowych lub politycznych. Ryzyko obejmuje nieuzasadnioną ingerencję w sferę praw i wolności jednostki, a także obejście zakazów z art. 9 RODO. Istotną cechą wielu współczesnych modeli predykcyjnych jest ich nietransparentność, definiowana w literaturze jako mechanizm „czarnej skrzynki" (*black-box*)[9]. Oznacza to strukturalną niemożność rekonstrukcji wewnętrznych parametrów operacyjnych modelu i sposobu hierarchizacji poszczególnych danych, które zdeterminowały wygenerowanie konkretnej inferencji. Ograniczona zostaje kontrola *ex ante* i weryfikacja *ex post*, a potęguje wykorzystywanie zmiennych zastępczych, rozumianych jako parametry pozornie neutralne, jednak silnie skorelowane z kategorią danych wrażliwych[10].

Przetwarzanie danych wywnioskowanych przez AI generuje wielowymiarowe ryzyka wynikające bezpośrednio z natury tych procesów. Przykładowym,

[7] Wyrok TSUE z dnia 20 grudnia 2017 r., C-434/16.
[8] Wyrok TSUE z dnia 19 października 2016 r., C-582/14.
[9] G. Bar, *4. Główne parametry stosowane w systemach rekomendacji*, [w:] J. Gołaczyński (red.), R. Skibicki (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa 2024, art. 27.
[10] A. Holzinger, A. Saranti, C. Molnar, P. Biecek, W. Samek, *Explainable AI Methods – A Brief Overview*, [w:] A. Holzinger (red.), R. Goebel (red.), R. Fong (red.), T. Moon (red.), K.R. Müller (red.), W. Samek (red.), *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020*, Cham 2022, s. 27-28.

wspomnianym wyżej obszarem, jest sektor zatrudnienia. Systemy wspomagające rekrutację oraz zarządzanie personelem coraz częściej operują na algorytmicznych profilach kandydatów, obejmujących np. ich efektywność. Inferencje te, choć prezentowane jako technologicznie obiektywne, mogą w praktyce prowadzić do niejawnej selekcji oraz utrwalania barier w dostępie do rynku pracy, naruszając zasadę równego traktowania. Przetwarzanie danych wywnioskowanych, pozbawione adekwatnej kontroli, prowadzi do znacznego osłabienia pozycji osoby fizycznej, traktując ją jako bierny obiekt algorytmicznej oceny, a nie aktywny podmiot ochrony danych osobowych[11]. Dane wywnioskowane wchodzą w szczególnie intensywny konflikt z zasadą prawidłowości, ponieważ statystyczny charakter treści zwiększa podatność na błąd, a tym samym wymusza mechanizmy weryfikacyjne silniejsze niż w przypadku danych deklaratywnych. Zasada przejrzystości napotyka ograniczenia wynikające z konstrukcji modeli typu *black-box*, co osłabia praktyczną wykonalność prawa dostępu (art. 15 RODO), sprostowania (art. 16 RODO) oraz ograniczenia przetwarzania (art. 18 RODO), a przede wszystkim sprzeciwu (art. 21 ust. 1 RODO)[12]. Dodatkowe znaczenie uzyskuje uwarunkowanie ról podmiotowych. W środowisku systemów AI może dojść do rozproszenia odpowiedzialności między podmiotem wdrażającym narzędzie, dostawcą modelu, podmiotem utrzymującym infrastrukturę oraz podmiotem wykorzystującym wynik w procesie decyzyjnym. Kryterium „celów i sposobów" z art. 4 pkt 7 RODO wymaga każdorazowej rekonstrukcji, kto determinuje cele wykorzystania inferencji oraz kto kształtuje istotne elementy sposobu przetwarzania[13].

2. ILUZORYCZNOŚĆ PRAWA DO SPRZECIWU (ART. 21 UST. 1 RODO) W ŚRODOWISKU AI

Prawo do sprzeciwu, uregulowane w art. 21 ust. 1 RODO, stanowi jedno z kluczowych uprawnień ochronnych i mechanizm korekcyjny, mający umożliwić osobie fizycznej zakwestionowanie przetwarzania opartego na art. 6 ust. 1 lit. e

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689), motyw 56.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), motyw 129.

[13] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym*, Warszawa 2018, s. 56-58.

lub f. Prawodawca w art. 21 ust. 1 RODO wyraźnie zaznacza także możliwość sprzeciwienia się profilowaniu, zdefiniowanemu w art. 4 pkt 4 RODO jako dowolna forma zautomatyzowanego przetwarzania danych osobowych ukierunkowana na ocenę czynników osobowych, w szczególności analizę lub prognozę aspektów dotyczących m.in. efektów pracy, sytuacji ekonomicznej lub zdrowotnej. Konstrukcja art. 21 ust. 1 RODO zakłada utrzymanie równowagi interesów i przywrócenie jednostce kontroli w sytuacji, gdy wnioskowanie algorytmiczne prowadzi do wytworzenia oceny oraz jej wykorzystania w procesie decyzyjnym[14]. Skuteczność sprzeciwu pozostaje jednak warunkowa i uzależniona od zdolności wykazania relewantnych okoliczności po obu stronach. Wymaga to minimalnej wiedzy co do zakresu i logiki przetwarzania. W odniesieniu do nieprzejrzystych inferencji algorytmicznych, sprzeciw przybiera zatem postać uprawnienia iluzorycznego[15].

Prawo do sprzeciwu rozkłada ciężar dowodu pomiędzy każdą ze stron. Podmiot danych wskazuje przyczyny związane ze swoją „szczególną sytuacją". Na poziomie praktycznym oznacza to konieczność wykazania, że w danym stanie faktycznym przetwarzanie wywołuje szczególny ciężar, szczególne ryzyko lub szczególną ingerencję w sferę praw i wolności, w stopniu większym niż wobec ogółu podmiotów danych[16]. Tak ujęta metodologia jest racjonalna przy danych deklaratywnych lub obserwowanych, ponieważ jednostka dysponuje przynajmniej orientacyjną wiedzą o zakresie informacji przekazanych albo o zachowaniach zarejestrowanych. W odniesieniu do danych wywnioskowanych ten punkt odniesienia zanika. Osoba otrzymuje sam rezultat wnioskowania, często w formie oceny, kategorii bądź rekomendacji, bez informacji o przesłankach prowadzących do jego powstania oraz o danych wejściowych, które w największym stopniu ukształtowały wynik. Sprzeciw wymaga wówczas argumentacji niemożliwej do zbudowania[17].

Z kolei po stronie administratora pojawia się obowiązek wykazania „ważnych prawnie uzasadnionych podstaw" nadrzędnych wobec interesów, praw i wolności osoby bądź podstaw związanych z ustaleniem, dochodzeniem lub obroną roszczeń. W ujęciu systemowym przesłanka „wykazania" pozostaje ściśle związana z zasadą rozliczalności (art. 5 ust. 2 RODO). Nie wystarcza zatem samo powołanie interesu administratora; konieczne pozostaje przedstawienie uzasadnienia umożliwiającego

[14] M. Czerniawski, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa (red.), D. Lubasz (red.), Warszawa 2018, art. 21.
[15] K. Maciejewska, *4. Etyka systemów sztucznej inteligencji dla wymiaru sprawiedliwości*, [w:] *Prawo sztucznej inteligencji i nowych technologii 3*, B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), Warszawa 2023.
[16] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. III*, Warszawa 2025, art. 21.
[17] G. Bar, *4. Główne parametry stosowane w systemach rekomendacji… op.cit.*, art. 27.

weryfikację, dlaczego w realiach konkretnej sprawy interes ten przeważa. Powstaje zatem dysonans, gdzie norma wymaga weryfikowalnej argumentacji, a technologia dostarcza jedynie rezultatu bez przesłanek. W tym przypadku sprzeciw nie inicjuje realnego ważenia interesów, ponieważ żadna ze stron nie ma dostępu do informacji dla stosownego uzasadnienia stanowiska. Efektem jest decyzja oparta na praktyce organizacyjnej, a nie na mechanizmie prawnym[18].

Powyższy deficyt jest wielowymiarowy. Po pierwsze – obecna jest niepewność co do samego faktu wytworzenia danych wywnioskowanych, gdyż operacje inferencyjne przebiegają „w tle", natomiast obowiązki informacyjne bywają realizowane ogólnikowo[19]. Po drugie – nawet przy świadomości istnienia inferencji, brak dostępu do danych wejściowych oraz do oceny ich jakości uniemożliwia wskazanie błędów wynikających z nieaktualności i niepoprawności. Po trzecie – w modelach typu *black-box* nie jest znane znaczenie poszczególnych zmiennych w konkretnej predykcji. Analogicznie niewidoczny pozostaje problem zmiennych zastępczych, gdzie parametr formalnie neutralny pełni funkcję substytutu cechy wrażliwej, prowadząc do dyskryminacji pośredniej. Po czwarte – niejasny bywa także status inferencji w procesie decyzyjnym, gdzie informacja może mieć charakter wyłącznie pomocniczy albo wręcz dominujący[20].

Iluzoryczność prawa do sprzeciwu wzmacnia relacja art. 21 i art. 22 RODO. Treść art. 22 ust. 1 przewiduje możliwość niepodlegania decyzji, wywołującej skutek prawny lub podobnie istotny wpływ, opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Zastosowanie tego reżimu zależy więc od spełnienia przesłanki „wyłączności" automatyzacji, z zastrzeżeniem wyjątków przewidzianych w art. 22 ust. 2 RODO. Mianowicie w przypadkach określonych w art. 22 ust. 2 lit. a i c administrator obowiązany jest zapewnić co najmniej gwarancje z art. 22 ust. 3 RODO, tj. prawo do uzyskania interwencji ludzkiej ze strony administratora, prawo do wyrażenia własnego stanowiska oraz prawo do zakwestionowania takiej decyzji[21]. W praktyce procesy decyzyjne bywają projektowane tak, aby formalnie wyłączyć art. 22 RODO poprzez dodanie „czynnika ludzkiego" sprowadzonego do

[18] J. Rzymowski, *2. Prawa i wolności, doniosłość zjawiska na gruncie RODO*, „Przegląd Prawa Publicznego" 2024, nr 4, s. 1-2.

[19] P. Fajgielski, *Rzetelność jako ogólna zasada przetwarzania danych osobowych*, „Gdańskie Studia Prawnicze" 2021, nr 4, s. 15-17.

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689), motyw 67.

[21] D. Lubasz, *3. Zasada przejrzystości*, [w:] *Rok RODO*, W.R. Wiewiórowski (red.), H. Wolska (red.), Warszawa 2019.

akceptacji rekomendacji algorytmu. Taki zabieg nie przesądza jednak jeszcze o braku „wyłączności" automatyzacji, ponieważ rozstrzygające znaczenie ma realny charakter interwencji ludzkiej. Pozorny udział człowieka może oznaczać utrzymanie decyzji w rozumieniu art. 22 ust. 1 RODO, co sprzyja kwalifikowaniu wielu procesów jako „niewyłącznie" zautomatyzowanych, w efekcie czego ciężar ochrony zostaje przesunięty na art. 21 ust. 1 RODO, obciążony wymogiem wykazania „szczególnej sytuacji", trudnym do zrealizowania bez wglądu w przesłanki inferencji[22]. Znaczenie problemu uwydatnia wyrok Trybunału Sprawiedliwości Unii Europejskiej z 7 grudnia 2023 r. w sprawie UF i AB przeciwko Land Hessen (sygn. akt C-26/22)[23]. TSUE wskazał, iż nawet automatyczne ustalenie punktacji (*scoring*) może mieścić się w ramach art. 22 RODO, jeżeli w sposób dominujący kształtuje rozstrzygnięcie podejmowane wobec osoby przez podmiot trzeci. Orzeczenie to ogranicza możliwość obejścia art. 22 RODO przez rozłożenie procesu na etapy i przedstawianie wyniku algorytmu jako neutralnej informacji pomocniczej. Nie eliminuje jednak źródła iluzoryczności sprzeciwu. Przepis nie obejmuje wielu konfiguracji przetwarzania danych wywnioskowanych, typowych dla rekrutacji i zarządzania personelem, w których inferencje służą chociażby preselekcji lub tworzeniu rekomendacji, przy utrzymaniu czysto formalnego udziału człowieka. W takich przypadkach ochrona bywa redukowana do art. 21 ust. 1 RODO, obciążonego wymogiem wykazania „szczególnej sytuacji". Bez dostępu do przesłanek inferencji wymóg ten staje się trudny do zrealizowania, a ponowne ważenie interesów przybiera postać deklaratywną. Z tego względu rozstrzygnięcie kwalifikacyjne na styku art. 21 i art. 22 RODO nie osłabia tezy o konieczności zastosowania XAI, lecz ją wzmacnia. Wyjaśnialność stanowi bowiem warunek pozwalający podmiotowi danych skonkretyzować sprzeciw, a administratorowi – rozliczalnie wykazać podstawy dalszego przetwarzania, jak również zweryfikować, czy interwencja ludzka miała charakter rzeczywisty, czy wyłącznie formalny (pozorny)[24].

3. XAI JAKO WARUNEK SKUTECZNOŚCI PRAWA DO SPRZECIWU

Mechanizm XAI należy ujmować jako zbiór metod interpretacyjnych służących uzyskaniu funkcjonalnego wglądu w działanie modeli uczenia maszynowego,

[22] D. Lubasz, *1. Profilowanie a zautomatyzowane podejmowanie decyzji* [w:] *Rok RODO*, W.R. Wiewiórowski (red.), H. Wolska (red.), Warszawa 2019.
[23] Wyrok TSUE z dnia 07 grudnia 2023 r., C-26/22.
[24] A. Monarcha-Matlak, *3. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach oraz profilowanie* [w:] *Internet. Przetwarzanie danych osobowych. Processing of personal data*, K. Czaplicki (red.), G. Szpor (red.), Warszawa 2019.

zwłaszcza modeli typu *black-box*. W perspektywie prawnej pełni rolę infrastrukturalną wobec zasady przejrzystości, ponieważ umożliwia przedstawienie przyczyn ukształtowania inferencji w postaci zrozumiałej dla człowieka. Stanowi nie tylko zestaw narzędzi, lecz również zasady doboru techniki adekwatnej do typu modelu, celu wyjaśnienia oraz ryzyk prawnych związanych z daną operacją przetwarzania. Tak rozumiana wyjaśnialność posiada znaczenie *stricte* normatywne, ponieważ warunkuje zdolność urzeczywistnienia konstrukcji praw podmiotowych opartych na indywidualizacji, argumentacji oraz weryfikacji proporcjonalności działań administratora[25].

Kluczowym elementem tej koncepcji jest rozróżnienie pomiędzy wyjaśnieniami globalnymi a lokalnymi. Wyjaśnienia globalne odnoszą się do ogólnej logiki modelu i systemowego znaczenia zmiennych, umożliwiając ocenę zgodności systemu z założonymi celami przetwarzania. Z kolei wyjaśnienia lokalne koncentrują się na jednostkowym przypadku, pozwalając na identyfikację cech wejściowych, które zdeterminowały konkretną inferencję. W kontekście art. 21 ust. 1 RODO relewantność wyjaśnialności lokalnej ma charakter priorytetowy. Sprzeciw wymaga bowiem wskazania przyczyn związanych ze „szczególną sytuacją". Wyjaśnienia globalne nie zapewniają tego efektu, gdyż operują poziomem abstrakcji niewystarczającym do wykazania, jakie parametry przesądziły o wyniku wnioskowania oraz dlaczego dalsze przetwarzanie narusza interesy lub prawa osoby, której dane dotyczą[26].

Realizacja wyjaśnialności lokalnej przebiega za pośrednictwem technik takich jak *Local Interpretable Model-agnostic Explanations* („LIME") oraz *SHapley Additive exPlanations* („SHAP"). Technika LIME przeprowadza analizę działania sieci poprzez konstruowanie uproszczonego modelu zastępczego, symulującego zachowanie modelu głównego. Z kolei SHAP przypisuje poszczególnym cechom wkład w wynik predykcji względem wartości bazowej, wskazując, które elementy danych wejściowych ukształtowały wynik. Ich wspólny mianownik stanowi koncepcja *post-hoc*, polegająca na wyjaśnianiu wyniku już po jego wygenerowaniu, bez ingerencji w parametry ani kod źródłowy. Zapewniają wgląd funkcjonalny, wystarczający do poddania wyniku kontroli pod kątem rzetelności, adekwatności oraz zgodności z celem przetwarzania[27]. W konsekwencji możliwe staje się sformułowanie zarzutu konkretnego, odnoszonego do danych wejściowych, ich jakości, relewantności oraz do relacji między cechami a rezultatem. W przypadku danych wywnioskowanych ma to znaczenie szczególne, ponieważ błąd lub stronniczość ujawnia się często nie na

[25] K. Maciejewska, *Etyka systemów sztucznej inteligencji… op.cit.*
[26] Y. Yamada, *Judicial Decision-Making and Explainable aI (XAI) – Insights from the Japanese Judicial System*, „Studia Iuridica Lublinensia" 2023, nr 4, s. 163-165.
[27] A. Holzinger, A. Saranti, C. Molnar, P. Biecek, W. Samek, *Explainable AI Methods – A Brief Overview…*, *op.cit.*, s. 15-16, 24-26.

poziomie danych pierwotnych, lecz na poziomie zależności statystycznych i ważenia cech determinujących wynik. Wyjaśnialność staje się warunkiem *sine qua non* materialnej wykonalności prawa do sprzeciwu.

Uzupełnienie powyższych metod stanowią techniki atrybucji cech (*feature attribution*), służące do oceny wpływu poszczególnych zmiennych wejściowych w kontekście finalnego wyniku. Tego rodzaju narzędzia umożliwiają operacjonalizację zasad z art. 5 RODO w wymiarze indywidualnym. Zasada minimalizacji przestaje mieć charakter deklaratywny, gdyż możliwe staje się wykazanie, iż wynik oparto na danych zbędnych, marginalnie związanych z celem lub na cechach wrażliwych. W kontekście spełnienia zasady prawidłowości, wyjaśnialność pozwala ujawnić, czy predykcję zbudowano na danych nieaktualnych, błędnych, niekompletnych bądź przeniesionych z kontekstu odmiennego od celu przetwarzania. Z kolei zasada rzetelności zostaje zachowana poprzez możliwość zbadania, czy model nie wzmacnia uprzedzeń obecnych w danych treningowych oraz czy nie konstruuje substytutów danych szczególnych kategorii w sytuacji formalnego braku przetwarzania na podstawie art. 9 RODO[28].

Doniosłe znaczenie mają również analizy kontrfaktyczne (*counterfactual explanations*). Polegają na wskazaniu takich zmian w parametrach wejściowych, które – przy założeniu niezmienności pozostałych cech – prowadziłyby do odmiennego wyniku, przykładowo do zmiany oceny kandydata w procesie rekrutacyjnym. Techniki te pozwalają na odtworzenie procesu wnioskowania oraz zrozumienie struktur danych i zależności, którymi kierował się system podczas procesowania informacji. Z punktu widzenia ochrony danych osobowych istotne jest, że powyższe metody nie wymagają pełnego ujawnienia kodu źródłowego. W konsekwencji możliwe staje się wskazanie braku adekwatności przetwarzania oraz wykazanie, iż w konkretnej sytuacji jego kontynuacja prowadzi do nieproporcjonalnej ingerencji w sferę praw osoby, której dane dotyczą, w tym do ryzyka dyskryminacji pośredniej[29]. W szerszej perspektywie instytucjonalnej XAI należy postrzegać jako integralny element systemu *compliance* oraz urzeczywistnienie koncepcji *explainability-by-design*. Koncepcja ta pozostaje w ścisłej relacji z zasadą *privacy by design*, zakładającą konieczność

[28] A. Holzinger, A. Saranti, C. Molnar, P. Biecek, W. Samek, *Explainable AI: Past and Present* [w:] *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020*, A. Holzinger (red.), R. Goebel (red.), R. Fong (red.), T. Moon (red.), K.R. Müller (red.), W. Samek (red.), Cham 2022, s. 5-6.

[29] A. Holzinger, A. Saranti, C. Molnar, P. Biecek, W. Samek, *XAI: Counterfactual Explanations and Algorithmic Recourse*, [w:] *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020*, A. Holzinger (red.), R. Goebel (red.), R. Fong (red.), T. Moon (red.), K.R. Müller (red.), W. Samek (red.), Cham 2022, s. 143-144.

wbudowania mechanizmów ochrony praw jednostki już na etapie programowania systemów (art. 25 RODO)[30].

Pomimo istotnego potencjału XAI nie stanowi rozwiązania wolnego od wad. Należy wskazać na trudności w wymiarze finansowym, a także organizacyjnym. Integracja metod XAI z istniejącymi systemami predykcyjnymi wymaga dodatkowych zasobów obliczeniowych, specjalistycznej wiedzy oraz niekiedy modyfikacji architektury modelu, co może stanowić istotną barierę zwłaszcza dla mniejszych przedsiębiorstw. Dodatkowe ryzyko stanowi zjawisko *explainability-washing*. Polega ono na przedstawianiu pozornych lub nadmiernie uproszczonych wyjaśnień, które formalnie spełniają wymogi, jednak w rzeczywistości nie umożliwiają pozyskania kluczowych informacji na temat procesu wnioskowania, tym bardziej na temat potencjalnych źródeł błędu lub dyskryminacji. W konsekwencji zjawisko *explainability-washing* stanowi utrzymanie iluzoryczności ochrony, mimo technicznego wdrożenia XAI[31].

4. POSTULATY *DE LEGE FERENDA*

Zapewnienie realnej ochrony danych osobowych w środowisku algorytmicznym wymaga wzmocnienia standardów przejrzystości przetwarzania danych wywnioskowanych oraz samych praw podmiotowych[32]. W obowiązującym brzmieniu RODO można wskazać podstawy do formułowania oczekiwań dotyczących przejrzystości i rozliczalności, zwłaszcza w świetle art. 5 ust. 2 RODO oraz wymogu doboru środków adekwatnych do ryzyka. Oczekiwania te mają jednak w znacznej mierze charakter rekonstrukcyjny i interpretacyjny, a przez to nie zapewniają jednolitego, weryfikowalnego standardu wykonywania art. 21 ust. 1 RODO w realiach nieprzejrzystych modeli. Postulaty *de lege ferenda* zmierzają zatem do ich doprecyzowania poprzez wskazanie minimalnego standardu wyjaśnialności jako warunku *sine qua non* przywrócenia rzeczywistej autonomii informacyjnej jednostki.

Zasadne pozostaje wprowadzenie obowiązku stosowania rozwiązań zapewniających funkcjonalny wgląd w przesłanki inferencji w sektorach wysokiego ryzyka, priorytetowo w obszarach, gdzie dane wywnioskowane oddziałują na dostęp do dóbr podstawowych oraz na sytuację prawną lub ekonomiczną podmiotu danych, w szczególności zatrudnienie. Na tym tle istotne znaczenie zyskuje art. 13 ust. 2

[30] A. Bogucki, *Ethical, legal, and socioeconomic aspects of implementing artificial intelligence in tax administration*, „Annales Universitatis Lodziensis. Folia Iuridica" 2025, nr 110, s. 23-24.
[31] Z. Cheng, Y. Wu, Y. Li, L. Cai, B. Ihnaini, *A Comprehensive Review of Explainable Artificial Intelligence (XAI) in Computer Vision*, „Sensors" 2025, t. 25, art. 4166, DOI: https://doi.org/10.3390/s25134166.
[32] M. Czerniawski, *RODO. Ogólne rozporządzenie…*, *op.cit.*, art. 21.

lit. f RODO, którego zakres zastosowania ujawnia jednak kluczowe ograniczenia. Przepis pozostaje funkcjonalnie powiązany z konstrukcją art. 22 RODO, co prowadzi do jego pełniejszej realizacji, przede wszystkim w sytuacjach podejmowania decyzji wywołujących skutki prawne lub w podobny sposób istotnie wpływających na osobę fizyczną. Tymczasem znacząca część procesów inferencyjnych zachodzi na wcześniejszych etapach przetwarzania lub przybiera postać mechanizmów wspomagających decyzję, nie spełniając formalnych przesłanek zastosowania tego reżimu, mimo że w praktyce może determinować dalszy przebieg procesu decyzyjnego, jak ma to miejsce chociażby w procesach rekrutacyjnych czy ocenie ryzyka kredytowego.

W konsekwencji zakres obowiązku informacyjnego nie odpowiada rzeczywistemu znaczeniu generowanych inferencji dla sytuacji jednostki. Minimalny standard wyjaśnialności powinien mieć charakter funkcjonalny, a nie deklaratywny, oraz obejmować identyfikację kluczowych zmiennych i ich wpływu na rozstrzygnięcie. Uzupełnienie powinien stanowić wymóg udostępniania wyjaśnień kontrfaktycznych, pozwalających na ustalenie, jakie zmiany parametrów wejściowych prowadziłyby do odmiennego wyniku, a tym samym pozwalających wykryć zależności uboczne oraz użycie zmiennych zastępczych. Kluczowe znaczenie uzyskuje w tym kontekście obowiązek dostarczania wyjaśnień lokalnych, dotyczących konkretnych przypadków, które umożliwiałyby sformułowanie sprzeciwu spełniającego wymóg indywidualizacji oraz uruchomienie rzeczywistego, a nie jedynie iluzorycznego, ważenia interesów[33].

Analogiczne ograniczenia dostrzegalne są na gruncie AI Act. Obowiązki transparentności, przewidziane chociażby przez art. 13 AI Act, koncentrują się na relacji pomiędzy dostawcą a podmiotem stosującym system AI, natomiast regulacje odnoszące się bezpośrednio do osoby fizycznej, w tym art. 50 AI Act, mają charakter fragmentaryczny. Motyw 171 AI Act podkreśla znaczenie wyjaśnialności jako elementu godnej zaufania AI, nie kreując jednak samodzielnego standardu umożliwiającego rekonstrukcję procesu inferencyjnego przez podmiot danych. Aktualny model regulacyjny prowadzi do sytuacji, w której zakres obowiązku informacyjnego pozostaje uzależniony od formalnej kwalifikacji przetwarzania, zamiast od rzeczywistego znaczenia generowanych inferencji dla sytuacji osoby fizycznej.

Podobna trudność ujawnia się w kontekście „szczególnej sytuacji" jako przesłanki skutecznego wykonania prawa do sprzeciwu. W warunkach ograniczonej przejrzystości modeli algorytmicznych wymóg ten napotyka na istotne bariery dowodowe. W związku z tym rozważenia wymaga ustanowienie autonomicznego

[33] Ł. Osowicki, Ł. Kiełbus, R. Jóźwiak, *2. Zaufana sztuczna inteligencja – wyjaśnialność oraz przyczynowość* [w:] *Prawo sztucznej inteligencji i nowych technologii 2,* B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), Warszawa 2022.

uprawnienia do uzyskania wyjaśnienia odnoszącego się do konkretnego przypadku, obejmującego minimalny zakres informacji pozwalający na rekonstrukcję przesłanek wnioskowania oraz na ocenę, czy wynik oparto na danych adekwatnych, prawidłowych i proporcjonalnych w relacji do celu przetwarzania. W obszarach wysokiego ryzyka uzasadnienie przedstawia również modyfikacja rozkładu ciężaru dowodu. Administrator powinien wykazywać nie tylko formalną podstawę kontynuowania przetwarzania po wniesieniu sprzeciwu, lecz także rzetelność i niedyskryminacyjny charakter wnioskowania w odniesieniu do danej osoby, w tym brak oparcia wyniku na zmiennych zastępczych[34].

PODSUMOWANIE

Prawo do sprzeciwu, ujęte w art. 21 ust. 1 RODO, wobec przetwarzania danych wywnioskowanych ujawnia ograniczenia o charakterze strukturalnym. Opiera się na ponownym ważeniu interesów oraz indywidualizacji podstaw. W praktyce zakłada dostęp do informacji pozwalających zidentyfikować, jakie przesłanki doprowadziły do wytworzenia oraz wykorzystania danej inferencji. W warunkach algorytmicznego wnioskowania, zwłaszcza przy modelach typu *black-box*, wiedza ta nie jest zapewniana w stopniu umożliwiającym sformułowanie merytorycznych zarzutów. Podmiot danych konfrontuje się z rezultatem, bez możliwości ustalenia czynników decydujących, ich wagi oraz zależności wykorzystanych w procesie predykcyjnym. Prowadzi to do bariery proceduralnej, w ramach której „szczególna sytuacja" pozostaje przesłanką formalnie wymaganą, lecz faktycznie trudną do wykazania.

Dane wywnioskowane, mimo probabilistycznego charakteru, mogą stanowić dane osobowe w rozumieniu art. 4 pkt 1 RODO, o ile odnoszą się do osoby zidentyfikowanej lub możliwej do zidentyfikowania oraz oddziałują na nią. Inferencje dotyczące zdrowia lub preferencji rozszerzają zakres informacji o jednostce, zwiększają podatność na błąd oraz intensyfikują ryzyko dyskryminacji pośredniej, zwłaszcza przy wykorzystaniu zmiennych zastępczych. W konsekwencji osłabieniu ulega nie tylko możliwość zakwestionowania treści, lecz również praktyczne wyegzekwowanie zasad z art. 5 RODO. Zasada prawidłowości wymaga weryfikowalności, zasada minimalizacji – identyfikacji danych rzeczywiście relewantnych, a zasada rzetelności – wykrywalności stronniczości. Bez rekonstrukcji przesłanek przetwarzania realizacja tych standardów ulega redukcji do poziomu formalnego (iluzorycznego).

[34] K. Maciejewska, *Przejrzystość i identyfikowalność systemów sztucznej inteligencji* [w:] *Prawo Nowych Technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, J. Gołaczyński (red.), Warszawa 2022.

Ograniczenia dotyczą również administratora. Treść art. 21 ust. 1 RODO dopuszcza dalsze przetwarzanie po wniesieniu sprzeciwu jedynie przy wykazaniu „ważnych prawnie uzasadnionych podstaw" nadrzędnych wobec interesów, praw i wolności osoby fizycznej. Przy technologiach typu *black-box* administrator nierzadko nie dysponuje materiałem pozwalającym uzasadnić w sposób rozliczalny konieczność oraz proporcjonalność dalszego przetwarzania. Uzasadnienia przyjmują wówczas postać ogólnych odwołań do efektywności bądź optymalizacji, bez powiązania z indywidualnym stanem faktycznym. Powstaje paradoksalny mechanizm pozorności, gdzie podmiot danych nie dysponuje podstawą do skonkretyzowania sprzeciwu, administrator nie przedstawia weryfikowalnej odpowiedzi opartej na merytorycznych przesłankach, natomiast rozstrzygnięcie wynika z utrwalonych procedur organizacyjnych, a nie z rzeczywistego ważenia interesów wymaganego przez art. 21 RODO.

Przeprowadzona analiza prowadzi do potwierdzenia tezy, zgodnie z którą materialna skuteczność prawa do sprzeciwu wobec przetwarzania danych wywnioskowanych pozostaje uzależniona od technicznej możliwości rekonstrukcji logiki inferencji, a zatem od wdrożenia rozwiązań XAI. Wyjaśnialność, w szczególności w wariancie lokalnym, umożliwia identyfikację czynników przesądzających o wyniku, skalę wpływu poszczególnych cech, a także ułatwia wykrycie zmiennych zastępczych oraz pozwala wskazać, czy inferencja opiera się na danych błędnych, nieaktualnych lub nieadekwatnych do celu przetwarzania. Dopiero wówczas sprzeciw może przyjąć postać merytorycznej argumentacji oraz uruchomić kontrolę konieczności i proporcjonalności dalszego przetwarzania po stronie administratora. Przy braku takiego wglądu, art. 21 ust. 1 RODO ulega redukcji do uprawnienia iluzorycznego, niezdolnego do odtworzenia autonomii informacyjnej w warunkach wnioskowania, zwłaszcza w sektorach wysokiego ryzyka, gdzie inferencje pełnią funkcję *de facto* decyzyjną.

BIBLIOGRAFIA

LITERATURA

Bar G., *4. Główne parametry stosowane w systemach rekomendacji* [w:] *Akt o usługach cyfrowych. Komentarz*, J. Gołaczyński (red.), R. Skibicki (red.), Warszawa 2024, art. 27.

Bogucki A., *Ethical, legal, and socioeconomic aspects of implementing artificial intelligence in tax administration*, „Annales Universitatis Lodziensis. Folia Iuridica" 2025, nr 110, s. 23-24.

Cheng Z., Wu Y., Li Y., Cai L., Ihnaini B., *A Comprehensive Review of Explainable Artificial Intelligence (XAI) in Computer Vision*, „Sensors" 2025, t. 25, art. 4166. https://doi.org/10.3390/s25134166.

Czerniawski M., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa (red.), D. Lubasz (red.), Warszawa 2018, art. 21.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. III, Warszawa 2025, art. 21.

Fajgielski P., *Rzetelność jako ogólna zasada przetwarzania danych osobowych*, „Gdańskie Studia Prawnicze" 2021, nr 4, s. 15-17.

Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, *III.3.6. Prawo sprzeciwu oraz dalsze czynniki* [w:] *Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE*, 844/14/PL, WP 217, s. 50.

Gumularz M., *Ochrona danych osobowych w sektorze publicznym*, Warszawa 2018.

Gumularz M., *Akt o usługach cyfrowych. Komentarz*, M. Gumularz (red.), Warszawa 2024, art. 6.

Holzinger A., Saranti A., Molnar C., Biecek P., Samek W., *Explainable AI: Past and Present* [w:] *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020*, A. Holzinger (red.), R. Goebel (red.), R. Fong (red.), T. Moon (red.), K.R. Müller (red.), W. Samek (red.), Cham 2022, s. 5-6.

Holzinger A., Saranti A., Molnar C., Biecek P., Samek W., *Explainable AI Methods – A Brief Overview* [w:] *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020*, A. Holzinger (red.), R. Goebel (red.), R. Fong (red.), T. Moon (red.), K.R. Müller (red.), W. Samek (red.), Cham 2022, s. 27-28.

Holzinger A., Saranti A., Molnar C., Biecek P., Samek W., *XAI: Counterfactual Explanations and Algorithmic Recourse* [w:] *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020*, A. Holzinger (red.), R. Goebel (red.), R. Fong (red.), T. Moon (red.), K.R. Müller (red.), W. Samek (red.), Cham 2022, s. 143-144.

Lubasz D., *1. Profilowanie a zautomatyzowane podejmowanie decyzji* [w:] *Rok RODO*, W. R. Wiewiórowski (red.), H. Wolska (red.), Warszawa 2019.

Lubasz D., *3. Zasada przejrzystości*, [w:] *Rok RODO*, W. R. Wiewiórowski (red.), H. Wolska (red.), Warszawa 2019.

Maciejewska K., *4. Etyka systemów sztucznej inteligencji dla wymiaru sprawiedliwości* [w:] *Prawo sztucznej inteligencji i nowych technologii 3*, B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), Warszawa 2023.

Maciejewska K., *Przejrzystość i identyfikowalność systemów sztucznej inteligencji*, [w:] *Prawo Nowych Technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, J. Gołaczyński (red.), Warszawa 2022.

Monarcha-Matlak A., *3. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach oraz profilowanie*, [w:] *Internet. Przetwarzanie danych osobowych. Processing of personal data*, K. Czaplicki (red.), G. Szpor (red.), Warszawa 2019.

Osowicki Ł., Kiełbus Ł., Jóźwiak R., *2. Zaufana sztuczna inteligencja – wyjaśnialność oraz przyczynowość*, [w:] *Prawo sztucznej inteligencji i nowych technologii 2*, B. Fischer (red.), A. Pązik (red.), M. Świerczyński (red.), Warszawa 2022.

Rzymowski J., *2. Prawa i wolności, doniosłość zjawiska na gruncie RODO*, „Przegląd Prawa Publicznego" 2024, nr 4, s. 1-2.

Sakowska-Baryła M., *2.2.7.7. Dane osobowe* [w:] *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

Yamada Y., *Judicial Decision-Making and Explainable AI (XAI) – Insights from the Japanese Judicial System*, „Studia Iuridica Lublinensia" 2023, nr 4, s. 163-165.

AKTY PRAWNE

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 (Dz.U.UE.L. z 2016 r. Nr 119 z późn. zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Dz.U.UE.L. z 2024 r. poz. 1689).

ORZECZNICTWO

Wyrok TSUE z dnia 19 października 2016 r., C-582/14.

Wyrok TSUE z dnia 20 grudnia 2017 r., C-434/16.

Wyrok TSUE z dnia 07 grudnia 2023 r., C-26/22.

THE EFFECTIVENESS OF THE RIGHT TO OBJECT IN RELATION TO DATA INFERRED BY EXPLAINABLE ARTIFICIAL INTELLIGENCE

Summary: The dynamic evolution of artificial intelligence systems has led to the widespread use of inferred data, generated through algorithmic prediction rather than through the direct collection of information from individuals. Despite its indirect nature, this data significantly shapes the legal and economic situation of individuals in main areas such as the labour market. The effectiveness of the right to object, referred to in article 21 (1) 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 processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (L 119/1), is based on the transparency of processing operations. However, in the case of black-box models, this assumption becomes completely illusory. The lack of insight into the inference process and the inability to obtain information about the significance of individual variables makes it impossible for the data subject to demonstrate their „particular situation", which is a requirement under the aforementioned provision. This phenomenon leads to a radical information asymmetry, degrading the institution of the right to object to a purely facade dimension. An additional threat is posed by the phenomenon of generative model hallucinations and their use of proxy variables, which may result in indirect discrimination. In such circumstances, the burden of proof effectively falls on the individual, who lacks the tools necessary to challenge erroneous or arbitrary reasoning processes. Restoring the full effectiveness of legal protection requires the implementation of explainable artificial intelligence, which will allow for the reconstruction of decision-making premises and substantive verification of the reliability of predictions. In the algorithmic paradigm, explainable artificial intelligence is not merely an optional element of transparency, but a prerequisite for the realisation of information autonomy and the exercise of real control over one's own personal data.

Keywords: algorithmic transparency; artificial intelligence; GDPR; inferred data; personal data protection; right to object

Alina Pyrcz
Uniwersytet Komisji Edukacji Narodowej w Krakowie
alaula2002@gmail.com
ORCID: 0009-0001-8951-2197

AUTOMATYCZNE SYSTEMY NADZORU MASOWEGO A PRAWO DO PRYWATNOŚCI

Streszczenie: W dobie cyfryzacji i dynamicznego rozwoju technologii sztucznej inteligencji coraz powszechniejsze stają się automatyczne systemy nadzoru masowego, wykorzystywane zarówno przez państwa, jak i podmioty prywatne. Ich stosowanie wywołuje jednak poważne wątpliwości prawne i etyczne, w szczególności w kontekście prawa do prywatności oraz wolności jednostki. Artykuł podejmuje analizę legalności oraz granic i skutków stosowania systemów nadzoru masowego w świetle prawa międzynarodowego, ze szczególnym uwzględnieniem orzecznictwa Europejskiego Trybunału Praw Człowieka. W części empirycznej zastosowano ankietę przeprowadzoną wśród ogółu społeczeństwa, której celem jest zbadanie opinii obywateli na temat dopuszczalnych granic masowego monitoringu, poziomu akceptacji nadzoru cyfrowego oraz postrzeganego wpływu systemów monitoringu na prawa człowieka i poczucie prywatności. Wyniki ankiety pozwoliły określić społeczne oczekiwania i obawy związane z nadzorem masowym, wskazując obszary największego ryzyka naruszeń praw jednostki.

Słowa kluczowe: nadzór masowy, prawo do prywatności, prawa człowieka

WPROWADZENIE

Obecnie możemy zaobserwować niezwykle dynamiczny rozwój technologii informacyjnych i komunikacyjnych i to na bardzo szeroką skalę. XXI wiek zdecydowanie jest wiekiem najszybszego rozwoju technologicznego w historii, a współczesny świat wkroczył w erę niespotykanych dotąd możliwości gromadzenia, przetwarzania i analizowania danych. Nieodłącznym elementem naszego codziennego życia stały się najnowocześniejsze odkrycia technologiczne, takie jak smartfony, media

społecznościowe, monitoring wizyjny czy płatności elektroniczne. Każdego dnia oferują nam one wygodę w codziennych czynnościach, usprawniają naszą pracę oraz dają nam poczucie bezpieczeństwa. Jednocześnie jednak te same technologie stworzyły warunki do powstania i rozwoju systemów nadzoru masowego, które umożliwiają stałe i niemal nieograniczone monitorowanie aktywności obywateli. Powoduje to bardzo wiele obaw wśród społeczeństwa, co dokładnie uwidacznia, przeprowadzone na potrzeby analizy autonomicznych systemów nadzoru w poniższym artykule, badanie naukowe ujęte w dalszej części tego opracowania. Podkreślenia wymaga fakt, że nadzór masowy coraz częściej odbywa się w sposób zautomatyzowany, niewidoczny dla jednostki i obejmuje nie tylko osoby podejrzane o łamanie prawa, lecz całe społeczeństwa lub bardzo szerokie grupy społeczne. Tego rodzaju praktyki rodzą istotne pytania o granice ingerencji w życie prywatne, o zasadę domniemania niewinności oraz o to, w jakim stopniu bezpieczeństwo publiczne może usprawiedliwiać powszechną kontrolę. Debata wokół nadzoru masowego wciąż się toczy i nie dotyczy wyłącznie aspektów technologicznych, lecz także kwestii etycznych, prawnych i społecznych. Zwolennicy takich systemów podkreślają ich skuteczność w zapobieganiu przestępczości i terroryzmowi, przeciwnicy natomiast wskazują na ryzyko nadużyć władzy, dyskryminacji oraz stopniowego ograniczania wolności obywatelskich[1]. W niniejszym artykule przybliżona zostanie istota systemu nadzoru masowego, omówione zostaną jego główne mechanizmy oraz zostanie także przeprowadzona analiza konsekwencji, jakie niesie on dla funkcjonowania współczesnych demokracji i codziennego życia jednostki.

1. DEFINICJA ORAZ CECHY SYSTEMU NADZORU MASOWEGO

Na samym początku w celu lepszego zrozumienia poniższego artykułu warto jest skupić się na rozwinięciu definicji systemu nadzoru masowego. Jest to pojęcie, które coraz częściej pojawia się w codziennym użytkowaniu, ale wciąż jednak jest ono stosunkowo nowe i wiąże się ściśle z coraz szybszym rozwojem technologii. System nadzoru masowego można bowiem tłumaczyć jako zestaw technologii, procedur i działań umożliwiających zbieranie, analizowanie oraz przechowywanie danych o dużych grupach ludzi bez ich indywidualnych podejrzeń ani zgody[2]**.** Celem może być np. zapewnienie bezpieczeństwa państwa, kontrola społeczna, zarządzanie

[1] M. Rojszczak, *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka,* „Studia Prawa Publicznego" 2022.

[2] European Parliamentary Research Service, *Mass Surveillance – Part 1: Risks, Opportunities and Mitigation Strategies*, *EPRS Study no. 527409 (Annex 1),* online: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN1)_EN.pdf [dostęp: 2.03.2026].

informacją lub inne działania administracyjne, ale w każdym przypadku cel ten będzie kwestią bardzo indywidualnie powiązaną z rodzajem zastosowania[3]. Nadzór taki jest zazwyczaj prowadzony przez lokalne i federalne władze lub też organizacje rządowe , ale również często używają go większe korporacje[4]. Warto w tym miejscu wspomnieć, że agencje takie jak np. Agencja Bezpieczeństwa Narodowego („NSA") informują, że prowadzenie masowego nadzoru jest często konieczne do walki z terroryzmem, zapobiegania przestępczości i niepokojom społecznym, ochrony bezpieczeństwa narodowego lub też kontroli populacji[5]. Podkreślenia wymaga fakt, że masowy nadzór budzi wiele kontrowersji i często zarzuca się naruszanie prawa do prywatności, ograniczanie praw i wolności obywatelskich i politycznych oraz bycie nielegalnym w niektórych systemach prawnych lub konstytucyjnych[6]. W literaturze polskiej, jak i zagranicznej automatyczne systemy nadzoru masowego zazwyczaj opisywane są jako „systemy masowej inwigilacji", jednak na potrzeby niniejszego artykułu wprowadzono pojęcie „automatycznych systemów nadzoru masowego" w celu lepszego oddania sposobu ich działania oraz wciąż rozwijających się zastosowań technologicznych. W tym miejscu podkreślić należy, że pojęcie „masowa inwigilacja" ma charakter mocno związany historycznie z standardowymi rodzajami działalności operacyjno-rozpoznawczej państw, którym im mogą być np. podsłuch, czy też kontrola korespondencji. Tak użyty termin skupia się przede wszystkim na rezultacie ingerencji w prywatność, ale nie oddaje wystarczająco specyfiki nowoczesnych systemów, które bez wątpienia wykorzystują najnowszą technologię skupiającą się na np. automatyzacji. W związku z tym wprowadzenie nowego terminu umożliwi objęcie nim szerszej kategorii nowych technologii. Systemy masowej inwigilacji działają nie tylko poprzez podsłuchiwanie i przechowywanie znacznych ilości danych (tzw. przechwytywanie masowe), ale również często wymagają od dostawców usług łączności elektronicznej („CSP") ogólnego zachowywania i przechowywania komunikacji użytkowników i powiązanych danych komunikacyjnych oraz umożliwienia organom krajowym dostępu do tych danych, albo w sposób bezpośredni i nieograniczony, albo na podstawie ukierunkowanych wniosków[7].

Najważniejszymi cechami systemu nadzoru masowego są przede wszystkim

[3] *Ibidem.*
[4] *Ibidem.*
[5] M. Rojszczak, *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka,* „Studia Prawa Publicznego" 2022.
[6] Organizacja Narodów Zjednoczonych, *Mass surveillance is a violation of human right to privacy*, https://www.liberties.eu/en/stories/un-mass-surveillance-is-a-violation-of-human-right-to-privacy-sn-892/19916 [dostęp: 2.03.2026].
[7] Masowa inwigilacja – Orzecznictwo ETPC i TSUE, Wspólny arkusz informacyjny, aktualizacja: 28.02.2025.

automatyczne gromadzenie danych na wielką skalę, a także analiza i profilowanie zachowań z użyciem algorytmów i sztucznej inteligencji[8]. Ciągłe, zautomatyzowane i długotrwałe zbieranie ogromnych ilości danych dotyczących codziennego funkcjonowania obywateli w zdecydowanej większości przypadków odbywa się bez bezpośredniej ingerencji człowieka i bez wiedzy osób nadzorowanych. Gromadzone w ten sposób dane obejmują m.in. dane telekomunikacyjne, dane lokalizacyjne, dane z monitoringu wizyjnego, aktywność internetową oraz dane finansowe[9]. Skala gromadzonych danych jest tak duża, że ręczna analiza jest niemożliwa, dlatego systemy te opierają się na zaawansowanych technologiach informatycznych. Poprzez zgromadzone dane przekazywane są informacje o połączeniach telefonicznych, SMS-ach, e-mailach, obraz z kamer CCTV umieszczonych w przestrzeni publicznej, historia przeglądania stron, wyszukiwania, a także informacje o transakcjach kartą płatniczą, przelewach bankowych i płatnościach elektronicznych, a także wiele innych wrażliwych danych[10]. Kolejną istotną cechą wartą poddania głębszej analizie jest odejście od zasady ukierunkowanego nadzoru, który dotyczyłby wyłącznie osób podejrzanych o konkretne przestępstwa[11]. W systemie nadzoru masowego bowiem monitorowani są wszyscy obywatele lub bardzo szerokie grupy społeczne, niezależnie od ich zachowania, wyglądu, czy występujących zachowań niepożądanych w przeszłości. Można więc stwierdzić, że granica między osobą „podejrzaną" a „zwykłym obywatelem" ulega całkowitemu zatarciu i każda osoba tak naprawdę staje się możliwym podejrzanym. Budzi to poważne kontrowersje etyczne i prawne, zwłaszcza w kontekście prawa do prywatności i domniemania niewinności. Zgromadzone informacje są w następnej kolejności poddawane zaawansowanej analizie z wykorzystaniem algorytmów, uczenia maszynowego oraz sztucznej inteligencji[12]**.** Analiza taka może obejmować nie tylko rozpoznawanie wzorców zachowań np. poprzez wykrywanie nietypowych tras przemieszczania się, ale również przewidywanie przyszłych działań jednostki. Systemy nadzoru masowego mają zastosowanie np. w sieciach kamer CCTV z funkcją rozpoznawania twarzy[13] (umożliwiających identyfikację i śledzenie

[8] European Parliamentary Research Service, *Mass Surveillance – Part 1: Risks, Opportunities and Mitigation Strategies*, *EPRS Study no. 527409 (Annex 1),* online: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN1)_EN.pdf [dostęp: 2.03.2026].

[9] Privacy International, *The Global Surveillance Industry*, https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf [dostęp: 2.03.2026].

[10] *Ibidem.*

[11] Council of Europe, *Mass Surveillance. Report by the Committee on Legal Affairs and Human Rights* https://pace.coe.int/en/files/21583 [dostęp: 2.03.2026].

[12] M. Rojszczak, *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka,* „Studia Prawa Publicznego" 2022, s. 112.

[13] Innex, *Systemy CCTV – z czego się składają*, https://innex.pl/systemy-cctv-z-czego-sie-skladaja/ [dostęp: 2.03.2026].

osób w czasie rzeczywistym), masowym zbieraniu metadanych komunikacji, analizie mediów społecznościowych czy monitoringu transakcji elektronicznych.

Podczas próby właściwego zdefiniowania automatycznego nadzoru masowego nie można także zapomnieć o odróżnieniu właśnie tego nadzoru od nadzoru ukierunkowanego oraz operacyjnego. Nadzór ukierunkowany bowiem, jak już sama nazwa wskazuje, odnosi się do działań podejmowanych wobec konkretnie oznaczonej osoby lub wąskiej grupy osób, wobec których istnieje uprzednie, uzasadnione podejrzenie naruszenia prawa lub zagrożenia dla porządku publicznego[14]. Jest on zatem ukierunkowany na konkretną jednostkę lub niewielką grupę. W przeciwieństwie do nadzoru masowego ma on charakter selektywny i celowy. Podstawową cechą nadzoru ukierunkowanego jest więc jego personalizacja oraz ograniczenie czasowe i przedmiotowe. W odróżnieniu od nadzoru masowego nie obejmuje on zbiorowości jako takiej, lecz koncentruje się na jednostce, wobec której organy państwa są w stanie wskazać konkretne przesłanki faktyczne i prawne uzasadniające zastosowanie określonych środków[15]. Co do zasady, środki tego rodzaju wymagają wyraźnej podstawy prawnej oraz podlegają kontroli instytucjonalnej. Nadzór operacyjny stanowi natomiast szczególną oraz najbardziej ingerencyjną postać nadzoru ukierunkowanego**,** realizowaną w ramach czynności operacyjno-rozpoznawczych prowadzonych przez wyspecjalizowane organy państwowe, takie jak policja, służby specjalne czy organy bezpieczeństwa wewnętrznego[16]. Jego podstawowym celem jest pozyskiwanie informacji o charakterze niejawnym, które nie mogłyby zostać zdobyte przy użyciu standardowych środków procesowych. Osoba objęta tym rodzajem nadzoru co do zasady nie jest świadoma faktu prowadzenia wobec niej działań kontrolnych[17]. Niejawność ta pomaga prowadzić skuteczniejsze działania operacyjne, jednak jednocześnie znacząco podnosi poziom ryzyka naruszenia praw jednostki, w szczególności prawa do prywatności, tajemnicy komunikowania się oraz autonomii informacyjnej. W tym miejscu warto zasygnalizować, że w orzecznictwie Europejskiego Trybunału Praw Człowieka („ETPC"), w szczególności w sprawie Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu[18], podkreślono, że brak precyzyjnych reguł dotyczących selekcji, przechowywania i niszczenia danych prowadzi do naruszenia art. 8 EKPC[19].

---

[14] Masowa inwigilacja – Orzecznictwo ETPC i TSUE, *Wspólny arkusz informacyjny*, aktualizacja: 28.02.2025.

[15] A. Grzelak, *Fundamental Rights Protection in the Context of Mass Surveillance in the European Union,* "Przegląd Prawa i Administracji" 107, 2016.

[16] E. Wójcik, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, Warszawa 2011.

[17] A. Grzelak, *Fundamental Rights Protection in the Context of Mass Surveillance in the European Union,* "Przegląd Prawa i Administracji" 107, 2016.

[18] Wyrok ETPC z dnia 25 maja 2021 r., wnioski nr 58170/13, 62322/14 i 24960/15, §361, §425 .

19 Europejska Konwencja Praw Człowieka z 4 listopada 1950 r. (Dz.U.1993.61.284) – dalej EKPC.

2. AUTOMATYCZNY NADZÓR MASOWY W ŚWIETLE PRAWA MIĘDZYNARODOWEGO I EUROPEJSKIEGO

Podstawowym aktem prawa międzynarodowego regulującym dopuszczalność stosowania środków nadzoru przez państwo jest EKPC, sporządzona w 1950 r. w ramach Rady Europy[20]. Centralne znaczenie w kontekście problematyki nadzoru ma art. 8 EKPC[21], który ustanawia prawo każdej osoby do poszanowania jej życia prywatnego i rodzinnego, mieszkania oraz korespondencji[22]. Przepis ten stanowi jeden z filarów systemu ochrony praw jednostki w Europie i obejmuje swoim zakresem nie tylko klasyczne formy ingerencji w prywatność, lecz również nowoczesne, technologicznie zaawansowane mechanizmy gromadzenia i przetwarzania danych[23]. Zakres ochrony wynikający z art. 8 EKPC jest interpretowany przez ETPC w sposób niezwykle szeroki i dynamiczny, odpowiadający zmieniającym się warunkom społeczno-technologicznym[24]. ETPC wyraźnie podkreśla, że pojęcie „życia prywatnego" nie podlega ścisłej definicji i obejmuje nie tylko intymną sferę egzystencji jednostki, lecz również jej tożsamość, relacje społeczne, aktywność komunikacyjną oraz możliwość swobodnego funkcjonowania w przestrzeni publicznej bez nieuzasadnionej ingerencji państwa[25]. W tym ujęciu ochrona konwencyjna rozciąga się także na dane osobowe, informacje telekomunikacyjne oraz inne formy cyfrowych śladów pozostawianych przez jednostkę[26]. Szczególnego znaczenia nabiera art. 8 EKPC w kontekście rozwoju nowoczesnych technologii informacyjnych, które umożliwiają masowe, automatyczne i długotrwałe gromadzenie oraz przetwarzanie danych. Trybunał przyjmuje, że EKPC jako tzw. „żywy instrument" musi być interpretowana w sposób pozwalający na objęcie jej ochroną również takich form ingerencji, które nie były znane w momencie jej ratyfikacji[27]. Jest to z całą pewnością wyrok kluczowy i niezwykle ważny w analizowanym problemie, ponieważ jasno wskazuje, że nie ma znaczenia jak nowoczesna i zmienna jest technologia. Nawet jeśli prawo się nie zmienia, interpretacja jego przepisów powinna być adekwatna do zmian zachodzących w danym okresie. Ponadto ETPC zasygnalizował także, że objęcie nadzorem całych zbiorowości, bez konieczności wykazania związku pomiędzy daną osobą a określonym zagrożeniem,

[20] *Ibidem.*
[21] *Ibidem.*
[22] *Ibidem.*
[23] *Ibidem.*
[24] M. Rojszczak, *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka,* „Studia Prawa Publicznego" 2022, s. 115-121.
[25] Wyrok ETPC z dnia 16 grudnia 1992 r., skarga nr 13710/88, §29.
[26] Wyrok ETPC z dnia 16 lutego 2000 r., skarga nr 27798/95, §66-67.
[27] Wyrok ETPC z dnia 25 kwietnia 1978 r., skarga nr 5856/72, §31.

znacząco zwiększa ryzyko arbitralności działań władzy publicznej. W takim modelu nadzoru jednostka staje się potencjalnym przedmiotem kontroli wyłącznie z uwagi na fakt uczestnictwa w życiu społecznym i komunikacyjnym, co pozostaje w sprzeczności z zasadą proporcjonalności oraz zasadą minimalizacji ingerencji[28]. Ten przypadek oczywiście pozostawia też wiele wątpliwości etycznych. W tym zakresie szczególną uwagę należy zwrócić na wyrok Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu, w którym ETPC dokonał kompleksowej oceny brytyjskiego systemu hurtowego przechwytywania danych komunikacyjnych. ETPC uznał, że tego rodzaju praktyki, nawet takie, które są uzasadniane potrzebą ochrony bezpieczeństwa narodowego, stanowią wyjątkowo intensywną ingerencję w sferę prywatności i wymagają szczególnie rygorystycznych zabezpieczeń prawnych[29]. Wyraźnie stwierdzono, że sam fakt automatycznego charakteru przetwarzania danych oraz zastosowania algorytmicznych mechanizmów selekcji nie może prowadzić do obniżenia standardów ochrony praw jednostki. Wręcz przeciwnie, automatyzacja nadzoru zwiększa skalę i głębokość ingerencji, ponieważ umożliwia szybkie przetwarzanie ogromnych wolumenów danych oraz tworzenie szczegółowych profili zachowań jednostek[30]. Z tego względu państwo zobowiązane jest do wprowadzenia dodatkowych gwarancji ograniczających ryzyko nadużyć. W szczególności ETPC zaakcentował, że automatyczna selekcja danych przy użyciu algorytmów absolutnie nie zwalnia państwa z obowiązku zapewnienia jasnych i precyzyjnych kryteriów wyboru danych, które muszą być określone na poziomie ustawowym. Kryteria te powinny w sposób jednoznaczny i łatwo zrozumiały wskazywać, jakie kategorie danych mogą podlegać przechwytywaniu, w jakim celu oraz w jakich okolicznościach, tak aby ograniczyć uznaniowość organów stosujących nadzór[31]. W konsekwencji orzeczenie w sprawie Big Brother Watch i inni przeciwko Zjednoczonemu Królestwu potwierdza ugruntowaną linię orzeczniczą ETPC, zgodnie z którą automatyczny nadzór masowy, pozbawiony indywidualizacji oraz skutecznych gwarancji proceduralnych, pozostaje zasadniczo nie do pogodzenia z wymogami Konwencji[32].

Zaś na gruncie prawa Unii Europejskiej niezwykle ważne znaczenie dla oceny dopuszczalności masowego i automatycznego nadzoru mają przepisy Karty praw podstawowych Unii Europejskiej („KPP UE")[33], która zgodnie z art. 6 Traktatu o Unii

[28] Wyrok ETPC z dnia 1 lipca 2008 r., skarga nr 58243/00, §62-69.
[29] Wyrok ETPC z dnia 25 maja 2021 r., wnioski nr 58170/13, 62322/14 i 24960/15, §347-348, §387-388.
[30] *Ibidem.*
[31] *Ibidem*.
[32] *Ibidem.*
[33] Karta praw podstawowych Unii Europejskiej (Dz.U.UE.C.2016.202.389).

Europejskiej posiada moc równą traktatom[34]. W kontekście gromadzenia i przetwarzania danych szczególną rolę odgrywają tu art. 7 KPP UE, gwarantujący poszanowanie życia prywatnego i rodzinnego, oraz art. 8 KPP UE, ustanawiający autonomiczne prawo do ochrony danych osobowych[35]. TSUE konsekwentnie podkreśla, że art. 7 i 8 KPP UE należy interpretować łącznie, ponieważ masowe systemy nadzoru niemal zawsze ingerują jednocześnie w sferę prywatności jednostki oraz w jej prawo do kontroli nad własnymi danymi osobowymi. W orzecznictwie TSUE przyjmuje się w tym przypadku szerokie rozumienie pojęcia ingerencji, obejmujące nie tylko faktyczne wykorzystanie danych, lecz już samo ich gromadzenie, przechowywanie oraz techniczną możliwość dalszego przetwarzania[36]. W przełomowym wyroku Digital Rights Ireland Trybunał jednoznacznie stwierdził, że masowe i niezróżnicowane gromadzenie danych dotyczących całej populacji, bez związku z konkretnym zagrożeniem lub podejrzeniem, stanowi ingerencję o wyjątkowo wysokiej intensywności[37]. TSUE podkreślił także, że retencja danych telekomunikacyjnych umożliwia tworzenie bardzo szczegółowych wniosków dotyczących życia prywatnego jednostek, takich jak ich relacje społeczne, codzienne nawyki, miejsca pobytu czy aktywność zawodowa[38]. Zaznaczono jednocześnie, że brak jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w odniesieniu do kategorii osób, danych lub okresów retencji prowadzi do naruszenia istoty praw zagwarantowanych w art. 7 i 8 KPP UE[39]. W tym sensie masowy charakter gromadzenia danych nie może być usprawiedliwiony samym celem ochrony bezpieczeństwa publicznego lub zwalczania poważnej przestępczości[40]. Stanowisko to zostało rozwinięte w wyroku Tele2 Sverige, w którym TSUE jednoznacznie zakazał ogólnej i niezróżnicowanej retencji danych, nawet jeśli towarzyszą jej mechanizmy automatycznego przetwarzania. Warto zaznaczyć ponadto, że szczególnie krytycznie TSUE odnosi się do automatycznego przetwarzania i profilowania, które pozwalają na przewidywanie zachowań jednostek oraz ocenę ich „ryzyka" w oparciu o algorytmiczną analizę danych. W ocenie TSUE takie praktyki naruszają nie tylko zasadę proporcjonalności, lecz również samą istotę prawa do ochrony danych osobowych, ponieważ pozbawiają jednostkę realnej kontroli nad sposobem wykorzystania jej danych[41]. W nowszym orzecznictwie, w szczególności w sprawach La

[34] Traktat o Unii Europejskiej (Dz.U.2004.90.864/30).
[35] Karta praw podstawowych Unii Europejskiej (Dz.U.UE.C.2016.202.389).
[36] Wyrok TSUE z dnia 8 kwietnia 2014 r., C-293/12,§ 26-30, § 34-37.
[37] *Ibidem*.
[38] *Ibidem*.
[39] Karta praw podstawowych Unii Europejskiej (Dz.U.UE.C.2016.202.389).
[40] Wyrok TSUE z dnia 8 kwietnia 2014 r., C-293/12, §56-69.
[41] Wyrok TSUE z dnia 21 grudnia 2016 r., sprawy połączone C-203/15 i C-698/15, § 98-101.

Quadrature du Net oraz Privacy International[42], TSUE dopuścił jedynie wyjątkowe i ściśle ograniczone formy masowego gromadzenia danych, pod warunkiem istnienia rzeczywistego i poważnego zagrożenia dla bezpieczeństwa narodowego oraz zastosowania rygorystycznych zabezpieczeń prawnych. Nawet w takich sytuacjach Trybunał wykluczył możliwość stałej, powszechnej i automatycznej inwigilacji społeczeństwa[43]. W konsekwencji na podstawie orzecznictwa TSUE można więc dojść do wniosku, że masowe, niezróżnicowane i zautomatyzowane gromadzenie danych jest co do zasady sprzeczne z art. 7 i 8 KPP UE[44], zwłaszcza gdy umożliwia profilowanie jednostek bez indywidualnych przesłanek oraz bez skutecznych mechanizmów kontroli sądowej i instytucjonalnej.

Warto ponadto uzupełnić analizę prawa Unii Europejskiej o niezwykle istotną pod kątem tego zagadnienia Dyrektywę e-Privacy (2002/58/WE) z dnia 12 lipca 2002 roku dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. Jej podstawowym celem jest ograniczenie możliwości prowadzenia systemów nadzoru masowego w sektorze komunikacji elektronicznej. W tym miejscu wyróżnić należy m.in. art. 5 ust. 1 tejże Dyrektywy e-Privacy, który stanowi, że „Państwa Członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności”[45]. Jest to przepis ważny, ponieważ jasno wskazuje, że zakaz dotyczy działań podjętych przez podmioty inne niż użytkownicy, z wyjątkiem sytuacji, gdy użytkownik wyraził zgodę lub też działanie jest związane z tzw. *legally authorised* mające swoją podstawę we wspomnianym w przepisie art. 15 ust. 1. Ponadto wskazany zakres zakazu obejmuje wiele różych czynności np. podsłuch, czy też monitorowanie, co daje szeroki przekrój omawianego artykułu. Ponadto w tym miejscu wskazać również trzeba zasygnalizowany już art. 15 ust 1, który stanowi, że

[42] Wyrok TSUE z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18, §137-139, §168-178.
[43] *Ibidem.*
[44] Karta praw podstawowych Unii Europejskiej (Dz.U.UE.C.2016.202.389).
[45] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. U. UE. L. z 2002 r. Nr 201, str. 37 z późn. zm.) („Dyrektywa e-Privacy”).

Państwa Członkowskie mogą ograniczać prawa wynikające z art. 5, 6, 8 oraz 9, jeśli jest to konieczne, adekwatne, a także proporcjonalne. Oznacza to, że dane państwo musi szczegółowo wykazać m.in. niezbędność zastosowania danego środka. Istotne znaczenie w omawianiu przedstawionej problematyki ma także art. 6 ust. 1 oraz 2 Dyrektywy e-Privacy, które brzmi, że „Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu (…)" oraz, że „można przetwarzać dane o ruchu niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich. Przetwarzanie takie jest dozwolone tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym należy uiścić opłatę". Oznacza to bowiem, że ogranicza on znacznie możliwość transmisji danych, które to muszą zostać usunięte lub zanonimizowane, gdy nie są już niezbędne do przekazania transmisji komunikatu. Art. 6 Dyrektywy e-Privacy jest zatem obecnie jednym z najważniejszych aktów dotyczących ochrony prywatności w komunikacji elektronicznej. W kontekście nadzoru masowego ma on bardzo ważne znaczenie, ponieważ to właśnie takie systemu nadzoru opierają się na długoterminowym gromadzeniu i analizie meta danych zwykłych członków społeczeństwa. Prowadzi to do powstania konfliktu pomiędzy rodzajem funkcjonowania tych systemów a samymi postanowieniami Dyrektywy e-Privacy.

Istotne znaczenie ma także sprawa Centrum för rättvisa v. Sweden[46]. ETPC orzekł, że szwedzki system wywiadu elektronicznego, który zezwalał na masowe przechwytywanie niektórych komunikatów online, nie naruszał prawa do poszanowania korespondencji. ETPC zwrócił uwagę na nieścisłości w szwedzkim ustawodawstwie, m.in. w brak publicznego uzasadnienia decyzji podejmowanych przez jeden z organów nadzorczych, ale mimo to orzekł, że szwedzki system masowego przechwytywania zapewnia odpowiednie i wystarczające zabezpieczenia przed ryzykiem nadużyć. Można więc stwierdzić, że ETPC przyznał państwom szeroki margines swobody w zakresie przyjmowania systemów masowego przechwytywania w świetle obecnego zagrożenia globalnym terroryzmem i poważną przestępczością transgraniczną. Podkreślono także, że strony nie negowały tego, że szwedzka ustawa o rozpoznaniu radioelektronicznym miała podstawę prawną w prawie krajowym oraz że kwestionowane środki służyły uzasadnionym celom w interesie bezpieczeństwa narodowego poprzez wspieranie szwedzkiej polityki zagranicznej, obronnej i bezpieczeństwa oraz identyfikację zewnętrznych zagrożeń dla kraju[47]. Warto także wspomnieć o wyroku

[46] Wyrok ETPC z dnia 25 maja 2021 r., skarga nr 35252/08.
[47] *Ibidem.*

z 13 lutego 2024 r. Podchasov v. Russia[48]. Ma on istotne znaczenie, ponieważ ETPC orzekł, że nakazanie odszyfrowania danych typu E2EE stanowi naruszenie art. 8 EKPC. Sprawa ta dotyczyła kontrowersyjnej ustawy, która ustanowiła system retencji danych oraz zezwoliła organom ścigania na nakazanie odszyfrowania zebranych danych. Użytkownik Telegrama, zaskarżył nakaz zobowiązujący do odszyfrowania jego komunikacji chronionej szyfrowaniem typu E2EE. Trybunał orzekł, że system zatrzymywania danych i dostępu narusza prawo do prywatności, ponieważ nie zapewnia odpowiednich zabezpieczeń przed nadużyciami, biorąc pod uwagę powagę ingerencji[49]. Warto ponadto przybliżyć wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni v. Polska[50]. ETPC zaznaczył, że doszło do naruszenia art. 8 EKPC o ochronie praw człowieka i podstawowych wolności, w odniesieniu do reżimu kontroli operacyjnej, zatrzymywania danych telekomunikacyjnych i wykorzystywania ich na potrzeby służb oraz niejawnego nadzoru prowadzonego na podstawie przepisów ustawy antyterrorystycznej. Uznano, że prawo krajowe nie zapewnia odpowiednich zabezpieczeń przeciwko nadmiernemu korzystaniu z nadzoru i zbyt dużej ingerencji w życie prywatne osób inwigilowanych, tym samym więc Polska została zobowiązana do zmiany i zapewnienia odpowiednich przepisów[51].

Zarówno ETPC, jak i TSUE coraz częściej zwracają uwagę na problem tzw. „czarnej skrzynki" algorytmicznej[52], który polega przede wszystkim na braku przejrzystości mechanizmów podejmowania decyzji opartych na zautomatyzowanym przetwarzaniu danych. Zjawisko to jest szczególnie widoczne w kontekście automatycznego nadzoru masowego, w którym algorytmy predykcyjne służą do selekcji, klasyfikacji oraz profilowania ogromnych zbiorów informacji, często bez udziału czynnika ludzkiego na kluczowych etapach procesu decyzyjnego[53] .Warto w tym miejscu także zaznaczyć, że w ocenie sądów europejskich brak przejrzystości danych prowadzi do istotnego osłabienia gwarancji proceduralnych przysługujących jednostce[54]. Bowiem jak można dochodzić swoich praw nie wiedząc nawet, że są łamane? ETPC wielokrotnie zaznaczał, że skuteczność środków ochrony prawnej uzależniona jest od minimalnego poziomu transparentności działań państwa, nawet w obszarze bezpieczeństwa narodowego[55]. Na marginesie warto zaznaczyć, że często jest to pro-

[48] Wyrok ETPC z dnia 13 lutego 2024 r., skarga nr 33696/19, §46-52, §76-94.
[49] *Ibidem*.
[50] Wyrok ETPC z dnia 28 maja 2024 r., skargi nr 72038/17 i 25237/18, §206-243.
[51] *Ibidem*.
[52] D. Lyon, *Surveillance Society: Monitoring Everyday Life*, Open University Press 2001.
[53] *Ibidem*.
[54] Wyrok ETPC z dnia 4 grudnia 2015 r., skarga nr 47143/06, §229-255.
[55] Wyrok ETPC z dnia 12 stycznia 2016 r., skarga nr 37138/14, §57-69.

cedura tak bardzo zautomatyzowana, że nawet sami administratorzy danych nie mają pełnej świadomości działania tychże technologii oraz sposobu w jaki zbierają one dane. . Warto wspomnieć o rozporządzeniu o ochronie danych („RODO"), które w art. 22 ustanawia zasadę ograniczenia zautomatyzowanego podejmowania decyzji wywołujących wobec osoby fizycznej skutki prawne lub w podobny sposób istotnie na nią wpływające[56]. Przepis ten jest o tyle ważny, że przyznaje on jednostce prawo do tego, aby nie podlegać decyzji opartej wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu, oraz nakłada obowiązek zapewnienia przejrzystości, możliwości interwencji człowieka i zakwestionowania decyzji[57]. Choć RODO formalnie przewiduje wyjątki w odniesieniu do działalności służb w zakresie bezpieczeństwa narodowego, to zarówno TSUE, jak i ETPC traktują jego rozwiązania jako punkt odniesienia i standard interpretacyjny przy ocenie dopuszczalności automatycznego nadzoru masowego. Zasady przejrzystości, minimalizacji danych oraz rozliczalności algorytmów wyrażone w RODO wyznaczają bowiem minimalny poziom ochrony, którego brak może prowadzić do naruszenia art. 8 EKPC[58] oraz art. 7 i 8 KPP UE[59]. Co istotne ETPC w wyrokach zaznaczył, że w szczególnym kontekście tajnych środków nadzoru „przewidywalność" oznacza, że prawo krajowe musi być wystarczająco jasne, żeby móc zapewnić obywatelom odpowiednie wskazanie okoliczności oraz warunków, w których władze publiczne są uprawnione do stosowania takich środków, oraz musi wskazywać zakres swobody uznania i sposób jej wykonywania z wystarczającą jasnością, aby zapewnić jednostce odpowiednią ochronę przed arbitralnością[60].

Warto ponadto przytoczyć wyrok ETPC z 12 września 2023 roku Wieder i Guarnieri przeciwko UK. Sprawa dotyczyła brytyjskiego systemu przechwytywania komunikacji elektronicznej prowadzonego przez służby wywiadowcze[61]. W wyniku sprawy orzeczono, że Wielka Brytania dopuściła się naruszenia prawa do życia prywatnego poprzez używanie systemu nadzoru masowego. ETPC uznał, że ingerencja w prywatność następuje tam, gdzie komunikacja jest przechwytywana, analizowana i używana[62]. Ponadto ETPC wskazał, że naruszono art. 8 EKPC, czyli wspomnianego już wyżej prawa do prywatności. Podkreślono, że masowa ingerencja

[56] 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 (RODO) (Dz.U.UE.L.2016.119.1).
[57] *Ibidem.*
[58] Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.) („EKPC").
[59] Karta praw podstawowych Unii Europejskiej (Dz.U.UE.C.2016.202.389).
[60] Wyrok ETPC z dnia 25 maja 2021 r., wnioski nr 58170/13, 62322/14 i 24960/15, §315-317.
[61] Wyrok ETPC z dnia 12 września 2023 r., skargi nr 64371/16 i 64407/16, §1-118.
[62] *Ibidem*.

w komunikację wymaga bardzo silnych gwarancji, a hurtowe przechwytywanie danych nie może być prowadzone w sposób nieograniczony[63].

Ponadto uwzględnienia wymaga także orzeczenie Wielkiej Izby TSUE z dnia 30 kwietnia 2024 roku M.N. (EncroChat), C-670/22. Było to postępowanie karne, które dotyczyło szyfrowanej platformy komunikacyjnej EncroChat. Miała ona być używana przez niebezpieczne zorganizowane grupy przestępcze do niebezpiecznych celów. Dzięki temu, że platforma oferowała usługi zmodyfikowanych telefonów i szyfrowanych wiadomości stanowiła idealne tło dla środowiska przestępczego. Francuskie służby, za wyraźnym przyzwoleniem sądu, zinwigilowały urządzenia EncroChat i objęły w posiadanie znaczną ilość danych komunikacyjnych. Dane te zostały następnie przekazane władzom niemieckim. TSUE wskazał, że prawo unijne nie zabrania wykorzystywania dowodów pozyskanych z EncroChat w celach postępowania karnego. Ponadto wskazano, że nie ma przeszkód ku temu, aby „europejski nakaz dochodzeniowy mający na celu przekazanie materiału dowodowego, którym właściwe organy państwa wykonującego już dysponują, wydał prokurator, jeżeli ów materiał dowodowy został pozyskany w następstwie przechwycenia przez te organy, na terytorium państwa wydającego, przekazów telekomunikacyjnych wszystkich użytkowników telefonów komórkowych pozwalających, dzięki specjalnemu oprogramowaniu i zmodyfikowaniu urządzenia, na korzystanie z szyfrowanej komunikacji typu end-to-end, pod warunkiem że nakaz ów spełnia wszystkie warunki przewidziane w stosownym wypadku w prawie państwa wydającego w odniesieniu do przekazywania takiego materiału dowodowego w sytuacji czysto wewnętrznej w tym państwie”[64]. Jest to orzeczenie istotne z punktu analizy systemów nadzoru masowego, ponieważ francuskie służby dokonały masowej inwigilacji, nie tylko pojedynczej osoby i uzyskały przy tym dostęp do danych komunikacyjnych wielu użytkowników platformy.

Edoardo Celeste i Giulia Formici wskazują, że kwestia wprowadzenia pewnego rodzaju ograniczeń i warunków dla narzędzi nadzoru masowego jest istotnym problemem, który obecnie niestety posiada wciąż jednego konkretnego rozwiązania. Wskazują, że jest to szerszy element procesu konstytucjonalizacji, który przymusza system konstytucyjny do reagowania na rozwój nowych technologii[65]. Ważne jest także do przytoczenia stanowisko Marcina Rojszczaka, który podkreślił, że masowa inwigilacja może nieść za sobą znaczne osłabienie kluczowych fundamentów państwa

[63] *Ibidem*.
[64] Wyrok TSUE (Wielka Izba) z dnia 30 kwietnia 2024 roku, C-670/22, §86-124.
[65] E. Celeste, G. Formici, *Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism and Legislative Inertia*, “German Law Journal”, s. 445-446.

demokratycznego. Autor podkreślił także, że masowa inwigilacja może przyczyniać się do stopniowego przyzwyczajania się społeczeństwa do coraz to większej ingerencji w ich życie prywatne, co niesie za sobą liczne negatywne konsekwencje, jakimi są np. osłabienie standardów ochrony praw jednostki, a zarazem zwiększenia się akceptowalnej kontroli państwa nad nim. W konsekwencji można dojść do wniosku, że pomimo niezaprzeczalnie ważnej roli zadbania o bezpieczeństwo ludzi, to różnorakie formy prowadzenia przez państwa nadzoru masowego nie są niezbędne dla systemów demokratycznych[66]. Filip Radoniewicz również wskazuje, że wciąż są obecne luki w orzecznictwie dotyczące systemów masowej inwigilacji. Podkreślił także, że ewolucja w orzecznictwie przebiega nie adekwatnie od rozwoju nowych technologii i nie nadąża za tak szybkim ulepszaniem narzędzi technologicznych[67].

Ponadto wspomnieć należy w skrócie o wyroku TSUE z dnia 6 października 2020 r. La Quadrature du Net i In. Trybunał rozstrzygał, czy unijna Dyrektywa o prywatności i łączności elektronicznej (2002/58/WE) oraz KPP UE umożliwiają państwom członkowskim wprowadzanie przepisów nakazujących uogólnione i niezróżnicowane przechowywanie danych obywateli. TSUE w tymże wyroku zdecydowanie nie zgodził się z prowadzeniem masowej inwigilacji. Stwierdził tym samym, że jest to zbyt duża ingerencja w prywatność obywateli. Potwierdza to zarazem również inne orzeczenia, ugruntowując podejście, że walka o bezpieczeństwo nie może usprawiedliwiać prowadzenia stałego nadzoru obywateli[68].

Powyższa analiza automatycznych systemów nadzoru w świetle zasad państwa prawa prowadzi do wniosku, że rozwiązania te pozostają co do zasady trudne do pogodzenia z klasycznymi standardami demokratycznego państwa prawnego, zwłaszcza gdy mają charakter masowy i nieselektywny. Automatyzacja nadzoru bowiem nie tylko nie redukuje intensywności ingerencji w prawa jednostki, lecz często ją potęguje, osłabiając jednocześnie przejrzystość, pewność prawa oraz skuteczność mechanizmów kontrolnych. Zgodność automatycznych systemów nadzoru z zasadami państwa prawa wymaga więc wprowadzania wyjątkowo silnych gwarancji prawnych, instytucjonalnych i proceduralnych. Bez ich zapewnienia automatyczny nadzór masowy należy uznać za rozwiązanie sprzeczne z podstawowymi wartościami leżącymi u podstaw europejskiego porządku prawnego i godzącymi w prywatność jednostki.

---

[66] M. Rojszczak, Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego, Studia nad Autorytaryzmem i Totalitaryzmem, Acta Universitatis Wratislaviensis, Wrocław 2020, s. 238-240.

[67] F. Radoniewicz, *The Issue of Surveillance Carried Out by Technical Means Within the Jurisprudence of the European Court of Human Rights and the Constitutional Tribunal*, "Przegląd Prawa Konstytucyjnego" 6(64), 2021, s. 300.

[68] Wyrok TSUE z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18.

3. PROBLEMY I ZAGROŻENIA PRAWNE AUTOMATYCZNEGO NADZORU MASOWEGO

Jak już można zauważyć, automatyczny nadzór masowy stanowi bardzo poważne wyzwanie dla współczesnych systemów ochrony praw jednostki. Jego cele oraz istota, która polega na nieselektywnym oraz zautomatyzowanym gromadzeniu i analizie danych dotyczących bardzo szerokiego kręgu osób sprawia, że dochodzi do niezwykle wysokiej ingerencji w prawo do poszanowania życia prywatnego oraz w prawo do ochrony danych osobowych. Jest to przedmiot wielu dyskusji. Szczególne zagrożenie wynika z możliwości tworzenia kompleksowych profili jednostek, obejmujących ich relacje społeczne, aktywność komunikacyjną, wzorce zachowań oraz preferencje. Automatyzacja procesu analizy danych już obecnie jest na tyle mocno rozwinięta, że sprawia, że ingerencja ta ma charakter ciągły, długotrwały i trudny do ograniczenia, co pozostaje w sprzeczności z zasadą minimalizacji danych oraz zasadą proporcjonalności[69]. Jednym z fundamentalnych problemów prawnych automatycznego nadzoru masowego jest odejście od klasycznej zasady indywidualizacji ingerencji. W tradycyjnym modelu państwa prawa środki nadzorcze są stosowane wobec konkretnych osób na podstawie uprzedniego, uzasadnionego podejrzenia. Automatyczny nadzór masowy odwraca tę logikę, obejmując nadzorem całe populacje, a dopiero na etapie późniejszej analizy algorytmicznej dokonując selekcji potencjalnie „podejrzanych" jednostek[70]. Orzecznictwo ETPC wskazuje, że taki model prowadzi do niedopuszczalnego rozszerzenia kompetencji władzy publicznej oraz narusza zasadę domniemania niewinności. Automatyczny nadzór masowy opiera się na algorytmicznych mechanizmach selekcji i profilowania, których działanie jest często nieprzejrzyste zarówno dla jednostek, jak i dla organów kontrolnych. Brak przejrzystości algorytmów prowadzi do osłabienia gwarancji proceduralnych i uniemożliwia skuteczne zakwestionowanie legalności ingerencji[71]. Ostatnim, lecz nie mniej istotnym zagrożeniem prawnym automatycznego nadzoru masowego jest jego negatywny wpływ na relację pomiędzy jednostką a państwem. Świadomość istnienia systemów powszechnej i zautomatyzowanej inwigilacji może prowadzić do tzw. efektu mrożącego, polegającego na ograniczaniu przez obywateli korzystania z wolności komunikowania się, wolności wypowiedzi czy wolności zgromadzeń. ETPC podkreślił, że sama świadomość istnienia takich mechanizmów nadzoru może oddziaływać na

[69] Wyrok TSUE z dnia 8 kwietnia 2014 r., C-293/12, §27-59.
[70] Wyrok ETPC z dnia 12 stycznia 2016 r., skarga nr 37138/14, §58-70.
[71] Wyrok ETPC z dnia 25 maja 2021 r., wnioski nr 58170/13, 62322/14 i 24960/15; Wyrok TSUE z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18, §387-389, §364-367, §430-433.

zachowania obywateli, a brak odpowiednich gwarancji ochronnych podważa zaufanie niezbędne w społeczeństwie demokratycznym[72].

3.1. WYNIKI BADAWCZE

Dla potrzeb niniejszego opracowania przeprowadzono badanie empiryczne w postaci ankiety, stanowiące uzupełnienie analizy prawnej automatycznego nadzoru masowego. Badanie miało na celu zidentyfikowanie postaw i opinii respondentów wobec stosowania zautomatyzowanych systemów nadzoru przez organy państwa oraz ocenę ich wpływu na ochronę praw podstawowych. Uzyskane wyniki pozwalają na ocenę społecznej percepcji omawianych rozwiązań, w szczególności w zakresie postrzegania zagrożeń dla praw i wolności jednostki oraz poziomu akceptacji dla stosowania zautomatyzowanych systemów nadzoru. W badaniu wzięło udział 64 osoby. Ponad 65% z nich stanowili mężczyźni. Pod względem miejsca zamieszkania największą grupę stanowili mieszkańcy wsi (54%), następnie mieszkańcy miast średnich (18,8%), natomiast pozostała część respondentów pochodziła z miast małych, dużych oraz bardzo dużych. Zastosowany podział miast według liczby mieszkańców (małe – do 20 tys., średnie – 20-100 tys., duże – 100-500 tys., bardzo duże – powyżej 500 tys.) pozwala na precyzyjne osadzenie wyników w kontekście urbanizacyjnym. Dominacja mieszkańców wsi może jednak wpływać na bardziej sceptyczne postawy wobec rozbudowanych systemów monitoringu, które są częściej kojarzone z dużymi aglomeracjami. Zdecydowana większość osób biorących udział w ankiecie posiadała wykształcenie średnie (65,6%). Wykształcenie wyższe posiadało zaś 15,6%. Ankieta składała się z 25 pytań mających na celu zbadanie opinii społecznej na temat automatycznych systemów nadzoru masowego. Jednym z kluczowych elementów badania było określenie poziomu świadomości społecznej w zakresie definicji i funkcjonowania automatycznych systemów nadzoru masowego. Uzyskane wyniki wskazują na wyraźny deficyt wiedzy w tym obszarze. Aż 46,9% respondentów zadeklarowało, że zna definicję systemów nadzoru masowego jedynie w niewielkim stopniu, natomiast 17,2% przyznało, że nie zna jej wcale. Oznacza to, że niemal dwie trzecie badanych nie posiada wystarczającej wiedzy umożliwiającej świadomą ocenę tego zjawiska. Jednoznacznie wskazuje to, że jest to wciąż zagadnienie obce wśród społeczeństwa, a ich wiedza na ten temat jest niewielka. Budzi to zatem pytania o poziom doinformowania społeczeństwa w tym temacie. Stanowi to istotny problem, gdyż brak wiedzy może prowadzić do sprzecznych postaw. Z jednej strony może

[72] Wyrok ETPC z dnia 25 maja 2021 r., wnioski nr 58170/13, 62322/14 i 24960/15, §495-498,

występować akceptacja idei monitoringu jako narzędzia bezpieczeństwa, z drugiej zaś sprzeciw wobec jego konkretnych form i zastosowań. Pomimo niskiego poziomu wiedzy deklarowanej przez respondentów, wyniki wskazują na relatywnie wysokie poparcie dla idei masowego monitoringu jako narzędzia zapewniania bezpieczeństwa publicznego. Na pytanie dotyczące zgody ze stwierdzeniem, że systemy masowego monitoringu są potrzebne do zapewnienia bezpieczeństwa publicznego, aż 48,4% respondentów odpowiedziało „zdecydowanie tak". Równocześnie 46,9% stwierdziło, że trudno im powiedzieć, czy w Polsce istnieje masowy nadzór obywateli, a 39,1% odpowiedział, że tak. Wyniki te potwierdzają niski poziom przejrzystości oraz niewystarczającą komunikację instytucji publicznych w zakresie stosowanych form monitoringu. Analiza odpowiedzi dotyczących konkretnych technologii nadzoru wskazuje na zdecydowany sprzeciw osób ankietowanych wobec ich stosowania. Aż 65,6% nie dopuszcza stosowania monitoringu miejskiego wykorzystującego technologię rozpoznawania twarzy. Jeszcze większy sprzeciw (aż 68,8%) dotyczy możliwości udostępniania państwu danych zbieranych przez firmy technologiczne, takie jak aplikacje mobilne czy portale społecznościowe. W pytaniu wielokrotnego wyboru dotyczącym sytuacji, w których zwiększony nadzór państwa jest uzasadniony, najczęściej wskazywano walkę z terroryzmem (43 odpowiedzi) oraz zapobieganie przestępczości (38 odpowiedzi). Mniej respondentów uznało za uzasadnioną kontrolę migracji (31 odpowiedzi), a jedynie 14 wskazało ochronę zdrowia publicznego. Co istotne, aż 15 respondentów zaznaczyło odpowiedź „nigdy", co świadczy o istnieniu wyraźnej grupy osób całkowicie odrzucających ideę zwiększonego nadzoru. Jednym z najbardziej jednoznacznych wyników badania jest bardzo niski poziom zaufania respondentów do instytucji państwowych w zakresie ochrony danych osobowych. Aż 64,1% badanych odpowiedziało „zdecydowanie nie" na pytanie o zaufanie w tym obszarze. Wynik ten koreluje z wysokim sprzeciwem wobec śledzenia lokalizacji telefonu w celu ochrony zdrowia publicznego – 78,1% respondentów zdecydowanie nie akceptuje takiego rozwiązania. Ocena przejrzystości informacji dotyczących monitoringu w Polsce była bardzo zróżnicowana: 37,5% respondentów uznało ją za niską, 31,3% za średnią, natomiast 28,1% nie miało zdania. Brak dominującej odpowiedzi sugeruje dezorientację społeczną oraz niewystarczający poziom debaty publicznej w tym zakresie. Jednocześnie aż 68,8% respondentów zdecydowanie uważa, że masowy monitoring narusza prawa człowieka i stanowi bardzo duże zagrożenie dla prywatności. Kolejne 15,6% wskazało odpowiedzi umiarkowanie negatywne („raczej tak" oraz „średnie zagrożenie"). Pokazuje to, że systemy nadzoru cyfrowego są postrzegane jako poważne ryzyko dla podstawowych wolności obywatelskich. Respondenci w zdecydowanej większości opowiedzieli się za koniecznością uzyskania zgody

obywateli na prowadzenie monitoringu obejmującego dane osobowe. Aż 70,3% wybrało odpowiedź „zdecydowanie tak", a kolejne 20,3% – „raczej tak". Świadczy to o silnym przywiązaniu do zasady autonomii informacyjnej jednostki. Za najbardziej wrażliwe dane uznano lokalizację (53 odpowiedzi) oraz dane biometryczne (46 odpowiedzi), co potwierdza obawy związane z możliwością śledzenia oraz identyfikacji osób. Mniej wrażliwe, choć nadal istotne, okazały się historia przeglądania oraz kontakty. Ocena poziomu obaw w skali od 0 do 10 jednoznacznie wskazuje na wysoki poziom niepokoju społecznego. Ponad połowa ankietowanych (51,6%) wskazała maksymalną wartość 10, co oznacza bardzo silny lęk przed systemami nadzoru masowego. Pozostałe odpowiedzi rozłożyły się niemal równomiernie, co sugeruje brak grupy respondentów całkowicie obojętnych wobec tego zjawiska[73].

PODSUMOWANIE

Podsumowując już powyższy artykuł, nie bez przesady można stwierdzić, że automatyczny nadzór masowy, zwłaszcza w swojej obecnej bardzo nieselektywnej i powszechnej postaci, stanowi poważne zagrożenie dla podstawowych zasad państwa prawa. Wprowadzenie i stosowanie tego rodzaju systemów wymaga nie tylko precyzyjnych podstaw prawnych, lecz także realnych mechanizmów ich kontroli, transparentności. Bez spełnienia tych warunków automatyczne systemy nadzoru masowego nie mogą być uznane za rozwiązania zgodne z europejskim standardem ochrony praw człowieka i stanowią istotne wyzwanie dla przyszłości demokratycznych społeczeństw. Zarówno orzecznictwo Europejskiego Trybunału Praw Człowieka, jak i Trybunału Sprawiedliwości Unii Europejskiej konsekwentnie podkreślają, że masowe i niezróżnicowane gromadzenie danych stanowi ingerencję o wyjątkowo wysokiej intensywności w prawo do poszanowania życia prywatnego oraz w prawo do ochrony danych osobowych.

BIBLIOGRAFIA

LITERATURA

Celeste E., Formici G., *Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism and Legislative Inertia*, "German Law Journal" 2024.

Grzelak A., *Fundamental Rights Protection in the Context of Mass Surveillance in the European Union*, "Przegląd Prawa i Administracji" 107, 2016.

[73] Opracowanie własne.

Lyon D., *Surveillance Society: Monitoring Everyday Life*, Open University Press, Buckingham 2001.

Radoniewicz F., *The Issue of Surveillance Carried Out by Technical Means Within the Jurisprudence of the European Court of Human Rights and the Constitutional Tribunal*, Przegląd Prawa Konstytucyjnego, 6(64), 2021.

Rojszczak M., *Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego*, „Acta Universitatis Wratislaviensis", Wrocław 2020.

Rojszczak M., *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka*, „Studia Prawa Publicznego" 2022.

Wójcik E., *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, Warszawa 2011.

AKTY PRAWNE

Karta praw podstawowych Unii Europejskiej (Dz.U. UE.C.2016.202.389).

Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.).

Traktat o Unii Europejskiej (Dz.U.2004.90.864/30).

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 (Dz.U. UE.L.2016.119.1).

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. U. UE. L. z 2002 r. Nr 201, str. 37 z późn. zm.).

ORZECZNICTWO

Wyrok ETPC z dnia 25 kwietnia 1978 r., skarga nr 5856/72.

Wyrok ETPC z dnia 16 grudnia 1992 r., skarga nr 13710/88.

Wyrok ETPC z dnia 16 lutego 2000 r., skarga nr 27798/95.

Wyrok ETPC z dnia 1 lipca 2008 r., skarga nr 58243/00.

Wyrok ETPC z dnia 4 grudnia 2015 r., skarga nr 47143/06.

Wyrok ETPC z dnia 12 stycznia 2016 r., skarga nr 37138/14.

Wyrok ETPC z dnia 25 maja 2021 r., wnioski nr 58170/13, 62322/14 i 24960/15.

Wyrok ETPC z dnia 25 maja 2021 r., skarga nr 35252/08.

Wyrok ETPC z dnia 12 września 2023 r., skargi nr 64371/16 i 6440716.

Wyrok ETPC z dnia 13 lutego 2024 r., skarga nr 33696/19.

Wyrok ETPC z dnia 28 maja 2024 r., skargi nr 72038/17 i 25237/18.

Wyrok TSUE z dnia 8 kwietnia 2014 r., C-293/12.

Wyrok TSUE z dnia 21 grudnia 2016 r., sprawy połączone C-203/15 i C-698/15.

Wyrok TSUE z dnia 6 października 2020 r., C-623/17.

Wyrok TSUE z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18.

Wyrok TSUE (Wielka Izba) z dnia 30 kwietnia 2024 roku, C-670/22.

INNE PUBLIKACJE

Council of Europe, *Mass Surveillance. Report by the Committee on Legal Affairs and Human Rights* https://pace.coe.int/en/files/21583 [dostęp: 2.03.2026].

European Parliamentary Research Service, *Mass Surveillance – Part 1: Risks, Opportunities and Mitigation Strategies*, *EPRS Study no. 527409 (Annex 1),* online: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409(ANN1)_EN.pdf [dostęp: 2.03.2026].

Masowa inwigilacja – Orzecznictwo ETPC i TSUE, *Wspólny arkusz informacyjny*, aktualizacja: 28.02.2025.

Privacy International, *The Global Surveillance Industry*, online: https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf [dostęp: 2.03.2026].

Innex, *Systemy CCTV – z czego się składają*, https://innex.pl/systemy-cctv-z-czego-sie-skladaja/ [dostęp: 2.03.2026].

Organizacja Narodów Zjednoczonych *Mass surveillance is a violation of human right to privacy*, https://www.liberties.eu/en/stories/un-mass-surveillance-is-a-violation-of-human-right-to-privacy-sn-892/19916 [dostęp: 2.03.2026].

AUTOMATED MASS SURVEILLANCE SYSTEMS AND THE RIGHT TO PRIVACY

Summary: In the era of digitalization and the dynamic development of artificial intelligence technologies, automated mass surveillance systems are becoming increasingly widespread, being used by both states and private entities. Their application, however, raises serious legal and ethical concerns, particularly in the context of the right to privacy and individual freedom. This article analyzes the legality, limits, and consequences of the use of mass surveillance systems in light of international law, with particular emphasis on the case law of the European Court of Human Rights. The empirical part of the study employs a survey conducted among the general public, aimed at examining citizens' opinions on the permissible limits of mass monitoring, the level of acceptance of digital surveillance, and the perceived impact of monitoring systems on human rights and the sense of privacy. The survey results made it possible to identify social expectations and concerns related to mass surveillance, indicating areas of the greatest risk of violations of individual rights.

Keyworlds: mass surveillance, right to privacy, human rights

Anna Toporowska
Università degli Studi di Roma Tor Vergata, Rzym
anna.toporowska@students.uniroma2.eu
https://orcid.org/0009-0002-3842-6050

WYKORZYSTANIE DUŻYCH MODELI JĘZYKOWYCH DO ANONIMIZACJI DOKUMENTÓW POSTĘPOWANIA SĄDOWEGO – ASPEKTY ETYCZNE

Streszczenie: Narzędzia sztucznej inteligencji są coraz częściej wykorzystywane przez organy administracji publicznej. Niesie to ze sobą znaczące konsekwencje dla praktyki stosowania prawa. Celem pracy jest wskazanie i analiza prawnych oraz etycznych aspektów anonimizacji danych osobowych zawartych w dokumentach organów administracji publicznej oraz aktach postępowania sądowego, dokonywanej przy użyciu dużych modeli językowych. Autor wskazuje zarówno na korzyści płynące z ich wykorzystania, jak i na potencjalne zagrożenia z tym związane. Przeprowadzona zostaje analiza dotychczasowych przypadków wykorzystania LLM przez sądy i organy administracji publicznej w wybranych krajach, w połączeniu z przeglądem literatury technicznej.

Słowa kluczowe: LLM; duże modele językowe; anonimizacja; AI w orzecznictwie; ChatGPT; BERT.

WPROWADZENIE

Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego definiuje anonimizację jako „proces zmiany informacji sektora publicznego w informacje anonimowe, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, lub proces zmiany danych osobowych w dane anonimowe w taki sposób, że identyfikacja osoby, której dane dotyczą, nie jest lub już nie jest możliwa". Jedna z przestrzeni, w których taka anonimizacja jest konieczna, dotyczy danych postępowania sądowego. Przede

wszystkim obejmuje to treść orzeczeń sądów powszechnych, które zostają publicznie udostępniane (np. w ramach Portalu Orzeczeń Sądów Powszechnych, jak również – następczo – w systemach informacji prawnej). Anonimizacja może też jednak służyć do innych celów, przykładowo do utajnienia danych osobowych świadka w postępowaniu karnym w sytuacjach określonych k.p.k.

Z uwagi na dużą liczbę informacji podlegających anonimizacji zgodnie z przepisami prawa, a także mając na uwadze pojawienie się nowych technologii, pojawia się pytanie, czy możliwe i zasadne byłoby wykorzystanie narzędzi sztucznej inteligencji, w tym przede wszystkim dużych modeli językowych (*Large Language Models*, „LLM"), do anonimizacji danych postępowania sądowego, a jeśli odpowiedź byłaby twierdząca – z jakimi prawnymi i etycznymi wyzwaniami się to wiąże oraz jak na te wyzwania odpowiedzieć.

Celem niniejszego rozdziału jest więc próba odpowiedzi na pytanie, jakie są możliwości wykorzystania LLM w zakresie anonimizacji danych postępowania sądowego, z jakimi zagrożeniami się to wiąże oraz jakie środki zaradcze należałoby wprowadzić, by te zagrożenia zminimalizować.

W celu udzielenia odpowiedzi na powyższe pytania zasadne będzie wykorzystanie następujących metod:

(1) przeprowadzenie analizy dotychczasowego wykorzystania LLM przy anonimizacji danych w wybranych krajach europejskich;
(2) analiza dostępnej literatury technicznej dotyczącej możliwości dużych modeli językowych w zakresie anonimizacji danych osobowych;
(3) analiza zagrożeń wiążących się z wykorzystaniem LLM przy anonimizacji danych postępowania sądowego za pomocą aksjologicznego badania prawa – analizy krytycznej treści obowiązującego prawa w kontekście etycznym;
(4) analiza potencjalnych sposobów minimalizacji zagrożeń, o których mowa powyżej.

1. DOTYCHCZASOWE WYKORZYSTANIE LLM PRZY ANONIMIZACJI DANYCH

Narzędzia sztucznej inteligencji są już teraz wykorzystywane do deidentyfikacji i anonimizacji dokumentów postępowania sądowego w niektórych krajach Unii Europejskiej[1]. Niekoniecznie jednak narzędzia te wykorzystują generatywne LLM –

[1] I. Glaser, T. Schamberger, F. Matthes, *Anonymization of german legal court rulings* [na:] *Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law*, New York 2021, s. 205-209.

często ograniczają się do innych narzędzi, wykorzystujących NER (*Named Entity Recognition*), jednak niemających funkcji generatywnych[2].

W Austrii ministerstwo sprawiedliwości wraz z Federalnym Centrum Obliczeniowym (Österreichs Bundesrechenzentrum) ogłosiło projekt wprowadzenia AI do anonimizacji orzeczeń sądowych ("Einsatz von künstlicher Intelligenz bei der Anonymisierung von Gerichtsentscheidungen")[3]. W jego ramach powstało oprogramowanie, wykorzystywane w orzeczeniach publikowanych w federalnym systemie informacji prawnej (RIS[4]). Oprogramowanie wykorzystuje uczenie maszynowe oraz NLP[5], a modele są uczone na ręcznie adnotowanych orzeczeniach sądowych, nie są natomiast wprost wykorzystywane LLM. Propozycje anonimizacji są zupełnie automatyczne. W miejsce nazw własnych wstawiane są tokeny i gwiazdki w taki sposób, by zachować czytelność dokumentu jako całości[6].

W niektórych krajach wprowadzono jednak rozwiązania oparte na modelu językowym BERT. Przykładowo w Finlandii wprowadzony został system ANOPPI. System ten został sfinansowany przez fińskie Ministerstwo Sprawiedliwości[7]. Zasada jego działania jest dość prosta – ma on za zadanie wyszukiwać rzeczowniki podlegające anonimizacji. Odbywa się to z jednej strony za pomocą gotowych narzędzi – przede wszystkim modelu FinBERT, tj. fińskiego modelu bazującego na BERT[8], a także *Stanford NER* – z drugiej poprzez zestaw predefiniowanych wzorów rozpoznawania określonych typów nazw własnych, a dodatkowo z użyciem danych z rejestru ludności, pozwalających wykrywać fińskie imiona i nazwiska. Angażowany jest też *Turku Neural Parser*, służący do identyfikacji cech gramatycznych słów[9], a w konsekwencji – do rozpoznawania, czy dane słowo w konkretnym kontekście stanowi nazwę własną. Następnie wyniki otrzymane przez dane narzędzia są

[2] L. Gianola et al., *Automatic Removal of Identifying Information in Official EU Languages for Public Administrations: The MAPA Project* [w:] *Legal Knowledge and Information Systems*, IOS Press, Brno 2020, s. 223-226.

[3] heise online, *Preis für Vorreiter: Österreich anonymisiert Justizentscheidungen mit KI-Einsatz* [na:] „Developer", https://www.heise.de/news/Preis-fuer-Vorreiter-Oesterreich-anonymisiert-Justizentscheidungen-mit-KI-Einsatz-7305474.html, 12 października 2022 r., [dostęp: 2.03.2026].

[4] *RIS Legal Information System* [w:] https://www.ris.bka.gv.at/defaultEn.aspx [dostęp: 2.03.2026].

[5] M. Hackl, D. Steinbauer, *Anonymization of court decisions in Austria*, https://commission.europa.eu/system/files/2021-04/anonymisation_webinar_29032021_austria.pdf , Wiedeń 2021 [dostęp: 2.03.2026].

[6] Bundesminister für Justiz, *IT Applications in the Austrian Justice System* [na:] https://perma.cc/D8LN-JRJF, 2018 r. [dostęp: 2.03.2026].

[7] K. Terzidou, *Automated Anonymization of Court Decisions: Facilitating the Publication of Court Decisions through Algorithmic Systems* [w:] *Proceedings of the Nineteenth International Conference on Artificial Intelligence and Law*, Braga 2023, s. 297-305.

[8] A. Nurmi, *FinBERT in recognition of named entities in Finnish texts*, Helsingin yliopisto, Helsinki 2024, s.17.

[9] *Turku neural parser pipeline* [na:] „Turku-neural-parser-pipeline", http://turkunlp.org/Turku-neural-parser-pipeline/ (dostęp 22 listopada 2025 r.).

analizowane pod kątem najczęściej powtarzających się interpretacji. Po scaleniu wyników następuje właściwa anonimizacja – wyrazy są zaznaczone odpowiednimi kolorami i symbolami w zależności od typu desygnatu[10]. Dodatkowo rzeczownikom przypisywane jest unikalne ID, przez co jedna nazwa występująca w tekście wielokrotnie będzie miała za każdym razem to samo ID[11]. W następnej kolejności nazwy są zamieniane na odpowiednie frazy, typu „osoba A", „miasto B", itd.[12], przy czym do odpowiedniej odmiany tych fraz po raz kolejny wykorzystuje się *Turku Neural Parser*. Istnieje także możliwość ręcznej modyfikacji treści, co umożliwia poprawianie ewentualnych błędów popełnianych przez oprogramowanie. Dokładność programu pierwotnie szacowano na 86%, natomiast po dokonaniu usprawnień ostatnie eksperymenty wskazują na dokładność rzędu 93%[13].

Włoski *Corte dei Conti* wykorzystuje do anonimizacji model językowy – GiusBERTo, podobnie jak rozwiązanie fińskie bazujący na modelu BERT. Został on wytrenowany na danych z Wikipedii, a także na tekstach z korpusu OSCAR[14]. Analizy wskazują na 97% dokładności tego modelu na poziomie tokenów[15].

Obecnie żadne z państw Unii Europejskiej nie wykorzystuje w sposób oficjalny generatywnych LLM. Modele oparte na BERT chętnie się jednak wprowadza[16] - z jednej bowiem strony mają one wysoki poziom dokładności w porównaniu z mechanizmami uczenia maszynowego nieobejmującymi LLM[17], z drugiej zaś wskazuje się, że wykorzystanie modeli generatywnych mogłoby skutkować powstawaniem błędów, których przy obecnym oprogramowaniu łatwiej jest uniknąć[18].

---

[10] A. Oksanen et al., *ANOPPI: A Pseudonymization Service for Finnish Court Documents* [w:] *Frontiers in Artificial Intelligence and Applications*, IOS Press, Brno 2019, 251-254.

[11] T. Deußer et al., *A Survey on Current Trends and Recent Advances in Text Anonymization*, „arXiv" nr arXiv:2508.21587v1, 2025, DOI: 10.48550/arXiv.2508.21587.

[12] Ministry of Justice, 2018, *Anoppi project*, https://oikeusministerio.fi/en/project?tunnus=OM042:00/2018, dostęp 21 listopada 2025 r.

[13] A. Oksanen, *An Anonymization Tool for Open Data Publication of Legal Documents,* [w:] *The International Workshop on Artificial Intelligence Technologies for Legal Documents (AI4LEGAL) and the International Workshop on Knowledge Graph Summarization (KGSum), 3257,* Hangzhou 2022, s.12-19.

14 D. Pettazzoni, R. Bertè, G. Salierno, *L'intelligenza artificiale nella Pubblica Amministrazione: studi e casi concreti*, https://www.procedamus.it/images/2024pdf/SaliernoBertePettazzoni.pdf, Rzym 2024 [dostęp: 2.03.2026].

[15] G. Salierno et al., *GiusBERTo: A Legal Language Model for Personal Data De-identification in Italian Court of Auditors Decisions*, arXiv, 2024 r., http://arxiv.org/abs/2406.15032 [dostęp: 2.03.2026].

[16] L. Martin et al., *CamemBERT: a Tasty French Language Model* [w:] D. Jurafsky et al. (red.), *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, 2020, s. 7203-7219.

[17] T. Deußer et al., *A Survey on Current Trends and Recent Advances in Text Anonymization, 10.48550/arXiv.2508.21587, 2025* [dostęp: 2.03.2026].

[18] I. Khuhro et al., *Artificial Intelligence and Machine Learning at the Intersection of Privacy and Archives*, „Archeion", Warszawa 2024 nr 125, s. 56-74.

2. MECHANIZMY ANONIMIZACJI DANYCH PRZY POMOCY LLM – UJĘCIE TEORETYCZNE

Obecnie najbardziej popularnymi LLM są te oparte na transformerach[19], i takie właśnie modele będą analizowane w niniejszej pracy. LLMy te można kategoryzować pod kątem architektury na enkoderowe, dekoderowe i enkoderowo-dekoderowe[20].

Zasada działania modeli o architekturze dekoderowej polega na przetwarzaniu tekstu wejściowego na tokeny, ich analizie, a następnie generowaniu kolejnych tokenów i przetwarzaniu ich na tekst[21]. Modele te charakteryzują się jednak mechanizmem *causal attention masking*, co powoduje, że elementy dalsze w kolejności są niejako zamaskowane – model widzi jedynie treść wejściową i tokeny dotychczas wygenerowane, i na ich podstawie tworzy dalszą treść[22]. Taki mechanizm działania powoduje, że modele dekoderowe są przede wszystkim wykorzystywane do generowania tekstu, mogą się jednak gorzej sprawdzać do jego analizy. Są w stanie przeprowadzić analizę w pewnym zakresie, jednak z uwagi na swoje ograniczenia są przy tym często mniej efektywne niż modele enkoderowe[23]. Do modeli dekoderowych zaliczamy m.in. GPT-4, Llama 4, czy DeepSeek-R1[24], a więc podstawę dla wielu współczesnych chatbotów.

Modele enkoderowe z kolei służą przede wszystkim do analizy znaczenia tekstu. Ich mechanizm opiera się na przetwarzaniu tekstu stworzonego w języku naturalnym na tokeny, a następnie analizie tokenów. Nie występuje tu jakikolwiek *causal attention masking*[25], modele te opierają się o dwukierunkową uwagę – każdy token może tutaj „patrzeć" na wszystkie pozostałe elementy, a nie tylko na poprzednio wygenerowane. Enkodery jednak same w sobie nie są zaprojektowane do generowania długich tekstów, tylko tworzą matematyczną reprezentację tekstu przeanalizowanego.

---

[19] G.F. Luger, *LLMs: Their Past, Promise, and Problems*, „International Journal of Semantic Computing" t. 18 nr 03, 2024, DOI: 10.1142/S1793351X24300085, s. 501-544.

[20] M. Moradi, *A Critical Review of Methods and Challenges in Large Language Models*, [w:] *Computers, Materials and Continua t. 82 nr 2 (2025), DOI: 10.32604/cmc.2025.061263, s. 1681-1698.*

[21] J. Roberts, *How Powerful are Decoder-Only Transformer Neural Models?* [w:] *2024 International Joint Conference on Neural Networks (IJCNN)*, Łódź 2024.

[22] Q. Yin et al., *StableMask: Refining Causal Masking in Decoder-only Transformer*, arXiv, 7 lutego 2024 r., http://arxiv.org/abs/2402.04779.

[23] M.R. Qorib, G. Moon, H.T. Ng, *Are Decoder-Only Language Models Better than Encoder-Only Language Models in Understanding Word Meaning?* [w:] L.-W. Ku, A. Martins, V. Srikumar (red.), *Findings of the Association for Computational Linguistics: ACL 2024*, Bangkok 2024, s. 16339–16347.

[24] Z. Xu et al., *DeepSeek: Implications for Data Science and Management in the AI Era*, „Data Science and Management" (2025), DOI: 10.1016/j.dsm.2025.09.001, https://www.sciencedirect.com/science/article/pii/S2666764925000451 [dostęp: 2.03.2026].

[25] N. Karagodin, Y. Polyanskiy, P. Rigollet, *Clustering in Causal Attention Masking,* [w:] *Advances in Neural Information Processing Systems, 37, 115652-11568, 2024*.

Do modeli enkoderowych zalicza się przede wszystkim BERT, na którym zostały oparte różnorodne rozwiązania (RoBERTa, GiusBERTo itp.)[26].

Przewaga modeli opartych na BERT nad tradycyjnym wykorzystaniem NER wynika m.in. z możliwości analizowania przez modele językowe także kontekstu, w jakim dane słowo się pojawia[27] – jakkolwiek klasyczne techniki NER będzą w stanie z wysoką dokładnością ustalić, czy dane słowo stanowi nazwę własną, może wystąpić problem z określeniem, które z nich powinny być zanonimizowane – część bowiem, jak np. nazwiska sędziów, anominizacji nie podlega.

Modele enkoderowo-dekoderowe (czy też *sequence-to-sequence*, „seq2seq") składają się z komponentu enkoderowego i dekoderowego[28]. Enkoder przetwarza sekwencję wejściową na reprezentacje wektorowe, uwzględniając cały kontekst dzięki mechanizmowi dwukierunkowej uwagi. Z reprezentacji tych korzysta dekoder, który następnie generuje tekst, biorąc pod uwagę całą ww. reprezentację i wszystkie dotychczas wygenerowane tokeny. Do modeli tych należą m.in. BART i T5[29].

Pomimo, że modele dekoderowe mają możliwość analizy tekstu, jak wskazano powyżej, robią to często mniej efektywnie niż modele enkoderowe. Różnica ta jest przede wszytkim widoczna przy przeprowadzaniu analizy na dużą skalę – w takich wypadkach modele enkoderowe działają znacznie szybciej. Ponadto BERT, w przeciwieństwie do modeli GPT można z powodzeniem wykorzystywać lokalnie[30], co może mieć znaczenie w kontekście bezpieczeństwa danych. Kolejnym aspektem jest to, że BERT jest modelem przejawiającym większy determinizm podczas wykorzystania[31], dlatego też do takich samych danych wejściowych powinny być za każdym razem dopasowane takie same dane wyjściowe, co w wypadku modeli charakteryzujących się *causal attention masking* może być niemożliwe. Praktycznie oznacza to, że w ramach zestawu tekstów, czy nawet w obrębie jednego tekstu BERT każde

[26] B. Warner et al., *Smarter, Better, Faster, Longer: A Modern Bidirectional Encoder for Fast, Memory Efficient, and Long Context Finetuning and Inference* [w:] W. Che et al. (red.), *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, Wiedeń 2025.
[27] *O. Bridal Named-entity recognition with BERT for anonymization of medical records,* Linköping 2021, s. 10.
[28] B. Liu, *Comparative Analysis of Encoder-Only, Decoder-Only, and Encoder- Decoder Language Models* [w:] *Proceedings of the 1st International Conference on Data Science and Engineering*, Singapore, Singapore 2024.
[29] E. Alhazmi et al., *Fine-Tuning Encoder-Decoder Models with Contrastive Learning for In-Context Distractor Generation* [w:] *Association for Computational Linguistics, Suzhou 2025,* s. 10056-10070.
[30] C. Boschenriedter et al., *Automated Protocol Suggestions for Cranial MRI Examinations Using Locally Fine-tuned BERT Models*, „Clinical Neuroradiology", 2025, https://doi.org/10.1007/s00062-025-01554-z.
[31] Y. Masri et al., *Comparative Analysis of BERT and GPT for Classifying Crisis News with Sudan Conflict as an Example*, „Algorithms" t. 18 nr 7, 2025, DOI: 10.3390/a18070420, https://www.mdpi.com/1999-4893/18/7/420 [dostęp: 2.03.2026].

z wielu wystąpień imienia Jan Kowalski powinien zanonimizować ten sam sposób, zaś GPT może raz go określić jako IMIĘ_1, innym zaś razem jako OSOBA_1 czy NAME_1. Jeśli natomiast chodzi o wykorzystanie do anonimizacji modeli o architekturze seq2seq, by skorzystać z zalet modeli enkoderowych oraz modeli dekoderowych – nie jest to niemożliwe, jednak z uwagi na fakt, że architektura ta jest bardziej skomplikowana, występuje tu większa podatność na błędy i mniejsza stabilność, zaś dla osiągnięcia tego samego celu może być konieczne wykorzystanie bardziej złożonych promptów. Wydaje się zatem, że skoro modele enkoderowe pozwalają osiągnąć ten sam efekt szybciej, co więcej – są mniej narażone na błędy, a z powodu bardziej deterministycznego charakteru także bardziej konsekwentne, to one mogą być z największym powodzeniem wykorzystywane przy anonimizacji znacznych ilości tekstu.

3. WYZWANIA ZWIĄZANE Z WYKORZYSTANIEM LLM PRZY ANONIMIZACJI DANYCH

Wykorzystywanie LLM w procesie anonimizacji danych może ten proces znacząco przyspieszyć, a w efekcie wspomóc sprawne publikowanie orzeczeń sądowych. Wiąże się ono jednak również z licznymi wyzwaniami natury technicznej, prawnej i etycznej.

Jednym z problemów, z jakim mierzą się podmioty wykorzystujące LLM, jest tendencja do halucynacji. Jest to sytuacja, w której model językowy tworzy tekst, który – choć często gramatycznie poprawny i wewnętrznie spójny – zawiera fałszywe informacje[32]. Problem ten dotyczy szczególnie modeli generatywnych. Przyczyny takich halucynacji mogą zarówno leżeć w nieścisłościach i sprzecznościach informacji zawartych w tekstach treningowych, jak i pojawić się w trakcie przetwarzania informacji przez model. Z jednej bowiem strony dekoder może zwrócić uwagę na niewłaściwą część tekstu źródłowego, i w konsekwencji zacząć generować nieprawidłową odpowiedź, z drugiej – mechanizm generowania tekstów opiera się m.in. na przewidywaniu najbardziej prawdopodobnej kontynuacji sekwencji na podstawie sekwencji poprzednio wygenerowanych. To z kolei może powodować coraz bardziej narastające rozbieżności pomiędzy stanem faktycznym a opisem zawartym w wygenerowanym tekście. Takie halucynacje są problemem podczas różnego rodzaju zastosowań LLM, także podczas jego wykorzystywania w procesie anonimizacji. Mogą bowiem zarówno wpływać na rozbieżności pomiędzy tekstem pierwotnym a tekstem

[32] Z. Ji et al., *Towards Mitigating LLM Hallucination via Self Reflection* [w:] H. Bouamor, J. Pino, K. Bali (red.), *Findings of the Association for Computational Linguistics: EMNLP 2023*, Singapore 2023, s. 1827-1840.

zanonimizowanym, w tym np. powodować dopowiadanie informacji, których nie ma w tekście źródłowym, jak i kreować nowe dane osobowe nieistniejących osób, których w tekście nie było. Istnieje także ryzyko pomylenia przez LLM osób występujących w tekście, w tym m.in. stron procesu, co ostatecznie może doprowadzić do błędnych interpretacji orzeczeń.

Kolejną kwestią jest problem określany jako *black box*. Pojęcie to odnosi się do sytuacji, w której wewnętrzne mechanizmy działania sztucznej inteligencji są niewystarczająco przejrzyste[33]. Problem ten dotyczy przede wszystkim zaawansowanych modeli podejmujących decyzje na podstawie wielokrotnych przekształceń danych wejściowych. Jest to szczególnie istotne w obszarach takich jak postępowanie sądowe, także w zakresie anonimizacji danych. Z jednej bowiem strony niemożliwe może się okazać ustalenie dlaczego model uznał określone słowo czy wyrażenie za podlegające anonimizacji bądź nie, co może utrudniać osiągnięcie powtarzalności efektów[34]. Z drugiej strony *black box* może jeszcze zwiększać wskazane powyżej ryzyko halucynacji, a ponadto brak pełnego dostępu do mechanizmu działania modelu może utrudniać ich usunięcie i zmuszać do każdorazowego ręcznego ich poprawiania. Kwestia ta jest także istotna w kontekście przetwarzania danych, mając na uwadze zasadę rozliczalności, o której mowa w art. 5 ust. 2 RODO – omawiane zjawisko może bowiem znacznie utrudnić wykazanie przestrzegania zasad dotyczących przetwarzania danych osobowych.

Z *black box* związany jest także kolejny problem, tj. możliwe uprzedzenia i dyskryminacja[35]. Te ostatnie mogą pojawiać się m.in. wtedy, gdy dane, na których model jest trenowany, już zawierają elementy dyskryminujące – w takim wypadku mechanizm działania algorytmów może jeszcze to zjawisko zwiększać. Wspomniany już *black box* powoduje, że uprzedzenia te trudno jest wychwycić i im przeciwdziałać. Problem ten ma znaczenie przede wszystkim w wypadku wykorzystywania LLM przy procesie podejmowania decyzji, jednak może się pojawić także w kontekście anonimizacji, przykładowo poprzez różny poziom anonimizacji w zależności od grupy etnicznej.

Wykorzystanie LLM do anonimizacji danych postępowania wiąże się także z potencjalnymi zagrożeniami związanymi z bezpieczeństwem danych treningowych.

---

[33] Y. Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation* [w:] *Harvard Journal of Law & Technology,* 31(2), 2018, s. 906.

[34] K. Murphy et al., *Artificial intelligence for good health: a scoping review of the ethics literature*, „BMC Medical Ethics" t. 22 nr 1 (2021), DOI: 10.1186/s12910-021-00577-8

[35] B.A. Herrera-Tapias et al., *Algorithmic discrimination and explainable artificial intelligence in the judiciary: a case study of the Constitutional Court of Colombia*, „Procedia Computer Science" t. 257 (2025), s. 1227-1232 DOI: 10.1016/j.procs.2025.03.164.

By model językowy mógł skutecznie rozpoznawać dane osobowe, koniecznym jest wytrenowanie go na odpowiednich zbiorach danych uwzględniających właśnie takie informacje. Jeśli jednak dane osobowe zostaną w ten sposób wykorzystany, pojawia się ryzyko ich wycieku oraz uzyskania dostępu do nich przez osoby do tego nieuprawnione[36]. To ryzyko także zwiększa się w związku z opisanym powyżej zjawiskiem *black box,* natomiast istnieje ono nawet bez tego czynnika. Jest to generalnie kwestia istotna przy rozważaniu trenowania LLM na danych osobowych, tym bardziej zaś może być brzemienna w skutki, jeśli są to dane postępowania sądowego. Te bowiem mogą zawierać zarówno istotne informacje dotyczące majątku poszczególnych osób w sprawach cywilnych, stanu rodzinnego w sprawach rodzinnych i opiekuńczych, czy też np. karalności. Nierzadko dane postępowania sądowego zawierają też dane wrażliwe, jak np. stan zdrowia, zarówno fizycznego, jak i psychicznego, czy orientacja seksualna. To powoduje, że każdy nieuprawniony dostęp i przetwarzanie takich danych może mieć poważne skutki dla osób, których dane są w nich zawarte.

Wykorzystanie dużych modeli językowych ma jednak konsekwencje nie tylko prawne, i nie tylko istotne z punktu widzenia interesu jednostki. Kolejną bowiem kwestią, którą należy rozważyć przy tej okazji, jest wpływ wykorzystania sztucznej inteligencji na środowisko naturalne. Wykorzystanie AI – szczególnie na etapie jej trenowania – wiąże się z wykorzystaniem dużej mocy obliczeniowej, co z kolei wpływa w znaczący sposób na zużycie energii elektrycznej. Badacze szacują także, że wytrenowanie jednego dużego modelu językowego wymaga wyprodukowania ilości dwutlenku węgla w przybliżeniu odpowiadającej pięciokrotności produkcji dwutlenku węgla przez przeciętny samochód osobowy przez cały jego czas używania[37]. Dodatkowo, wskazuje się na znaczące wykorzystanie wody przy utrzymywaniu infrastruktury pozwalającej na trenowanie LLM[38].

Kwestię wykorzystania LLM w kontekście postępowania sądowego – także przy anonimizacji danych – należy także rozważyć z perspektywy odpowiedzialności prawnej. Podczas anonimizacji dużych ilości informacji należy się liczyć z ryzykiem popełniania błędów. W takiej sytuacji pojawia się jednak pytanie, kto byłby odpowiedzialny za błąd popełniony przez duży model językowy. Poszczególne systemy prawne oraz gałęzie prawa regulują kwestię odpowiedzialności na różny sposób, brak jest jednak normy prawnej, która by pozwalała podchodzić do tego w sposób

[36] T. Ching et al., *Opportunities and obstacles for deep learning in biology and medicine*, [w:] *Journal of The Royal Society Interface,* t. 15 nr 141 (2018), DOI: 10.1098/rsif.2017.0387.
[37] E. Strubell, A. Ganesh, A. McCallum, *Energy and Policy Considerations for Deep Learning in NLP*, arXiv, 5 czerwca 2019 r., http://arxiv.org/abs/1906.02243 [dostęp: 2.03.2026].
[38] S. Agrawal, *Climate and Environmental Impacts of Artificial Intelligence* [w:] *Journal of High School Research*, 2024, DOI: 10.70671/2ft99c50.

jednolity. Na marginesie, można zastanawiać się, czy pewne aspekty podmiotowości prawnej nie powinny zostać przyznane samej sztucznej inteligencji (w tym LLM), i takie pytania są obecnie zadawane. Nawet jednak przy uznaniu takiej możliwości istotnym pozostaje pytanie, jak miałoby się to do ponoszenia odpowiedzialności prawnej za błędy popełnione przez duże modele językowe.

4. REKOMENDACJE

Wskazane powyżej wyzwania związane z wykorzystaniem dużych modeli językowych przy anonimizacji danych postępowania sądowego domagają się rozwiązań ułatwiających wdrożenie LLM w tym zakresie. Problemy opisane powyżej trudno kategorycznie rozwiązać, jednak możliwe - i rekomendowane - jest wprowadzenie pewnych zmian mających na celu zmniejszenie ich negatywnego wpływu.

Po pierwsze, *de lege ferenda* należy podnieść postulat uregulowania kwestii odpowiedzialności za błędy popełniane podczas anonimizacji danych przez LLM. Można tu rozważyć różne modele, jednak w wypadku kwestii tak istotnych, jak bezpieczeństwo danych osobowych, konieczne jest jednoznaczne przypisanie takiej odpowiedzialności. Ponadto należałoby wprowadzić pewne standardy (weryfikowalne np. poprzez odpowiednią certyfikację), od których spełnienia można uzależnić dopuszczenie danego narzędzia do użytku. Mając na uwadze wpływ wykorzystania LLM na środowisko naturalne, należałoby także rozważyć wykorzystanie technik anonimizacji w sposób proporcjonalny – tj. dokonać analizy, w jakim zakresie do tego zadania wystarczające byłyby bardziej przyjazne dla środowiska narzędzia, jak klasyczne modele NER, a w jakim faktycznie wykorzystanie LLM przyniesie wymierne korzyści.

Po drugie, z perspektywy podmiotów mających wykorzystywać modele językowe do anonimizacji, tj. w tym wypadku sądów, należy się zastanowić nad możliwymi rozwiązaniami ułatwiającymi jej dokonywanie zgodnie ze standardami. Przede wszystkim konieczne byłoby wprowadzenie zasady *human in the loop*, zgodnie z którą przy każdej anonimizacji dokonywanej z użyciem LLM proces ten musi być nadzorowany przez człowieka. Jest to nie tylko konieczne dla ograniczenia błędów, ale także wymagane przez przepisy prawa – zgodnie z art. 14 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) „[s]ystemy AI wysokiego ryzyka

[w tym mające zastosowanie w wymiarze sprawiedliwości] projektuje się i rozwija w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie ich wykorzystywania systemu AI mogły być skutecznie nadzorowane przez osoby fizyczne".

Po trzecie, wskazany powyżej przepis jest także istotny z perspektywy twórców oprogramowania. Ustanawia on bowiem wymóg właśnie dla osób tworzących systemy AI. By sądy były w stanie w sposób właściwy zadbać o bezpieczeństwo przetwarzania danych, twórcy oprogramowania muszą to umożliwić poprzez odpowiednie projektowanie systemów. Dodatkowo, konieczne jest rozważenie, jaka architektura modelu pozwoli na osiągnięcie efektu przy jednoczesnym uniknięciu jak największej liczby błędów. Wydaje się, że z uwagi na cechy charakterystyczne modeli enkoderowych, w tym przede wszystkim mniejszą skłonność do halucynacji, to one mają potencjał w tym zakresie. Należy także dołożyć starań, by jak najbardziej zminimalizować problem *black box*. Wydaje się, że jest to w pewnym zakresie możliwe poprzez zwiększenie kompletności i przejrzystości dokumentacji, pomocne powinno być także wykorzystanie metod zwiększenia wyjaśnialności modeli poprzez wprowadzanie postulatów xAI[39].

PODSUMOWANIE

Wykorzystanie LLM w procesie anonimizacji danych postępowania sądowego ma potencjał, by rzeczywiście ten proces usprawniać. Mając jednak na uwadze wskazane w niniejszej pracy wyzwania, koniecznym jest dołożenie starań, by to wykorzystanie było faktycznie efektywne, a przede wszystkim zgodne z prawem i etyką informacyjną. Starania te winny być podejmowane zarówno przez prawodawców, jak i przez twórców oprogramowania oraz sądy.

BIBLIOGRAFIA

LITERATURA

Agrawal S., *Climate and Environmental Impacts of Artificial Intelligence*, „Journal of High School Research" t. 1 nr 1 (2024), DOI: 10.70671/2ft99c50.

Alhazmi E., Sheng Q.Z., Zhang W.E., et al., *Fine-Tuning Encoder-Decoder Models with Contrastive Learning for In-Context Distractor Generation*.

Anoppi project [na:] „Ministry of Justice", https://oikeusministerio.fi/en/project?tunnus=OM042:00/2018, dostęp 21 listopada 2025 r.

[39] K. Devireddy, *A Comparative Study of Explainable AI Methods: Model-Agnostic vs. Model-Specific Approaches*, arXiv, 5 kwietnia 2025 r., http://arxiv.org/abs/2504.04276.

Bathaee Y., *The Artificial Intelligence Black Box and the Failure of Intent and Causation*.

Boschenriedter C., Rubbert C., Vach M., Caspers J., *Automated Protocol Suggestions for Cranial MRI Examinations Using Locally Fine-tuned BERT Models*, „Clinical Neuroradiology" (2025), DOI: 10.1007/s00062-025-01554-z, https://doi.org/10.1007/s00062-025-01554-z.

Bridal O., *Named-entity recognition with BERT for anonymization of medical records,* Linköping 2021.

Ching T., Himmelstein D.S., Beaulieu-Jones B.K., et al., *Opportunities and obstacles for deep learning in biology and medicine*, „Journal of The Royal Society Interface" t. 15 nr 141 (2018), DOI: 10.1098/rsif.2017.0387.

Deußer T., Sparrenberg L., Berger A., et al., *A Survey on Current Trends and Recent Advances in Text Anonymization*, „arXiv" nr arXiv:2508.21587v1 (2025).

Devireddy K., *A Comparative Study of Explainable AI Methods: Model-Agnostic vs. Model-Specific Approaches*, arXiv, 5 kwietnia 2025 r., http://arxiv.org/abs/2504.04276.

Gianola L., Ajausks Ē., Arranz V., et al., *Automatic Removal of Identifying Information in Official EU Languages for Public Administrations: The MAPA Project* [w:] *Legal Knowledge and Information Systems*, IOS Press 2020.

Glaser I., Schamberger T., Matthes F., *Anonymization of german legal court rulings* [w:] *Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law*, Nowy Jork 2021.

Hackl M., Steinbauer D., *Anonymization of court decisions in Austria*, Wiedeń 2021.

Herrera-Tapias B.A., Guzmán D.H., Zambam N.J., et al., *Algorithmic discrimination and explainable artificial intelligence in the judiciary: a case study of the Constitutional Court of Colombia*, „Procedia Computer Science" t. 257, 2025, DOI: 10.1016/j.procs.2025.03.164.

IT Applications in the Austrian Justice System [w:] https://perma.cc/D8LN-JRJF, 2018 r., dostęp 22 listopada 2025 r.

Ji Z., Yu T., Xu Y., et al., *Towards Mitigating LLM Hallucination via Self Reflection* [w:] H. Bouamor, J. Pino, K. Bali (red.), *Findings of the Association for Computational Linguistics: EMNLP 2023*, Singapur 2023.

Karagodin N., Polyanskiy Y., Rigollet P., *Clustering in Causal Attention Masking, 2024*.

Khuhro I., Gilmore E., Suderman J., Hofman D.L., *Artificial Intelligence and Machine Learning at the Intersection of Privacy and Archives*, „Archeion" t. 2024 nr 125, 2024.

Liu B., *Comparative Analysis of Encoder-Only, Decoder-Only, and Encoder- Decoder Language Models:* [w:] *Proceedings of the 1st International Conference on Data Science and Engineering*, Singapur 2024.

Luger G.F., *LLMs: Their Past, Promise, and Problems*, „International Journal of Semantic Computing" t. 18 nr 03, 2024, DOI: 10.1142/S1793351X24300085.

Martin L., Muller B., Ortiz Suárez P.J., et al., *CamemBERT: a Tasty French Language Model* [w:] D. Jurafsky, J. Chai, N. Schluter, J. Tetreault (red.), *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, Online 2020.

Masri Y., Wang Z., Malarvizhi A.S., et al., *Comparative Analysis of BERT and GPT for Classifying Crisis News with Sudan Conflict as an Example*, „Algorithms" t. 18 nr 7, 2025, DOI: 10.3390/a18070420, https://www.mdpi.com/1999-4893/18/7/420.

Moradi M., *A Critical Review of Methods and Challenges in Large Language Models* [w:] *Computers, Materials and Continua* t. 82 nr 2 (2025), DOI: 10.32604/cmc.2025.061263.

Murphy K., Di Ruggiero E., Upshur R., et al., *Artificial intelligence for good health: a scoping review of the ethics literature*, „BMC Medical Ethics" t. 22 nr 1, 2021, DOI: 10.1186/s12910-021-00577-8.

Nurmi A., *FinBERT in recognition of named entities in Finnish texts*, Helsingin yliopisto, Helsinki 2024.

Oksanen A., *An Anonymization Tool for Open Data Publication of Legal Documents* [w:] *The International Workshop on Artificial Intelligence Technologies for Legal Documents (AI4LEGAL) and the International Workshop on Knowledge Graph Summarization (KGSum), 3257,* Hangzhou 2022.

Oksanen Arttu, Tamper Minna, Tuominen Jouni, et al., *ANOPPI: A Pseudonymization Service for Finnish Court Documents* [w:] *Frontiers in Artificial Intelligence and Applications*, IOS Press 2019.

online heise, *Preis für Vorreiter: Österreich anonymisiert Justizentscheidungen mit KI-Einsatz* [na:] „Developer", https://www.heise.de/news/Preis-fuer-Vorreiter-Oesterreich-anonymisiert-Justizentscheidungen-mit-KI-Einsatz-7305474.html, 12 października 2022 r., dostęp 22 listopada 2025 r.

Pettazzoni D., Bertè R., Salierno G., *L'intelligenza artificiale nella Pubblica Amministrazione: studi e casi concreti*, 2024.

Qorib M.R., Moon G., Ng H.T., *Are Decoder-Only Language Models Better than Encoder-Only Language Models in Understanding Word Meaning?* [w:] L.-W. Ku, A. Martins, V. Srikumar (red.), *Findings of the Association for Computational Linguistics: ACL 2024*, Bangkok 2024.

RIS Legal Information System [na:] https://www.ris.bka.gv.at/defaultEn.aspx, dostęp 22 listopada 2025 r.

Roberts J., *How Powerful are Decoder-Only Transformer Neural Models?* [w:] *2024 International Joint Conference on Neural Networks (IJCNN)*, 2024.

Salierno G., Bertè R., Attias L., et al., *GiusBERTo: A Legal Language Model for Personal Data De-identification in Italian Court of Auditors Decisions*, arXiv, 21 czerwca 2024 r., http://arxiv.org/abs/2406.15032.

Strubell E., Ganesh A., McCallum A., *Energy and Policy Considerations for Deep Learning in NLP*, arXiv, 5 czerwca 2019 r., http://arxiv.org/abs/1906.02243.

Terzidou K., *Automated Anonymization of Court Decisions: Facilitating the Publication of Court Decisions through Algorithmic Systems* [w:] *Proceedings of the Nineteenth International Conference on Artificial Intelligence and Law*, Braga Portugal 2023.

Turku neural parser pipeline [na:] „Turku-neural-parser-pipeline", http://turkunlp.org/Turku-neural-parser-pipeline/, dostęp 22 listopada 2025 r.

Warner B., Chaffin A., Clavié B., et al., *Smarter, Better, Faster, Longer: A Modern Bidirectional Encoder for Fast, Memory Efficient, and Long Context Finetuning and Inference* [w:] W. Che, J. Nabende, E. Shutova, M. T. Pilehvar (red.), *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, Wiedeń 2025.

Xu Z., Liu S., Huang W., et al., *DeepSeek: Implications for Data Science and Management in the AI Era*, „Data Science and Management" (2025), DOI: 10.1016/j.dsm.2025.09.001, https://www.sciencedirect.com/science/article/pii/S2666764925000451.

Yin Q., He X., Zhuang X., et al., *StableMask: Refining Causal Masking in Decoder-only Transformer*, arXiv, 7 lutego 2024 r., http://arxiv.org/abs/2402.04779.

THE USE OF LARGE LANGUAGE MODELS FOR ANONYMIZATION OF JUDICIAL DOCUMENTS – ETHICAL ASPECTS

Summary: Artificial Intelligence tools are being increasingly used by public administration organs. This trend carries significant consequences for practice of legal application. The aim of this paper is to identify and analyze legal and ethical aspects of anonymization of personal data contained in documents of public administration and in judicial case files, performer using large language models. The author identifies both the benefits of using them, and the potential risks connected with it. The study includes an analysis of existing cases of the use of LLM by courts and administration organs in selected countries, together with a review of technical literature.

Keywords: LLM; large language models; anonymization; AI in judiciary; ChatGPT; BERT.

Trzeci tom monografii stanowi wszechstronną odpowiedź doktrynalną na proces głębokiej rekonfiguracji europejskiego i krajowego systemu ochrony danych. W obliczu dynamicznego rozwoju technologicznego tradycyjne instrumenty RODO wchodzą dziś w złożone interakcje z nową siatką unijnych aktów prawnych, na czele z aktem w sprawie sztucznej inteligencji (AI Act), aktem o danych (Data Act) oraz dyrektywą NIS 2.

Autorzy podejmują kluczowe problemy współczesnego prawa nowych technologii, badając m.in. transgraniczne transfery danych, granice komercjalizacji baz danych, cyberbezpieczeństwo w sektorze ochrony zdrowia, a także status prawny notariusza czy specyfikę procedur antydopingowych. Istotny wkład w dyskurs stanowią również studia nad transparentnością algorytmiczną, prawem do sprzeciwu wobec wnioskowań AI oraz wykorzystaniem dużych modeli językowych w wymiarze sprawiedliwości.

Monografia stanowi cenne źródło metodologiczne dla środowiska akademickiego oraz niezbędne wsparcie dla praktyków poszukujących odpowiedzi na wyzwania prawne i cyfrowe.

ISBN: 978-83-68410-86-0