PRAWO DO OCHRONY DANYCH OSOBOWYCH

TOM II

REDAKCJA
MIKOŁAJ BRZÓSTOWICZ

Studenckie Koło Naukowe
Ochrony Danych Osobowych

ARCHAEGRAPH
Wydawnictwo Naukowe

PRAWO DO OCHRONY DANYCH OSOBOWYCH

TOM II

REDAKCJA

MIKOŁAJ BRZÓSTOWICZ

PRAWO DO OCHRONY DANYCH OSOBOWYCH

REDAKCJA
MIKOŁAJ BRZÓSTOWICZ

TOM II

Studenckie Koło Naukowe
Ochrony Danych Osobowych

ARCHAEGRAPH
Wydawnictwo Naukowe

REDAKCJA:
MIKOŁAJ BRZÓSTOWICZ

RECENZJA NAUKOWA:

DR HAB. KINGA BĄCZYK-ROZWADOWSKA, PROF. UMK
DR NATALIA DAŚKO
DR DAMIAN KACZAN
DR KAROLINA ROKICKA-MURSZEWSKA

KOREKTA REDAKTORSKA, SKŁAD I PROJEKT OKŁADKI

KAROL ŁUKOMIAK

ISBN: 978-83-68410-16-7

Monografia została sfinansowana ze środków Wydziału Prawa i Administracji UMK oraz UMK

Studenckie Koło Naukowe
Ochrony Danych Osobowych

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

ARCHAEGRAPH
Wydawnictwo Naukowe

ŁÓDŹ 2025

SPIS TREŚCI

PRZEDMOWA **9**

CZĘŚĆ 1

OCHRONA DANYCH OSOBOWYCH
A ADMINISTRACJA PUBLICZNA

MIKOŁAJ BRZÓSTOWICZ

ZASADA INTEGRALNOŚCI I POUFNOŚCI A BEZPIECZEŃSTWO DANYCH OSOBOWYCH W PODMIOTACH PUBLICZNYCH: STUDIA PRZYPADKÓW **11**

AGNIESZKA GIZLER

ŚRODKI PUBLICZNOPRAWNE WYKORZYSTYWANE W ADMINISTRACJI PUBLICZNEJ W CELU OCHRONY DANYCH OSOBOWYCH **25**

DOMINIKA FILIPEK

DYLEMATY PRAWNE NA STYKU JAWNOŚCI ŻYCIA PUBLICZNEGO I PRYWATNOŚCI. STUDIA PRZYPADKÓW UDOSTĘPNIANIA INFORMACJI PUBLICZNEJ A OCHRONA DANYCH OSOBOWYCH **41**

MICHAŁ POCZWARDOWSKI

OCHRONA DANYCH OSOBOWYCH A ARCHIWA PAŃSTWOWE – ZAGADNIENIA WYBRANE **55**

MICHAŁ ZAWADA

ROLA FEDERALNEGO KOMISARZA DS. OCHRONY DANYCH I INFORMACJI (FDPIC) W SZWAJCARII W KONTEKŚCIE WEJŚCIA W ŻYCIE NOWELIZACJI SZWAJCARSKIEGO PRAWA OCHRONY DANYCH OSOBOWYCH (NFADP) 1 WRZEŚNIA 2023 R. **71**

CZEŚĆ 2

OCHRONA DANYCH OSOBOWYCH A CYBERBEZPIECZEŃSTWO I SZTUCZNA INTELIGENCJA

MIKOŁAJ BRZÓSTOWICZ

ZASADA INTEGRALNOŚCI I POUFNOŚCI (ART. 5 UST. 1 LIT. F RODO) A ZAGROŻENIA CYFROWE. CZY NOWE REGULACJE EUROPEJSKIE SĄ W STANIE ZWIĘKSZYĆ BEZPIECZEŃSTWO CYFROWE? **87**

LAURA BŁASZCZAK

SZTUCZNA INTELIGENCJA W ŚRODOWISKU PRACY W DOBIE RODO I AI ACT **107**

AGNIESZKA SZYMCZAK

OCHRONA DANYCH OSOBOWYCH W ERZE AI – WYZWANIA PRAWNE I TECHNOLOGICZNE **129**

CZEŚĆ 3
OCHRONA DANYCH OSOBOWYCH A MEDYCYNA

KINGA PARCHEM
BEZPIECZEŃSTWO DANYCH GENETYCZNYCH W POLSKIM PORZĄDKU PRAWNYM **141**

ALEKSANDRA PAWEŁEK
OCHRONA DANYCH OSOBOWYCH W MIĘDZYNARODOWYCH BADANIACH KLINICZNYCH I LECZENIU PACJENTÓW ZA GRANICĄ **159**

MIKOŁAJ RESZKOWSKI
BIOBANKI I OCHRONA DANYCH OSOBOWYCH **179**

SŁOWEM WSTĘPU

Szanowni Państwo,

oddaję w Państwa ręce kolejne wydanie monografii naukowej poświęconej ochronie danych osobowych, która powstała z inicjatywy Studenckiego Koła Naukowego Ochrony Danych Osobowych działającego przy Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu. Niniejsza publikacja porusza różnorodne aspekty prawne związane z ochroną danych osobowych, analizując je na gruncie administracji publicznej, cyberbezpieczeństwa, sztucznej inteligencji oraz medycyny. Autorzy, reprezentujący środowisko akademickie wielu polskich uczelni, w sposób kompleksowy i interdyscyplinarny omawiają najważniejsze problemy i wyzwania prawne, przed jakimi stoją współczesne społeczeństwa informacyjne.

Wydanie tej monografii było możliwe dzięki wsparciu finansowemu udzielonemu przez Wydział Prawa i Administracji oraz Rektora Uniwersytetu Mikołaja Kopernika w Toruniu. Wyrazy serdecznego podziękowania składam kolegium dziekańskiemu, na czele z Dziekanem prof. dr hab. Maciejem Serowańcem, a także dr hab. Monice Wałachowskiej, prof. UMK, prorektorce ds. studenckich i kształcenia, których życzliwość i zaangażowanie umożliwiły realizację tego przedsięwzięcia.

Szczególne podziękowania kieruję do naszych recenzentów: dr hab. Kingi Bączyk-Rozwadowskiej, prof. UMK, dr Natalii Daśko, dr Damiana Kaczana oraz dr Karoliny Rokickiej-Murszewskiej, którzy swoją wiedzą, wnikliwością oraz cennymi uwagami przyczynili się do podniesienia jakości publikacji.

Osobiste słowa wdzięczności pragnę skierować do prof. dr hab. Arkadiusza Lacha, opiekuna naszego koła naukowego, który przez cały okres mojej kadencji Prezesa Studenckiego Koła Naukowego Ochrony Danych Osobowych wspierał

nasze inicjatywy, służył radą oraz motywował do ciągłego rozwoju naukowego, w tym przy poprzednim wydaniu monografii oraz obecnym.

W szczególny sposób chciałbym także podziękować adwokatce Justynie Wilczyńskiej-Baraniak, Alicji Guzy oraz radczyni prawnej Gabrieli Sacha. Wasze zaangażowanie, profesjonalizm oraz codzienne wsparcie, jakiego udzielacie młodym prawnikom, zasługują na najwyższe uznanie. To właśnie Wam dedykuję tę publikację, jako symbol mojej głębokiej wdzięczności do waszej codziennej pracy.

Na zakończenie chciałbym gorąco podziękować wszystkim autorom, którzy swoimi tekstami wzbogacili niniejszą monografię. Wasza praca, determinacja oraz zaangażowanie są dowodem na to, jak istotną rolę w świecie nauki odgrywa pasja i nieustanna chęć poszerzania wiedzy.

Z wyrazami wdzięczności,

Mikołaj Brzóstowicz

Redaktor monografii
Założyciel oraz Prezes SKNODO (2023-2025)

MIKOŁAJ BRZÓSTOWICZ
UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU
ORCID 0009-0001-0920-8751

ZASADA INTEGRALNOŚCI I POUFNOŚCI A BEZPIECZEŃSTWO DANYCH OSOBOWYCH W PODMIOTACH PUBLICZNYCH: STUDIA PRZYPADKÓW.

Streszczenie: W obliczu rosnących zagrożeń cyfrowych zasada integralności i poufności danych osobowych odgrywa kluczową rolę w sektorze publicznym. Rozdział analizuje podstawy prawne ochrony danych, wskazując na wymogi RODO i krajowych regulacji. Omówione studia przypadków ukazują typowe naruszenia, ich przyczyny oraz konsekwencje prawne i organizacyjne. Wskazano, że brak skutecznych środków technicznych i organizacyjnych prowadzi do incydentów, takich jak ataki ransomware czy nieuprawnione ujawnienie danych. Rozdział podkreśla konieczność wdrażania strategii zarządzania ryzykiem, regularnych audytów i szkoleń, by zwiększyć poziom ochrony informacji i zgodność z przepisami.

Słowa kluczowe: Ochrona danych osobowych, integralność danych, poufność danych, rodo, cyberbezpieczeństwo.

1. WSTĘP

W dobie dynamicznej cyfryzacji i rosnącego znaczenia informacji, zasada integralności i poufności danych osobowych nabiera kluczowego znaczenia, szczególnie w kontekście funkcjonowania podmiotów publicznych. Jednostki samorządu terytorialnego oraz inne instytucje publiczne przetwarzają ogromne ilości danych, obejmujących zarówno informacje zwykłe, jak i szczególne kategorie danych osobowych, których nieuprawnione ujawnienie może prowadzić do

naruszenia prywatności obywateli. Artykuł 5 ust. 1 lit. f RODO ustanawia zasadę integralności i poufności jako jeden z filarów ochrony danych osobowych, zobowiązując administratorów do stosowania odpowiednich środków technicznych i organizacyjnych minimalizujących ryzyko ich przypadkowej utraty, uszkodzenia lub nieuprawnionego dostępu (Bielak-Jomaa i Lubasz 2018, art. 5).

Sektor publiczny, jako zbiór jednostek realizujących zadania o charakterze administracyjnym, społecznym i gospodarczym, jest szczególnie narażony na incydenty naruszenia bezpieczeństwa danych. Ataki cybernetyczne, błędy ludzkie oraz nieodpowiednie procedury zarządzania informacjami mogą prowadzić do poważnych konsekwencji prawnych i finansowych, czego dowodem są liczne decyzje Prezesa UODO, nakładające sankcje na instytucje za niewłaściwe zabezpieczenie danych (DKN.5131.56.2022 2022). Analiza tych przypadków pozwala na identyfikację kluczowych zagrożeń i wskazanie dobrych praktyk w zakresie wzmacniania ochrony informacji w sektorze publicznym.

Rozdział uwzględnia stan prawny obowiązujący w dniu 1 lutego 2025 r.

2. PODSTAWY PRAWNE OCHRONY DANYCH OSOBOWYCH

Podstawy ochrony danych osobowych w Unii Europejskiej oraz w Polsce opierają się na Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), które ustanawia jednolite standardy przetwarzania danych osobowych, w tym zasady dotyczące ich integralności i poufności (Bielak-Jomaa i Lubasz 2018, art. 5). Zgodnie z art. 5 ust. 1 lit. f RODO, dane osobowe powinny być przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (por. Fajgielski 2019).

Jednym z podstawowych przepisów związanych z integralnością i poufnością danych jest art. 32 RODO, który zobowiązuje administratorów oraz podmioty przetwarzające do wdrożenia środków technicznych i organizacyjnych uwzględniających: stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania (Fajgielski 2022, art. 32). Środki te powinny obejmować m.in. pseudonimizację i szyfrowanie danych osobowych, zdolność do zapewnienia ciągłej poufności, integralności, dostępności i odporności systemów oraz regularne testowanie skuteczności stosowanych zabezpieczeń (Bielak-Jomaa i Lubasz 2018, art. 32). RODO nakłada również obowiązek przeprowadzania analizy ryzyka, dzięki której administratorzy mogą dostosować poziom ochrony do konkretnych zagrożeń.

Na gruncie polskiego prawa kwestie te uzupełnia ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781)(dalej: u.o.d.o.), której celem jest dostosowanie krajowego porządku prawnego do rozporządzenia. Zgodnie z jej postanowieniami, Prezes Urzędu Ochrony Danych Osobowych pełni funkcję organu nadzorczego, uprawnionego do kontroli administratorów oraz nakładania sankcji za naruszenie przepisów. W odniesieniu do podmiotów publicznych istotnym aspektem jest ograniczenie wysokości kar administracyjnych – w przypadku instytucji państwowych i samorządowych maksymalna kara wynosi 100 000 zł (art. 102 ust. 1 pkt 1 u.o.d.o.).

Ochrona integralności i poufności danych osobowych w sektorze publicznym wiąże się także z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.), która zobowiązuje wybrane podmioty publiczne do wdrażania środków minimalizujących ryzyko cyberataków oraz raportowania incydentów do zespołów CSIRT (Bielak-Jomaa i Lubasz 2018, art. 5). Szczególnie istotne w tym kontekście są ataki ransomware, które w ostatnich latach stały się poważnym zagrożeniem dla jednostek samorządowych oraz instytucji publicznych (Klimczuk 2025 [dostęp 28.02.2025]).

Ponadto, integralność i poufność danych osobowych pozostają w ścisłym związku z zasadą rozliczalności (art. 5 ust. 2 RODO), nakładającą na administratorów obowiązek wykazania, że wdrożone środki bezpieczeństwa są adekwatne do zagrożeń (Fajgielski 2022, art. 5). W praktyce oznacza to konieczność prowadzenia regularnych audytów, testowania procedur awaryjnych oraz zapewnienia odpowiednich szkoleń dla pracowników, co pozwala zminimalizować ryzyko naruszenia ochrony danych (UODO ZSPU.421.2.2018).

Przepisy prawa kształtujące ochronę integralności i poufności danych osobowych są kluczowe dla prawidłowego funkcjonowania podmiotów publicznych. Ich stosowanie nie tylko pozwala na uniknięcie sankcji administracyjnych, ale przede wszystkim wzmacnia zaufanie obywateli do instytucji państwowych i samorządowych, które przetwarzają ich dane osobowe.

3. STUDIA PRZYPADKÓW – ANALIZA WYBRANYCH DECYZJI PREZESA UODO

Analiza decyzji Prezesa Urzędu Ochrony Danych Osobowych pozwala zidentyfikować najczęstsze naruszenia zasady integralności i poufności w podmiotach publicznych oraz ocenić konsekwencje prawne i organizacyjne tych incydentów. W niniejszym rozdziale przedstawione zostaną wybrane przypadki, które

obrazują różne źródła zagrożeń – od ataków cybernetycznych, przez błędy proceduralne, po niewłaściwe udostępnienie danych obywateli.

3.1. DECYZJA DOTYCZĄCA NARUSZENIA INTEGRALNOŚCI I POUFNOŚCI DANYCH W ADMINISTRACJI SAMORZĄDOWEJ

Administracja samorządowa pełni kluczową rolę w przetwarzaniu danych osobowych obywateli, obejmujących informacje identyfikacyjne, dane finansowe oraz dokumentację urzędową. Wymaga to szczególnej dbałości o przestrzeganie zasad integralności i poufności określonych w art. 5 ust. 1 lit. f RODO. Pomimo tego dochodzi czasem do incydentów naruszających ochronę danych osobowych, czego przykładem jest decyzja Prezesa Urzędu Ochrony Danych Osobowych (PUODO), znak sprawy: DKN.5131.34.2022.

W omawianym przypadku nałożono administracyjną karę pieniężną w wysokości 50 000 zł na Wójta Gminy za niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych. Do incydentu doszło po otwarciu przez pracownika Urzędu zainfekowanego załącznika e-mail, co uruchomiło *ransomware* szyfrujący serwer zawierający dane osobowe pracowników, byłych pracowników oraz kontrahentów JST. Dane te obejmowały m.in.: imiona i nazwiska, adresy zamieszkania, numery PESEL, rachunków bankowych, serie i numery dowodów osobistych oraz telefony kontaktowe. Dalsza analiza wykazała także wyciek danych do sieci. Ze względu na brak odpowiednich kopii zapasowych oraz nieaktualne zabezpieczenia, część danych została bezpowrotnie utracona.

PUODO stwierdził naruszenie art. 5 ust. 1 lit. f oraz art. 32 RODO, które nakładają na administratorów obowiązek stosowania adekwatnych środków technicznych i organizacyjnych chroniących dane. Dodatkowo, administrator nie wykonał wymaganej analizy ryzyka, czym naruszył także art. 24 ust. 1 i art. 25 ust. 1 RODO. Urząd nie dysponował skutecznymi mechanizmami umożliwiającymi wykrycie i powstrzymanie ataku w czasie rzeczywistym, ani efektywnymi procedurami backupowymi.

Zastosowanie odpowiednich środków technicznych i organizacyjnych powinno uwzględniać aktualny stan wiedzy technologicznej oraz poziom zagrożeń. W analizowanym przypadku zabrakło aktualizacji systemów operacyjnych, segmentacji sieci, mechanizmów *Data Loss Prevention* oraz regularnych testów zabezpieczeń. W efekcie atak ransomware powiódł się, a dane osobowe stały się

dostępne dla nieuprawnionych osób. PUODO podkreślił, że ciągłość działania instytucji publicznych powinna stanowić priorytet, co nie zostało spełnione.

Decyzja PUODO zobowiązała Wójta Gminy do wdrożenia efektywnych środków zapobiegających takim incydentom, w tym regularnych audytów bezpieczeństwa, szkoleń personelu z zakresu cyberbezpieczeństwa, polityki minimalizacji ryzyka przy przesyłaniu załączników e-mail oraz wielowarstwowej ochrony danych z szyfrowaniem i izolacją baz danych. Podjęte działania mają na celu przywrócenie zgodności z RODO oraz zwiększenie bezpieczeństwa danych w jednostce samorządowej. Przypadek ten podkreśla, że niewłaściwe zabezpieczenie danych w urzędach samorządowych może prowadzić do poważnych konsekwencji finansowych oraz utraty zaufania społecznego.

Analiza tego zdarzenia dowodzi, iż skuteczna ochrona integralności i poufności danych osobowych w administracji samorządowej wymaga kompleksowego podejścia, obejmującego analizę ryzyka, regularne wykonywanie kopii zapasowych, szkolenia pracowników oraz ciągłe monitorowanie infrastruktury IT. Decyzja PUODO wskazuje jednoznacznie, że naruszenia zasad ochrony danych są zagadnieniem nie tylko technicznym, ale także organizacyjnym i prawnym, wobec czego bezpieczeństwo danych powinno stanowić kluczowy element działalności administracji samorządowej.

3.2. DECYZJA DOTYCZĄCA INCYDENTU CYBERBEZPIECZEŃSTWA W JEDNOSTCE ADMINISTRACJI PUBLICZNEJ

Administracja publiczna staje się coraz częściej celem cyberataków, prowadzących do naruszenia zasady integralności i poufności danych osobowych. Pomimo obowiązków wynikających z art. 5 ust. 1 lit. f oraz art. 32 RODO dotyczących wdrażania skutecznych środków technicznych i organizacyjnych, praktyka pokazuje, że nie wszystkie podmioty publiczne odpowiednio je realizują.

Jednym z przykładów poważnego naruszenia jest sprawa Burmistrza Miasta Z. (znak sprawy: DKN.5131.56.2022.), ukaranego przez Prezesa UODO karą administracyjną w wysokości 30 000 zł. Incydent miał miejsce w czerwcu 2022 r., gdy doszło do ataku *ransomware*, w wyniku którego zaszyfrowane zostały wszystkie pliki na serwerach urzędu, w tym dane osobowe ok. 9400 osób (imiona, nazwiska, numery PESEL, adresy, numery rachunków bankowych, dane finansowe oraz kontaktowe). Powodem incydentu było otwarcie przez pracownika zainfekowanego załącznika e-mail oraz wykorzystanie przez atakujących luk

w nieaktualizowanym systemie operacyjnym. Brak backupu systemu skutkował utratą danych z ostatnich dwóch lat, co znacznie utrudniło funkcjonowanie urzędu.

Prezes UODO stwierdził naruszenie przepisów RODO, w szczególności art. 5 ust. 1 lit. f, art. 32 ust. 1 i 2, art. 24 ust. 1 oraz art. 25 ust. 1, wskazując na brak odpowiednich zabezpieczeń technicznych, organizacyjnych oraz niewystarczającą analizę ryzyka. Decydujące były: brak regularnego testowania systemów ochrony, nieaktualizowana infrastruktura IT oraz brak mechanizmów wielowarstwowego zabezpieczenia.

Właściwe zarządzanie ryzykiem cyberbezpieczeństwa wymaga m.in. segmentacji sieci, regularnych aktualizacji systemowych, monitorowania aktywności użytkowników, szkoleń z zakresu cyberzagrożeń, skutecznych procedur backupu oraz stosowania uwierzytelniania wieloskładnikowego (MFA - *Multi-Factor Authentication*). Brak tych zabezpieczeń umożliwił przeprowadzenie skutecznego ataku.

W decyzji Prezesa UODO zobowiązano Burmistrza Miasta Z. do wdrożenia systemu regularnego testowania i monitorowania infrastruktury IT, przeprowadzenia szkoleń pracowników, wprowadzenia odpornych na ransomware procedur backupu oraz przeprowadzania regularnych audytów bezpieczeństwa wraz z analizą ryzyka i raportowaniem wyników organowi nadzorczemu.

Incydent ten dowodzi, że cyberzagrożenia stanowią realne ryzyko dla administracji publicznej, a skutki zaniedbań w zakresie ochrony danych mogą mieć poważne konsekwencje prawne, organizacyjne i społeczne. Kluczowa jest proaktywna polityka bezpieczeństwa, regularne analizy ryzyka oraz systematyczne szkolenia personelu, co pozwoli uniknąć podobnych zdarzeń w przyszłości.

3.3. DECYZJA DOTYCZĄCA NIEWŁAŚCIWEGO UDOSTĘPNIENIA DANYCH PRZEZ PODMIOT PUBLICZNY

Ochrona danych osobowych w podmiotach publicznych wymaga szczególnej staranności, zwłaszcza w kontekście realizacji zasady poufności i integralności informacji. Nieprawidłowe udostępnienie danych, zwłaszcza w trybie dostępu do informacji publicznej, może prowadzić do poważnych naruszeń praw osób fizycznych (Fajgielski 2022, art. 5). Przykładem takiego incydentu jest decyzja Prezesa UODO dotycząca prokuratury rejonowej, która bezprawnie ujawniła dane osobowe trzech osób fizycznych, realizując wniosek dziennikarza o dostęp do akt zakończonego postępowania przygotowawczego (znak sprawy: DKN.5131.45.2022). Wnioskodawca uzyskał dostęp do imion, nazwisk,

adresów zamieszkania, numerów PESEL oraz informacji o stanie zdrowia jednej z osób występujących w charakterze świadka, co stanowiło naruszenie art. 9 RODO dotyczącego szczególnej ochrony danych wrażliwych.

Prezes UODO stwierdził, że prokuratura naruszyła kilka przepisów RODO, przede wszystkim art. 5 ust. 1 lit. f (zasada integralności i poufności), art. 32 ust. 1 i 2 (brak odpowiednich środków technicznych i organizacyjnych zabezpieczających dane przed bezprawnym udostępnieniem), art. 33 (niezgłoszenie naruszenia organowi nadzorczemu) oraz art. 34 (brak powiadomienia osób, których dane ujawniono, o naruszeniu). Organ wskazał, że administrator, którym była prokuratura, nie przeprowadził odpowiedniej analizy ryzyka naruszenia prywatności ani nie konsultował działań z inspektorem ochrony danych (IOD).

W konsekwencji nałożono na prokuraturę administracyjną karę pieniężną w wysokości 20 000 zł oraz zobowiązano ją do wdrożenia procedur anonimizacji dokumentów, przeprowadzenia audytu ochrony danych osobowych, przeszkolenia pracowników odpowiedzialnych za dostęp do informacji publicznej oraz wdrożenia mechanizmów oceny ryzyka przy każdym wniosku. Ponadto Prezes UODO zobowiązał administratora do poinformowania osób poszkodowanych o naruszeniu ich prywatności, umożliwiając podjęcie ewentualnych działań ochronnych.

Analiza tego przypadku potwierdza, że instytucje publiczne mają obowiązek każdorazowo analizować konsekwencje udostępnienia informacji publicznej pod kątem ochrony danych osobowych, gdyż samo powołanie się na ustawę o dostępie do informacji publicznej nie zwalnia z przestrzegania przepisów RODO. Podkreśla również rolę inspektora ochrony danych oraz konsekwencje prawne i finansowe wynikające z nieprzestrzegania zasad ochrony danych osobowych.

4. PRZYCZYNY I KONSEKWENCJE NARUSZEŃ ZASADY INTEGRALNOŚCI I POUFNOŚCI W PODMIOTACH PUBLICZNYCH

Zasada integralności i poufności danych osobowych, uregulowana w art. 5 ust. 1 lit. f RODO, nakłada na administratorów obowiązek stosowania odpowiednich środków technicznych i organizacyjnych w celu ochrony przetwarzanych informacji (Bielak-Jomaa i Lubasz 2018). W podmiotach publicznych, takich jak administracja samorządowa, organy wymiaru sprawiedliwości czy instytucje ochrony zdrowia, naruszenie tej zasady może wynikać zarówno z zaniedbań organizacyjnych, jak i zewnętrznych ataków na systemy informatyczne. Analizując decyzje Prezesa UODO, można wskazać kilka powtarzających się

przyczyn naruszeń, które prowadzą do istotnych konsekwencji prawnych, finansowych i organizacyjnych dla jednostek administracji publicznej.

Jednym z najczęstszych źródeł naruszeń jest niewystarczające zabezpieczenie systemów informatycznych, co czyni instytucje publiczne podatnymi na ataki cybernetyczne, w tym ransomware. W sprawie dotyczącej urzędu miejskiego (UODO DKN.5131.56.2022) atakujący wykorzystali nieaktualizowane oprogramowanie oraz brak wdrożonych mechanizmów testowania skuteczności zabezpieczeń, co doprowadziło do zaszyfrowania danych i ich wycieku do sieci. Problemem była nie tylko luka w systemie, ale także brak strategii zapobiegania zagrożeniom oraz nieskuteczne monitorowanie aktywności w sieci. Wiele instytucji publicznych nie prowadzi regularnych audytów bezpieczeństwa ani testów odporności infrastruktury IT na potencjalne zagrożenia, co sprawia, że wykrycie incydentu następuje zbyt późno (Fajgielski 2022, art. 5). W analizowanych przypadkach ataki były możliwe m.in. ze względu na brak uwierzytelniania wieloskładnikowego oraz stosowanie przez urzędników haseł o niskim poziomie bezpieczeństwa, co ułatwiało przejęcie kontroli nad systemami przez osoby nieuprawnione.

Kolejną istotną przyczyną naruszeń jest czynnik ludzki, który przejawia się w nieodpowiednich procedurach postępowania z danymi, błędach popełnianych przez pracowników oraz braku odpowiednich szkoleń. Przykładem jest decyzja dotycząca prokuratury rejonowej, która w odpowiedzi na wniosek o dostęp do informacji publicznej udostępniła dokumenty zawierające dane osobowe, nie stosując mechanizmów anonimizacji (UODO DKN.5131.45.2022). Zaniechanie to wynikało nie tylko z braku świadomości ryzyka, ale również z błędnej interpretacji przepisów o jawności informacji publicznej. Niejednokrotnie pracownicy instytucji publicznych traktują udostępnianie danych jako czynność administracyjną, a nie proces wymagający szczególnej ostrożności, co skutkuje przypadkowymi wyciekami danych. Innym przykładem naruszenia wynikającego z błędów ludzkich jest sytuacja, w której pracownik urzędu skopiował dane na prywatny nośnik USB, nie zdając sobie sprawy z konsekwencji takiego działania, co naraziło instytucję na postępowanie przed organem nadzorczym (UODO DKN.5131.44.2022).

Nieodpowiednie zarządzanie ryzykiem oraz brak wdrożonych procedur reagowania na incydenty również stanowią istotne czynniki prowadzące do naruszeń. W analizowanych przypadkach administratorzy często nie podejmowali działań mających na celu ocenę zagrożeń i wdrożenie skutecznych środków zaradczych. W sprawie dotyczącej urzędu gminy incydent cyberbezpieczeństwa

nie został odpowiednio zgłoszony i przeanalizowany, co spowodowało dalsze komplikacje w zakresie przywracania utraconych danych oraz zapewnienia zgodności z RODO (UODO DKN.5131.34.2022). Obowiązek zgłaszania naruszeń, określony w art. 33 i 34 RODO, nie zawsze jest realizowany przez podmioty publiczne, co prowadzi do dodatkowych sankcji nakładanych przez UODO. Wiele instytucji nie wdraża skutecznych polityk ochrony danych, przez co w sytuacji wystąpienia incydentu brak jest jasno określonych procedur pozwalających na minimalizację skutków naruszenia i szybkie podjęcie działań naprawczych (Fajgielski 2022, art. 5).

Konsekwencje naruszeń zasady integralności i poufności danych w podmiotach publicznych mogą być dotkliwe zarówno dla jednostek administracyjnych, jak i osób, których dane dotyczą. Po pierwsze, jednostki publiczne narażone są na odpowiedzialność administracyjną w postaci kar finansowych nakładanych przez Prezesa UODO. W przypadku analizy omawianych decyzji kary wynosiły od 10 000 zł do 50 000 zł, przy czym ich wysokość uzależniona była od wagi naruszenia oraz liczby osób poszkodowanych. Oprócz sankcji finansowych, instytucje muszą wdrożyć działania naprawcze, co wiąże się z dodatkowymi kosztami organizacyjnymi, w tym koniecznością modernizacji systemów IT, przeszkolenia personelu czy opracowania nowych polityk ochrony danych.

Po drugie, naruszenia te prowadzą do konsekwencji prawnych i mogą dodatkowo skutkować odpowiedzialnością cywilnoprawną. Osoby, których dane zostały ujawnione lub utracone, mogą dochodzić roszczeń z tytułu naruszenia ich prywatności, powołując się na art. 82 RODO, który przewiduje możliwość uzyskania odszkodowania za szkody wynikające z niewłaściwego przetwarzania danych osobowych (Bielak-Jomaa i Lubasz 2018, art. 32). W szczególności w przypadkach ujawnienia danych wrażliwych, takich jak informacje o stanie zdrowia, istnieje realne ryzyko procesów sądowych oraz konieczność wypłaty zadośćuczynienia poszkodowanym.

Kolejnym aspektem konsekwencji jest utrata zaufania społecznego oraz negatywny wpływ na wizerunek instytucji publicznej. W przypadku urzędów, szpitali czy prokuratur naruszenie ochrony danych może skutkować obawami obywateli co do bezpieczeństwa powierzanych informacji, co wpływa na postrzeganie profesjonalizmu danej jednostki. Media często nagłaśniają incydenty związane z wyciekami danych, co dodatkowo potęguje społeczne konsekwencje i może prowadzić do konieczności prowadzenia działań mających na celu odbudowanie reputacji instytucji.

Analizując powyższe przypadki, można stwierdzić, że skuteczna ochrona integralności i poufności danych w podmiotach publicznych wymaga wdrożenia kompleksowych środków technicznych i organizacyjnych. Kluczową rolę odgrywa systematyczna analiza ryzyka, wdrażanie polityki regularnych audytów oraz stosowanie procedur szybkiego reagowania na incydenty. Odpowiednie szkolenia pracowników oraz ścisła współpraca z inspektorem ochrony danych pozwalają na minimalizację ryzyka naruszeń i zapewnienie zgodności z obowiązującymi przepisami. Pomimo obowiązujących regulacji, wciąż występują istotne luki w zakresie zarządzania bezpieczeństwem informacji w sektorze publicznym, co wymaga dalszych działań zarówno na poziomie organizacyjnym, jak i legislacyjnym. Wdrażanie dobrych praktyk w zakresie ochrony danych osobowych powinno stać się priorytetem w zarządzaniu instytucjami publicznymi, aby skutecznie chronić prywatność obywateli oraz unikać konsekwencji wynikających z naruszeń RODO.

5. WNIOSKI I REKOMENDACJE

Analiza przypadków naruszenia zasady integralności i poufności danych osobowych w podmiotach publicznych wskazuje na istotne luki w systemach ochrony informacji oraz braki w organizacyjnych i technicznych środkach bezpieczeństwa. Każdy z omówionych incydentów ujawnia różne źródła problemów – od błędów ludzkich, przez zaniedbania proceduralne, aż po przestarzałą infrastrukturę IT. Wspólnym mianownikiem wszystkich tych naruszeń jest niedostateczna świadomość administratorów co do skali zagrożeń oraz konsekwencji prawnych wynikających z nieprzestrzegania przepisów RODO. O ile regulacje prawne wyraźnie nakładają na podmioty publiczne obowiązek zapewnienia adekwatnego poziomu ochrony danych, w praktyce stosowanie tych wymogów często okazuje się powierzchowne lub niepełne, co prowadzi do poważnych konsekwencji zarówno dla samych instytucji, jak i dla osób, których dane dotyczą.

Jednym z najistotniejszych problemów jest brak spójnej polityki zarządzania ryzykiem oraz niewłaściwa analiza potencjalnych zagrożeń. Podmioty publiczne, choć posiadają obowiązek przeprowadzania oceny skutków dla ochrony danych, często traktują ten proces jako formalność, nie dostosowując wdrażanych środków do rzeczywistych zagrożeń (Bielak-Jomaa i Lubasz 2018, art. 5). Skutkuje to niewystarczającymi mechanizmami prewencyjnymi, co szczególnie wyraźnie widać w przypadkach ataków ransomware na urzędy miejskie i gminne (por. UODO DKN.5131.56.2022). Brak regularnych aktualizacji systemów, niestosowanie

zaawansowanych mechanizmów uwierzytelniania oraz niewłaściwa polityka backupowa powodują, że instytucje te stają się łatwym celem cyberprzestępców (UODO DKN.5131.32.2023). W omawianym przypadku urzędu miejskiego, w którym doszło do zaszyfrowania serwerów, konsekwencje ataku mogły zostać znacząco ograniczone, gdyby jednostka posiadała skuteczny system odzyskiwania danych oraz zabezpieczenia chroniące przed tego rodzaju zagrożeniami. Podobne wnioski płyną z decyzji dotyczącej nieautoryzowanego kopiowania danych na prywatny nośnik przez pracownika administracji samorządowej – niewdrożenie mechanizmów kontroli dostępu oraz brak procedur monitorowania aktywności użytkowników skutkowały utratą poufności przechowywanych informacji.

Innym kluczowym problemem jest niewłaściwe postępowanie z wnioskami o dostęp do informacji publicznej i brak procedur anonimizacji dokumentów przed ich udostępnieniem. Decyzja PUODO dotycząca prokuratury, w której ujawniono dane osób niepełniących funkcji publicznych, jednoznacznie wskazuje na konieczność wypracowania standardów umożliwiających zachowanie równowagi pomiędzy jawnością życia publicznego a ochroną prywatności (UODO ZSPU.421.2.2018). Brak konsultacji z inspektorem ochrony danych oraz pochopne udostępnienie informacji doprowadziły do naruszenia zasady poufności, co wiązało się zarówno z konsekwencjami prawnymi, jak i reputacyjnymi dla organu administracji (UODO ZSPU.421.2.2018). Podobne sytuacje miały miejsce w innych jednostkach samorządowych, gdzie niedostateczna świadomość personelu w zakresie ochrony danych skutkowała nieuprawnionym ujawnieniem danych obywateli. Problem ten można skutecznie ograniczyć poprzez wdrożenie mechanizmów oceny ryzyka przed udostępnieniem informacji oraz stosowanie technologii automatycznej anonimizacji dokumentów.

Równie istotnym wnioskiem wynikającym z analizy naruszeń jest konieczność zapewnienia efektywnej współpracy z inspektorem ochrony danych, który powinien pełnić aktywną rolę w monitorowaniu zgodności z przepisami RODO. W wielu jednostkach administracyjnych IOD jest traktowany wyłącznie jako formalny doradca, zamiast jako realny element systemu zarządzania bezpieczeństwem danych. Właściwe zaangażowanie inspektora mogłoby zapobiec wielu naruszeniom poprzez odpowiednie doradztwo i kontrolę wdrażanych procedur (UODO 2025). Brak specjalistycznego nadzoru w analizowanych przypadkach był jednym z czynników, które doprowadziły do incydentów, co świadczy o konieczności zwiększenia jego roli w codziennej działalności podmiotów publicznych (UODO DKN.5131.56.2022).

Podmioty publiczne powinny również w większym stopniu wykorzystywać dostępne narzędzia technologiczne w celu zabezpieczenia danych osobowych. Szyfrowanie informacji, kontrola dostępu do baz danych, wieloskładnikowe uwierzytelnianie oraz systemy wykrywania anomalii w ruchu sieciowym stanowią podstawowe elementy współczesnych strategii ochrony danych, które powinny być standardem w administracji publicznej (Bielak-Jomaa i Lubasz 2018, art. 5). W decyzjach UODO często podkreślano, że zastosowane środki ochrony były niewystarczające w stosunku do rzeczywistych zagrożeń, co wynikało z braku ich regularnej aktualizacji oraz niedostatecznego testowania skuteczności wdrożonych rozwiązań (UODO DKN.5131.32.2023). Wdrożenie mechanizmów regularnej oceny skuteczności zabezpieczeń oraz testowania procedur odzyskiwania danych mogłoby znacząco ograniczyć skutki ewentualnych incydentów.

Podsumowując, naruszenia integralności i poufności danych osobowych w sektorze publicznym wynikają przede wszystkim z braku świadomości zagrożeń, niedostatecznych procedur ochrony oraz niskiego poziomu zabezpieczeń technicznych. Kluczowe rekomendacje obejmują wdrażanie skutecznych polityk zarządzania ryzykiem, zwiększenie roli inspektora ochrony danych, stosowanie nowoczesnych rozwiązań technologicznych oraz regularne szkolenia personelu administracyjnego. Konieczne jest także wypracowanie jednolitych standardów w zakresie anonimizacji danych przed ich udostępnieniem oraz zapewnienie skutecznych procedur reagowania na incydenty. Odpowiednie dostosowanie organizacyjne i techniczne może nie tylko zapobiec naruszeniom ochrony danych, ale także zwiększyć zaufanie obywateli do podmiotów publicznych oraz poprawić efektywność ich działania. Wdrażanie środków zgodnych z zasadą *privacy by design* i *privacy by default* powinno stać się standardem w funkcjonowaniu administracji publicznej, aby minimalizować ryzyko naruszeń i zapewnić zgodność z przepisami RODO w długoterminowej perspektywie.

BIBLIOGRAFIA

Monografia

Fajgielski P.

2019 Prawo ochrony danych Osobowych. Zarys wykładu, Warszawa.

2021 Ochrona danych osobowych w administracji publicznej, Warszawa.

2022 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. II, Warszawa 2022, art. 5.

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

Monografia wieloautorska

Drobek P.
art. 5, [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. Bielak-Jomaa E., Lubasz D., Warszawa.

Lubasz D.
2022 Zasady dotyczące przetwarzania danych osobowych [w:] Meritum. Ochrona danych osobowych, red. Lubasz D., Warszawa, wyd. II.

Źródła internetowe

Klimczuk O., Najważniejsze incydenty w 2024 roku, https://cyberdefence24.pl/cyberbezpieczenstwo/najwazniejsze-incydenty-w-2024-roku [dostęp: 28.02.2025]

Urząd Ochrony Danych Osobowych, Poradnik dotyczący naruszeń ochrony danych osobowych [dostęp: 28.02.2025]

Orzecznictwo

Decyzja PUODO z 6.04.2019 r., ZSPU.421.2.2018, LEX nr 3285040.
Decyzja PUODO z 20.12.2023 r., DKN.5131.32.2023, LEX nr 3646392.
Decyzja PUODO z 16.05.2023 r., DKN.5131.56.2022, LEX nr 3573929.

INTEGRITY AND CONFIDENTIALITY PRINCIPLE AND PERSONAL DATA SECURITY IN PUBLIC ENTITIES: CASE STUDIES

Abstract: In the face of growing digital threats, the principle of data integrity and confidentiality plays a crucial role in the public sector. This chapter examines the legal foundations of data protection, highlighting the requirements of the GDPR and national regulations. Case studies illustrate common violations, their causes, and legal and organizational consequences. The analysis reveals that the lack of effective technical and organizational measures leads to incidents such as ransomware attacks or unauthorized data disclosures. The chapter emphasizes the need for risk management strategies, regular audits, and staff training to enhance data security and ensure regulatory compliance.

Keywords: data protection, data integrity, data confidentiality, gdpr, cybersecurity

AGNIESZKA GIZLER

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

ŚRODKI PUBLICZNOPRAWNE WYKORZYSTYWANE W ADMINISTRACJI PUBLICZNEJ W CELU OCHRONY DANYCH OSOBOWYCH

Streszczenie: Niniejsza praca ma na celu pokazanie jak istotnym i wciąż aktualnym problemem jest skuteczna ochrona danych osobowych. Z tego względu, omówione zostały instrumenty oraz mechanizmy publicznoprawne podjęte w administracji publicznej, które mają za zadanie sprostać obowiązkom wynikającym z ogólnego rozporządzenia o danych osobowych, ustawy o ochronie danych osobowych czy innych aktów prawnych. Zwrócono uwagę na ciągłą potrzebę nowelizowania i uszczegółowiania przepisów prawnych związaną z stałym rozwojem elektroniki i powstaniem tzw. e-administracji. Poruszono problematykę przestrzegania zasady legalizmu przez organy administracji państwowej. Podkreślono wzmocnienie ochrony danych osobowych poprzez wprowadzenie reformy przekształcającej Biuro Generalnego Inspektora Ochrony Danych Osobowych w Urząd Ochrony Danych Osobowych. W konsekwencji, zwiększono rolę tego organu nadzorczego wraz z przyznaniem mu większej niezależności. Wreszcie wskazano, że za naruszenie ochrony danych osobowych nie grozi jedynie odpowiedzialność karna, a może również zostać nałożona administracyjna kara pieniężna.

Słowa kluczowe: ochrona danych osobowych, administracja publiczna, RODO, e-administracja, odpowiedzialność administracyjna

UWAGI WPROWADZAJĄCE

Organy administracji publicznej wykonując powierzone im zadania, mogą jednocześnie mieć do czynienia z danymi osobowymi swoich klientów, które gromadzą czy też przetwarzają. W polskim systemie prawnym za dane osobowe

zostały uznane takie informacje, które umożliwią lub mogą umożliwić identyfikację danej osoby. Stały wzrost informatyzacji i automatyzacji różnych sektorów gospodarki ma odzwierciedlenie również w administracji publicznej. W konsekwencji, przekłada się to na ciągłą potrzebę nowelizowania przepisów prawnych dotyczących ochrony danych osobowych, tak by nie było żadnych luk prawnych czy też, tak aby postęp informatyczny nie wyprzedzał regulacji prawnych, które mają za zadanie dopiero go wdrożyć. Organy państwowe muszą przestrzegać konstytucyjnej zasady legalizmu, czyli działają one w granicach wyznaczonych przez prawo, a ich kompetencje i prawo do prowadzenia danej sprawy, postępowania czy kontroli wynikają wprost z aktów prawnych. Zatem pojawia się pytanie: czy obecne przepisy prawne w sposób kompleksowy i wystarczający regulują problematykę ochrony danych osobowych (Prasal, Perłakowska, Abgarowicz 2023).

ŹRÓDŁA PRAWA ZAPEWNIAJĄCE OCHRONĘ DANYCH OSOBOWYCH

Podstawowym źródłem nakładającym obowiązek ochrony danych osobowych jest 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 (dalej: RODO). Zostało ono wprowadzone z dwóch zasadniczych względów. Po pierwsze, przepisy dotyczące tej materii potrzebowały usystematyzowania i ujednolicenia, aby zapewnić przejrzystość prawa. Po drugie, miały być odpowiedzią na stały wzrost informatyzacji i umożliwić przy tym odpowiednią i adekwatną do niego ochronę dobra jakim są dane osobowe. Z tego względu w rozporządzeniu tym ujęto w sposób możliwie jak najbardziej szeroki przedmiot ochrony. Określono, że są to dane dotyczące osoby fizycznej zautomatyzowane, ewentualnie chociaż częściowo podlegające automatyzacji lub dane „będące częścią zbioru czy mające być jego częścią". Ujęte w ten sposób pojęcie przetwarzania danych, powoduje, że rozporządzenie jest wciąż aktualne, pomimo dynamicznego pojawiania się nowych technologii. Specjalnie zostało wykorzystane niedookreślone sformułowanie „automatyzacji", zamiast poszczególnych wyliczeń urządzeń elektronicznych. Co za tym, idzie nawet pojedyncze urządzenie może przetwarzać dane osobowe, jeśli jest tylko związane z Internetem. Co więcej, urządzenie samo w sobie bez ingerencji człowieka również może przetwarzać dane. Rozporządzenie nie jest jedynym unijnym źródłem prawa w tym zakresie, ponieważ w prawie pierwotnym również znajdują

się bezpośrednie odniesienia do ochrony danych osobowych. Należy podkreślić, że umieszczenie tego rodzaju regulacji w prawie pierwotnym ma o wiele większe znaczenie niż tylko i wyłącznie nakreślenie w jaką stronę Unia Europejska powinna zmierzać w tym zakresie. Przepisy dotyczące tej materii znaleźć można w Traktacie o funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. czy w Karcie Praw Podstawowych Unii Europejskiej z dnia 26 października 2012 r. Oznacza to, że ochrona danych osobowych należy się każdemu, jest to jego podstawowe prawo związane z prawem do prywatności, a nieprzestrzeganie czy naruszenie go pociąga za sobą konsekwencje prawne (Mostowik 2022).

W krajowym porządku prawnym w dniu 10 maja 2018 r. została uchwalona ustawa o ochronie danych osobowych (dalej: u.o.d.o.). Ustawodawca krajowy w akcie prawnym nie wskazał dokładnie, które z danych są uznawane za dane osobowe. Nie zastosował on katalogu zamkniętego, z tego względu, że nie da się jednoznacznie i wystarczająco określić, które z informacji dotyczących osób fizycznych będą danymi osobowymi. Nie ma wątpliwości, że takie dane jak imię, nazwisko, nr PESEL czy adres zamieszkania/ zameldowania stanowią dane osobowe, ponieważ umożliwiają bezpośrednią identyfikację ich właściciela (Litwiński 2007). W dobie cyfryzacji danymi będą także identyfikatory internetowe m.in. adres IP (Skoczylas 2019, s.48). Jednak są sytuacje, w których na pozór zwykłe informacje zostają również uznane za dane osobowe, które trzeba szczególnie chronić. Wynika to z drugiej części ustawowej definicji, czyli z możliwości zidentyfikowania osoby fizycznej za pomocą tych informacji. Taka sytuacja ma miejsce m.in. wtedy, gdy jedna informacja w połączeniu z drugą umożliwi ustalenie osoby fizycznej. W przypadku, w którym np. jeden organ będzie w posiadaniu tych dwóch informacji uznać należy je za dane osobowe, ponieważ nic nie stoi na przeszkodzie by nie był on w stanie powziąć wiedzy kogo one dotyczą. Nawet jeśli by nie skorzystał z tych informacji to i tak są one uznane za dane osobowe, ponieważ wystarczy sam fakt, że była realna możliwość zidentyfikowania osoby bez narażenia organu na nadmierne koszty czy działania. Z powyższego względu, każdą sytuację dotyczącą przetwarzania informacji należy w sposób indywidualny rozpatrzyć. Pod pojęciem przetwarzania danych osobowych kryje się szereg działań związanych z danymi osobowymi. Nie są to tylko czynności wymienione w art. 7 pkt. 2 u.o.d.o., takie jak przechowywanie, zmienianie, udostępnianie czy usuwanie danych osobowych. Ustawodawca również w tym przypadku pozostawił katalog otwarty. Jest to celowy zabieg mający za zadanie zapewnić jak najszerszą ochronę danych osobowych (Litwiński 2007).

W krajowym porządku prawnym wciąż wiele sporów budzi nachodzący na siebie miejscami zakres prawa do udostępnienia informacji publicznej z prawem do ochrony danych. Z jednej strony każdy ma prawo do zażądania informacji np. o działalności organów publicznych czy zapoznania się z treściami decyzji administracyjnych, które stanowią informację publiczną. Z drugiej strony powstaje dylemat, co jeśli w dokumentach tych znajdują się dane osób, a każdy z kolei ma prawo do prywatności. Co ciekawe, ochronę danych osobowych w tym przypadku wywodzi się z ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, a konkretniej z art. 5 ust. 2. Na jego podstawie można zarówno udostępnić informację, gdy dotyczy ona m.in. wykonywania zadań publicznych przez uprawniony podmiot. Jednocześnie artykuł ten może być również podstawą do odmowy np. ze względu na tajemnice przedsiębiorcy. Reasumując, decyzję o udostępnieniu informacji uzależniono od podmiotu, którego dotyczy. Każdą sytuację trzeba rozważyć indywidualnie a szerokie pole w tym zakresie mają sądy administracyjne. W udostępnionej informacji w celu ochrony danych stosuję się szyfrowanie części danych, które mogłyby doprowadzić do zidentyfikowania osoby (Nosarzewski 2023).

PROCEDURA PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe są przetwarzane przez administratora danych lub przez podmiot przetwarzający. Wyodrębniono te 2 grupy podmiotów z tego względu, że posiadają one odmienne obowiązki, a więc w konsekwencji i ich odpowiedzialność za naruszenia będzie zróżnicowana. W sprawach z zakresu administracji publicznej administratorem danych są organy państwowe. Aby określić, który organ jest właściwy do przetwarzania danych jako administrator, w pierwszej kolejności należy zajrzeć do ustaw zawierających materialne regulacje dotyczące danego rodzaju sprawy. Przykładowo, administratorem danych osobowych pochodzących ze spisu powszechnego jest Prezes Głównego Urzędu Statystycznego, ponieważ w ustawie o narodowym spisie powszechnym ludności i mieszkań w 2021 r. znajduję się przepis upoważniający go do tego. Jest to najbardziej pożądana sytuacja, gdy w jednym miejscu, w tym przypadku w ustawie, znajduję się wprost przepis wskazujący organ oraz dane, które podlegają przetworzeniu przez niego. W rzeczywistości jednak w większości przypadków, należy sięgnąć do przepisów dotyczących właściwości rzeczowej oraz miejscowej organów. W przypadku, gdy toczy się postępowanie administracyjne warto zajrzeć do Kodeksu Postępowania Administracyjnego, gdzie uregulowano właściwość miejscową organów. Następnie

w ustawowych przepisach sprawdzić czy dany organ ma legitymizacje do prowadzenia danego postępowania, czyli czy posiada odpowiednie kompetencje, należy to do jego zadań i czy nie jest wyłączony z prowadzenia tego rodzaju kategorii spraw. W tego rodzaju przypadkach, których jest znacznie więcej w praktyce, to właśnie organ właściwy do prowadzenia postępowania jest również jednocześnie administratorem danych. Co za tym idzie, już w obrębie jednej gminy może działać kilku odrębnych od siebie administratorów ze względu na inny rodzaj postępowań jakie prowadzą. Warto również wspomnieć, że w administracji państwowej niektóre zadania organy administracji rządowej przekazują organom samorządowym. Dzieję się tak głównie, jeżeli powierzone zadania np. wydawanie decyzji administracyjnych wymaga szczegółowej znajomości stanu faktycznego danego regionu. Wraz z przekazaniem zadań między organami, zostaje również przekazane uprawnienie do przetwarzania danych osobowych. Odtąd ciężar odpowiedzialności spoczywać będzie na organie samorządowym. Przekazanie kompetencji i statusu administratora ma miejsce w formie porozumienia, które jest wiążące tzn. organy nie mogą wykraczać poza jego granicę (Skoczylas 2019, s. 49). Podkreślone zostało, że nie wszystkie zadania można przekazać m.in. nie wolno przekazać obowiązku wyznaczenia inspektora ochrony danych. Na przykład, na organy finansowe nałożono nie tylko uprawnienie w postaci możliwości jego powołania, ale wręcz obowiązek jego wyznaczenia (Żmuda-Matan 2023, s. 97).

Podobna sytuacja ma miejsce w przypadku podmiotu przetwarzającego dane. Jego legitymizacja może wynikać wprost z przepisów prawa, gdy przekazanie kompetencji jest obligatoryjne lub może przybrać formę porozumienia, gdy przepisy prawne na to przyzwalają. Należy pamiętać, że podmiot ten przetwarza dane w imieniu administratora danych. Podczas, gdy pod pojęciem przetwarzania danych przez administratora rozumiane się władztwo nad tymi danymi, nawet jeśli nie ma on do nich dostępu i ich nie posiada. Co istotne, osoba fizyczna np. upoważniony do przetwarzania danych pracownik urzędu gminy nie może zostać pociągnięty do odpowiedzialności za naruszenia, ponieważ administratorem jest urząd gminy i to on zostanie rozliczany z swoich obowiązków. Zdarzają się przypadki, w których organ administracji publicznej przekazuje kompetencje do przetwarzania danych podmiotowi prywatnemu i jak najbardziej jest to dopuszczalne. W przypadku, w którym organ prywatny miałby do czynienia z zadaniami publicznymi, wtedy wymagany jest przepis prawny umożliwiający takie przekazanie. W polskim systemie prawnym wyróżnić można jeszcze współadministrowanie, które jest dość nową konstrukcją, nieznaną przed wejściem w życie rozporządzenia RODO. Ma ono miejsce wtedy, gdy więcej niż jeden podmiot/

organ jest potrzebny do przetwarzania danych osobowych. Bez współdziałania tych organów, nie byłoby możliwe przetworzenie danych. Wskazuję się, że można przez to rozumieć wydanie wspólnej decyzji czy też wydanie różnych decyzji, które wzajemnie się uzupełniają. Każdy z organów biorących udział w tym procesie czerpie dane osobowe z tego samego zbioru, ale niekoniecznie musi wykorzystywać je w tym samym celu. Najczęściej o współadministrowaniu można mówić, gdy jeden organ odpowiedzialny jest za prowadzenie centralnego zbioru danych osobowych, do którego dane wprowadza uprawniony do tego inny organ (Litwiński 2022).

Podsumowując, przetwarzanie danych osobowych przez organy administracji państwowej zostało uregulowane w nieco odmienny sposób niż przetwarzanie tych danych przez inne podmioty. W administracji to przepisy prawne stanowią, który organ i jakie dane może przetworzyć. Gdy w pozostałych przypadkach to stan faktyczny przesądza o tym kto powinien zostać administratorem i w jaki sposób wykonywać swoje obowiązki (Litwiński 2022).

OBOWIĄZKI ADMINISTRATORA DANYCH ZWIĄZANE Z UPRAWNIENIAMI OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Do zadań podmiotu przetwarzającego dane należy ocena procesu przetwarzania pod względem możliwości naruszeń praw i wolności jednostek. Na podstawie sporządzonej oceny ryzyka, administrator danych ma za zadanie stworzyć odpowiedni system, który w jak największym stopniu będzie chronić dane. Służą mu do tego wytyczne wskazujące jak taki system powinien wyglądać. Znajdują się one m.in. w rozporządzeniu RODO. Po pierwsze, już na etapie projektowania bazy administrator powinien zadbać o ochronę danych. Po drugie, wszystkie jego czynności powinny być zgodne z prawem i w jego granicach. Co, więcej musi zostać sprecyzowany cel istnienia takiej bazy. Tak jak wyżej wspomniano są przypadki, w których przepis prawny określa wprost, który organ ma obowiązek być administratorem i jakie dane może przetwarzać, tym samym też w jakim celu. Po trzecie, administrator danych może na każdym etapie tworzenia i funkcjonowania bazy wprowadzać zmiany i zabezpieczenia, wręcz jest to nawet konieczne do zapewniania coraz to lepszej ochrony. Aby dane mogły zostać użyte i wprowadzone do bazy potrzebna jest zgoda osoby fizycznej, do której one należą. Zgoda ta powinna być świadoma i dobrowolna, a forma pisemna, w tym elektroniczna lub ustna (Prasal, Perłakowska, Abgarowicz 2023). Jest to najstarsze istniejące zabezpieczenie danych i jednocześnie do dziś fundamentalne. Określa się

je mianem indywidualnej kontroli jednostki nad swoimi danymi, ponieważ nie pozostaje ona bierna a ma prawo decydować o sobie i korzystać z przysługujących jej praw. Umożliwiono jej, aby realnie zadbała o swoje dobro i określiła, które wartości chcę w największym stopniu ochronić (Mostowik 2022).

Na indywidualne zarządzanie swoimi danymi składa się szereg narzędzi w jakie jednostka została wyposażona m.in. uprawnienia informacyjne, decyzyjne i kontrolne. Przede wszystkim osoba fizyczna ma prawo na bieżąco być informowana m.in., które z jej danych zostaną wykorzystane, dlaczego i przez jakie podmioty będą administrowane i przetwarzane oraz czy trafią do państw trzecich (Mostowik 2022). Obowiązek informacyjny spoczywa na administratorze danych. Został on zobowiązany do rzetelnych działań, które będą jednocześnie przejrzyste dla jednostki. Wynika to z prymatu zasady rzetelności w procesie przetwarzania danych. Osoba fizyczna musi być świadoma m.in. całego procesu przetwarzania, praw jakie w związku z nim posiada i wiedzieć w jaki sposób może skontaktować się z administratorem danych. Administrator danych musi ją o tym w odpowiedni sposób poinformować, czyli w taki by mógł być on dla niej zrozumiały i łatwo dostępny. Informacje powinny być napisane konkretnie, zwięźle, językiem kierowanym do danej osoby tzn. jeśli nie jest to osoba, zorientowana w regulacjach prawnych to administrator powinien użyć słownictwa potocznego a nie języka prawniczego. Co więcej, informacja ta powinna być wyczerpująca, znajdować się w niej powinny wszystkie najważniejsze kwestie, w tym wskazanie strony, która będzie wykorzystywać dane. Jednostka nie powinna mieć potrzeby domniemywać, ponieważ informacje powinny być na tyle jasne i pełne, że bez problemu na ich podstawie można określić przyszłe skutki takiego przetworzenia danych. Zasadą jest, że administrator przekazuję takie informacje w formie pisemnej. Co więcej, bardzo często na swojej stronie internetowej czy to np. na stronie Biuletynu Informacji Publicznej zamieszczona zostaje ogólna informacja o przetwarzaniu danych. Przybrać może ona wtedy nie tylko formę pisemną, ale również ikonograficzną czy być udostępniona w postaci filmiku. W przypadku, w którym osoba, której dane mają zostać przetworzone, zażąda telefonicznego poinformowania, organ ma prawo w takiej formie jej go udzielić. W razie wątpliwości co do tożsamości osoby fizycznej, administrator identyfikuję rozmówcę m.in. zadając pytania o szczegółowe dane. Udzielenie informacji o przetworzeniu danych nie ma charakteru jednorazowego tzn. administrator nie informuję osoby fizycznej tylko wtedy, kiedy chcę od niej uzyskać zgodę na przetwarzanie. Ma on obowiązek informowania jej również w czasie przetwarzania danych, np. gdy pozyska on informację od osób trzecich na jej temat, które chcę wykorzystać w bazie. Osoba

fizyczna obligatoryjnie musi zostać poinformowana o każdym naruszeniu jej danych, które skutkować może utratą lub ograniczeniem jej podstawowych praw i wolności (Litwiński 2022).

Przejawem ochrony danych osobowych jest zasada, że dane osobowe mogą zostać przetworzone tylko wtedy, gdy osoba fizyczna, której one dotyczą wyrazi uprzednio zgodę na to. Jednak istnieją wyjątki enumeratywnie wymienione w przepisach. Do takiego wyjątku należy m.in. sytuacja, gdy dane mają posłużyć ochronie żywotnych interesów osoby fizycznej lub też przyczyniać się do wykonania obowiązku prawnego czy zabezpieczenia interesu publicznego. W tym drugim przypadku, dane te gromadzone są najczęściej w celach badawczych, statystycznych czy archiwalnych. Administrator danych ma obowiązek stworzenia bazy tylko z tych danych, które są niezbędne do osiągnięcia celu. Co więcej, powinien on te dane poddać przynajmniej pseudonimizacji. Jest to odwracalny proces i polega na przetworzeniu danych w taki sposób, aby uniemożliwić zidentyfikowanie konkretnej osoby, która jest ich właścicielem. Wymienione powinności administratora są przejawem urzeczywistnienia się zasady minimalizacji danych, ponieważ cały proces przetwarzania podlega ścisłym zasadą i ma pełnić określone funkcje (Prasal, Perłakowska, Abgarowicz 2023).

Kolejnym prawem informacyjnym jednostki jest jej wystąpienie z prośbą do administratora o udostępnienie kopii przetwarzanych danych. Ma to na celu, umożliwienie jej osobistego zweryfikowania czy w bazie znajdują się prawidłowo wprowadzane dane oraz czy są przetwarzane zgodnie z przepisami prawa. Organ administracji państwowej, który jest administratorem ma obowiązek odpowiedzieć na wniosek, a w przypadku nierozłączalności danych z nośnikiem, także udostępnić kopię tego nośnika. Udostępnienie odbywa się bezpłatnie tak jak to było w przypadku informowania osób, których dane są przetwarzane. Ochrona danych osobowych nie dotyczy tylko wybranej grupy ludzi, stąd omawiane prawa jednostki dotyczą każdego. Każdy może skorzystać z nadanych mu przez prawodawcę uprawnień. Z powyższego względu, mimo braku dokładnej regulacji przyjęto praktykę, aby pełnomocnik danej osoby mógł również złożyć wniosek. Ma to zapobiec ograniczeniu prawa do ochrony danych osobom, którym np. zdrowie nie pozwala na osobiste złożenie wniosku. Nie jest wymagana szczególna forma wniosku, ale administrator musi mieć pewność, że w imieniu właściwej osoby działa pełnomocnik (Litwiński 2022).

W przypadku, w którym jednostka zauważy, że dane zawarte w bazie nie zgadzają się z rzeczywistymi danymi ma prawo złożyć wniosek do administratora danych o ich sprostowanie. Niekiedy zdarzają się błędy pisarskie, dane potrzebują

uaktualnienia lub jednostka stwierdzi, że dane są niepełne i wymagają uzupełnienia. W każdym takim wypadku jednostka, może wnioskować o to, ale administrator nie jest tym żądaniem bezwzględnie związany. Niekoniecznie zdanie jednostki co do braków w bazie będzie słuszne. Administrator działając na podstawie zasady ograniczenia celu przetwarzania danych, może podjąć decyzje, że informacje zawarte w bazie są wystarczające do realizacji tego celu. W takim przypadku powinien on poinformować jednostkę o odmowie sprostowania danych, najlepiej w formie pisemnej. Błędy w bazie nie zawsze mogą pojawiać się z winy podmiotu przetwarzającego dane, niekiedy są to też błędy pisarskie jednostki, które wymagają korekty. Warto również pamiętać, że są przypadki, w których jednostka ma obowiązek poinformowania administratora o zmianie danych np. gdy podczas studiowania zmieni nazwisko w związku z zawarciem małżeństwa. Powinna ona wtedy do swojego żądania dołączyć dokument potwierdzający m.in. odpis aktu stanu cywilnego (Błażewski, Behr 2018, s. 160- 163).

Narzędziem kontrolującym przetwarzanie danych jest prawo jednostki do żądania usunięcia danych osobowych. Konstrukcja ta została zawarta w art. 17 rozporządzenia RODO i miała być odpowiedzią na rozwijający się w zatrważającym tempie Internet. Powstała po to by wyjść poza tylko i wyłącznie ochronę wewnętrzną baz danych. Chciano rozciągnąć jej zakres także na kolejne przetworzenia dokonywane przez następnych administratorów i nie tylko. W rzeczywistości jednak regulacja nie sprostała wymagającym realiom. Z prawa tego można skorzystać po zajściu wymienionych w przepisie okoliczności. Poza taką sytuacją, w której jednostka wycofuje zgodę, z uprawnienia tego może również skorzystać, gdy przetwarzanie jest niezgodne z prawem. Jest to funkcjonalnie trudna do przeprowadzenia procedura, ponieważ ciężar dowodowy jest po stronie osoby fizycznej, a środki jakimi dysponuje administrator mają być adekwatne do naruszeń. Nie ma więc wymienionych konkretnych środków umożliwiających usunięcie danych osobowych np. z Internetu. Z logicznego punktu widzenia użycie przez ustawodawcę nieostrego pojęcia „adekwatności" jest uzasadnione. Administrator ma sam zdecydować w jaki sposób usunie dane. Ma on być dostosowany do sposobu i celu przetwarzania danych. To oznacza, że inaczej będzie wyglądać usuwanie danych znajdujących się w aktach w archiwum, a inaczej tych znajdujących się w chmurze. Prawdziwy problem pojawia się, z tego względu, że bardzo często nie ma możliwości dotarcia do wszystkich podmiotów, które przetworzyły dane, zwłaszcza ma to miejsce w Internecie, gdzie nie ma realnego wglądu do tego, kto pobrał, wykorzystał dane znajdujące się na stronach internetowych. Grupa, która przetworzyła dane jest wtedy nieznana i nieoznaczona. Jedynym rozwiązaniem

w takim przypadku pozostaje udostępnienie oświadczenia, na stronie, z której można było skopiować dane, że nie ma zgody na przetwarzanie danych, które były w tym miejscu zamieszczone. Jak widać w praktyce, bardzo trudno jest usunąć dane, które pojawiły się na stronach internetowych, w trybie online. Często zdarzają się sytuacje, że dane takie są nadal w obiegu mimo wycofanej zgody, co więcej nawet po śmierci wnioskodawcy one wciąż gdzieś mogą krążyć w Internecie. Pomimo tego, że administrator miał obowiązek niezwłocznie usunąć dane i przekazać to innym administratorom przetwarzającym dane, co przyczynia się do wniosku, że jest to prawo trudne do wyegzekwowania w rzeczywistości (Nasiadka 2023, s. 88-91).

W kolejnym przepisie rozporządzenia RODO również zawarto prawo kontrolne jednostki jakim jest ograniczenie przetwarzania danych osobowych. Jest to bardzo zbliżone prawo do poprzedniego jednak nie tak daleko idące w swoich skutkach. Ogranicza się ono do tego, że jednostka zgadza się, aby administrator nadal mógł przechowywać dane, ale żąda by nie dokonywał on już żadnych innych czynności na nich. Tak jak to było w poprzednim przypadku, nie ma określnej formy żądania, najważniejsze jest by administrator mógł zidentyfikować, że uprawniona do tego osoba, występuje z żądaniem. Najlepiej jednak jakby miało ono formę pisemną. Analogicznie prawo to również nie jest ograniczone czasowo, a administrator ma swobodę w doborze rozwiązania, ma je dopasować do sposobu w jaki dane były przetwarzane i celu w jaki je zebrano. Przykładowo, może ograniczyć dostęp podmiotów do strony internetowej z tymi danymi. Warunkować działania będzie też powód żądania jednostki. Jeśli uzna ona, że przetwarzanie danych jest niezgodne z prawem albo dane są nieprawidłowe, administrator powinien to poddać zbadaniu. Jeśli jednostka uzna, że jej dane nie są już potrzebne do wypełnienia celu to na administratorze spoczywa obowiązek skontrolowania tego. W całym procesie przetwarzania administrator musi kierować się zasadą celowości, czyli gromadzić tylko te dane, które są potrzebne do realizacji celu (Błażewski, Behr 2018, s. 160- 163).

Podsumowując, prawa takie jak: prawo do wyrażenia zgody na przetwarzanie danych, prawo jej wycofania, prawo dostępu do tych informacji, prawo do sprostowania, usunięcia czy przeniesienia danych lub prawo ograniczenia przetwarzania są środkami prawnymi ochrony danych o charakterze bezpośrednim. Należy pamiętać, że prawa te nie przysługują w każdej sytuacji, ponieważ przepisy prawa przewidują ograniczenia w ich zakresie. Szczególną uwagę na to muszą zwracać administratorzy w samorządach terytorialnych, ponieważ to oni najczęściej mają do czynienia z sprawami, gdzie dane prawo podlega wyłączeniu. Przykładowo,

prawo do usunięcia danych nie będzie mieć zastosowania w dziedzinie zdrowia publicznego ze względu na interes publiczny. Gdyby mimo to jednostka wyraziła swoje roszczenie, administrator jest zobowiązany do wydania pisma informacyjnego o braku podstaw do spełnienia go. Przyjmuję się, że administrator jest związany terminem nieprzekraczającym miesiąca od dnia otrzymania wniosku. Po upływie tego terminu, jednostka może złożyć skargę na bezczynność administratora do Prezesa Urzędu Ochrony Danych Osobowych. Wydanie pisma również można zaskarżyć do tego samego organu, odwołując się na błędne przeprowadzenie przez administratora postępowania wyjaśniającego. PUODO również w tym przypadku rozpatrywać będzie jako organ nadzorczy czy doszło do bezczynności administratora (Jabłoński, Sakowska- Baryła, Wygoda 2018, s. 144).

PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH (PUODO)

Z dniem wejścia w życie ustawy o ochronie danych osobowych przekształcono Biuro Generalnego Inspektora Ochrony Danych Osobowych w Urząd Ochrony Danych Osobowych, tym samym organem nadzorczym został Prezes Urzędu Ochrony Danych Osobowych. Ustawodawca, dokonał zmiany nazewnictwa, przede wszystkim by zapewnić przejrzystość prawa i terminologii. Rozporządzenie RODO wprowadziło do polskiego systemu prawnego nowy podmiot jakim jest inspektor ochrony danych, aby monitorował on przetwarzanie danych. Należy podkreślić, że nie jest to organ nadzorczy, tym bardziej nie można go utożsamiać z Generalnym Inspektorem czy pracownikami jego biura. Stąd by nie budzić wątpliwości i pozornej sprzeczności, dokonano przekształcenia. Dodatkowo wskazuję się, że oprócz podjęcia próby ujednolicenia prawa w Unii Europejskiej za pomocą rozporządzenia RODO, nowe regulacje wywarły również pozytywny skutek w postaci zwiększenia niezależności PUODO. Przykładem może być rozwinięcie katalogu zasad przeprowadzania przez niego kontroli przetwarzania danych czy umożliwienie dopuszczenia wszelkich środków dowodowych przy przeprowadzaniu kontroli. Należy podkreślić, że zostały wyróżnione 2 tryby wszczęcia kontroli przez PUODO (Szustakiewicz 2018, 807-808, 812-813). To do niego trafiają informację o wszelkich naruszeniach w ochronie danych, które zgłasza administrator (Kalina 2018, s. 35).

Za naruszenie danych zgodnie z definicją zawartą w art. 4 pkt 12 rozporządzenia RODO rozumie się: „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych

przesyłanych, przechowywanych lub w inny sposób przetwarzanych" (Kalina 2018, s. 35). Zgodnie z tą definicją naruszeniem może być sytuacja, w której urzędnik państwowy wysłał wiadomość elektroniczną zawierającą dane osób trzecich na inny adres pocztowy niż powinien (Litwiński 2022). Administrator ma obowiązek niezwłocznie, najlepiej w przeciągu 72h od zaistnienia incydentu zgłosić go. Z wyjątkiem sytuacji, w której po przeprowadzonej ocenie ryzyka stwierdzi, że naruszenie nie spowoduje ograniczeń praw czy wolności jednostki lub jest to tak mało prawdopodobne, że raczej niemożliwe (Kalina 2018, s. 35). Administrator nawet jeśli uzna, że do naruszenia nie doszło to powinien pozostawić namacalny ślad w postaci dokumentu, że rozpatrywał sprawę pod kątem możliwego naruszenia. Ma to go uchronić od odpowiedzialności za bezczynność, gdyby w toku późniejszej kontroli PUODO wyszło, że miało miejsce naruszenie (Litwiński 2022).

W związku z możliwością naruszeń przed każdym administratorem stoi zadanie opracowania i wprowadzenia w życie procedur na wypadek naruszeń, które będą zgodne z wytycznymi rozporządzenia RODO. Przede wszystkim powinien on prowadzić rzetelną dokumentację, w której zawarte będą informację o okolicznościach naruszeń, ich skutkach i środkach jakie zostały powzięte by do nich nie dopuścić lub im zapobiec (Kalina 2018, s. 35). Będzie to jednocześnie jeden z przejawów zasady rozliczalności, która dotyczy całego procesu przetwarzania danych i której podlega administrator. Polega ona na swobodzie w kreowaniu procedury jaką ma administrator, lecz musi być ona zgodna z przepisami prawnymi m.in. z zasadami przetwarzania danych. Udokumentowanie we właściwy sposób naruszeń jest idealnym przykładem przestrzegania prawa (Jabłoński, Sakowska-Baryła, Wygoda 2018, s. 33).

Administratorzy, poza tym że w sposób techniczny dbają o bazy, prowadzą wszelkiego rodzaju rejestry to powinni oni jeszcze poddawać testom środki jakie wprowadzili do ochrony baz. To do nich należy należyte przygotowanie sieci, urządzeń i pracowników na możliwe naruszenia (Skoczylas 2019, s. 48). Odpowiadają oni za szkolenie pracowników w zakresie ochrony danych np. za przeszkolenie, aby wiadomości do petentów były zaszyfrowane, z kluczem dostępu możliwe do otwarcia. Takim kluczem dostępu może być nr PESEL. Co więcej, gdy dojdzie do naruszenia administrator ma za zadanie poinformować także osoby, których dane zostały narażone, chyba że użył środki, które zabezpieczyły dane w taki sposób, aby nieuprawniony podmiot nie był w stanie odtworzyć informacji. Kolejnym wyjątkiem od tej zasady jest nieproporcjonalność nakładów m.in. finansowych w celu skutecznego poinformowania wszystkich jednostek, których

dane zostały narażone stąd administrator może wystosować ogólny komunikat. Każdy administrator powinien prowadzić rejestr naruszeń, który będzie w stanie udostępnić podczas kontroli (Litwiński 2022).

PUODO może kontrolować zarówno administratora danych, jak i podmiot przetwarzający dane. Jego kontrola może być planowa lub też doraźna w związku z pozyskanymi informacjami. Zgodnie z obowiązującymi przepisami prawa, przeprowadzenie kontroli może odbyć się bez uprzedniego zawiadomienia o potrzebie jej wszczęcia. Jednak w rzeczywistości ze względów praktycznych kilka dni przed kontrolą administrator danych, jak i podmiot przetwarzający dane są informowani, po to aby przygotowali potrzebne dokumenty, które będą sprawdzane. W tym przypadku kontrola ta jest niezwiązana z postępowaniem administracyjnym, ale jej rezultat może doprowadzić do wszczęcia tegoż postępowania (Litwiński 2022).

Wyróżniono też drugi tryb kontroli, gdy PUODO prowadzi postępowanie administracyjne, podczas którego wychodzą braki dowodowe, w tym celu zlecone zostaje wszczęcie kontroli. Istnieją szczegółowe regulacje dotyczące przeprowadzania kontroli, z czego najważniejsze z nich dotyczą zespołu kontrolnego. Składa się on zazwyczaj z 2/3 inspektorów, czyli pracowników urzędu, którzy mają stosowne upoważnienie od PUODO do przeprowadzenia kontroli w jego imieniu. Gdy zajdzie taka potrzeba w ich skład może wejść również podmiot niebędący pracownikiem urzędu, ale mający wymaganą wiedzę specjalistyczną akurat do tego przypadku kontroli. Pełni on rolę biegłego. Zespół ten kieruje się głównymi zasadami kontroli np. ma prawo wstępu do miejsc kontrolowanych wyłącznie w godzinach 6.00-22.00, ale także związani są upoważnieniem, które w sposób szczegółowy określa ich obowiązki. Przede wszystkim kontrola powinna rozpocząć się od przedstawienia sprawdzanemu podmiotowi należytego upoważnienia oraz legitymacji, a zakończyć protokołem. Co ciekawe, podmiot sprawdzany nie może zakwestionować zgodności działań zespołu kontrolnego z prawem, bezpośrednio w trakcie trwania kontroli, a może to ująć w uwagach do protokołu lub ewentualnie wnieść, któryś z środków odwoławczych przysługujących na rozstrzygnięcie PUODO. Złożenie zastrzeżeń przez podmiot sprawdzany przed podpisaniem protokołu może skutkować ponownym sprawdzeniem stanu faktycznego. W konsekwencji PUODO może utrzymać swoje stanowisko lub zmienić je, co doprowadzi do dołączenia aneksu do protokołu pokontrolnego. Istnieją 2 możliwości rozstrzygnięcia: w razie braku zastrzeżeń postępowanie będzie kończyć protokół. Gdyby jednak zostały wykryte naruszenia, PUODO wszczyna postępowanie administracyjne w tym zakresie (Kowalik 2018, s.40).

Ma on prawo nakładania kar administracyjnych w formie decyzji administracyjnej na administratorów i podmioty przetwarzające m.in. za brak poinformowania PUODO lub osób, których dane zostały narażone (Litwiński 2022). Należy pamiętać, że to na administratorze danych spoczywa ciężar dowodowy, to on ma wykazać, że należycie wykonywał swoje obowiązki poprzez wdrażanie odpowiednich środków zabezpieczających, we właściwy sposób prowadził system, sprawdzał jego skuteczność i zapewnił poufność dostępność i integralność systemów oraz usług przetwarzania. Przewidziano, że maksymalna kara administracyjna dla organów publicznych będzie niższa niż ta przeznaczona dla podmiotów prywatnych, przedsiębiorców. Jej górna granica dla administracji publicznej wynosi 100000zł (Prasal, Perłakowska, Abgarowicz 2023).

BIBLIOGRAFIA

Akty prawne

Traktat Ustanawiający Europejską Wspólnotę Gospodarczą (Dz. U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.).

Karta praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 z późn. zm.).

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2024 r. poz. 572).

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

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

Monografie

Błażewski M., Behr J.
2018 Środki prawne ochrony danych osobowych, Wrocław.

Litwiński P.
2022 Ochrona danych osobowych w sektorze publicznym, Warszawa.

Mostowik M.
2022 Ochrona danych osobowych w Internecie rzeczy w prawie UE, Warszawa.

Prasal A., Perłakowska E., Abgarowicz G.
2023 Procedury elektronicznego zarządzania dokumentacją w administracji, Warszawa.

Czasopisma

Kalina P.
2018 Dokumentacja ochrony danych osobowych w RODO, „Informacja w administracji publicznej", nr 3.

Kowalik P.
2018 Kontrola Prezesa Urzędu Ochrony Danych Osobowych- schemat postępowania, „Informacja w administracji publicznej", nr 3.

Nasiadka Ł.
2023 Prawo do bycia zapomnianym w perspektywie przetwarzania danych osobowych, „Studia Prawa Publicznego", nr 2.

Nosarzewski Ł.
2023 Ochrona danych osobowych w informacji publicznej, ,,Przegląd Prawa Publicznego", nr 6

Skoczylas M.
2019 Obowiązki organów administracji publicznej w zakresie przetwarzania danych w systemach zinformatyzowanych przed i po wejściu w życie RODO i nowelizacji ustawy o ochronie danych osobowych, „Młody Jurysta 2019/1".

Szustakiewicz P.
2018 Pozycja prawna Prezesa Urzędu Ochrony Danych Osobowych, „Kontrola państwowa".

Żmuda-Matan K.
2023 Zasady powierzania samorządowej jednostce obsługującej zadań związanych z ochroną danych osobowych, „Roczniki Administracji i Prawa XXIII".

PUBLIC LAW MEASURES USED IN PUBLIC ADMINISTRATION FOR THE PROTECTION OF PERSONAL DATA

Abstract: This work aims to show how important and still relevant the problem of effective personal data protection is. For this reason, the instruments and public-legal mechanisms undertaken in the public administration to meet the obligations under the General Data Regulation, the Law on Personal Data Protection or other legal acts are discussed. Attention was drawn to the constant need for amending and detailing legal regulations related to the constant development of electronics and the emergence of so-called e-government. The issue of observance of the principle of legalism by state administration bodies was raised. Strengthening the protection of personal data by introducing a reform transforming the Office of the Inspector General for Personal Data Protection into the Office for Personal Data Protection was emphasized. Consequently, the role of this supervisory authority was increased, along with granting it greater independence. Finally, it was pointed out that violations of personal data protection are not only punishable by criminal liability, but may also be subject to administrative fines.

Key words: personal data protection, public administration, GDPR, e-administration, administrative liability

mgr **DOMINIKA FILIPEK**

AKADEMIA LEONA KOŹMIŃSKIEGO W WARSZAWIE

DYLEMATY PRAWNE NA STYKU JAWNOŚCI ŻYCIA PUBLICZNEGO I PRYWATNOŚCI. STUDIA PRZYPADKÓW UDOSTĘPNIANIA INFORMACJI PUBLICZNEJ A OCHRONA DANYCH OSOBOWYCH

Streszczenie: Rozdział analizuje złożone zagadnienie konfliktu między transparentnością życia publicznego a ochroną prywatności w kontekście udostępniania informacji publicznej. W pierwszym podrozdziale omówiono fundamentalne napięcie między tymi dwoma wartościami, podkreślając ich znaczenie dla demokratycznego państwa prawa oraz wyzwania związane z ich równoważeniem. Analiza prawna w drugim podrozdziale skupia się na interpretacji przepisów o dostępie do informacji publicznej w świetle RODO, wskazując na kluczowe aspekty, takie jak podstawa prawna przetwarzania danych, zasada minimalizacji czy obowiązki informacyjne. Trzeci podrozdział prezentuje studia przypadków, ilustrując konkretne sytuacje, w których doszło do konfliktu między jawnością a prywatnością, wraz z analizą rozstrzygnięć sądowych. Rozdział podkreśla konieczność indywidualnego podejścia do każdego przypadku, stosowania zasady proporcjonalności oraz ciągłego dostosowywania interpretacji przepisów do zmieniających się realiów społecznych i technologicznych. Wnioski wskazują na potrzebę wypracowania spójnych procedur przez organy administracji publicznej oraz śledzenia rozwoju orzecznictwa w tej dziedzinie.

Słowa kluczowe: informacja publiczna, dane osobowe, transparentność administracji publicznej

1. WPROWADZENIE

W dobie społeczeństwa informacyjnego i rosnącego znaczenia transparentności działań władzy publicznej, kwestia równoważenia prawa do informacji publicznej z prawem do prywatności nabiera szczególnego znaczenia. Niniejszy rozdział ma na celu dogłębną analizę tego złożonego problemu, uwzględniając zarówno aspekty teoretycznoprawne, jak i praktyczne implikacje wynikające z orzecznictwa sądów administracyjnych oraz stanowisk organów ochrony danych osobowych.

Fundamentalne znaczenie dla omawianej problematyki ma art. 61 Konstytucji Rzeczypospolitej Polskiej, który stanowi podstawę prawa do informacji publicznej, oraz art. 47, gwarantujący prawo do ochrony życia prywatnego. Te dwie normy konstytucyjne, choć równorzędne w hierarchii źródeł prawa, często wchodzą ze sobą w kolizję, co wymaga każdorazowego wyważenia konkurujących wartości. Ustawodawca, dążąc do realizacji obu tych praw, uchwalił ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2022 r., poz. 902 ze zm., dalej jako: „ustawa o dostępie do informacji publicznej" lub „u.d.i.p."), która stanowi kluczowy akt prawny regulujący zasady i tryb udostępniania informacji o sprawach publicznych.

Jednakże, wraz z wejściem w życie 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), problematyka ta zyskała nowy wymiar. RODO wprowadziło szereg nowych obowiązków i zasad przetwarzania danych osobowych, które muszą być uwzględniane przy udostępnianiu informacji publicznej (Barta i Litwiński 2016, s. 78-79). Szczególne znaczenie ma w tym kontekście art. 86 RODO, który odnosi się do kwestii pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych.

W niniejszym artykule podjęto próbę kompleksowej analizy prawnej tego zagadnienia, uwzględniając zarówno przepisy prawa krajowego, jak i unijnego. Analiza ta obejmuje szeroki zakres aspektów prawnych, od interpretacji przepisów konstytucyjnych po szczegółowe regulacje RODO. Ponadto, rozdział zgłębia praktyczne implikacje tych przepisów, prezentując studia przypadków i analizując orzecznictwo sądów administracyjnych. Rozważania te mają na celu nie tylko przedstawienie aktualnego stanu prawnego, ale także wskazanie potencjalnych kierunków rozwoju tej dziedziny prawa.

Celem rozdziału jest nie tylko przedstawienie aktualnego stanu prawnego i orzecznictwa, ale także wskazanie kierunków rozwoju tej problematyki oraz potencjalnych obszarów wymagających interwencji ustawodawcy. Szczególna uwaga zostanie poświęcona zasadzie proporcjonalności oraz konieczności indywidualnego podejścia do każdego przypadku.

Rozdział uwzględnia stan prawny obowiązujący w dniu 1 lutego 2025 r.

2. KONFLIKT WARTOŚCI: TRANSPARENTNOŚĆ ŻYCIA PUBLICZNEGO A PRAWO DO PRYWATNOŚCI

W demokratycznym państwie prawa fundamentalne znaczenie mają dwie, często pozostające ze sobą w konflikcie wartości: transparentność życia publicznego oraz prawo do prywatności. Z jednej strony, jawność działań władzy publicznej i dostęp do informacji publicznej stanowią filary społeczeństwa obywatelskiego i mechanizm kontroli nad władzą (Fajgielski 2021, s. 54). Z drugiej strony, prawo do prywatności jest jednym z podstawowych praw człowieka, chroniącym sferę życia prywatnego jednostki przed nieuprawnionym dostępem osób trzecich, w tym również instytucji państwowych.

Transparentność życia publicznego wynika z zasady jawności działania organów władzy publicznej, która jest fundamentem demokratycznego państwa prawa. W polskim porządku prawnym zasada ta znajduje swoje umocowanie w art. 61 Konstytucji RP, który stanowi, że obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa (Barta i Markiewicz 1999, s. 134-135).

Uszczegółowieniem konstytucyjnej zasady jawności jest ustawa o dostępie do informacji publicznej. Zgodnie z art. 1 ust. 1 tej ustawy, każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w tej ustawie. Prawo do informacji publicznej obejmuje uprawnienia do uzyskania informacji publicznej,

w tym uzyskania informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego, wglądu do dokumentów urzędowych, oraz dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów.

Z kolei prawo do prywatności, choć nie zostało wprost wyrażone w Konstytucji RP, wywodzi się z art. 47, który stanowi, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Prawo to jest również chronione przez art. 8 Europejskiej Konwencji Praw Człowieka oraz art. 7 Karty Praw Podstawowych Unii Europejskiej.

W polskim systemie prawnym ochrona prywatności realizowana jest m.in. poprzez przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781 ze zm.) oraz 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).

Konflikt między transparentnością życia publicznego a prawem do prywatności uwidacznia się szczególnie w sytuacjach, gdy udostępnienie informacji publicznej wiąże się z ujawnieniem danych osobowych lub innych informacji dotyczących sfery prywatnej osób fizycznych (Fajgielski 2019, s. 34-36). Problem ten dotyczy zwłaszcza osób pełniących funkcje publiczne, których działalność z jednej strony podlega szerszej kontroli społecznej, z drugiej zaś - które również korzystają z ochrony prawa do prywatności.

W orzecznictwie sądów polskich oraz Trybunału Konstytucyjnego wielokrotnie podkreślano, że prawo do prywatności osób pełniących funkcje publiczne podlega silniejszym ograniczeniom niż w przypadku osób prywatnych (Sagan-Jeżowska 2018, s. 23-24). Wynika to z faktu, że osoby te, decydując się na udział w życiu publicznym, muszą liczyć się z większym zainteresowaniem opinii publicznej ich działalnością. Jednakże, nawet w przypadku osób publicznych, ingerencja w sferę prywatności musi być proporcjonalna i uzasadniona interesem publicznym. W praktyce oznacza to konieczność każdorazowego wyważenia między prawem do informacji publicznej a prawem do prywatności (Litwiński 2009, s. 53-55). Organy administracji publicznej, sądy oraz inne podmioty zobowiązane do udostępniania informacji publicznej muszą dokonywać skrupulatnej analizy, czy w konkretnym przypadku interes publiczny związany z jawnością przeważa nad prawem do prywatności.

Warto zauważyć, że ustawa o dostępie do informacji publicznej przewiduje mechanizmy mające na celu ochronę prywatności w procesie udostępniania informacji publicznej. Art. 5 ust. 2 ww. ustawy stanowi, że: prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy jednak informacji

o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

W kontekście ochrony danych osobowych, kluczowe znaczenie ma art. 86 RODO, który stanowi, że dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia.

Rozstrzyganie konfliktu między transparentnością życia publicznego a prawem do prywatności wymaga zatem każdorazowej, indywidualnej oceny okoliczności konkretnej sprawy. Organy stosujące prawo muszą brać pod uwagę takie czynniki jak: charakter informacji, której dotyczy wniosek o udostępnienie, status osoby, której dane mają zostać ujawnione, związek między żądanymi informacjami a pełnioną funkcją publiczną, a także potencjalne skutki ujawnienia informacji zarówno dla interesu publicznego, jak i dla prywatności osoby, której dane dotyczą (Grzelak 2019, s. 68-69).

W praktyce orzeczniczej wykształciły się pewne ogólne zasady dotyczące rozstrzygania tego konfliktu. Na przykład, w odniesieniu do wynagrodzeń osób pełniących funkcje publiczne, sądy administracyjne co do zasady uznają, że informacje te podlegają udostępnieniu jako informacja publiczna. Naczelny Sąd Administracyjny (dalej również jako: „NSA") w wyroku z dnia 18 lutego 2015 r. (sygn. I OSK 695/14) stwierdził, że:

> „(…) informacja o wysokości zarobków osoby zatrudnionej przez podmiot publiczny (…), stanowi informację publiczną w rozumieniu art. 1 ust. 1 u.d.i.p. (…) Udzielenie informacji publicznej w postaci danych o wysokości wynagrodzenia osób zatrudnionych w jednostkach finansowanych ze środków publicznych (zarówno pełniących funkcje publiczne, jak też personelu pomocniczego) zazwyczaj nie musi się wiązać z koniecznością ingerencji w ich prawnie chronioną sferę prywatności. Dzieje się tak przede wszystkim wówczas, gdy w danym podmiocie na określonym stanowisku zatrudnionych jest kilka osób. Udostępnienie informacji publicznej polega bowiem na ujawnieniu wysokości wynagrodzenia wypłacanego na określonym stanowisku, bez wskazywania danych osobowych konkretnej osoby".

Z drugiej strony, w odniesieniu do danych osobowych zwykłych pracowników, którzy nie pełnią funkcji publicznych, sądy są bardziej skłonne do

przyznawania priorytetu ochronie prywatności. W wyroku z dnia 25 kwietnia 2014 r. (sygn. I OSK 2499/13) NSA uznał, że:

> „Umowy o dzieło zawierane przez Szefa Kancelarii Prezydenta RP z ekspertami prezentującymi swoje opinie w przedmiocie ewentualnych zmian legislacyjnych związanych z systemem ubezpieczeń społecznych nie czyniły z autorów tych opinii osób pełniących funkcje publiczne, gdyż osoby te we wskazanym zakresie nie tylko nie działały w ramach instytucji publicznej, lecz i ponad wszelką wątpliwość nie przysługiwał im z tytułu przygotowania opinii jakikolwiek zakres kompetencji decyzyjnej (zwłaszcza w ramach instytucji publicznej). Przygotowanie opinii eksperckiej stanowi pewien rodzaj usługi polegającej na zaprezentowaniu określonego poglądu na bazie posiadanej wiedzy, umiejętności czy autorytetu w celu umożliwienia podmiotowi korzystającemu z opinii uwzględnienia w swoim procesie decyzyjnym jak największego spektrum okoliczności i uwarunkowań związanych z określona tematyką - w tym przypadku z problematyką regulacji prawnej systemu ubezpieczeń społecznych. Kompetencja decyzyjna nie leży jednak po stronie autorów opinii. Tym bardziej samo zawarcie umowy o dzieło nie wyposaża tych osób w jakiekolwiek kompetencje decyzyjne."

3. ANALIZA PRAWNA UDOSTĘPNIANIA INFORMACJI PUBLICZNEJ W KONTEKŚCIE RODO

Udostępnianie informacji publicznej w świetle przepisów o ochronie danych osobowych, w szczególności 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), stanowi złożone zagadnienie prawne, wymagające każdorazowej analizy konkretnego przypadku.

Podstawowym aktem prawnym regulującym kwestie dostępu do informacji publicznej w Polsce jest ustawa o dostępie do informacji publicznej. Zgodnie z wcześniej przywołanym art. 1 ust. 1 u.d.i.p., każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w tej ustawie. Jednakże, prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych (art. 5 ust. 1 u.d.i.p.).

W kontekście ochrony danych osobowych, kluczowe znaczenie ma art. 5 ust. 2 u.d.i.p., który stanowi, że prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia

i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

RODO, jako akt prawa unijnego bezpośrednio stosowany w państwach członkowskich, wprowadza szereg zasad i obowiązków związanych z przetwarzaniem danych osobowych. Zgodnie z art. 4 pkt 1 RODO, dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (Kamińska i Rozbicka-Ostrowska 2021, s. 142-143). W kontekście udostępniania informacji publicznej, kluczowe znaczenie ma wcześniej przywołany art. 86 RODO, który stanowi, że dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia.

Analizując relację między u.d.i.p. a RODO, należy zwrócić uwagę na kilka kluczowych aspektów:

1. Podstawa prawna przetwarzania danych osobowych: udostępnianie informacji publicznej zawierającej dane osobowe stanowi formę przetwarzania danych w rozumieniu RODO. Zgodnie z art. 6 ust. 1 lit. c RODO, przetwarzanie jest zgodne z prawem, jeżeli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. W tym przypadku, obowiązek ten wynika z u.d.i.p.
2. Zasada minimalizacji danych: zgodnie z art. 5 ust. 1 lit. c RODO, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. W kontekście udostępniania informacji publicznej oznacza to, że organy powinny udostępniać tylko te dane osobowe, które są niezbędne do realizacji celu, jakim jest zapewnienie transparentności działań władzy publicznej.
3. Prawa osób, których dane dotyczą: RODO przyznaje osobom, których dane dotyczą, szereg praw, w tym prawo dostępu do danych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania. W kontekście udostępniania informacji publicznej, realizacja tych praw może być ograniczona ze względu na nadrzędny interes publiczny.
4. Obowiązki informacyjne: zgodnie z art. 13 i 14 RODO, administrator danych ma obowiązek poinformowania osoby, której dane dotyczą, o przetwarzaniu jej danych osobowych.

5. W przypadku udostępniania informacji publicznej, realizacja tego obowiązku może być utrudniona, szczególnie gdy dane są pozyskiwane z innych źródeł niż osoba, której dotyczą.
6. Zasada przejrzystości: art. 5 ust. 1 lit. a RODO wymaga, aby dane osobowe były przetwarzane zgodnie z zasadą przejrzystości. W kontekście udostępniania informacji publicznej oznacza to, że organy powinny informować osoby, których dane są udostępniane, o fakcie i zakresie udostępnienia, chyba że jest to niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.
7. Anonimizacja: w celu pogodzenia wymogów RODO z obowiązkiem udostępniania informacji publicznej, organy mogą stosować techniki anonimizacji danych osobowych.
8. Odpowiedzialność administratora: zgodnie z art. 5 ust. 2 RODO, administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie. W kontekście udostępniania informacji publicznej oznacza to, że organy muszą być w stanie uzasadnić decyzję o udostępnieniu lub odmowie udostępnienia danych osobowych.
9. Ocena skutków dla ochrony danych: w przypadku, gdy udostępnienie informacji publicznej zawierającej dane osobowe może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator powinien przeprowadzić ocenę skutków dla ochrony danych zgodnie z art. 35 RODO.
10. Współadministrowanie danymi: w sytuacji, gdy w proces udostępniania informacji publicznej zaangażowanych jest kilka podmiotów, może dojść do współadministrowania danymi w rozumieniu art. 26 RODO. W takim przypadku podmioty te powinny w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności.
11. Przekazywanie danych do państw trzecich: w przypadku, gdy udostępnienie informacji publicznej wiąże się z przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej, należy uwzględnić przepisy rozdziału V RODO.

Podsumowując powyższe, analiza prawna udostępniania informacji publicznej w kontekście RODO wymaga każdorazowego wyważenia interesu publicznego związanego z jawnością działań władzy publicznej oraz prawa do ochrony danych osobowych (Sagan-Jeżowska 2018, s. 114-116). Organy zobowiązane do

udostępniania informacji publicznej muszą stosować przepisy RODO w sposób, który nie będzie prowadził do nadmiernego ograniczenia prawa do informacji, jednocześnie zapewniając odpowiedni poziom ochrony danych osobowych. Kluczowe znaczenie ma tutaj zasada proporcjonalności oraz indywidualna ocena każdego przypadku (Sitniewski 2021, s. 86-87).

W praktyce, organy administracji publicznej powinny wypracować wewnętrzne procedury uwzględniające wymogi zarówno u.d.i.p., jak i RODO. Procedury te powinny obejmować m.in. zasady oceny, czy dana informacja stanowi informację publiczną, metody anonimizacji danych osobowych, sposoby realizacji obowiązków informacyjnych wobec osób, których dane są udostępniane, oraz zasady dokumentowania procesu decyzyjnego związanego z udostępnianiem lub odmową udostępnienia informacji publicznej zawierającej dane osobowe (Wyka i Mielczarek 2019, s. 130-133).

Warto również zaznaczyć, że orzecznictwo sądów administracyjnych oraz stanowiska organów nadzorczych ds. ochrony danych osobowych będą odgrywać istotną rolę w kształtowaniu praktyki stosowania przepisów o dostępie do informacji publicznej w kontekście RODO.

4. STUDIA PRZYPADKÓW: KONTROWERSYJNE SYTUACJE NA STYKU JAWNOŚCI I PRYWATNOŚCI

W praktyce stosowania prawa dostępu do informacji publicznej oraz ochrony danych osobowych często dochodzi do sytuacji, w których te dwie wartości wchodzą ze sobą w konflikt. Analiza konkretnych przypadków pozwala na lepsze zrozumienie złożoności tego zagadnienia oraz wskazanie kierunków interpretacji przepisów prawa w tym zakresie.

Jednym z przypadków, który poruszył temat granic jawności życia publicznego i prawa do prywatności, była sprawa dotycząca udostępnienia informacji o nagrodach i premiach wypłaconych pracownikom urzędu jednostki samorządy terytorialnego. W wyroku z dnia 8 lipca 2015 r. (sygn. I OSK 1530/14) NSA uznał, że:

> „ (…) za osobę pełniącą funkcję publiczną należy uznać każdego, kto pełni funkcję w organach władzy publicznej lub też w strukturach osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej, jeżeli tylko funkcja ta ma związek z dysponowaniem majątkiem państwowym lub samorządowym albo zarządzaniem sprawami związanymi z wykonywaniem swych zadań przez władze publiczne, a także inne podmioty, które tę władzę realizują lub gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. (…) Godzi się zauważyć, że

> przesądzenie, iż dana osoba pełni funkcję publiczną w rozumieniu art. 5 ust. 2 u.d.i.p. nie oznacza jednak jeszcze, że żądana informacja może zostać udostępniona wnioskodawcy z wyłączeniem ochrony prywatności tej osoby. Należy bowiem podkreślić, że stosownie do art. 5 ust. 2 u.d.i.p., dla ograniczenia prawa do prywatności konieczne jest także, aby żądana informacja o osobie pełniącej funkcję publiczną miała związek z pełnieniem tej funkcji publicznej. Innymi słowy, musi istnieć adekwatny związek między informacją odnoszącą się do danej osoby a funkcjonowaniem tej osoby w sferze publicznej".

Ciekawym przypadkiem była również sprawa dotycząca obowiązku noszenia przez personel medyczny identyfikatorów a ochrona danych osobowych. W wyroku z dnia 5 kwietnia 2013 r. (sygn. I OSK 192/13) NSA stwierdził, że:

> „Podobna sytuacja zachodzi w razie odmowy udostępnienia informacji publicznej z uwagi na potrzebę ochrony danych osobowych. Ocena takiej odmowy musi bazować na tym, co znajduje się w ofertach objętych wnioskiem o ich udostępnienie. Zaznaczyć przy tym trzeba, iż sam obowiązek noszenia przez personel medyczny identyfikatorów (m.in. z imieniem i nazwiskiem) w siedzibie jednostki udzielającej świadczeń medycznych, który wynika z art. 36 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (tekst jedn.: Dz. U. z 2013 r. poz. 217), nie oznacza, iż z tej przyczyny wyłączona jest ochrona danych osobowych tych osób".

W dalszej kolejności, w sądownictwie pojawiało się często zagadnienie dysponowania majątkiem publicznym. W wyroku z dnia 11 września 2012 r. (sygn. I OSK 903/12) NSA uznał, że:

> „Majątek, którym dysponuje Sąd Najwyższy, jest majątkiem publicznym i sposób dysponowania tym majątkiem jest informacją publiczną co wynika zarówno z art. 6 ust. 2 lit. f ustawy jak i art. 1 ust. 1 ustawy. Zgodnie z orzecznictwem sądów administracyjnych informacja może dotyczyć sprawy publicznej, nie tylko wtedy, gdy została wytworzona przez podmioty wskazane w art. 4 ust. 1 ustawy, ale również wtedy, gdy odnosi się do nich w zakresie wykonywanych przez nie zadań publicznych i gospodarowania majątkiem publicznym. Dlatego informacją publiczną jest też treść umów cywilnoprawnych dotyczących majątku publicznego".

Analizując powyższe przypadki, można zauważyć, że sądy administracyjne w swoich orzeczeniach starają się wypracować pewne ogólne zasady rozstrzygania konfliktu między jawnością życia publicznego a ochroną prywatności (Litwiński 2009, s. 45-48).

Do kluczowych kryteriów branych pod uwagę należą:

1. Status osoby, której dotyczą informacje - osoby pełniące funkcje publiczne muszą liczyć się z większym zakresem ingerencji w ich prywatność.

2. Związek informacji z pełnioną funkcją publiczną - udostępnieniu podlegają informacje mające bezpośredni związek z wykonywaniem zadań publicznych.
3. Interes publiczny - ocena, czy udostępnienie informacji służy realizacji ważnego interesu społecznego.
4. Proporcjonalność ingerencji - rozważenie, czy udostępnienie informacji nie stanowi nadmiernej ingerencji w prywatność jednostki w stosunku do celu, jakim jest zapewnienie transparentności życia publicznego.

Podsumowując, studia przypadków kontrowersyjnych sytuacji na styku jawności i prywatności pokazuje, że rozstrzyganie tego konfliktu wymaga każdorazowo wnikliwej analizy okoliczności konkretnej sprawy. Orzecznictwo sądów administracyjnych, choć stara się wypracować pewne ogólne zasady, nie daje jednoznacznych i uniwersalnych rozwiązań. Jednocześnie, analiza tych przypadków pozwala na lepsze zrozumienie złożoności problematyki dostępu do informacji publicznej i ochrony danych osobowych, co może być pomocne zarówno dla organów stosujących prawo, jak i dla obywateli korzystających z prawa do informacji.

6. PODSUMOWANIE

Podsumowując rozważania zawarte w artykule, należy podkreślić, że kwestia równoważenia prawa do informacji publicznej z prawem do ochrony prywatności stanowi jedno z kluczowych wyzwań współczesnego prawa administracyjnego i konstytucyjnego. Analiza przepisów prawnych, orzecznictwa sądów administracyjnych oraz praktyki organów administracji publicznej wskazuje na złożoność tego zagadnienia i potrzebę ciągłego dostosowywania regulacji prawnych do zmieniających się realiów społecznych i technologicznych.

W świetle przeprowadzonych badań, można sformułować szereg postulatów mających na celu optymalizację systemu prawnego w zakresie udostępniania informacji publicznej przy jednoczesnym poszanowaniu prawa do prywatności.

W szczególności, *de lege ferenda* należy rozważyć wprowadzenie do ustawy o dostępie do informacji publicznej szczegółowych przepisów regulujących proces ważenia interesu publicznego związanego z jawnością życia publicznego oraz prawa do prywatności. Przepisy te powinny zawierać katalog kryteriów, które organy zobowiązane do udostępnienia informacji publicznej muszą brać pod uwagę przy podejmowaniu decyzji o udostępnieniu lub odmowie udostępnienia informacji zawierającej dane osobowe. Oprócz powyższego, wskazane jest ustawowe

uregulowanie kwestii anonimizacji danych osobowych w procesie udostępniania informacji publicznej. Regulacja ta powinna określać standardy i metody anonimizacji, uwzględniające najnowsze osiągnięcia technologiczne w zakresie ochrony danych osobowych. *De lege ferenda* warto rozważyć wprowadzenie do ustawy o dostępie do informacji publicznej przepisów regulujących kwestię tzw. nadużycia prawa do informacji publicznej, w tym mechanizmów pozwalających na odrzucenie wniosków, które w sposób oczywisty nie służą realizacji prawa do informacji, lecz mają na celu np. paraliżowanie pracy urzędu.

De sententia ferenda sądy administracyjne powinny w swoim orzecznictwie w większym stopniu uwzględniać specyfikę ochrony danych osobowych wynikającą z RODO. W szczególności, orzecznictwo powinno precyzyjniej odnosić się do takich kwestii jak zasada minimalizacji danych, ocena ryzyka naruszenia praw i wolności osób fizycznych czy obowiązki informacyjne administratorów danych. Wskazane jest również wypracowanie w orzecznictwie bardziej szczegółowych kryteriów oceny, kiedy ingerencja w prywatność osób pełniących funkcje publiczne jest uzasadniona interesem publicznym. Kryteria te powinny uwzględniać różnorodność funkcji publicznych i związany z nimi zakres odpowiedzialności. Oprócz powyższego, *de sententia ferenda* wskazane jest, aby orzecznictwo w większym stopniu uwzględniało kontekst społeczny i etyczny udostępniania informacji publicznej, w tym potencjalne konsekwencje ujawnienia określonych informacji dla osób, których dane dotyczą.

Przedstawione postulaty *de lege ferenda i de sententia ferenda* mają na celu optymalizację systemu prawnego w zakresie udostępniania informacji publicznej przy jednoczesnym poszanowaniu prawa do prywatności. Ich realizacja wymaga jednak szerokiej dyskusji z udziałem przedstawicieli doktryny, praktyki oraz organizacji społecznych. Tylko kompleksowe podejście, uwzględniające zarówno aspekty prawne, jak i etyczne oraz społeczne, pozwoli na wypracowanie rozwiązań, które będą skutecznie chronić zarówno prawo do informacji publicznej, jak i prawo do prywatności, stanowiąc tym samym fundament dla transparentnego i jednocześnie respektującego prawa jednostki funkcjonowania demokratycznego państwa prawa.

BIBLIOGRAFIA

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 r., poz. 483).

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

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.

Orzecznictwo

Wyrok Naczelnego Sądu Administracyjnego z dnia 8 lipca 2015 r., I OSK 1530/14, LEX nr 1794746.

Wyrok Naczelnego Sądu Administracyjnego z dnia 18 lutego 2015 r., I OSK 695/14, LEX nr 1657860.

Wyrok Naczelnego Sądu Administracyjnego z dnia 25 kwietnia 2014 r., I OSK 2499/13, LEX nr 1463584.

Wyrok Naczelnego Sądu Administracyjnego z dnia 5 kwietnia 2013 r., I OSK 192/13, LEX nr 1336339.

Wyrok Naczelnego Sądu Administracyjnego z dnia 11 września 2012 r., I OSK 903/12, LEX nr 1394106.

Literatura

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

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

Fajgielski P.
2021 Ochrona danych osobowych w administracji publicznej, Warszawa.
2019 Prawo ochrony danych osobowych. Zarys wykładu, Warszawa.

Grzelak A.
2019 Ochrona danych osobowych w sądach i prokuraturze, Warszawa.

Kamińska I., Rozbicka-Ostrowska M.
2021 Ochrona danych osobowych a prawo do informacji publicznej, Warszawa.

Litwiński P.
2009 Ochrona danych osobowych w ogólnym postępowaniu administracyjnym, Warszawa.

Sagan-Jeżowska A.
2018 Klauzule RODO, Wzory klauzul z praktycznym komentarzem, Warszawa.

Sitniewski P.
2021 Udzielanie informacji publicznej przez sądy powszechne. Poradnik z wzorami pism, Warszawa.

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

LEGAL DILEMMAS AT THE INTERSECTION OF PUBLIC LIFE TRANSPARENCY AND PRIVACY. CASE STUDIES OF PUBLIC INFORMATION DISCLOSURE VERSUS PERSONAL DATA PROTECTION

Abstract: The chapter analyzes the complex issue of conflict between public life transparency and privacy protection in the context of public information disclosure. The first subchapter discusses the fundamental tension between these two values, emphasizing their importance for a democratic state governed by the rule of law and the challenges associated with balancing them. The legal analysis in the second subchapter focuses on interpreting public information access regulations in light of GDPR, pointing out key aspects such as the legal basis for data processing, the principle of data minimization, and information obligations. The third subchapter presents case studies, illustrating specific situations where conflicts between transparency and privacy occurred, along with an analysis of court decisions. The chapter emphasizes the need for an individual approach to each case, applying the principle of proportionality, and continuously adapting the interpretation of regulations to changing social and technological realities. The conclusions indicate the need to develop coherent procedures by public administration bodies and to monitor the development of case law in this field.

Keywords: public information, personal data, transparency of public administration

MICHAŁ POCZWARDOWSKI

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

ORCID: 0009-0009-4058-4489

OCHRONA DANYCH OSOBOWYCH A ARCHIWA PAŃSTWOWE - ZAGADNIENIA WYBRANE

Streszczenie: Rozdział przedstawia wybrane zagrożenia dotyczące ochrony danych osobowych w toku działalności archiwów państwowych. Opracowanie obejmuje swoistą część ogólną, poświęconą podstawowym normom prawnym regulującym działalność sieci archiwalnej i specyfikę prawa ochrony danych osobowych odnoszącą się do działalności archiwów. Dalsza część obejmuje wybrane zagadnienia szczegółowe. W jej ramach przedstawione zostały potencjalne ryzyka naruszenia przepisów odnoszących się do ochrony danych osobowych w kontekście udostępniania akt metrykalnych oraz kopert dowodowych.

Słowa kluczowe: rodo, archiwum państwowe, koperty dowodowe, usc, akta stanu cywilnego.

1. WPROWADZENIE

Ochrona danych osobowych zajmuje co do zasady drugorzędne miejsce w zakresie działalności prowadzonej przez archiwa państwowe. Wynika to z faktu, iż z reguły zajmują się one gromadzeniem, przetwarzaniem i udostępnianiem dokumentacji obejmującej dane osób zmarłych, a tym samym stawiają się poza zakresem działania regulacji prawa ochrony danych osobowych. Istnieje jednak kilka obszarów działalności archiwów, w ramach których dochodzi do przetwarzania danych osób wciąż żyjących, a które cechują się specyfiką niespotykaną w ramach działalności innych instytucji publicznych i prywatnych. W związku

z tym powstaje potencjalne ryzyko naruszenia przepisów zapewniających ochronę danych osobowych, a przez to należy rozważyć katalog środków temu zapobiegających z uwzględnieniem specyfiki działalności archiwów państwowych. W ramach dalszych rozważań przedstawione zostały dwa wybrane zagadnienia tj. ochrona danych osobowych w odniesieniu do aktów stanu cywilnego i aktów zbiorowych ich rejestracji, a także kopert dowodowych.

2. ZARYS DZIAŁALNOŚCI ARCHIWÓW PAŃSTWOWYCH

Archiwa państwowe są państwowymi jednostkami budżetowymi, podlegającymi nadzorowi Naczelnego Dyrektora Archiwów Państwowych. Zostały one powołane przede wszystkim do prowadzenia działalności archiwalnej w zakresie państwowego zasobu archiwalnego, przy czym nie są one jedynymi podmiotami do tego uprawnionymi. Zakres przewidzianej przez ustawodawcę działalności archiwalnej został umieszczony w art. 28 Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2020 r. poz. 164 z późn. zm.; dalej: u.n.z.a.). Należy również dodać, iż jest to katalog otwarty. Natomiast sama działalność archiwalna została zdefiniowana jako gromadzenie, ewidencjonowanie, przechowywanie, opracowanie, zabezpieczenie i udostępnianie materiałów archiwalnych oraz prowadzenie działalności informacyjnej. W świetle art. 2 Ustawy o narodowym zasobie archiwalnym i archiwach, narodowy zasób archiwalny służy nauce, kulturze, gospodarce narodowej oraz potrzebom obywateli i dzieli się na państwowy i niepaństwowy zasób archiwalny. Pierwszy z nich składa się z dokumentów archiwalnych wytworzonych w toku działalności enumeratywnie wyliczonych podmiotów publicznych, a także innych ściśle określonych podmiotów jeżeli materiały te stały się własnością Skarbu Państwa (w odniesieniu do poszczególnych elementów wchodzących w skład państwowego zasobu archiwalnego por. Niewęgłowski 2019, s. 98-104). Ponadto uważa się za wchodzące w jego skład również te z powyżej przywołanych dokumentów archiwalnych, które na podstawie prawa lub zwyczajów międzynarodowych powinny być przekazane Polsce. Drugi z zasobów zdefiniowany został przez ustawodawcę w art. 41, przy czym definicja ta ma charakter negatywny i stanowi pośrednie odesłanie do definicji zasobu państwowego. Zgodnie z nią w jego skład wchodzą bowiem wszelkie materiały archiwalne nienależące do państwowego zasobu archiwalnego (W zakresie jego typologii oraz dalszej budowy zob. Konstankiewicz i Niewęgłowski 2016, 463-466).

Podstawową przesłanką przynależności do któregokolwiek z przywołanych zasobów jest przynależność do szerszej grupy materiałów archiwalnych, których definicja zwarta została w art. 1 u.n.z.a. Ma ona charakter zamknięty, jednak jest na tyle szeroka, że dokładne posługiwanie się nią na łamach niniejszego rozdziału nie wydaje się być uzasadnione. Doktryna prawa archiwalnego, wychodząc z podobnego założenia, ukuła więc definicję następującej treści: „materiał archiwalny to dobro niematerialne o charakterze intelektualnym, utrwalone w przedmiocie materialnym lub ustalone w inny sposób […], które stanowi źródło informacji o wartości historycznej o wszelkich aspektach przeszłości. Materiałem archiwalnym są źródła informacyjne mające charakter ponadczasowy i uniwersalny" (Konstankiewicz i Niewęgłowski 2019, s. 160). Przechowywane są one wieczyście i nie podlegają brakowaniu, w przeciwieństwie do materiałów niearchiwalnych, do której to grupy należy każda dokumentacja, która nie została zaliczona do materiałów archiwalnych, a która powstała w toku działalności jednostek publicznych lub też do nich napłynęła (por. art. 5 ust. 1 pkt 2 u.n.z.a.).

Jak już zostało wspomniane, działania podejmowane przez archiwa państwowe nie zostały przez ustawodawcę ograniczone do wymienionych enumeratywnie. Wynika to z faktu, że działalność taka ma charakter wielopoziomowy i zróżnicowany. Archiwa są pracodawcami, lecz w tym zakresie ich działalność nie różni się od innych zakładów pracy. Działalność taka nie jest w związku z tym objęta zakresem niniejszego opracowania. Spośród przykładowego katalogu działań archiwów państwowych zawartego w art. 28 u.n.z.a., największe znaczenie dla dalszych rozważań ma przede wszystkim udostępnianie materiałów archiwalnych. Może ono bowiem nastąpić zarówno w formie indywidualnej lub zbiorowej. Pierwsza sytuacja występuje w przypadku osobistej styczności pomiędzy użytkownikiem archiwum a dokumentem archiwalnym lub w przypadku udostępnienia materiału na odległość za pomocą środków cyfrowych lub tradycyjnych konkretnemu podmiotowi. Drugi wariant udostępnienia dokumentacji archiwalnej polega na wykonaniu kopii cyfrowych i zamieszczeniu ich na stronie internetowej w celu umożliwienia dostępu do nich potencjalnie nieograniczonej kategorii osób (jako przykłady takich stron należy wymienić przede wszystkim portale: www.genealogiawarchiwach.pl [dostęp: 28.02.2025] i www.szukajwarchiwach.gov.pl [dostęp: 28.02.2025]).

3. WYBRANE ZAGADNIENIA ZWIĄZANE Z OCHRONĄ DANYCH OSOBOWYCH

3.1. UWAGI OGÓLNE

W toku swojej niezwykle zróżnicowanej działalności archiwa państwowe wielokrotnie przetwarzają dane osobowe, przy czym nie dotyczy to wyłącznie osób korzystających z narodowego zasobu archiwalnego, ani osób tamże zatrudnionych. W tym bowiem zakresie archiwa podlegają zasadom ogólnym, w zasadzie niczym nieodbiegającym od sytuacji obecnych w innych instytucjach publicznych. Z tego też względu dalsze analizowanie tego zagadnienia nie wydaje się być konieczne. Nie dotyczy to jednak wyjątku zawartego w art. 22d pkt 1 u.n.z.a., który to został przeanalizowany w toku dalszych rozważań. Sytuacją wartą uwagi jest jednak przetwarzanie danych osobowych obecnych w przechowywanych w archiwach zasobach. Co prawda, zgodnie z art. 1 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 (dalej: RODO) ochronie podlegają dane osobowe wszystkich osób fizycznych, to jednak jego motyw 27 wyłącza swoje zastosowanie w stosunku do osób zmarłych (podobną regulację zawierają również motywy 158 i 160 w odniesieniu do badań historycznych i celów archiwalnych, przy czym stanowią on swoiste odniesienie do motywu 50). Państwom członkowskim przyznana została kompetencja do rozciągnięcia ochrony wynikającej z RODO również na tę grupę danych osobowych, jednak Polska nie zdecydowała się na taki krok. W związku z tym większość danych osobowych przetwarzanych w toku działalności archiwów państwowych nie podlega aktom prawnym regulującym ich ochronę. Nie oznacza to jednak, że żadna ochrona nie jest im zapewniana, gdyż można się jej domagać na podstawie przepisów prawa cywilnego regulujących ochronę dóbr osobistych (tak też: Partyk 2021 i przywołane tam orzecznictwo).

W celu umożliwienia działalności sieci archiwów państwowych w sposób zgodny z prawem, przy jednoczesnym uwzględnieniu specyfiki jej działalności ustawodawca zdecydował się na wprowadzenie specyficznych uregulowań o charakterze lex specialis w stosunku do RODO. Na podstawie art. 22d pkt 1 w związku z art. 22 ust. 1 pkt 1 u.n.z.a. archiwa państwowe przetwarzają dane osobowe wieczyście. Należy stwierdzić, iż jest to zgodne z dyspozycją art. 5 ust. 1 lit. e RODO i stanowi jej dookreślenie. Norma ta pozwala bowiem

przetwarzać dane osobowe przez okres dłuższy, niż niezbędny dla celu, w którym są one przetwarzane, o ile służy to realizacji celów archiwalnych w interesie publicznym. Ślady takiego zamysłu prawodawcy unijnego można również odnaleźć w motywie 50, który statuuje swoistą fikcję prawną przetwarzania danych osobowych w tym celu, jako zgodnym z pierwotnie założonym (por. Fajgielski 2022, art. 89). W artykule 5 RODO zostało zawarte również odesłanie do stosowania art. 89 tego rozporządzenia, który odnosi się do regulacji zawartej w tym artykule i uzupełnia ją. Norma odczytana na podstawie tych dwóch przepisów pozwala na stwierdzenie, iż pomimo specyfiki regulacji dotyczącej działalności archiwalnej, zasadniczo podlega ona pod wszystkie normy ogólne RODO, przy czym cel tejże działalności ma nad nimi charakter nadrzędny, a regulacje te muszą być interpretowane przez jego pryzmat. Jako przykład takiej sytuacji przewidzianej na gruncie rozporządzenia, należy wskazać ograniczenie prawa do bycia zapomnianym, o ile mogłoby to uniemożliwić lub poważnie utrudnić realizację wspomnianych celów (por. Fajgielski 2022, art. 89). Ponadto ustawodawcy krajowemu przyznane zostało uprawnienie do ograniczenia prawa dostępu do danych przysługującego osobie, której one dotyczą, prawa do sprostowania danych, prawa do ograniczenia przetwarzania danych, prawa do sprzeciwu, obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania oraz prawa do przenoszenia danych, przy czym ponownie, jedynie w kontekście realizacji celów określonych w ramach RODO (Kuba 2018, s. 1103-1106).

W ramach swojej działalności archiwa państwowe przetwarzają również dane osób żyjących, choć stanowi to zdecydowaną mniejszość ich działalności. Dotyczy to przede wszystkim Archiwum Państwowego w Warszawie Oddziału w Milanówku, które przede wszystkim zajmuje się przechowywaniem i udostępnianiem dokumentacji osobowej i płacowej. Dokumentacja ta, w dość znaczącym zakresie, dotyczy osób wciąż żyjących pracowników zlikwidowanych zakładów pracy, które przekazały posiadaną przez siebie dokumentację ich dotyczącą do tego Archiwum. Dostęp do takiej dokumentacji jest jednak ograniczony. Artykuł 51na u.n.z.a. stanowi, że dokumentacja taka jest udostępniana wyłącznie na żądanie osoby której dotyczy. Co prawda, sytuacja objęta hipotezą tej normy dotyczy przedsiębiorców, to jednak, jak się wydaje, na mocy art. 51a ust. 2 pkt 2 rozciąga ona swoje zastosowanie również na archiwa państwowe. Ponadto dokumenty przechowywane w archiwach na podstawie tych przepisów nie podlegają również pod ogólny reżim dotyczący udostępniania dokumentów archiwalnych, gdyż uznane zostały za dokumentację niearchiwalną. Tym samym uprawnione jest stosowanie przepisów dotyczących przedsiębiorców do archiwów państwowych

w drodze analogii. Tym samym w zakresie objętym tą działalnością archiwa są administratorami danych osobowych podlegającymi regulacjom ogólnym prawa ochrony danych osobowych. Należy dodać, że jest to sytuacja przewidziana przez ustawodawcę w art. 51u ust. 3 u.n.z.a., zaś informację taką można znaleźć na stronie internetowej rzeczonego archiwum.

Istnieje jednak jeszcze jedna grupa, mająca największe znaczenie praktyczne. W przeciwieństwie do przytoczonej powyżej, wchodzi ona w skład narodowego zasobu archiwalnego i podlega, co do zasady nieograniczonemu udostępnianiu użytkownikom archiwów. Zawiera ona dokumentację podlegającą przekazaniu do właściwego miejscowo i rzeczowo archiwum państwowego po upłynięciu określonego czasu od jej wytworzenia lub śmierci osoby (względnie osób), której dotyczy. Grupa ta jest niezwykle zróżnicowana wewnętrznie i to właśnie z nią wiąże się najwięcej problemów dotyczących ochrony danych osobowych osób żyjących.

3.2. UDOSTĘPNIANIE MATERIAŁÓW WYTWORZONYCH W RAMACH DZIAŁALNOŚCI URZĘDÓW STANU CYWILNEGO

Zarówno obecnie obowiązująca ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (t.j. Dz. U. z 2023 r. poz. 1378 z późn. zm.) (dalej: pr.a.s.c.), jak i jej poprzedniczka (t.j. Ustawa z dnia 29 września 1986 r. Prawo o aktach stanu cywilnego (t.j. Dz. U. z 2011 r. Nr 212, poz. 1264 z późn. zm.)) rozróżniają akty stanu cywilnego oraz akta zbiorowe rejestracji stanu cywilnego. Pierwsze z nich są dokumentami urzędowymi dokumentującymi trzy typy zdarzeń: narodziny, małżeństwa i zgony. Stanowią one wyłączny dowód zdarzeń w nich stwierdzonych oraz potwierdzają zdarzenia i fakty stanowiące o stanie cywilnym osób, których dotyczą (por. krytycznie na ten temat - Smyczyński, Andrzejewski 2022, s. 13-14). Natomiast akta zbiorowe rejestracji stanu cywilnego można określić jako wszelkiego rodzaju dokumenty, na podstawie których sporządzono lub zmieniono akt stanu cywilnego. Oba typy dokumentów zostały wymienione w ramach art. 28 pr.a.s.c., a tym samym podlegają przekazaniu do właściwego archiwum państwowego po upływie okresów tam przewidzianych tj. 80 lat od końca roku kalendarzowego, w którym sporządzono akt małżeństwa i zgonu oraz 100 lat od końca roku kalendarzowego, w którym sporządzono akt narodzin. Okresy te stosuje się odpowiednio do akt zbiorowych rejestracji stanu cywilnego (Kurzawa 2022, s. 64). Ustawa różnicuje ponadto sytuację ksiąg wytworzonych przed 1 marca 2015 i powstałych po tej dacie. Ma to związek

z wprowadzoną z momentem wejścia w życie nowego aktu prawnego regulującego akta stanu cywilnego, elektronizacją rejestracji, a tym samym ksiąg stanu cywilnego. W przeciwieństwie do dyspozycji art. 28 pr.a.s.c., art. 128 tej ustawy stanowi, że okresy, po których następuje ich przekazanie do archiwum państwowego liczone są od zamknięcia księgi, a w przypadku tzw. mikstów (tj. ksiąg łączonych) od zamknięcia ostatniej księgi.

Uchwalenie RODO na poziomie unijnym wymusiło na ustawodawcy dokonanie nowelizacji pr.a.s.c., która miała zapewnić zgodność regulacji tam zawartych z rozporządzeniem. W wyniku wejścia w życie ustawy nowelizującej (t.j. Ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. poz. 730)), przechowywanie aktów narodzin i małżeństwa w Urzędzie Stanu Cywilnego, trwa aż do sporządzenia aktu zgonu lub zarejestrowania informacji o zgonie osób, których akt ten dotyczy. Regulacja ta nie ma jednak zastosowania do osób, którym nie został nadany numer PESEL, bowiem ustalenie czy pozostają one przy życiu, czy też nie, byłoby w praktyce niemożliwe. Udostępnianie aktów sporządzonych przed wejściem w życie nowego prawa o aktach stanu cywilnego, a które nie zostały jeszcze przekazane do właściwego archiwum państwowego następuje na zasadach ogólnych, właściwych dla narodowego zasobu archiwalnego. W stosunku do pojedynczych ksiąg stanu cywilnego wynika to wprost z art. 130 ust. 4 pr.a.s.c. Natomiast w kontekście ksiąg mieszanych, z których część ksiąg pojedynczych podlegałaby przekazaniu do archiwum państwowego, gdyby były miały charakter odrębny, obowiązek udostępniania ksiąg potwierdzony został w utrwalonej linii orzeczniczej sądów administracyjnych (por. wyrok WSA w Krakowie z 1.02.2024 r., III SA/Kr 1512/23, wyrok NSA z 1.03.2023 r., II OSK 192/22, wyrok WSA w Warszawie z 4.04.2019 r., IV SA/Wa 538/19). Regulacja zawarta w pr.a.s.c. nie ma jednak zastosowania do aktów sporządzonych po 1 marca 2015, które bezwzględnie przechowuje się w USC, aż do czasu sporządzenia aktu zgonu lub zarejestrowania informacji o zgonie osób, których akt ten dotyczy. Pomimo braku odpowiedniej regulacji w odniesieniu do akt zbiorowych rejestracji, należy domniemywać na podstawie art. 28 ust. 4 i 5, iż przechowywanie tych akt ma charakter wtórny w stosunku do ksiąg i związane jest z ich losem.

Ustawodawca polski poprzez wprowadzenie wyżej przytoczonych regulacji zdecydował się ustanowić pewnego rodzaju fikcje prawne związane z przetwarzaniem danych osobowych osób żyjących. W przypadku niemożliwości stwierdzenia, czy osoba której dokumentacja dotyczy pozostaje przy życiu wprowadzone zostały arbitralnie ustalone okresy, po których następuje jej włączenie w skład narodowego zasobu archiwalnego. Wspomniane okresy (wynoszące 80 i 100 lat) co do zasady zapewniają należytą ochronę osób żyjących, jednak przesuwająca się coraz dalej granica prognozowanej długości życia najprawdopodobniej prowadzić będzie do zwiększania się ilości osób, które przekroczą setny rok życia. Przewidziany przez ustawodawcę swoisty „bezpiecznik", jakim jest figurowanie w rejestrze PESEL w większości przypadków zapewni odpowiednią ochronę danych osobowych, jednakże nie jest to ochrona pełna. Pozostawia ona poza zasięgiem swojego oddziaływania osoby, którym nigdy nie został nadany numer PESEL. Sytuacje takie występują raczej incydentalnie i w większości dotyczą osób, które urodziły się lub zawarły związek małżeński w Polsce, a następnie opuściły ją jeszcze przed jego wprowadzeniem. Nie mniej stanowi to przykład sytuacji względnie niebezpiecznej, która może powodować naruszenie norm zapewniających ochronę danych osobowych. Z oczywistych względów ryzyko takie dotyczy wyłącznie aktów narodzin i małżeństw.

Inną kategorią, która wymaga przeanalizowania jest sytuacja prawna osób występujących w aktach stanu cywilnego, których one bezpośrednio nie dotyczą. W ramach tej grupy osób mieszczą się świadkowie i zgłaszający zdarzenia objęte obowiązkiem rejestracji. W aktach stanu cywilnego oraz w aktach zbiorowych rejestracji zawarte są dane pozwalające na jednoznaczną ich identyfikację, takie jak imię, nazwisko, wiek, zawód, a w odniesieniu do dokumentów występujących na gruncie poprzednich ustaw, również relacja rodzinna z osobą, której zdarzenie dotyczy. Ustawodawca w żaden jednak sposób nie uregulował kwestii dotyczących danych takich osób i są one irrelewantne z punktu widzenia przesłanek przynależności do zasobu archiwalnego. Jak się wydaje, problem ten nie występuje w przypadku aktów narodzin, bowiem okres 100 lat pomiędzy ich wytworzeniem a wejściem do narodowego zasobu archiwalnego, jest na tyle długi, że w zasadzie wyklucza możliwość naruszenia danych osobowych. Wynika to z faktu, iż osoba taka musiała mieć co do zasady ukończone 18 (względnie 16) lat, a to samo w sobie statuowałoby ją w gronie najstarszych ludzi w historii. Na gruncie obecnie obowiązującej ustawy zgłaszającym fakt urodzenia może być również ojciec lub matka dziecka, o ile ukończyła 16 rok życia i posiada ograniczoną zdolność do czynności prawnych. W pozostałych przypadkach świadkowie i zgłaszający

muszą legitymować się pełną zdolnością do czynności prawnych, a taką nabywa się co do zasady z chwilą ukończenia 18 roku życia, chyba że małoletni nabył ją wcześniej poprzez wstąpienie w związek małżeński. W kontekście ryzyka naruszenia należy wskazać, że najdłużej żyjącą osobą w historii była Francuzka Jeanne Louise Calment, która osiągnęła wiek 122 lat. Natomiast najstarszą Polką była Tekla Juniewicz, która dożyła 116 roku życia. Oznacza to, iż przyjęta przez ustawodawcę cezura czasowa jest niemal niemożliwa do przekroczenia, a tym samym praktycznie nigdy nie dojdzie do złamania przepisów odnoszących się od ochrony danych osobowych. W odniesieniu jednak do aktów małżeństw i zgonów ryzyko takie jest już o wiele bardziej realne. W przypadku założenia, iż występująca w akcie osoba spełniała minimalne wymagania wiekowe, wejście materiałów archiwalnych do narodowego zasobu archiwalnego nastąpi jeszcze przed ukończeniem przez nią setnego roku życia, co potencjalnie może skutkować złamaniem przepisów RODO w wyniku ich udostępnienia.

Jak już zostało wcześniej wskazane, udostępnienie takie może mieć charakter indywidualny lub zbiorowy. W pierwszym przypadku archiwum posiada ścisłą kontrolę nad udostępnianymi materiałami i może potencjalnie odmówić dostępu do dokumentacji, jeżeli miałoby to na celu ochronę danych osobowych. Kompetencja taka została bowiem expressis verbis przyznana archiwom państwowym na podstawie art. 16b ust. 1 pkt 2 lit. b u.n.z.a. W odniesieniu zaś do aktów stanu cywilnego i akt zbiorowej rejestracji nie wydaje się to jednak prawdopodobne, gdyż skala takiego naruszenia ma potencjalnie znikomy charakter, a samo prawdopodobieństwo jego wystąpienia jest niezwykle ograniczone. Kompetencja do odmowy istnieje również w przypadku dostępu zbiorowego, jednakże wydaje się to jeszcze mniej prawdopodobne, ze względu na charakter tej formy udostępnienia dokumentacji. W swoich założeniach ma bowiem na celu umożliwienie zapoznania się z nią jak największemu, potencjalnie nieograniczonemu gronu podmiotów. Niepublikowanie dokumentów w formie cyfrowej, która to jest obecnie docelową formą kontaktu użytkowników ze zgormadzonymi zbiorami (por. Strategia rozwoju Archiwów Państwowych na lata 2021-2030, s. 28-39), jest niezwykle daleko idącym środkiem zapobiegawczym, nieadekwatnym do ryzyka naruszenia. Tym samym, jak się wydaje, w żadnej z przytoczonych sytuacji środki takie nie powinny być stosowane, a ich dopuszczalność należałoby uzależnić od faktu posiadania przez archiwum wiedzy na temat pozostawania przy życiu jednej z obecnych w aktach osób. W obu przypadkach istnieje jeszcze możliwość anonimizacji lub pseudonimizacji danych osobowych. Jednakże również w odniesieniu do tej kategorii środków zapobiegających naruszeniu, ciężko

jest dopuścić ich stosowanie. Ponownie wynika to z faktu niewielkiego ryzyka naruszenia. Przyjęcie odmiennej interpretacji prowadziłoby do nałożenia obowiązku dokonywania każdorazowej analizy treści materiałów archiwalnych przez archiwistów, kopiowania ich, a następnie anonimizowania lub pseudonimizowania otrzymanych materiałów, co w praktyce byłoby niemożliwe. Należy jednak zaznaczyć, że przyjęcie takiej, a nie innej interpretacji wynika z chęci wyważenia pomiędzy realizacją celów prawa archiwalnego, które polegają na umożliwieniu korzystania z zachowanego dziedzictwa narodowego przez jak najszerszy krąg osób zainteresowanych, potencjalnie niewielkim ryzykiem naruszenia przepisów zapewniających ochronę danych osobowych.

3.3. UDOSTĘPNIANIE MATERIAŁÓW PRZECHOWYWANYCH W TZW. KOPERTACH DOWODOWYCH

W przeciwieństwie do dokumentacji związanej z aktami stanu cywilnego, gdzie zarówno prawdopodobieństwo naruszenia, jak i jego skutki są co do zasady niewielkie i raczej pomijalne w praktyce archiwalnej, udostępnianie dokumentów przechowywanych w kopertach dowodowych stwarza dużo większe ryzyko. Wynika to z faktu, iż w znaczącej ilości zawierają one w sobie dane osób wciąż żyjących. Wprawdzie dokumentacja ta przekazywana jest do archiwum dopiero po śmierci osoby, której wydano dowód osobisty, to jednak z reguły obejmuje również dane innych osób żyjących (np. współmałżonka lub dzieci tej osoby). Samo przekazywanie kopert dowodowych do archiwów państwowych nie jest procesem automatycznym, gdyż zostały one zakwalifikowane jako materiał niearchiwalny. Nie jest to jednak zbiór jednolity i składa się z trzech grup, z których jedynie pierwsza została zakwalifikowana do wieczystego przechowywania (w zakresie szczegółowego podziału zob. Archiwum Państwowe w Gorzowie Wielkopolskim).

Koperty dowodowe są zbiorczym określeniem na dokumentację przedstawioną przez stronę postępowania w sprawie wydania dowodu osobistego. Organami przechowującymi tę dokumentację są z mocy ustawy (t.j. Art. 60 Ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz. U. z 2022 r. poz. 671 z późn. zm.)) organy gminy oraz konsulowie RP. Należy zwrócić uwagę na fakt, iż podmioty te zostały przez ustawodawcę zobligowane do gromadzenia i przechowywania dokumentacji, tak więc muszą one *ex lege* dopuścić i przechowywać wszystkie dokumenty, które mogą mieć istotne znaczenie dla sprawy (Maciejko 2013, art. 60). Tym samym katalog potencjalnych dokumentów zgromadzonych

we współczesnych kopertach dowodowych jest w praktyce nieograniczony. Podobne założenie przyświecało ustawodawcy także na gruncie poprzednich ustaw (t.j. Dekret z dnia 22 października 1951 r. o dowodach osobistych (t.j. Dz. U. z 1962 r. Nr 2, poz. 5) oraz Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 1974 r. Nr 14, poz. 85).). W związku z tym do dokumentów w nich przechowywanych można zaliczyć m.in. przedwojenne dokumenty tożsamości, okupacyjne kenkarty, dowody osobiste z okresu PRL i III RP, a także różnego rodzaju życiorysy, wnioski, czy dokumentację meldunkową. Tak szeroki zakres dokumentów prowadzi do ogromnego zróżnicowania danych w nich zawartych. W okresie powojennym w ramach wniosków o wydanie dowodu osobistego obligatoryjnie musiały być zawarte dane osobowe małoletnich dzieci pozostających na utrzymaniu wnioskującego oraz dane małżonka. Z tego też względu, w tym przypadku występuje znacząco większe ryzyko udostępnienia danych osobowych osób żyjących. Obowiązek posiadania dowodu osobistego (a tym samym powstanie pierwszych kopert dowodowych), wprowadzony został dopiero w latach pięćdziesiątych XX wieku, co oznacza, że w ramach kategorii małoletnich dzieci mieściły się osoby urodzone w latach trzydziestych i młodsze. O ile więc sam dane posiadacza dowodu osobistego i jego małżonka z reguły nie będą objęte ochroną RODO, o tyle ich dzieciom taka ochrona co do zasady przysługuje.

Skutkuje to znaczącym ryzykiem złamania norm prawa ochrony danych osobowych w przypadku nierestryktywnego podejścia do udostępniania dokumentacji (por. wyrok Naczelnego Sądu Administracyjnego z dnia 13 grudnia 2023 r. o sygn. II OSK 1762/22). W związku z tym należy w większości sytuacji wykluczyć możliwość udostępnienia zbiorowego za pomocą środków elektronicznych. Takie udostępnienie ma charakter masowy i co do zasady materiały tam zawarte nie przechodzą weryfikacji treściowej, a są jedynie kopiowane, obrabiane cyfrowo, a następnie publikowane. Jeżeli jednak zostałyby wprowadzone środki pseudonimizujące, udostępnienie takie powinno być dozwolone. Ze względu na prezentowane powyżej zróżnicowanie dokumentów, nie mogłoby się to odbywać w sposób mechaniczny i wymagałoby każdorazowej weryfikacji *in concreto*. Prowadziłoby to do żmudnej i długotrwałej pracy archiwistów, która jednakże byłaby konieczna w celu zapewnienia należytej ochrony. W przypadku niemożności zachowania takich środków ochronnych udostępnianie materiałów powinno odbywać się w udostępnienia indywidualnego, a przy czym wszelkie powyższe ustalenia również i w tym przypadku powinny znaleźć zastosowanie. Jak się wydaje, tak daleko idący środek jak odmowa udostępnienia materiałów

na podstawie art. 16b ust. 1 pkt 2 lit. b u.n.z.a., nie powinien zostać wykorzystany. Wynika to z faktu, iż każda jednostka archiwalna składa się z jednej koperty dowodowej, a więc niewielkiego objętościowo materiału, w którym w dość prosty sposób można zasłonić dane osobowe podlegające ochronie. W celu znalezienia rozwiązania mającego w założeniu zapewnić szerszą dostępność zasobu archiwalnego, przy jednoczesnym poszanowaniu norm prawa ochrony danych osobowych, należy rozważyć możliwość szerszego wykorzystania środków pośrednich tj. udostępnienia w systemie teleinformatycznym wyłącznie takich danych, które nie są objęte taką ochroną. Taki system wprowadziło m.in. Archiwum Państwowe w Szczecinie oddział w Międzyzdrojach. W jego ramach udostępniane są w formie cyfrowej na portalu szukajwarchiwach.gov.pl wyłącznie dane osobowe zmarłego posiadacza dowodu osobistego, które jednak pozwalają na jej identyfikację w sposób dostateczny i umożliwiają udostępnienie materiału w ramach udostępnienia indywidualnego Wówczas możliwe jest pozyskanie danych potrzebnych do prowadzenia sprawnych badań archiwalnych, a następnie otrzymywania materiałów w trybie udostępnienia indywidualnego, które zostały poddane procesom zapewniającym bezpieczeństwo danych osobowych.

4. PODSUMOWANIE

Konkludując, należy stwierdzić, iż zagadnienie ochrony danych osobowych w ramach działalności archiwów państwowych jest niezwykle specyficzne, a przez to wymaga korzystania ze swoistych środków. Każdorazowo bowiem podmiot udostępniający materiały archiwalne powinien analizować ryzyko wystąpienia naruszenia, pod kątem jego prawdopodobieństwa, intensywności, z wykorzystaniem adekwatnych środków do tego celu. W każdym przypadku działanie takie musi być przeprowadzone z uwzględnieniem specyfiki i rodzaju udostępnianego materiału, a także naczelnych zasad prawa archiwalnego, zapewniających jak najszerszy dostęp do dokumentów wchodzących w skład narodowego zasobu archiwalnego. Inne bowiem środki znajdą zastosowanie do aktów stanu cywilnego i akt zbiorowych rejestracji, a inne do dokumentów zgromadzonych w ramach kopert dowodowych. Podstawową przesłanką jest w tej sytuacji stopień potencjalnego wystąpienia naruszenia norm chroniących dane osobowe, wynikający z rodzaju oraz momentu wytworzenia dokumentacji, której udostępnienie ma nastąpić.

BIBLIOGRAFIA

Akty prawne

Dekret z dnia 22 października 1951 r. o dowodach osobistych (t.j. Dz. U. z 1962 r. Nr 2, poz. 5)

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061 z późn. zm.)

Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. Nr 14, poz. 85)

Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2020 r. poz. 164 z późn. zm.)

Ustawa z dnia 29 września 1986 r. Prawo o aktach stanu cywilnego (t.j. Dz. U. z 2011 r. Nr 212, poz. 1264 z późn. zm.)

Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz. U. z 2022 r. poz. 671 z późn. zm.)

Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (t.j. Dz. U. z 2023 r. poz. 1378 z późn. zm.)

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.)

Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. z 2019 r. poz. 730)

Orzecznictwo

Wyrok Naczelnego Sądu Administracyjnego z 1 marca 2023 r. o sygn. II OSK 192/22, (LEX)

Wyrok Naczelnego Sądu Administracyjnego z 13 grudnia 2023 r. o sygn. II OSK 1762/22, (LEX)

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 4 kwietnia 2019 r. o sygn. IV SA/Wa 538/19, (LEX)

Wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z 1 lutego 2024 r. o sygn. III SA/Kr 1512/23, (LEX)

Literatura

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

Gumularz M., Izydorczyk T.
2021 Ochrona danych osobowych. Ocena ryzyka o skutków. Metody i praktyczne przykłady, Warszawa.

Konstankiewicz M., Niewęgłowski A.
2016 Narodowy zasób archiwalny i archiwa. Komentarz, Warszawa.

Konstankiewicz M., Niewęgłowski A.
2019 Glosa do postanowienia WSA z dnia 28 czerwca 2019 r., II SAB/Bk 43/19, Studia Iuridica Lublinensis, nr 2.

Kuba M.
2018 Komentarz do art. 89 [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa i D. Lubasz, Warszawa.

Kurzawa A.
2022 Komentarz do art. 28 [w:] Kotowicz B., Opaliński B., Kurzawa A., Prawo o aktach stanu cywilnego. Komentarz, Warszawa.

Maciejko W.
2013 Ustawa o dowodach osobistych. Komentarz, Warszawa.

Niewęgłowski A.
2019 Spór o własność tzw. "kancelarii hetmańskiej" Branickich. Glosa do wyroku SN z dnia 31 stycznia 2018 r., I CSK 195/17, Przegląd Sejmowy, nr 5

Partyk A.
2021 Ujawnienie danych osobowych człowieka w publikacji medialnej w kontekście naruszenia jego dóbr osobistych, LEX

Smyczyński T., Andrzejewski M.
2022 Prawo rodzinne i opiekuńcze, Warszawa

Źródła internetowe

2024 Broszura w sprawie kopert dowodowych Archiwum Państwowego w Gorzowie: https://gorzow.ap.gov.pl/wp-content/uploads/2024/10/Instrukcja-dotyczaca-przygotowania-kopert-dowodow-osobistych-do-przekazania-do-Archiwum-Panstwowego-w-Gorzowie-Wielkopolskim.pdf [dostęp 28.02.2025]

Genealogia w archiwach: https://www.genealogiawarchiwach.pl/ [dostęp: 28.02.2025]

Szukaj w archiwach: https://www.szukajwarchiwach.gov.pl/ [dostęp: 28.02.2025]

2022 Strategia rozwoju Archiwów Państwowych na lata 2021-2030: https://archiwa.gov.pl/wp-content/uploads/2022/02/Strategia_rozwoju_AP_2021-2030.pdf [dostęp 28.02.2025]

PERSONAL DATA PROTECTION AND STATE ARCHIVES – SELECTED ISSUES

Abstract: The chapter presents selected threads related to the protection of personal data in the operations of polish state archives. The study includes a general part devoted to the basic legal norms regulating the operations of the archival network and the specificity of personal data protection law in this field. The second part covers selected specific issues. It outlines the potential risks of violating regulations concerning the protection of personal data in selected specific areas.

Key words: GDPR, polish state archives, data protection, civil registry.

MICHAŁ ZAWADA

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

ORCID: 0000-0001-9892-396X

ROLA FEDERALNEGO KOMISARZA DS. OCHRONY DANYCH I INFORMACJI (FDPIC) W SZWAJCARII W KONTEKŚCIE WEJŚCIA W ŻYCIE NOWELIZACJI SZWAJCARSKIEGO PRAWA OCHRONY DANYCH OSOBOWYCH (NFADP) 1 WRZEŚNIA 2023 R.

Streszczenie: W 2020 r. parlament szwajcarski uchwalił nową Ustawę o Federalnej Ochronie Danych (New Federal Act on Data Protection: nFADP), która weszła w życie trzy lata później – 1 września 2023 r. i zastąpiła pierwszą FADP z 1992 r. Istotną rolę w zakresie nowej regulacji pełni Federalny Komisarz ds. Ochrony Danych i Informacji (Federal Data Protection and Information Commissioner: FDPIC), na którego zakresie kompetencji i zadań autor skupi się w swoich rozważaniach. Zostaną przy tym także omówione różnice pomiędzy regulacjami szwajcarskimi a unijnymi. Celem rozdziału zaś będzie podjęcie próby oceny regulacji przepisów dotyczących FDPIC. Ponadto, autor postara się odpowiedzieć na pytania dotyczące współpracy administracyjnej Komisarza z organami federalnymi i kantonalnymi oraz zagranicznymi organami ochrony danych, a także roli nowelizacji w kontekście dynamicznie rozwijających się nowych technologii. Wszystko to w oparciu o odpowiednie akty prawne oraz literaturę, zarówno polską, jak i zagraniczną. Zostaną zastosowane w tym opracowaniu metody: dogmatyczno-prawna oraz prawnoporównawcza.

Słowa kluczowe: Szwajcaria, nFADP, FDPIC, ochrona danych osobowych, współpraca administracyjna.

1. WPROWADZENIE

Zgodnie z art. 13 Konstytucji Federalnej Konfederacji Szwajcarskiej, „każdy ma prawo do poszanowania jego prywatnego i rodzinnego życia, mieszkania oraz korespondencji i telekomunikowania się, a także każdy ma prawo do ochrony przed nadużyciem jego danych osobowych" (Zob. Konstytucja Federalna Konfederacji Szwajcarskiej, tłum. Zdzisław Czeszejko-Sochacki, 2000) (por. Florczak-Wątor i Blonski 2015, s. 83-105). Podczas sesji jesiennej w 2020 r. parlament szwajcarski uchwalił w tej materii nową Ustawę o Federalnej Ochronie Danych (Federal Act on Data Protection (Data Protection Act, FADP) of 25 September 2020, SR 235.1, AS 2022 491 (z późn. zm.)) (dalej również jako: New Federal Act on Data Protection; nFADP), która weszła w życie trzy lata później – 1 września 2023 r. Zastąpiła ona pierwszą FADP z 1992 r. (Federal Act on Data Protection (FADP) of 19 June 1992, SR 235.1, AS 1993 1945 (z późn. zm.)). Od tego czasu Internet i smartfony stały się niezbędne w codziennym życiu, w tym również korzystanie z mediów społecznościowych, chmury czy Internetu rzeczy (IoT). W tym kontekście całkowita rewizja prawa ochrony danych – a nie tylko częściowa, jak miało to miejsce w poszczególnych latach (w tym również w 2009 i 2019 r.) – była niezbędna, aby zapewnić społeczeństwu odpowiednią ochronę danych dostosowaną do współczesnych zmian technologicznych i społecznych.

Kolejnym wyzwaniem była zgodność prawa szwajcarskiego z prawem europejskim, a w szczególności z tzw. Ogólnym Rozporządzeniem o Ochronie Danych z dnia 27 kwietnia 2016 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.)] (dalej również jako: RODO). Nowa ustawa powinna umożliwić utrzymanie swobodnego przepływu danych z Unią Europejską, a tym samym uniknięcie utraty konkurencyjności przez szwajcarskie firmy. Jest to o tyle istotne ze względu na to, że Szwajcaria jest uznawana jako państwo trzecie na gruncie RODO, gdyż nie jest ani członkiem UE, ani nie należy do Europejskiego Obszaru Gospodarczego (EOG), dlatego też wspomniane rozporządzenie unijne ją nie obowiązuje.

Istotną rolę w zakresie nowej regulacji pełni Federalny Komisarz ds. Ochrony Danych i Informacji (dalej również jako: Federal Data Protection and Information Commissioner; FDPIC). Sprawuje on bowiem bezpośredni nadzór nad przestrzeganiem przepisów nFADP. W przypadku naruszenia bezpieczeństwa

danych wymagane jest niezwłoczne powiadomienie FDPIC, który podejmuje decyzje wobec tego rodzaju nielegalnych działań. Dlatego też autor skupi się na tym organie państwowym w swoich rozważaniach, zwłaszcza w ramach zakresu jego kompetencji oraz zadań. Zostaną przy tym także omówione różnice pomiędzy regulacjami szwajcarskimi a unijnymi w materii ochrony danych.

Celem tego rozdziału będzie podjęcie próby oceny regulacji w zakresie przepisów dotyczących FDPIC. Ponadto, autor postara się odpowiedzieć na pytanie, czy w wystarczający sposób szwajcarski ustawodawca uregulował współpracę administracyjną FDPIC z organami federalnymi i kantonalnymi w świetle art. 54-55 nFADP, a także z zagranicznymi organami ochrony danych? Oprócz tego zostanie omówiona rola nowelizacji prawa ochrony danych osobowych w kontekście dynamicznie rozwijających się nowych technologii. Wszystko to w oparciu o odpowiednie akty prawne oraz literaturę, zarówno polską, jak i zagraniczną. Zostaną zastosowane w tym opracowaniu metody: dogmatyczno-prawna oraz prawnoporównawcza.

2. FEDERALNY KOMISARZ DS. OCHRONY DANYCH I INFORMACJI (FDPIC) W SZWAJCARII – ORGANIZACJA I STATUS PRAWNY

Jak już został wspomniane, Federalny Komisarz ds. Ochrony Danych i Informacji (FDPIC) jest kluczową instytucją odpowiedzialną za nadzór nad ochroną danych osobowych i dostępem do informacji publicznych w Szwajcarii. Jego rola została znacząco wzmocniona wraz z wejściem w życie nowej federalnej ustawy o ochronie danych osobowych (nFADP), która dostosowuje szwajcarskie przepisy do współczesnych wyzwań związanych z przetwarzaniem danych. Pod wpływem tego ustalono ścisłą procedurę wyboru kandydata na to stanowisko. Zgodnie z art. 43 nFADP, Komisarz jest wybierany przez Zgromadzenie Federalne Szwajcarii, co zapewnia mu silny mandat. Osoba ubiegająca się o tę funkcję musi posiadać czynne prawo wyborcze na szczeblu federalnym. Kadencja Komisarza natomiast wynosi cztery lata i może być przedłużona maksymalnie dwukrotnie (art. 44 ust. 1 nFADP). Okres urzędowania rozpoczyna się pierwszego dnia stycznia po rozpoczęciu nowej kadencji Rady Narodowej. Można zatem uznać, że system wyboru i długość kadencji Komisarza zapewniają stabilność urzędu oraz jego legitymację, co sprzyja konsekwentnej polityce ochrony danych, gdyż są one ściśle powiązane z organem, który go wybiera.

Jednym z fundamentalnych aspektów funkcjonowania FDPIC jest jego niezależność. Art. 43 ust. 4 nFADP jednoznacznie stanowi, że Komisarz wykonuje

swoje obowiązki niezależnie i nie podlega instrukcjom żadnej władzy ani strony trzeciej. Choć dla celów administracyjnych jest przypisany do Kancelarii Federalnej, posiada też własny sekretariat oraz budżet, co gwarantuje mu autonomię w podejmowanych przez niego działań (art. 43 ust. 5). Jest to istotne choćby ze względu na to, że zapewnienie niezależności Komisarza jest kluczowe dla skutecznej ochrony danych i unikania wpływów politycznych na decyzje dotyczące prywatności obywateli.

Komisarz jest zatrudniony zgodnie z Federalną Ustawą o Personelu z 24 marca 2000 r. (FPA) (Federal Act of March 24, 2000, on the Personnel of the Confederation, SR 172.220.1. (z późn. zm.)), z pewnymi wyjątkami określonymi w nFADP. Jego wynagrodzenie oraz ubezpieczenie emerytalne, inwalidzkie i na wypadek śmierci są zapewniane przez PUBLICA – Federalny Fundusz Emerytalny (art. 43 ust. 3). Ponadto, zgodnie z art. 43 ust. 3bis, Zgromadzenie Federalne określa szczegółowe przepisy dotyczące warunków zatrudnienia Komisarza w osobnym rozporządzeniu. Przejrzystość warunków zatrudnienia Komisarza z pewnością sprzyja jego niezależności i efektywności działania, eliminując potencjalne naciski finansowe.

FDPIC może natomiast zostać odwołany przez Zgromadzenie Federalne przed upływem kadencji jedynie w wyjątkowych przypadkach. Art. 44 ust. 3 przewiduje dwie przesłanki odwołania:

(a) poważne naruszenie obowiązków służbowych w wyniku umyślnego działania lub rażącego niedbalstwa,
(b) trwałą niezdolność do wykonywania obowiązków służbowych.

Ponadto, Komisja Sądownicza może nałożyć na FDPIC naganę w przypadku stwierdzenia uchybień w wykonywaniu obowiązków (art. 44a nFADP). Można na podstawie tego uznać, że mechanizmy odpowiedzialności Komisarza są w sposób wystarczający zdefiniowane, co pozwala z kolei na zapewnienie skutecznego nadzoru nad jego działalnością bez naruszania niezależności urzędu.

Organ ten posiada własny budżet, który jest składany corocznie za pośrednictwem Kancelarii Federalnej do Rady Federalnej. Zgodnie z art. 45 nFADP, budżet ten musi zostać przedstawiony Zgromadzeniu Federalnemu w niezmienionej formie, co dodatkowo wzmacnia niezależność finansową FDPIC. Gwarantowanie niezmienności budżetu przez Radę Federalną wzmacnia autonomię finansową Komisarza, co pozwala mu na realizację zadań bez presji politycznej. Łączy się to z kwestią odpłatności za wybrane usługi świadczone przez FDPIC. Zgodnie z artykułem 59 nFADP, opłaty są pobierane od osób prywatnych za:

- wydanie opinii dotyczącej kodeksów postępowania,
- zatwierdzanie standardowych klauzul ochrony danych i wiążących reguł korporacyjnych,
- konsultacje związane z oceną skutków ochrony danych,
- środki zapobiegawcze i interwencyjne w zakresie ochrony danych,
- doradztwo w sprawach ochrony danych.

Kwoty opłat oraz możliwość ich zniesienia lub obniżenia są określane przez Radę Federalną (art. 59 ust. 2-3 nFADP). System ten pozwala na pokrycie części kosztów działalności FDPIC oraz zapewnienie profesjonalnego wsparcia dla podmiotów przetwarzających dane.

Aby uniknąć konfliktu interesów, Komisarz nie może pełnić funkcji członka Zgromadzenia Federalnego ani Rady Federalnej, jak również nie może pozostawać w innym stosunku zatrudnienia z Konfederacją (art. 46 nFADP). Dodatkowo, następny artykuł zakazuje Komisarzowi podejmowania dodatkowej działalności zawodowej, chyba że Komisja Sądownicza uzna, iż nie narusza to jego niezależności i reputacji. Decyzja w tej sprawie musi być podana do publicznej wiadomości.

Restrykcyjne przepisy dotyczące niepołączalności stanowisk gwarantują pełną koncentrację Komisarza na ochronie danych i eliminują potencjalne konflikty interesów. W sytuacji, gdy pojawi się jednak wątpliwość co do bezstronności Komisarza w danej sprawie, decyzję o jego wyłączeniu podejmuje prezes odpowiedniego wydziału Federalnego Sądu Administracyjnego, kompetentnego w zakresie ochrony danych (art. 47a nFADP). Wprowadzenie mechanizmu wyłączenia Komisarza zapewnia obiektywność i bezstronność podejmowanych decyzji, co wzmacnia powszechne zaufanie do urzędu.

3. ZADANIA I OBOWIĄZKI FDPIC

Jako główne uprawnienie FDPIC należy wskazać to, że może on wszcząć dochodzenie z urzędu lub na podstawie zgłoszenia, jeśli istnieją wystarczające przesłanki wskazujące na naruszenie przepisów o ochronie danych. Może jednak zaniechać działań, jeśli naruszenie jest nieznaczne. Obowiązek współpracy z FDPIC spoczywa na podmiocie prywatnym lub organie federalnym, który musi dostarczyć wymagane informacje i dokumenty. Należy wskazać, że nie zostały określone przez ustawodawcę kryteria oceny „wystarczających przesłanek", które powinny być bardziej precyzyjne, aby uniknąć arbitralności decyzji FDPIC. Ponadto, możliwość odstąpienia od postępowania w przypadku „drobnych"

naruszeń wymaga jasnych wytycznych, aby nie prowadziło to do nierównego traktowania podmiotów.

Zgodnie z art. 51 nFADP, w przypadku stwierdzenia naruszenia przepisów ochrony danych, FDPIC może nakazać dostosowanie, zawieszenie lub zakończenie przetwarzania danych, a także ich częściowe lub całkowite usunięcie. Może również ograniczyć transfer danych za granicę, jeśli narusza on obowiązujące przepisy.

Komisarz jest zobowiązany również do zapewnienia odpowiednich mechanizmów kontrolnych w obrębie swojego urzędu. Zgodnie z art. 48 nFADP, w szczególności powinien wdrożyć skuteczne środki dotyczące bezpieczeństwa danych, aby zagwarantować zgodność z federalnym prawem ochrony danych. Wymóg samoregulacji wzmacnia transparentność i skuteczność działania Komisarza, a także minimalizuje ryzyko naruszeń ochrony danych. Według art. 56 nowelizacji, Komisarz prowadzi rejestr działalności przetwarzania danych realizowanych przez organy federalne. Rejestr ten jest udostępniany publicznie, co ma na celu zapewnienie przejrzystości w zakresie przetwarzania danych przez instytucje państwowe. Publikacja rejestru wzmacnia niewątpliwie kontrolę społeczną i umożliwia obywatelom monitorowanie sposobu, w jaki ich dane są wykorzystywane przez administrację publiczną.

FDPIC jest również zobowiązany, w myśl art. 57 nFADP, do corocznego przedstawiania raportu ze swojej działalności Zgromadzeniu Federalnemu oraz Radzie Federalnej (zob. Annual Report 2023/2024, Federal Data Protection and Information Commisioner (FDPIC)) . Raport ten podlega publikacji, co stanowi istotny mechanizm kontroli działań Komisarza. Ponadto, w przypadkach o szczególnym znaczeniu społecznym, FDPIC ma prawo do informowania opinii publicznej o swoich ustaleniach i decyzjach, co zwiększa świadomość społeczną w zakresie ochrony danych osobowych.

Jeśli chodzi o zakres kompetencji FDPIC, to został on rozszerzony na podstawie art. 58 nFADP, który określa jego dodatkowe obowiązki. Komisarz pełni funkcję doradczą, edukacyjną i kontrolną, współpracując zarówno z organami krajowymi, jak i zagranicznymi. Do kluczowych zadań FDPIC należą:

- Edukacja i doradztwo – informowanie, szkolenie i doradzanie zarówno organom federalnym, jak i osobom prywatnym w zakresie ochrony danych.
- Współpraca międzynarodowa – wsparcie organów kantonalnych oraz współpraca ze szwajcarskimi i zagranicznymi instytucjami zajmującymi się ochroną danych.

- Podnoszenie świadomości społecznej – ze szczególnym uwzględnieniem ochrony osób jej wymagających, w odniesieniu do ochrony danych.
- Wsparcie dla podmiotów danych – dostarczanie informacji o sposobie realizacji praw osób, których dane dotyczą.
- Opiniowanie aktów prawnych – Komisarz opiniuje projekty ustaw oraz inne środki prawne dotyczące przetwarzania danych.
- Tworzenie dobrych praktyk – opracowywanie narzędzi i rekomendacji dla administratorów, podmiotów przetwarzających dane oraz osób, których dane dotyczą, uwzględniając specyfikę poszczególnych sektorów oraz ochronę osób szczególnie wrażliwych.

Ponadto, Komisarz posiada uprawnienia do deklarowania wobec zagranicznych organów ochrony danych, że w Szwajcarii dopuszczalne jest bezpośrednie doręczanie dokumentów dotyczących ochrony danych, pod warunkiem zapewnienia wzajemności w tym zakresie (art. 58 ust. 3 nFADP).

4. WSPÓŁPRACA Z ORGANAMI KRAJOWYMI I ZAGRANICZNYMI

Zgodnie z art. 54 nFADP, szwajcarskie organy federalne i kantonalne są zobowiązane do udostępniania FDPIC wszelkich informacji oraz danych osobowych niezbędnych do realizacji jego ustawowych kompetencji. W ramach bowiem prowadzonego dochodzenia, jak zostało określone w art. 50 ustawy nowelizującej, FDPIC może żądać dostępu do informacji, dokumentacji, rejestrów przetwarzania oraz danych osobowych, a także przeprowadzać inspekcje, przesłuchiwać świadków oraz korzystać z opinii ekspertów. Może także zwrócić się o wsparcie do innych organów federalnych oraz policji. Oprócz tego, organy administracji federalnej zobowiązane są do konsultacji z FDPIC przed wydaniem decyzji dotyczących ochrony danych. Jeśli FDPIC prowadzi równolegle własne postępowanie, organy powinny koordynować swoje działania.

Niewątpliwie, przepisy te umożliwiają efektywną kontrolę oraz nadzór nad przestrzeganiem regulacji dotyczących ochrony danych w sektorze publicznym. Bez wątpienia obowiązek przekazywania informacji umożliwia sprawniejszą realizację zadań FDPIC, a ujednolicenie standardów współpracy między organami administracyjnymi zwiększa skuteczność ochrony danych.

Federalny Komisarz ds. Ochrony Danych i Informacji jest również zobowiązany do wspierania innych podmiotów administracji publicznej, dostarczając im informacji i danych osobowych niezbędnych do wykonywania ich zadań. W szczególności FDPIC współpracuje z krajowymi organami ochrony danych;

organami ścigania w przypadkach naruszeń przepisów przewidzianych w art. 65 ust. 2 nFADP; a także federalnymi i kantonalnymi organami policyjnymi w zakresie egzekwowania środków wynikających z art. 50 ust. 3 i art. 51 nFADP. Komisarz pełni zatem istotną funkcję w egzekwowaniu przepisów ochrony danych, a wsparcie organów ścigania umożliwia skuteczniejsze przeciwdziałanie naruszeniom prawa. Warto jednak przy tym doprecyzować ramy współpracy z organami ścigania, aby uniknąć nadmiernej ingerencji w prywatność obywateli.

Zgodnie z art. 55 nFADP, Komisarz może wymieniać informacje oraz dane osobowe z zagranicznymi organami ds. ochrony danych, pod warunkiem spełnienia określonych warunków. Kluczowym elementem takiej współpracy jest zasada wzajemności, zapewniająca, że wymiana informacji będzie odbywać się na równych warunkach. Ponadto, przekazane dane mogą być wykorzystywane wyłącznie w postępowaniach dotyczących ochrony danych, które stanowiły podstawę wniosku o pomoc administracyjną. Współpraca międzynarodowa zwiększa skuteczność ochrony danych osobowych na poziomie globalnym. Zasada wzajemności zabezpiecza interesy Szwajcarii w relacjach z zagranicznymi organami. Konieczne jest jednak dalsze harmonizowanie standardów wymiany danych na poziomie międzynarodowym, szczególnie w kontekście różnic w regulacjach prawnych.

Szwajcarski ustawodawca ustalił jednak pewne ograniczenia w przekazywaniu danych. FDPIC musi zapewnić ochronę poufnych informacji, takich jak tajemnice zawodowe, handlowe i produkcyjne. Przekazanie tych danych zagranicznym organom jest możliwe tylko po uprzednim poinformowaniu i umożliwieniu zainteresowanym podmiotom wyrażenia opinii, o ile nie jest to nieproporcjonalnie uciążliwe. Ponadto, odbiorcy danych zobowiązani są do zachowania tajemnicy zawodowej i stosowania przekazanych informacji zgodnie z nałożonymi ograniczeniami. Funkcjonowanie ścisłych procedur chroni wrażliwe dane podmiotów gospodarczych i obywateli. Informowanie zainteresowanych podmiotów umożliwia im aktywne uczestnictwo w ochronie ich danych. Oprócz tego, można rozważyć przy tym wprowadzenie wytycznych dotyczących maksymalnego czasu na reakcję dla podmiotów informowanych o przekazywaniu danych.

Efektywna współpraca Komisarza z organami krajowymi i międzynarodowymi jest kluczowa dla zapewnienia zgodności z przepisami ochrony danych osobowych w Szwajcarii. Umożliwia to skuteczne monitorowanie i egzekwowanie przepisów, zapewniając zarazem odpowiedni poziom ochrony prywatności obywateli oraz bezpieczeństwo przetwarzanych danych. Nowelizacja nFADP wprowadza jasne ramy prawne dla tej współpracy, co sprzyja jej efektywności

i transparentności. Skuteczna współpraca pomiędzy organami administracji publicznej podnosi standardy ochrony danych w kraju i za granicą. Warto przy tym jednak rozważyć stworzenie platformy wymiany informacji i doświadczeń pomiędzy krajowymi a zagranicznymi organami ochrony danych osobowych.

5. NOWELIZACJA A ROZWÓJ NOWYCH TECHNOLOGII

W literaturze zwraca się uwagę na to, że nFADP zapewnia odpowiedni poziom ochrony danych osobowych w kontekście sztucznej inteligencji (AI) (por. Kleiner i Heers, s. 3-16; Heers 2023, s. 3-8), który w ogólnym ujęciu nie jest gorszy od ochrony oferowanej przez unijny AI Act (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)) (por. Palacz 2023, s. 22-25; Rzymowski 2024, s. 56-63). Jednakże, zauważa się, że ochrona danych osobowych w zakresie ich gromadzenia i przetwarzania przez Szwajcarię jest słabsza, zwłaszcza w kontekście masowej inwigilacji miejsc publicznych oraz prowadzonych postępowań karnych. Według autorów, w tym kontekście bardziej szczegółowe regulacje w nFADP byłyby korzystne, a także należałoby wprowadzić konkretne środki dotyczące systemów AI oraz podobnych technologii do krajowego kodeksu postępowania karnego (por. Häuselmann 2024; Lessambo 2023, s. 119-123). Mimo to, ogólne podejście Szwajcarii ma kilka zalet. Nie próbuje ona określić i regulować wszystkich aspektów AI w jednym akcie prawnym ani nie tworzy zamkniętego katalogu systemów AI objętych zakazem (Houdrouge i Kruglak 2023, s. 20-24). Takie podejście z pewnością pozwala na większą elastyczność i sprzyja innowacjom.

Wśród wad należy jednak wymienić w szczególności brak jednolitych definicji AI i ryzyka może prowadzić do braku pewności prawnej. Zwłaszcza dotyczy to sytuacji, w której to w orzecznictwie mogą pojawić się rozbieżne interpretacje aż do momentu przyjęcia konkretnych regulacji prawnych. Ponadto, brak harmonizacji prawa szwajcarskiego z regulacjami UE może skutkować koniecznością stosowania różnych zasad w UE i w Szwajcarii, co utrudnia działalność poszczególnych firm (Houdrouge i Kruglak 2023, s. 22-23). Ostatnia z kwestii jest główną bolączką szwajcarskiego ustawodawcy, aby dopasować krajowe ustawodawstwo

do europejskiego w celu uniknięcia przede wszystkim problemów na tle gospodarczym. Pomimo jednak tych wyzwań, należy uznać obecne podejście Szwajcarii za sprzyjające wprowadzaniu innowacji i zwiększyć jej atrakcyjność dla firm z branży AI oraz innych nowych technologii. Zamiast wprowadzania całkowitych zakazów na wczesnym etapie, Szwajcaria daje przestrzeń innowatorom i przedsiębiorcom do tworzenia nowych rozwiązań.

6. RÓŻNICE POMIĘDZY SZWAJCARSKIMI A UNIJNYMI REGULACJAMI

Rozporządzenie Ogólne o Ochronie Danych (RODO) oraz szwajcarska Federalna Ustawa o Ochronie Danych (nFADP) to dwa istotne akty prawne regulujące kwestie ochrony danych osobowych w Europie. Mimo, że Szwajcaria nie jest członkiem Unii Europejskiej, jej przepisy dotyczące ochrony danych mają na celu zapewnienie odpowiedniego poziomu ochrony, zbliżonego do standardów unijnych. RODO ma zastosowanie do wszystkich podmiotów przetwarzających dane osobowe osób fizycznych przebywających na terenie Unii Europejskiej, niezależnie od lokalizacji siedziby firmy. Oznacza to, że przedsiębiorstwa spoza UE, które oferują towary lub usługi osobom w UE lub monitorują ich zachowania, również podlegają przepisom RODO. Z kolei nFADP obowiązuje na terytorium Szwajcarii i dotyczy podmiotów przetwarzających dane osobowe osób fizycznych w Szwajcarii. Chociaż treść nFADP jest inspirowana RODO, jej zakres terytorialny jest bardziej ograniczony i nie obejmuje podmiotów spoza Szwajcarii w takim stopniu jak RODO obejmuje podmioty spoza UE.

Oba akty prawne nakładają na administratorów danych obowiązek ochrony danych osobowych, jednak różnią się w szczegółach. RODO wymaga od niektórych organizacji wyznaczenia Inspektora Ochrony Danych (IOD), zwłaszcza gdy główna działalność polega na przetwarzaniu danych na dużą skalę lub regularnym monitorowaniu osób. Szwajcarska ustawa natomiast zaleca wyznaczenie doradcy ds. ochrony danych, ale nie czyni tego obowiązkowym. Ponadto, w przypadku naruszenia ochrony danych, RODO wymaga powiadomienia organu nadzorczego w ciągu 72 godzin, podczas gdy nFADP nakazuje dokonanie tego "jak najszybciej", bez określenia konkretnego terminu. Można zatem stwierdzić, że RODO nakłada bardziej rygorystyczne i precyzyjne obowiązki na administratorów danych w porównaniu do nFADP, co może skutkować większym obciążeniem administracyjnym dla organizacji działających na terenie UE.

Jedną z najbardziej znaczących różnic między RODO a nFADP są kary za dokonanie naruszeń. RODO przewiduje grzywny do 20 milionów euro lub 4%

całkowitego rocznego światowego obrotu firmy, w zależności od tego, która kwota jest wyższa. nFADP ustanawia znacznie niższe kary, z maksymalną grzywną wynoszącą 250 000 franków szwajcarskich. W przeciwieństwie do europejskich organów ochrony danych, FDPIC nie ma uprawnień do nakładania sankcji na mocy nowych przepisów. Osoby naruszające przepisy są karane grzywną przez kantonalne organy ścigania. Choć FDPIC może zgłosić przestępstwo jako oskarżyciel prywatny w postępowaniu (art. 65 ust. 2 nFADP), to nie ma prawa do złożenia skargi. W przeciwieństwie do nowego FADP, sankcje administracyjne na mocy RODO mają zastosowanie wyłącznie do osób prawnych (por. Pimenta Rodrigues i in. 2024, s. 3-20) .

Różnica ta odzwierciedla odmienne podejście obu regulacji do egzekwowania przepisów o ochronie danych (por. Bryce, Lang i Nagaroor 2024). Surowsze sankcje finansowe za naruszenia działają przede wszystkim jako silniejszy bodziec dla przedsiębiorstw do przestrzegania przepisów o ochronie danych i wskazują też na wagę ochrony prawnej oraz częstsze lub rzadsze łamanie przepisów.

Znajduje to również odbicie w porównaniu do przepisów amerykańskich. W literaturze uważa się, że Stany Zjednoczone i Szwajcaria znajdują się na przeciwległych biegunach jeśli chodzi o poziom przepisów dotyczących prywatności danych (Quay 2024, s. 710-715). Zdaniem autora, ich zakresy przypominają różnice „między mikroskopem a teleskopem". Zwraca on uwagę na to, że amerykańskie prawo dotyczące prywatności danych, podobnie jak mikroskop, koncentruje się na konkretnych jednostkach i obszarach, nie obejmując całego kraju. Natomiast szwajcarskie, niczym teleskop, ukazuje szerszy obraz, obejmujący większą liczbę osób oraz zakres terytorialny obowiązujących przepisów (Quay 2024, s. 716). W obliczu rosnącej tendencji w Szwajcarii, jak i w całej Europie, do szerokiego uregulowania kwestii dotyczących ochrony danych osobowych (zob. szerzej: Mulder i in. 2023), Stany Zjednoczone muszą więc według autora sprostać wymaganiom szybko globalizującego się świata, gdyż podejście oparte na regulacjach stanowych i sektorowych okazało się niewystarczające (por. Quay 2024, s. 716; Hoofnagle 2016, s. 169-177; Gottschalk 2023, s. 448-453). Świadczy to o zróżnicowanym podejściu poszczególnych prawodawców.

7. PODSUMOWANIE

Nowelizacja szwajcarskiej Ustawy o Ochronie Danych (nFADP) wprowadza istotne i dalekosiężne zmiany w funkcjonowaniu Federalnego Komisarza ds. Ochrony Danych i Informacji (FDPIC). Za najważniejszą reformę należy

uznać zmianę sposobu wyboru Komisarza – odtąd będzie on mianowany przez Parlament, a nie jak dotychczas przez Radę Federalną. Ta modyfikacja ma kluczowe znaczenie dla zapewnienia większej niezależności tej instytucji oraz jej demokratycznej legitymacji. Nowy sposób wyboru ma także zwiększyć zaufanie ze strony społeczeństwa szwajcarskiego do pracy FDPIC oraz podejmowanych przez niego decyzji w zakresie ochrony danych.

Nowe regulacje przewidują również rozszerzenie współpracy FDPIC z krajowymi i zagranicznymi organami administracyjnymi. Szwajcarskie instytucje publiczne mają obowiązek udzielania FDPIC wsparcia administracyjnego, zwłaszcza w zakresie dostępu do informacji niezbędnych do prowadzenia dochodzeń. FDPIC, z kolei, ma obowiązek udzielania wsparcia wyłącznie szwajcarskim organom ochrony danych, organom ścigania oraz federalnym służbom odpowiedzialnym za egzekwowanie jego zaleceń. Na podstawie tego można uznać te regulacje za wystarczające w zakresie współpracy na poziomie administracji publicznej, gdyż spełniają one swoje zasadnicze funkcje. Podobnie wygląda sytuacja na szczeblu międzynarodowym. FDPIC może współpracować z zagranicznymi organami ochrony danych, pod warunkiem spełnienia określonych wymogów, takich jak zasada wzajemności, poufność oraz ograniczenie wykorzystania przekazanych informacji wyłącznie do określonych postępowań.

Niewątpliwie Komisarz odgrywa kluczową rolę w egzekwowaniu prawa ochrony danych w Szwajcarii. Jego zadania obejmują zarówno funkcje kontrolne, edukacyjne, jak i doradcze, a jego działalność ma na celu zapewnienie wysokiego poziomu ochrony danych osobowych oraz przejrzystości działań administracji publicznej. Nowelizacja FADP znacząco wzmacnia pozycję FDPIC, umożliwiając mu skuteczniejsze działanie w dynamicznie zmieniającym się środowisku cyfrowym. Jest to istotne z tego względu, że przyszłość przepisów dotyczących ochrony danych w Szwajcarii będzie kształtowana w dalszym ciągu także przez rozwój technologii oraz rosnące zagrożenia związane z cyberbezpieczeństwem. Natomiast dotychczasowe zmiany mają przede wszystkim na celu dostosowanie szwajcarskiego systemu ochrony danych do wyzwań XXI wieku oraz spójność w jak największym stopniu z europejskimi standardami.

BIBLIOGRAFIA

Diaz P.
2022 Data protection: legal considerations for research in Switzerland, „FORS Guide", No. 17, Version 1.0, s. 1-12.

Driessen S., Gervasoni P.
2021 Response to comment on: Research projects in human genetics in Switzerland: analysis of research protocols submitted to Cantonal Ethics Commissions in 2018, „Swiss Medical Weekly", No. 151, s. 1-2.

Florczak-Wątor M., Blonski D.
2015 Problem horyzontalnej skuteczności prawa do ochrony danych osobowych w świetle przepisów konstytucyjnych Polski i Szwajcarii, „Przegląd Sejmowy", Nr 1(126), s. 83-105.

Gottschalk T.
2023 European Union. The EU-US Data Privacy Framework (DPF) – A Blueprint for International Data Transfers?, „European Data Protection Law Review", Vol. 9(4), s. 448-453.

Häuselmann A. N.
2024 EU privacy and data protection law applied to AI: unveiling the legal problems for individuals, Leiden.

Heers M.
2023 Data sharing in the Social Sciences, „FORS Guide", No. 21, Version 1.1, s. 1-10.

Houdrouge R., Kruglak K.
2023 Are Swiss data protection rules ready for AI?, „Jusletter", s. 1-24.

Hoofnagle C. J.
2016 US Regulatory Values and Privacy Consequences, „European Data Protection Law Review", Vol. 2(2), s. 169-177.
2000 Konstytucja Federalna Konfederacji Szwajcarskiej, tłum. Zdzisław Czeszejko-Sochacki, Warszawa.

Kleiner B., Heers M.
2024 Quantitative data anonymisation: practical guidance for anonymising social science data, „FORS Guide", No. 23, Version 1.0, s. 1-17.

Lessambo, F.I.
2023 AML/CFT and Cybersecurity Laws in Switzerland [:w] Anti-Money Laundering, Counter Financing Terrorism and Cybersecurity in the Banking Industry, Cham, s. 119-123.

Mulder V., Mermoud A., Lenders V., Tellenbach B.
2023 Trends in Data Protection and Encryption Technologies, Cham.

Newlands G., Lutz C., Tamò-Larrieux A. et al.
2020 Innovation under pressure: Implications for data privacy during the Covid-19 pandemic, „Big Data & Society", No. 7(2), s. 1-14.

Niksirat K.S., Korka D., Jacquemin Q., Vanini C., Humbert M., et al.
2024 Security and Privacy with Second-Hand Storage Devices: A User-Centric Perspective from Switzerland, „Proceedings on Privacy Enhancing Technologies", t. 2, s. 412-433.

Palacz K.
2023 Jak inteligentne jest prawo regulujące sztuczną inteligencję? Próba analizy AI Act na podstawie jej ugruntowania w przestrzeni komercyjnego użycia, „Prawo Mediów Elektronicznych", Nr 1, s. 22-25.

Pimenta Rodrigues G.A., Marques Serrano A.L. i in.
2024 Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review, „MDPI: Data", Vol. 9(2), s. 1-24.

Quay A.
2024 Desperation for Legislation: The Need for the American Data Privacy and Protection Act, „Wisconsin International Law Journal", vol. 41(4), s. 707-729.

Rzymowski J.
2024 Definicja prawnicza sztucznej inteligencji na podstawie rozporządzenia PE i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji, „Przegląd Prawa Publicznego", Nr 11, s. 56-63.

Stam A, Diaz P.
2023 Qualitative data anonymisation: theoretical and practical considerations for anonymising interview transcripts, „FORS Guide", No. 20, Version 1.1, s. 1-15.

Thir V., Wawra D., Kindsmüller K., Vollenschier V.
2023 Cultural Influences on Personal Data Disclosure Decisions – Swiss Perspectives, „University of Passau Institute for Law of the Digital Society Research Paper Series", No. 23-5.

Akty prawne:

Federal Act of March 24, 2000, on the Personnel of the Confederation, SR 172.220.1. (z późn. zm.).

Federal Act on Data Protection (Data Protection Act, FADP) of 25 September 2020, SR 235.1, AS 2022 491 (z późn. zm.).

Federal Act on Data Protection (FADP) of 19 June 1992, SR 235.1, AS 1993 1945 (z późn. zm.).

Konstytucja Federalna Konfederacji Szwajcarskiej z 18 kwietnia 1999 r., SR 101, AS 1999 2556 (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 (akt w sprawie sztucznej inteligencji) (Dz. U. UE. L. z 2024 r. poz. 1689).

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.).

Źródła internetowe:

Federal Data Protection and Information Commisioner (FDPIC)
2024 Annual Report 2023/2024, https://edb.reader.epaper.guru/de-CH/viewer/e3888600-c9e3-4282-bf28-d6713c9d007a/da5c2a4d-2a32-4b26-98b2-aa99b5a022f1# (dostęp: 20 lutego 2025 r.).

Bryce C., Lang K., Nagaroor S.
2024 Privacy Compliance – the GDPR and the Swiss Data Protection Law, https://arodes.hes-so.ch/record/14213/files/Bryce_2024_Privacy_compliance.pdf (dostęp: 26 lutego 2025 r.).

Federal Data Protection and Information Commisioner (FDPIC)
New FDPIC's role, https://www.edoeb.admin.ch/en/new-fdpics-role (dostęp: 17 lutego 2025 r.).

Federal Data Protection and Information Commisioner (FDPIC)
The new Data Protection Act from the FDPIC's perspective, https://backend.edoeb.admin.ch/fileservice/sdweb-docs-prod-edoebch-files/files/2025/01/15/b2a2f6c8-6ed5-4b69-b025-97e8c938aeb4.pdf, s. 7-8 (dostęp: 21 lutego 2025 r.).

PWC Switzerland
What does the revision of the Swiss Data Protection Act entail, and how does it relate to the GDPR and the ePrivacy Regulation? The E-FADP and the corresponding regulatory environment, https://www.pwc.ch/en/publications/2018/e-dsg-pov.pdf (dostęp: 21 lutego 2025 r.).

Regulatory Affairs Platform of the Swiss Clinical Trial Organisation (SCTO)
2023 Clinical Data Management Systems (CDMS) Evaluation Report. Edited by the SCTO: https://www.sctoplatforms.ch/admin/data/files/section_asset/file/53/the-new-federal-act-on-data-protection-(nfadp)-guidance-for-clinical-trials_scto_sept2023.pdf?lm=1697046425 (dostęp: 27 lutego 2025 r.).

THE ROLE OF THE FEDERAL DATA PROTECTION AND INFORMATION COMMISSIONER (FDPIC) IN SWITZERLAND IN THE CONTEXT OF THE ENTRY INTO FORCE OF THE REVISION OF THE SWISS DATA PROTECTION LAW (NFADP) ON 1 SEPTEMBER 2023

Abstract: In 2020, the Swiss Parliament passed the New Federal Act on Data Protection (nFADP), which came into force three years later on 1 September 2023 and replaced the first FADP of 1992. The Federal Data Protection and Information Commissioner (FDPIC), on whose terms of reference and tasks the author will focus his reflections, plays an important role in terms of the new regulation. It will also be discused differences between Swiss and EU regulations. In turn, the aim of the chapter will be to attempt to evaluate the regulation of the FDPIC legislation. Furthermore, the author will attempt to answer questions regarding the Commissioner's administrative cooperation with federal, cantonal authorities and foreign data protection authorities, as well as the role of new regulation in the context of dynamically developing new technologies. All this is based on the relevant legal acts and literature, both Polish and foreign. The following methods will be applied in this study: dogmatic-legal and comparative-legal.

Keywords: switzerland, nfadp, fdpic, data protection, administrative cooperation.

MIKOŁAJ BRZÓSTOWICZ

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

ORCID: 0009-0001-0920-8751

ZASADA INTEGRALNOŚCI I POUFNOŚCI (ART. 5 UST. 1 LIT. F RODO) A ZAGROŻENIA CYFROWE. CZY NOWE REGULACJE EUROPEJSKIE SĄ W STANIE ZWIĘKSZYĆ BEZPIECZEŃSTWO CYFROWE?

Streszczenie: Rozdział analizuje zasadę integralności i poufności danych osobowych określoną w art. 5 ust. 1 lit. f RODO oraz jej znaczenie w kontekście współczesnych zagrożeń cyfrowych. Podkreśla, że regulacje unijne, takie jak RODO, dyrektywa NIS-2 oraz rozporządzenie DORA, stanowią fundament ochrony informacji, jednak ich skuteczność zależy od praktycznej implementacji i zarządzania ryzykiem. Opisano najważniejsze zagrożenia, w tym ataki ransomware, phishing oraz naruszenia związane z błędami ludzkimi. Ponadto omówiono nowe regulacje UE mające na celu zwiększenie odporności cyfrowej, wskazując na ich zalety i potencjalne ograniczenia. W konkluzji podkreślono, że same przepisy nie wystarczą do zapewnienia pełnego bezpieczeństwa – kluczowe jest połączenie regulacji prawnych, nowoczesnych technologii oraz edukacji użytkowników.

Słowa kluczowe: integralność i poufność danych, rodo, cyberbezpieczeństwo, nis-2, dora.

1. WPROWADZENIE

Współczesne zagrożenia cyfrowe stanowią jedno z największych wyzwań dla ochrony danych osobowych oraz cyberbezpieczeństwa infrastruktury krytycznej. W dobie rosnącej liczby incydentów naruszeń bezpieczeństwa informacji, regulacje prawne Unii Europejskiej odgrywają kluczową rolę w kształtowaniu

standardów ochrony danych i odporności cyfrowej. W szczególności RODO, dyrektywa NIS-2 oraz rozporządzenie DORA wyznaczają ramy prawne mające na celu podniesienie poziomu bezpieczeństwa informacji oraz ochrony kluczowych systemów i usług przed cyberatakami.

Centralnym elementem ochrony danych w Unii Europejskiej jest zasada integralności i poufności, ujęta w art. 5 ust. 1 lit. f RODO, zgodnie z którą dane osobowe muszą być przetwarzane w sposób zapewniający ich bezpieczeństwo, w tym ochronę przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (Fajgielski 2022, art. 5). Wprowadzenie tej zasady ma na celu zagwarantowanie, że zarówno administratorzy, jak i podmioty przetwarzające, wdrożą odpowiednie środki techniczne i organizacyjne adekwatne do ryzyka związanego z przetwarzaniem danych. Jednak pomimo istniejących wymogów RODO, praktyka pokazuje, że wdrożenie skutecznych mechanizmów ochrony informacji jest złożonym procesem, wymagającym nie tylko zgodności z regulacjami, ale także efektywnego zarządzania ryzykiem cybernetycznym (Valsamism 2022).

W kontekście wzrastających zagrożeń, takich jak ataki ransomware, wycieki danych czy cyberprzestępczość ukierunkowana na infrastrukturę krytyczną, Unia Europejska wprowadziła dyrektywę NIS-2, mającą na celu podniesienie poziomu cyberbezpieczeństwa w kluczowych sektorach gospodarki (np. energetyce, transporcie, opiece zdrowotnej) oraz rozporządzenie DORA, nakładające szczegółowe wymogi dotyczące odporności cyfrowej na instytucje finansowe (Cybersecurity Is Gaining Momentum 2021). NIS-2 rozszerza katalog podmiotów zobowiązanych do stosowania środków cyberbezpieczeństwa oraz wprowadza bardziej rygorystyczne mechanizmy egzekwowania przepisów, natomiast DORA koncentruje się na zapewnieniu ciągłości działania systemów finansowych poprzez zarządzanie ryzykiem ICT oraz testowanie odporności operacyjnej (Scott 2021).

Niniejszy rozdział podejmuje problem badawczy, czy same regulacje prawne, takie jak RODO, NIS-2 i DORA, są wystarczające, by zwiększyć odporność cyfrową i bezpieczeństwo danych, czy też niezbędne są dodatkowe działania technologiczne i organizacyjne, aby skutecznie minimalizować ryzyko cyberzagrożeń. W świetle dotychczasowych badań i analiz praktycznych wdrożeń wskazuje się bowiem, że przepisy prawa, choć niezbędne, nie stanowią samodzielnej gwarancji ochrony informacji, a skuteczność systemu cyberbezpieczeństwa zależy od wielu czynników, takich jak implementacja polityk zarządzania ryzykiem, rozwój technologii zabezpieczających oraz edukacja użytkowników (Hydzik 2019).

Metodologicznie rozdział opiera się na analizie dogmatycznej prawa, czyli interpretacji przepisów RODO, NIS-2 i DORA w kontekście literatury prawniczej i praktyki stosowania regulacji. Ponadto wykorzystano studium przypadków wybranych incydentów cyberbezpieczeństwa, które ilustrują wyzwania w zakresie ochrony danych i systemów informatycznych. W analizie uwzględniono również raporty instytucji unijnych, takich jak ENISA i Komisja Europejska, które dostarczają empirycznych danych na temat skuteczności wdrażanych regulacji (ENISA Threat Landscape 2022; Komisja Europejska 2023).

2. ZASADA INTEGRALNOŚCI I POUFNOŚCI W RODO

Podstawową zasadą ochrony danych osobowych w prawie Unii Europejskiej jest zasada integralności i poufności, określona w art. 5 ust. 1 lit. f Ogólnego rozporządzenia o ochronie danych (RODO). Zgodnie z jej treścią, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (Bielak-Jomaa i Lubasz 2018, art. 5). Przepis ten nakłada na administratorów oraz podmioty przetwarzające obowiązek wdrożenia stosownych środków technicznych i organizacyjnych, adekwatnych do poziomu ryzyka związanego z przetwarzaniem danych (por. Fajgielski 2019).

2.1. TREŚĆ I ZNACZENIE ZASADY INTEGRALNOŚCI I POUFNOŚCI

Zasada integralności i poufności pełni kluczową funkcję w systemie ochrony danych osobowych, ponieważ stanowi podstawowy mechanizm zapobiegający naruszeniom bezpieczeństwa. Obejmuje ona dwa istotne aspekty:

1. **Poufność** – zapewnienie, że dane osobowe są chronione przed nieuprawnionym dostępem, ujawnieniem lub naruszeniem. Jest to szczególnie istotne w kontekście cyberzagrożeń, takich jak ataki hakerskie, phishing, wycieki danych czy ataki ransomware (Fajgielski 2022, art. 5).
2. **Integralność** – zagwarantowanie, że dane nie ulegną nieautoryzowanej modyfikacji lub uszkodzeniu, a ich treść pozostanie zgodna z oryginalnym stanem (por. Lubasz 2022). W praktyce oznacza to m.in. stosowanie środków kryptograficznych, takich jak szyfrowanie czy podpisy cyfrowe, które zabezpieczają dane przed manipulacją.

Zasada ta pozostaje ściśle związana z art. 32 RODO, który precyzuje wymogi dotyczące bezpieczeństwa przetwarzania. Nakazuje on administratorom oraz podmiotom przetwarzającym wdrożenie odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja, szyfrowanie, zdolność do przywrócenia dostępu do danych po incydencie oraz systematyczne testowanie środków ochronnych (por. Fajgielski 2022, art. 32)

Jednym z kluczowych elementów zasady integralności i poufności jest jej elastyczność, czyli możliwość dostosowania wdrażanych środków ochronnych do charakteru, zakresu, kontekstu i celów przetwarzania oraz poziomu ryzyka naruszenia praw i wolności osób fizycznych. Oznacza to, że administratorzy muszą dokonywać indywidualnej oceny ryzyka i wdrażać adekwatne mechanizmy ochrony (por. Lubasz 2022).

2.2. INTERPRETACJA ZASADY W DOKTRYNIE I PRAKTYCE

W literaturze prawniczej podkreśla się, że zasada integralności i poufności jest dynamicznym standardem, który wymaga od administratorów nie tylko spełnienia minimalnych wymogów prawnych, ale także ciągłego monitorowania i dostosowywania środków ochrony (Bielak-Jomaa i Lubasz 2018, art. 5). Koncepcja ta łączy się z podejściem opartym na ryzyku, które nakłada na administratorów obowiązek przeprowadzania analizy zagrożeń oraz stosowania środków adekwatnych do stopnia narażenia na incydenty.

Jednym z istotnych aspektów interpretacyjnych jest również powiązanie zasady integralności i poufności z zasadą rozliczalności, wynikającą z art. 5 ust. 2 RODO. Zgodnie z nią, administrator musi być w stanie wykazać zgodność z wymogami bezpieczeństwa i udowodnić, że wdrożone środki ochronne są skuteczne i adekwatne do ryzyka (Papakonstantinou i De Hert 2019, s. 10–12). W praktyce oznacza to konieczność prowadzenia dokumentacji polityki bezpieczeństwa, regularnych audytów oraz testowania mechanizmów ochrony.

2.3. PRZEGLĄD ORZECZNICTWA I DECYZJI ORGANÓW NADZORCZYCH

Orzecznictwo oraz praktyka organów nadzorczych potwierdzają, że naruszenie zasady integralności i poufności może skutkować poważnymi konsekwencjami prawnymi dla administratorów. Przykładem jest decyzja Prezesa Urzędu Ochrony Danych Osobowych (PUODO) z 2024 roku, w której nałożono karę finansową w wysokości 100 000 zł na spółkę, która nie wdrożyła odpowiednich

środków bezpieczeństwa, co doprowadziło do zgubienia niezabezpieczonego nośnika z danymi klientów (UODO DKN.5131.29.2023). Organ nadzorczy uznał, że administrator naruszył art. 5 ust. 1 lit. f RODO, nie zapewniając ochrony danych przed przypadkową utratą.

Podobne rozstrzygnięcia zapadły na poziomie europejskim, gdzie TSUE w sprawie *Google Spain* (C-131/12) zwrócił uwagę na konieczność efektywnego stosowania zasad ochrony danych w praktyce, wskazując, że administratorzy nie mogą ograniczać się jedynie do formalnego wdrożenia polityk ochrony, ale muszą aktywnie zarządzać ryzykiem naruszeń.

Warto również wspomnieć o decyzjach innych organów nadzorczych, na przykład francuski organ do spraw ochrony danych osobowych (*Commission Nationale de l'Informatique et des Libertés – CNIL*), który nałożył wysoką karę na firmę telekomunikacyjną za niedostateczne zabezpieczenia baz danych klientów, co doprowadziło do wycieku milionów rekordów (CNIL SAN-2024-019). Analogiczne sprawy miały miejsce w Niemczech, gdzie Federalny Komisarz ds. Ochrony Danych i Wolności Informacji (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI*) wymierzył karę 9,55 mln euro na firmę telekomunikacyjną, uznając, że jej systemy uwierzytelniania użytkowników były zbyt słabe, co ułatwiło dostęp osobom nieuprawnionym, co naruszyło zasadę integralności.

2.4. ZNACZENIE ZASADY INTEGRALNOŚCI I POUFNOŚCI DLA OCHRONY DANYCH OSOBOWYCH

Podsumowując, zasada integralności i poufności stanowi jeden z fundamentalnych filarów ochrony danych osobowych w Unii Europejskiej. Jej stosowanie wymaga od administratorów nie tylko wdrożenia odpowiednich polityk bezpieczeństwa, ale także ich aktywnego monitorowania i dostosowywania do zmieniającego się krajobrazu zagrożeń cyfrowych. Praktyka pokazuje, że choć RODO ustanawia jasne wymogi w zakresie ochrony danych, to ich skuteczność w dużej mierze zależy od faktycznej implementacji i egzekwowania przez organy nadzorcze.

Decyzje organów ochrony danych oraz orzecznictwo TSUE wskazują, że nieprzestrzeganie zasady integralności i poufności może prowadzić do znaczących sankcji finansowych oraz utraty zaufania użytkowników. W kontekście coraz bardziej zaawansowanych zagrożeń cybernetycznych, zapewnienie

integralności i poufności danych wymaga holistycznego podejścia, obejmującego zarówno środki prawne, techniczne, jak i organizacyjne.

3. ZAGROŻENIA CYFROWE DLA INTEGRALNOŚCI I POUFNOŚCI DANYCH

Współczesne zagrożenia cybernetyczne stanowią istotne wyzwanie dla ochrony danych osobowych oraz bezpieczeństwa infrastruktury krytycznej. W miarę wzrostu skali przetwarzania danych oraz rosnącej liczby cyberataków, organizacje publiczne i prywatne muszą zmierzyć się z ryzykiem naruszenia poufności, integralności oraz dostępności informacji (ENISA Threat Landscape 2022). W ramach RODO problem ten ujęty został w art. 4 pkt 12, który definiuje naruszenie ochrony danych osobowych jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych".

Z perspektywy cyberbezpieczeństwa naruszenie integralności i poufności danych może wynikać zarówno z celowych ataków (np. *ransomware*, *phishing*, ataki DDoS), jak i przypadkowych błędów lub niedopatrzeń (np. nieprawidłowa konfiguracja systemów, wycieki spowodowane błędami ludzkimi). W niniejszej części zostanie przedstawiona typologia głównych zagrożeń cyfrowych, które mogą prowadzić do naruszenia bezpieczeństwa danych oraz infrastruktury krytycznej.

3.1. ATAKI ZŁOŚLIWEGO OPROGRAMOWANIA (MALWARE) I RANSOMWARE

Jednym z najbardziej destrukcyjnych zagrożeń dla poufności i integralności danych są ataki złośliwego oprogramowania, w szczególności ransomware. *Ransomware* to rodzaj złośliwego oprogramowania, które zaszyfrowuje dane ofiary, uniemożliwiając do nich dostęp, a następnie żąda okupu za ich odszyfrowanie (ENISA Threat Landscape 2022). W ostatnich latach liczba tego typu ataków znacząco wzrosła, a ich celem coraz częściej stają się podmioty publiczne, szpitale oraz firmy prywatne (por. Banasiński 2023, 98-102).

Przykładem takiego incydentu był atak ransomware na irlandzką służbę zdrowia HSE w 2021 roku, który doprowadził do paraliżu systemów medycznych oraz ujawnienia wrażliwych danych pacjentów. Atak ten pokazał, że ransomware nie tylko blokuje dostęp do informacji, ale może również prowadzić

do naruszenia poufności danych osobowych i bezpośrednio zagrażać życiu i zdrowiu ludzi (Cyberdefence 2021).

3.2. ATAKI SIECIOWE I EXPLOITY

Kolejną kategorią zagrożeń są ataki sieciowe oraz *exploity* wykorzystujące luki w oprogramowaniu i infrastrukturze IT. Jednym z najczęstszych rodzajów takich ataków jest *SQL injection*, umożliwiający nieautoryzowany dostęp do baz danych i wykradanie informacji. Innym poważnym zagrożeniem są tzw. *exploity zero-day*, czyli ataki wykorzystujące nieznane wcześniej podatności systemów, zanim zostaną one naprawione przez producentów (por. Banasiński 2023, 98-102).

Jednym z najbardziej znanych incydentów tego typu był atak na serwis hotelowy Marriott, w wyniku którego ujawniono dane ponad 500 milionów użytkowników (por. Cyberdefence 2022). Innym przykładem był atak na firmę telekomunikacyjną *T-Mobile*, gdzie hakerzy uzyskali dostęp do danych klientów, wykorzystując lukę w systemach uwierzytelniania (por. Mróz 2021).

W kontekście infrastruktury krytycznej warto wspomnieć o ataku na ukraińską sieć energetyczną w 2015 roku, który doprowadził do blackoutu w kilku regionach Ukrainy. Atak ten został przeprowadzony przy użyciu złośliwego oprogramowania *BlackEnergy*, które umożliwiło cyberprzestępcom przejęcie kontroli nad systemami przemysłowymi i ich dezaktywację (por. Cyberdefence 2016).

3.3. ATAKI SOCJOTECHNICZNE (SOCIAL ENGINEERING)

Jednym z najbardziej niebezpiecznych zagrożeń wynikających z czynnika ludzkiego są ataki socjotechniczne, a zwłaszcza *phishing* i *spear phishing*. *Phishing* polega na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia danych logowania lub innych poufnych informacji. Ataki te mogą prowadzić do uzyskania dostępu do systemów informatycznych, a w konsekwencji do kradzieży danych osobowych i finansowych (por. Banasiński 2023, 259-261).

Jednym z najbardziej znanych incydentów phishingowych była operacja przeciwko firmie *Sony Pictures* w 2014 roku, która doprowadziła do ujawnienia poufnych danych pracowników i wewnętrznych dokumentów (Niewczas 2024). Kolejnym przypadkiem był atak na belgijską służbę bezpieczeństwa, gdzie hakerom udało się przejąć państwową korespondencję, w tym wiadomości wymieniane z prokuraturą i ministerstwami (Palczewski 2025).

3.4. ATAKI NA DOSTĘPNOŚĆ USŁUG (DOS/DDOS)

Choć ataki typu *Denial-of-Service* (DoS) i *Distributed Denial-of-Service* (DDoS) dotyczą przede wszystkim dostępności usług, mogą również prowadzić do wtórnych naruszeń integralności i poufności danych. Ataki DDoS polegają na przeciążeniu infrastruktury sieciowej poprzez wysyłanie dużej liczby zapytań, co prowadzi do zablokowania dostępu do systemów (por. Banasiński 2023, 94-96).

3.5. ZAGROŻENIA WEWNĘTRZNE (INSIDER THREATS)

Nie mniej istotnym zagrożeniem są tzw. zagrożenia wewnętrzne, czyli przypadki, gdy osoby mające dostęp do systemów IT celowo lub nieumyślnie powodują naruszenie bezpieczeństwa danych. Przykłady takich zagrożeń obejmują:

- umyślne ujawnienie poufnych danych przez pracownika,
- brak stosowania procedur bezpieczeństwa,
- sabotaż systemów IT.

3.6. SKUTKI ZAGROŻEŃ CYFROWYCH DLA DANYCH OSOBOWYCH I INFRASTRUKTURY KRYTYCZNEJ

Zagrożenia cybernetyczne mogą prowadzić do poważnych konsekwencji społecznych i ekonomicznych. Naruszenia poufności danych osobowych skutkują ryzykiem kradzieży tożsamości, oszustw finansowych i naruszenia prywatności, podczas gdy naruszenia integralności lub dostępności systemów infrastruktury krytycznej mogą powodować zakłócenia w dostawie energii, paraliż systemów medycznych i chaos gospodarczy.

Przykłady takich incydentów, jak atak *ransomware* na szpital w Düsseldorfie w 2020 roku, który doprowadził do śmierci pacjenta wskutek niedostępności systemu medycznego, czy wyciek danych *Facebook/Cambridge Analytica*, pokazują, że skuteczna ochrona poufności i integralności danych wymaga nie tylko regulacji prawnych, ale także proaktywnych działań technologicznych i organizacyjnych (por. ENISA Threat Landscape 2022).

4. NOWE REGULACJE EUROPEJSKIE: NIS-2 I DORA

Wzrost liczby cyberataków w Europie, obejmujących zarówno incydenty naruszenia ochrony danych osobowych, jak i ataki na infrastrukturę krytyczną, skłonił Unię Europejską do podjęcia działań mających na celu wzmocnienie odporności cyfrowej państw członkowskich oraz podmiotów gospodarczych. W efekcie w grudniu 2022 r. przyjęto dyrektywę NIS-2 (Dyrektywa (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) oraz rozporządzenie DORA (Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011). Oba akty prawne stanowią element strategii UE na rzecz poprawy cyberbezpieczeństwa i zarządzania ryzykiem cyfrowym, uzupełniając wcześniejsze przepisy, takie jak RODO oraz pierwsza dyrektywa NIS (2016/1148).

Dyrektywa NIS-2 zastąpiła pierwszą dyrektywę NIS, której ograniczona skuteczność wynikała z braku jednolitych standardów w państwach członkowskich oraz nieprecyzyjnych wymagań dotyczących cyberbezpieczeństwa dla operatorów usług kluczowych (Valsamis 2022). Nowa regulacja wprowadza szerszy zakres podmiotowy i sektorowy, zaostrza wymogi dotyczące zgłaszania incydentów oraz wdrażania środków ochronnych, a także przewiduje bardziej surowe sankcje za naruszenie przepisów.

Rozporządzenie DORA zostało z kolei opracowane z myślą o sektorze finansowym, który w obliczu coraz bardziej zaawansowanych ataków hakerskich wymaga jednolitych wymogów dotyczących odporności operacyjnej systemów informatycznych. Przepisy te mają zapewnić ciągłość świadczenia usług finansowych nawet w przypadku incydentów naruszenia bezpieczeństwa ICT, wprowadzając obowiązki w zakresie zarządzania ryzykiem, raportowania incydentów oraz testowania systemów cyfrowych.

Dyrektywa NIS-2 została przyjęta w odpowiedzi na rosnące cyberzagrożenia oraz nieskuteczność pierwszej dyrektywy NIS (2016/1148), której implementacja wykazała istotne luki w harmonizacji wymogów bezpieczeństwa w poszczególnych państwach członkowskich. Nowa regulacja znacząco rozszerza zakres podmiotów objętych obowiązkami cyberbezpieczeństwa, wprowadzając jednolite standardy ochrony infrastruktury krytycznej i podmiotów świadczących

kluczowe usługi. Dyrektywa obejmuje 18 sektorów uznanych za krytyczne dla gospodarki, w tym energetykę, transport, infrastrukturę cyfrową, sektor finansowy, dostawę wody, ochronę zdrowia, administrację publiczną oraz sektor spożywczy (Valsamis 2022). Kluczową zmianą jest wprowadzenie podziału podmiotów na kluczowe oraz ważne, co pozwala dostosować wymogi do ich znaczenia dla funkcjonowania państwa i gospodarki (Scott 2021).

Nowe przepisy harmonizują także obowiązki w zakresie cyberbezpieczeństwa, eliminując wcześniejsze rozróżnienie między operatorami usług kluczowych a dostawcami usług cyfrowych, co wprowadzało niejasności interpretacyjne. Dyrektywa wymaga od objętych podmiotów wdrożenia systemowego zarządzania ryzykiem cyberbezpieczeństwa oraz stosowania odpowiednich środków technicznych, operacyjnych i organizacyjnych, obejmujących m.in. polityki bezpieczeństwa, systemy wykrywania incydentów, szyfrowanie, kontrolę dostępu oraz zarządzanie podatnościami. Jednym z kluczowych elementów NIS-2 jest zaostrzenie obowiązków zgłaszania incydentów cybernetycznych. Podmioty objęte regulacją muszą dokonać wstępnego zgłoszenia naruszenia w ciągu 24 godzin, uzupełniającego raportu w ciągu 72 godzin, a pełnego raportu końcowego – w ciągu miesiąca (art. 23 ust. 4 lit. a Dyrektywy 2022/2555). Nowe podejście ma na celu zapewnienie szybkiej wymiany informacji oraz minimalizację skutków cyberataków poprzez wczesne ostrzeganie i koordynację działań w ramach Unii Europejskiej.

Istotnym elementem dyrektywy NIS-2 są mechanizmy egzekwowania przepisów oraz zaostrzenie sankcji za nieprzestrzeganie regulacji. Wprowadzono administracyjne kary pieniężne w wysokości do 10 milionów euro lub 2% globalnego obrotu przedsiębiorstwa, w zależności od tego, która kwota jest wyższa (art. 34 Dyrektywy 2022/2555). Nowością jest także możliwość pociągnięcia do odpowiedzialności osób zarządzających, co oznacza, że członkowie zarządów i kadry kierowniczej mogą odpowiadać za niedopełnienie obowiązków w zakresie cyberbezpieczeństwa, jeśli ich zaniedbania doprowadzą do incydentu naruszenia ochrony danych lub systemów informatycznych (art. 20 Dyrektywy 2022/2555). NIS-2 kładzie również większy nacisk na współpracę międzynarodową i wymianę informacji o zagrożeniach, przewidując mechanizmy współdziałania na poziomie UE, takie jak Grupa Współpracy NIS, zajmująca się opracowywaniem wytycznych i strategii bezpieczeństwa, oraz nowo utworzona Europejska Sieć Organizacji Łącznikowych ds. Kryzysów Cybernetycznych (EU-CyCLONe), której celem jest skuteczniejsze zarządzanie incydentami o charakterze transgranicznym (ENISA Threat Landscape 2022). Dyrektywa wymaga od państw członkowskich jej implementacji do 17 października 2024 roku, co oznacza konieczność

dostosowania krajowych regulacji, w tym np. zmiany ustawy o krajowym systemie cyberbezpieczeństwa w Polsce, czego organy prawodawcze na miesiąc sporządzania tekstu [luty 2025] nie zrealizowały.

Rozporządzenie DORA uzupełnia dyrektywę NIS-2 w sektorze finansowym, koncentrując się na cyfrowej odporności operacyjnej instytucji finansowych oraz ich dostawców usług ICT (por. Banasiński 2023, 417-419). DORA, jako rozporządzenie unijne, ma bezpośrednie zastosowanie we wszystkich państwach członkowskich, co oznacza brak konieczności implementacji do prawa krajowego. Regulacja ta powstała w odpowiedzi na rosnące cyberzagrożenia w sektorze bankowym i inwestycyjnym, które mogą prowadzić do zakłóceń funkcjonowania rynków finansowych oraz poważnych konsekwencji ekonomicznych (por. Banasiński 2023, 417-419). Kluczowym założeniem DORA jest zapewnienie ciągłości działania usług finansowych nawet w przypadku wystąpienia incydentów cybernetycznych, co ma kluczowe znaczenie dla stabilności sektora finansowego.

Podsumowując, zarówno NIS-2, jak i DORA wprowadzają bardziej rygorystyczne standardy bezpieczeństwa cyfrowego w Unii Europejskiej, jednak ich zakres i charakter są różne. Podczas gdy NIS-2 koncentruje się na ogólnogospodarczej odporności cyfrowej, DORA jest regulacją sektorową, ukierunkowaną na sektor finansowy. Obie regulacje w istotnym stopniu nakładają się na RODO, ponieważ naruszenia cyberbezpieczeństwa często prowadzą do incydentów związanych z danymi osobowymi. Dlatego skuteczna implementacja tych przepisów wymaga ścisłej współpracy Europejskiej Rady Ochrony Danych (EROD) oraz organów nadzorczych ds. cyberbezpieczeństwa i sektora finansowego, zarówno na szczeblu krajowym oraz europejskim.

5. OCENA SKUTECZNOŚCI REGULACJI W BUDOWANIU ODPORNOŚCI CYFROWEJ

Nowe regulacje europejskie, takie jak dyrektywa NIS-2 oraz rozporządzenie DORA, stanowią istotny krok w kierunku zwiększenia odporności cyfrowej i ochrony danych osobowych w Unii Europejskiej. W połączeniu z wymogami RODO tworzą one kompleksowy system regulacyjny, którego celem jest zarówno zapobieganie cyberzagrożeniom, jak i minimalizowanie skutków incydentów. W niniejszej części dokonana zostanie ocena skuteczności tych regulacji w kontekście ich faktycznego wpływu na bezpieczeństwo cyfrowe.

Podstawową zaletą nowych regulacji jest ujednolicenie standardów cyberbezpieczeństwa na poziomie unijnym, co eliminuje dotychczasowe rozbieżności

wynikające z różnych podejść krajowych (Valsamis 2022). Dzięki NIS-2 znacząco rozszerzono katalog sektorów objętych obowiązkami w zakresie cyberbezpieczeństwa, a poprzez mechanizmy raportowania incydentów oraz współpracy instytucjonalnej poprawiono zdolność do reagowania na zagrożenia w czasie rzeczywistym (ENISA Threat Landscape 2022). DORA natomiast wzmacnia odporność operacyjną sektora finansowego, standaryzując wymagania dotyczące testowania odporności cyfrowej i zarządzania ryzykiem ICT. Kluczowym atutem regulacji jest również zwiększenie świadomości zagrożeń wśród zarządów podmiotów objętych regulacjami. Wymóg stosowania procedur zarządzania ryzykiem i raportowania incydentów skłania organizacje do systematycznego podejścia do cyberbezpieczeństwa, a nie traktowania go jako sprawy wyłącznie działów IT.

Jednak pomimo wymienionych zalet, ustanowienie regulacji nie gwarantuje automatycznie poprawy poziomu bezpieczeństwa. Skuteczność NIS-2 i DORA w dużej mierze zależy od sposobu ich implementacji i egzekwowania. Analizy dotychczasowych regulacji pokazują, że same przepisy nie są wystarczające – konieczne jest także ich właściwe wdrożenie w praktyce. Przykładem może być pierwsza dyrektywa NIS, której skuteczność była ograniczona z powodu rozbieżnych interpretacji przepisów w poszczególnych krajach oraz niedostatecznej egzekucji obowiązków przez organy nadzorcze (Valsamis 2022). Jednym z problemów jest także niedobór wykwalifikowanych specjalistów ds. cyberbezpieczeństwa, który utrudnia wdrożenie nowych przepisów, zwłaszcza w mniejszych podmiotach.

Ważnym aspektem skuteczności regulacji jest także ich realne egzekwowanie. Choć zarówno NIS-2, jak i DORA przewidują wysokie sankcje finansowe (np. do 10 mln euro lub 2% globalnego obrotu), w praktyce kara nie zawsze oznacza realne zwiększenie poziomu bezpieczeństwa. RODO jest tego dobrym przykładem – mimo że przewiduje surowe sankcje, ich stosowanie bywa nierówne. Największe kary, takie jak te nałożone na *Google* czy *British Airways*, wzbudziły zainteresowanie mediów, ale wiele przypadków naruszeń danych kończy się jedynie ostrzeżeniem lub symbolicznymi grzywnami. Podobny problem może dotyczyć NIS-2 – jeśli organy nadzorcze nie będą miały wystarczających zasobów do monitorowania zgodności z regulacjami, kary mogą być nakładane sporadycznie, co osłabi efekt prewencyjny przepisów.

Kolejnym wyzwaniem jest relacja między zgodnością z regulacjami a faktycznym podnoszeniem poziomu bezpieczeństwa. Istnieje ryzyko, że wiele organizacji potraktuje wymogi NIS-2 i DORA jedynie jako kolejne formalności do spełnienia, koncentrując się na dokumentacji zgodności, zamiast na rzeczywistym wzmacnianiu ochrony danych i systemów. W literaturze przedmiotu podkreśla

się, że regulacje powinny iść w parze z budowaniem kultury bezpieczeństwa, a nie jedynie nakładaniem obowiązków biurokratycznych (Hydzik 2019). Wprowadzone przepisy mogą wymusić określone procedury, ale to realne działania, takie jak testy penetracyjne, stosowanie nowoczesnych technologii zabezpieczeń czy szkolenia pracowników, mają kluczowe znaczenie dla cyberodporności.

Jednym z najistotniejszych wyzwań dla regulacji jest także dostosowanie ich do dynamicznych zmian technologicznych. Zagrożenia cybernetyczne ewoluują bardzo szybko – pojawiają się nowe techniki ataków, wykorzystanie sztucznej inteligencji przez cyberprzestępców, zagrożenia dla IoT i systemów chmurowych (ENISA Threat Landscape 2022). Ramy prawne oparte na ogólnych zasadach, takich jak RODO, są elastyczne, ale regulacje sektorowe (np. DORA) mogą wymagać stałej aktualizacji w odpowiedzi na zmieniające się zagrożenia. W tym kontekście istotną rolę odgrywają standardy techniczne i normy branżowe, takie jak ISO 27001 czy certyfikacja zgodnie z *Cybersecurity Act*, które dostarczają bardziej szczegółowych wytycznych dotyczących najlepszych praktyk w cyberbezpieczeństwie.

Nie można również pomijać czynnika ludzkiego, który pozostaje jednym z najsłabszych ogniw cyberbezpieczeństwa. Większość incydentów wynika z błędów użytkowników, takich jak kliknięcie w złośliwy link, używanie słabych haseł czy nieostrożne korzystanie z poczty e-mail. Nawet najbardziej zaawansowane regulacje nie zapobiegną cyberatakom, jeśli pracownicy nie będą świadomi zagrożeń i odpowiednio przeszkoleni. NIS-2 wprowadza wymóg budowania polityk świadomości cyberbezpieczeństwa, ale ich efektywność będzie zależała od realnego zaangażowania organizacji w szkolenia i rozwój kompetencji pracowników (ENISA Threat Landscape 2022).

Ostatecznie, skuteczność regulacji zależy również od poziomu współpracy międzynarodowej i wymiany informacji o zagrożeniach. Mechanizmy takie jak Grupa Współpracy NIS, CSIRT Network oraz EU-CyCLONe mają poprawić koordynację w zakresie reagowania na incydenty, ale prywatne firmy często niechętnie dzielą się informacjami o naruszeniach z obawy przed konsekwencjami prawnymi i reputacyjnymi. Zaufanie między sektorem publicznym a prywatnym oraz skuteczność systemów raportowania będą kluczowe dla realizacji celów nowych regulacji.

Podsumowując, regulacje takie jak NIS-2 i DORA stanowią istotny element budowania odporności cyfrowej, ale same w sobie nie wystarczą do zapewnienia pełnego bezpieczeństwa. Dopiero połączenie odpowiedniego prawa, skutecznej egzekucji, zaawansowanych technologii ochronnych oraz odpowiednio

przeszkolonych użytkowników może stworzyć system realnie podnoszący poziom ochrony przed cyberzagrożeniami. Skuteczność regulacji będzie zależała od ich wdrożenia w praktyce i zdolności do adaptacji do dynamicznie zmieniającego się krajobrazu zagrożeń cybernetycznych.

6. WNIOSKI KOŃCOWE

Przeprowadzona analiza wykazała, że zasada integralności i poufności danych osobowych pozostaje fundamentalnym elementem systemu ochrony informacji w Unii Europejskiej, a jej realizacja wymaga zarówno skutecznych środków technicznych i organizacyjnych, jak i odpowiednich ram prawnych. W tym kontekście nowe regulacje europejskie, takie jak dyrektywa NIS-2 oraz rozporządzenie DORA, stanowią istotne wzmocnienie unijnej strategii cyberbezpieczeństwa, wprowadzając jednolite standardy i mechanizmy nadzoru w odpowiedzi na narastające zagrożenia cyfrowe. Ich celem jest nie tylko zwiększenie odporności sektora publicznego i prywatnego na cyberataki, ale także usprawnienie współpracy międzynarodowej oraz mechanizmów reagowania na incydenty naruszenia bezpieczeństwa informacji.

Jednak zgodnie z postawioną w rozdziale hipotezą, same regulacje prawne nie są wystarczającą gwarancją bezpieczeństwa cyfrowego. O ile tworzą one formalny szkielet ochrony, to ich skuteczność w praktyce zależy od zaangażowania podmiotów zobowiązanych do ich implementacji oraz od czynników pozaprawnych, takich jak inwestycje w infrastrukturę ochronną, rozwój technologii i edukacja użytkowników. Regulacje wyznaczają kierunek działań, lecz same w sobie nie mogą zastąpić aktywnego zarządzania ryzykiem oraz elastycznego dostosowywania strategii cyberbezpieczeństwa do zmieniającego się krajobrazu zagrożeń.

Przyjęcie kompleksowego podejścia jest warunkiem skutecznego podnoszenia odporności cyfrowej. Kluczowe znaczenie ma synergia trzech czynników: prawa, technologii oraz edukacji. Regulacje takie jak NIS-2 i DORA dostarczają podstawowych narzędzi prawnych, lecz ich implementacja musi iść w parze z inwestycjami w nowoczesne rozwiązania zabezpieczające, jak np. szyfrowanie, systemy detekcji intruzów czy sztuczna inteligencja w analizie cyberzagrożeń. Konieczne jest również budowanie kultury organizacyjnej opartej na proaktywnym zarządzaniu ryzykiem, w której cyberbezpieczeństwo traktowane jest jako ciągły proces, a nie jedynie formalność wynikająca z przepisów.

Regulacje prawne muszą także podlegać dynamicznej adaptacji, aby nadążać za zmieniającymi się zagrożeniami cyfrowymi. Przykładem tego podejścia

jest *Cyber Resilience Act*, będący kolejną inicjatywą Unii Europejskiej w zakresie wzmocnienia bezpieczeństwa produktów ICT. Wnioski z analizy wskazują, że odporność cyfrowa jest ruchomym celem – wymaga elastyczności przepisów oraz zdolności do ich szybkiej aktualizacji w odpowiedzi na nowe wektory ataków, np. cyberprzestępczość wykorzystującą sztuczną inteligencję czy rozwój zaawansowanych ataków na infrastrukturę chmurową.

Ważnym wnioskiem wynikającym z analizy jest znaczenie współpracy międzynarodowej oraz wymiany informacji. Wzmacnianie koordynacji działań między instytucjami UE, rządami krajowymi, regulatorami sektorowymi, sektorem prywatnym i obywatelami jest warunkiem skutecznego przeciwdziałania cyberzagrożeniom (ENISA Threat Landscape 2022). Sukces NIS-2 i DORA będzie w dużej mierze zależał od zdolności do realnej implementacji mechanizmów współpracy – zarówno na poziomie formalnym (np. przez działalność Grupy Współpracy NIS, EU-CyCLONe czy CSIRT Network), jak i operacyjnym, poprzez skuteczną wymianę informacji o zagrożeniach pomiędzy. Jednocześnie wyzwaniem pozostaje niechęć firm do dzielenia się danymi o incydentach z obawy przed konsekwencjami prawnymi i reputacyjnymi.

Ostatecznie, analiza potwierdza tezę rozdziału, że regulacje prawne są warunkiem koniecznym, ale niewystarczającym do zapewnienia pełnego poziomu odporności cyfrowej. Tworzą one fundament systemu ochrony, lecz ich realna skuteczność zależy od praktycznego wdrożenia i egzekwowania przepisów, a także od komplementarnych działań w zakresie technologii i edukacji. Luka między prawem a praktyką jest jednym z kluczowych wyzwań – nawet najlepiej skonstruowane regulacje mogą okazać się nieskuteczne, jeśli ich wymagania nie zostaną przełożone na realne działania wzmacniające cyberbezpieczeństwo. Przykłady licznych naruszeń ochrony danych, mimo istnienia RODO, czy różnice w egzekwowaniu pierwszej dyrektywy NIS pokazują, że przepisy same w sobie nie eliminują ryzyka.

Podsumowując, jedynie holistyczne podejście, łączące efektywne prawo, inwestycje w technologię oraz wzrost świadomości użytkowników, może realnie zwiększyć bezpieczeństwo cyfrowe w Unii Europejskiej. W obliczu narastających zagrożeń niezbędne jest zarówno konsekwentne wdrażanie istniejących regulacji, jak i ich bieżąca aktualizacja, aby dostosować się do zmieniającego się krajobrazu cyberzagrożeń. W tym kontekście zintegrowane działania na poziomie europejskim i krajowym, połączone z odpowiednią współpracą sektora publicznego i prywatnego, są kluczowe dla osiągnięcia wysokiego poziomu odporności cyfrowej.

BIBLIOGRAFIA

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie wspólnych środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (dyrektywa NIS 2). Dziennik Urzędowy Unii Europejskiej L 333/80, 27.12.2022.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie cyfrowej odporności operacyjnej sektora finansowego (DORA). Dziennik Urzędowy Unii Europejskiej L 333/1, 27.12.2022.

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 (ogólne rozporządzenie o ochronie danych - RODO). Dziennik Urzędowy Unii Europejskiej L 119/1, 4.5.2016.

Orzecznictwo

Decyzja PUODO z 29.04.2024 r., DKN.5131.29.2023, LEX nr 3714762.

CNIL, Délibération SAN-2024-019 du 14 novembre 2024,

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Wyrok Trybunału Sprawiedliwości z 13.05.2014 r., C-131/12, Google Spain SL i Google Inc. v. Agencia de Protección de Datos (AEPD) i Mario Costeja González, ZOTSiS 2014, nr 5, poz. I-317.

Monografie i rozdziały w monografiach Literatura

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

Drobek P.
2017 RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa.

Fajgielski P.
2019 Prawo ochrony danych osobowych. Zarys wykładu, Warszawa.
2022 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. II, Warszawa, art. 5.

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

Kuner C., Bygrave L. A., Docksey C.
2020 The EU General Data Protection Regulation (GDPR): A Commentary, Oxford: Oxford University Press.

Lubasz D.
2022 Zasady dotyczące przetwarzania danych osobowych, [w:] Meritum. Ochrona danych osobowych, red. D. Lubasz, wyd. II, Warszawa.

Papakonstantinou V., De Hert P.
2019 The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review, t. 35, nr 6.

Scott H. S.
2021 The EU's Digital Operational Resilience Act: Cloud Services & Financial Companies, Cambridge: Harvard Public Law Working Paper No. 21-28.

Valsamis E.

2022 Defining the reporting threshold for a cybersecurity incident under the NIS Directive and NIS 2, Computer Law & Security Review.

Raporty i opracowania instytucjonalne

ENISA
2022 ENISA Threat Landscape 2022, European Union Agency for Cybersecurity, https://www.enisa.europa.eu [dostęp: 28.02.2025].

Komisja Europejska
2023 Report on the implementation of the General Data Protection Regulation (GDPR), Brussels: European Commission, https://ec.europa.eu [dostęp: 28.02.2025].

Źródła internetowe

Cyberdefence.pl
2016 Cyberatak na ukraińską sieć energetyczną. USA pomagają w śledztwie, https://cyberdefence24.pl/cyberatak-na-ukrainska-siec-energetyczna--usa-pomagaja-w-sledztwie [dostęp: 28.02.2025].

Cyberdefence.pl
2021 Cyberatak na służbę zdrowia w Irlandii. Rząd odmawia hakerom, https://cyberdefence24.pl/polityka-i-prawo/cyberatak-nasluzbe-zdrowia--w-irlandiirzad-nie-spelni-zadan-hakerow [dostęp: 28.02.2025].

Cyberdefence.pl
2022 Kolejny wyciek danych w sieci hoteli Marriott. To przez cyberatak, https://cyberdefence24.pl/cyberbezpieczenstwo/kolejny-wyciek-danych-w-sieci-hoteli-marriott-to-przez-cyberatak [dostęp: 28.02.2025].

Mróz K.
2021 Odparliśmy atak DDoS na sieć T-Mobile, https://firma.t-mobile.pl/dla-mediow/aktualnosci/informacja-prasowa/2021/12/atak-ddos-na--siec-t-mobile.html [dostęp: 28.02.2025].

Niewczas K.
2024 Co to jest phishing i jak się przed nim ustrzec?, https://siplex.pl/blog/co-to-jest-phising-i-jak-sie-przed-nim-ustrzec#Atak_phishingowy_na_Sony_Pictures_2014 [dostęp: 28.02.2025].

Palczewski S.
2025 https://cyberdefence24.pl/armia-i-sluzby/wlamanie-do-belgijskiego--wywiadu-atak-chin [dostęp: 28.08.2025].

THE PRINCIPLE OF INTEGRITY AND CONFIDENTIALITY (ART. 5(1)(F) GDPR) AND DIGITAL THREATS. CAN NEW EUROPEAN REGULATIONS ENHANCE CYBERSECURITY?

Abstract: The chapter examines the principle of data integrity and confidentiality as outlined in Article 5(1)(f) of the GDPR and its relevance in the face of modern digital threats. It highlights that EU regulations, such as the GDPR, the NIS-2 Directive, and the DORA Regulation, form the foundation of data protection but require effective implementation and risk management to be truly effective. Key threats, including ransomware attacks, phishing, and human errors, are discussed in detail. Additionally, the chapter explores new EU regulations aimed at strengthening digital resilience, outlining their benefits and potential limitations. The conclusion emphasizes that legal regulations alone are insufficient to ensure full security – combining legal frameworks, advanced technology, and user education is crucial.

Keywords: data integrity and confidentiality, gdpr, cybersecurity, nis-2, dora.

LAURA BŁASZCZAK

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

SZTUCZNA INTELIGENCJA W ŚRODOWISKU PRACY W DOBIE RODO I AI ACT

Streszczenie: Wzrost zastosowania sztucznej inteligencji w środowisku pracy rodzi nowe wyzwania prawne i etyczne, szczególnie w zakresie ochrony danych osobowych. Sztuczna inteligencja znajduje zastosowanie w usprawnianiu procesów rekrutacyjnych, monitoringu pracowników oraz automatyzacji rutynowych zadań. RODO, regulujące zasady przetwarzania danych osobowych, zobowiązuje do przestrzegania wymogów przejrzystości i bezpieczeństwa, których pracodawcy powinni być świadomi. Dodatkowo, trzeba mieć na uwadze pojawienie się unijnego rozporządzenia AI Act, które nakłada nowe obowiązki na różne podmioty związane z wdrażaniem i stosowaniem systemów sztucznej inteligencji. Celem artykułu jest identyfikacja kluczowych wyzwań prawnych wynikających z wdrażania narzędzi AI przez pracodawców oraz analiza ich wpływu na sposób wykonywania pracy. Z przedstawionej analizy wynika, że brak możliwości pełnej kontroli nad działaniem systemów AI uniemożliwia zapewnienie skutecznej ochrony przed potencjalnie negatywnymi skutkami ich stosowania w środowisku pracy.

Słowa kluczowe: sztuczna inteligencja, prawo pracy, ochrona danych osobowych, AI Act, etyka w pracy

WSTĘP

W dobie dynamicznego rozwoju narzędzi technologicznych sztuczna inteligencja staje się nieodłącznym elementem współczesnego środowiska pracy. Znajduje ona zastosowanie przy wielu czynnościach m.in. w procesach rekrutacyjnych, w ocenie wydajności pracowników, czy w automatyzacji codziennych zadań pracowników. Trzeba mieć jednak na uwadze, że jej tak szerokie wykorzystywanie rodzi wyzwania prawne i etyczne, zwłaszcza w kontekście ochrony danych osobowych.

Unia Europejska, dostrzegając zarówno potencjał, jak i ryzyko związane z nieustannym rozwojem sztucznej inteligencji, podjęła próbę opracowania kompleksowej regulacji, mającej na celu wyznaczenie jej prawnych ram. Aktem ustanawiającym zharmonizowane przepisy dotyczące sztucznej inteligencji jest 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 (dalej jako: "AI Act"). Jego celem jest stworzenie kompleksowych ram prawnych, które zapewnią rozwój systemów AI zgodnie z zasadą poszanowania praw człowieka i transparentności (Flisak 2024). Pojawienie się przepisów dotyczących sztucznej inteligencji ma minimalizować ryzyko związane z jej używaniem, szczególnie w przypadkach, gdzie brak jest jasności co do powodów decyzji podejmowanych przez te systemy (Komisja Europejska).

Niniejszy rozdział stanowi analizę relacji pomiędzy regulacjami dotyczącymi ochrony danych osobowych a AI Act w kontekście wykorzystywania sztucznej inteligencji w środowisku pracy. Celem rozdziału jest identyfikacja kluczowych wyzwań prawnych związanych z wdrażaniem systemów AI przez pracodawców oraz ich wpływem na sposób wykonywania pracy przez pracowników. Rozważania rozpoczynają się od wyjaśnienia relacji między AI Act a Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnym przepływem takich danych (dalej: „RODO"). Następnie omawiane jest, czym w świetle AI Act jest system AI i jakie obowiązki wynikają z tego dla podmiotów go wdrażających. W artykule zastosowano metodę dogmatyczno-prawną, polegającą na analizie przepisów prawnych dotyczących ochrony danych osobowych oraz rozporządzenia AI Act.

RELACJA AI ACT I RODO

Wraz z opublikowaniem AI Act pojawiły się wątpliwości związane ze wzajemną relacją tej regulacji a RODO. W art. 2 ust. 7 AI Act wskazano, że rozporządzenie to funkcjonuje niezależnie od innych unijnych aktów prawnych dotyczących ochrony danych osobowych. Oznacza to, że regulacje zawarte w AI Act nie mają na celu zmiany ani zastąpienia przepisów ochrony danych osobowych, lecz współistnieją z nimi, stosując się równolegle do obowiązujących norm prawnych

w zakresie ochrony prywatności i danych. Wobec tego dostawcy i użytkownicy systemów AI będą musieli postępować w zgodzie z obiema regulacjami przy stosowaniu rozwiązań opartych o sztuczną inteligencję.

Co więcej należy pamiętać, że oba akty dotyczą różnych obszarów regulacyjnych. AI Act wprowadza podział systemów sztucznej inteligencji, niezależnie od aspektu związanego z ochroną danych osobowych. Z kolei RODO znajduje zastosowanie wyłącznie w sytuacjach, gdy dochodzi do przetwarzania danych osobowych.

Warto jednak mieć na uwadze, że AI Act wyraźnie nawiązuje do aksjologii wypracowanej na gruncie RODO. Wskazuje się, że ta regulacja stanowi próbę przeniesienia założeń koncepcyjnych wypracowanych na gruncie RODO na nowe pole regulacyjne (Pązik, Świerczyński i Fisher 2023, s.106). Przede wszystkim ten akt prawny opiera się na dwóch celach: jednym z nich jest rozwój sztucznej inteligencji, a drugim minimalizacja ryzyka związanego z jej potencjalnymi zagrożeniami. Takie ujęcie ma na celu wypracowanie wiodącej pozycji Unii Europejskiej w sektorze nowych technologii, bez uszczerbku dla jej wartości i gwarantowanych praw podstawowych. Konstrukcja tego podejścia przypomina strategię przyjętą wcześniej przy tworzeniu RODO.

Tak jak zostało wspomniane, AI Act w wielu swoich przepisach uwzględnia koncepcje znane z RODO. Pierwszą z inspiracji zaczerpniętych od RODO przez AI Act jest podejście oparte na ryzyku (*risk based approach*) (Konarski 2024). Jest ono zawarte w motywie 26 AI Act zgodnie z którym:

„Aby wprowadzić proporcjonalny i skuteczny zestaw wiążących zasad dotyczących systemów sztucznej inteligencji, należy zastosować jasno określone podejście oparte na analizie ryzyka. Takie podejście powinno polegać na dostosowywaniu rodzaju i treści takich zasad do intensywności i zakresu zagrożeń, jakie mogą powodować systemy sztucznej inteligencji".

Unijny prawodawca zdecydował się wprowadzić podział systemów AI ze względu na ryzyko związane z poszczególnymi prawami i wolnościami jednostek (Kozłowski 2024). W zależności od klasyfikacji danego systemu na dostawców systemów AI nałożone są różne obowiązki. Nie jest to jednak identyczne założenie, jakie przewidziane jest w RODO. W RODO chodzi o to, że środki ochrony danych osobowych powinny być dostosowane do ryzyka, jakie czynność przetwarzania stwarza dla praw i wolności osób fizycznych (Rzymowski 2024). Administrator musi samodzielnie przeprowadzać ocenę ryzyka związaną z przetwarzaniem danych. Powinien on w każdym przypadku wziąć pod uwagę charakter, zakres i cel tej czynności (Urząd Ochrony Danych Osobowych 2025b). W AI

Act to prawodawca narzuca określony poziom ryzyka w kontekście systemów sztucznej inteligencji.

Kolejnym przykładem podobnego podejścia AI Act i RODO jest podkreślenie znaczenia transparentności. Zasada przejrzystości została wyraźnie wskazana w art. 5 RODO zgodnie, z którym dane osobowe muszą być przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą. Ten wymóg wiąże się z tym, że na administratorach ciąży obowiązek formułowania komunikatów dla osób, których dane dotyczą w sposób łatwy do zrozumienia, czyli prostym i przystępnym językiem (Gudowska-Natanek, Kuca 2024, s. 55). Jeżeli chodzi o kwestię transparentności w AI Act, to w motywie 27 tego rozporządzenia wskazano, że:

> "systemy AI rozwija się i wykorzystuje w sposób umożliwiający odpowiednią identyfikowalność i wytłumaczalność, jednocześnie informując ludzi o tym, że komunikują się z systemem AI lub podejmują z nim interakcję, a także należycie informując podmioty stosujące o zdolnościach i ograniczeniach tego systemu AI, a osoby, na które AI ma wpływ, o przysługujących im prawach".

Obowiązek ten został uregulowany w art. 50 ust. 1 AI Act. W przepisie tym wskazano również wyjątek od wymogu informowania użytkowników o interakcji z systemem AI, który dotyczy sytuacji, gdy nawiązanie kontaktu z systemem AI jest oczywiste z punktu widzenia osoby fizycznej, która jest dostatecznie poinformowana, uważna i ostrożna, z uwzględnieniem okoliczności i kontekstu wykorzystywania. Jako przykład takiej sytuacji można wskazać dialog z robotem operującym na lotniskach, ułatwiającym podróżnym przemieszczanie się (Flisak 2024). Ponadto systemy AI wysokiego ryzyka mają dodatkowy obowiązek przejrzystości wskazany w art. 13 ust. 1 AI Act. Zgodnie z nim systemy te powinny być projektowane w sposób, który zapewni przejrzystość ich działania, umożliwiającą użytkownikom interpretację wyników działania systemu i ich właściwe wykorzystanie.

Nie jest jasne, w jaki sposób sposób należy zagwarantować wytłumaczalność oraz przejrzystość systemów AI, ponieważ w wielu przypadkach nie da się w pełni skontrolować ich wyników działania. Problem objaśnialności określany jest mianem deficytu "czarnej skrzynki" sztucznej inteligencji (Barzycka-Banaszczyk 2025, s. 77). Jak słusznie wskazała M. Jędrzejczak żaden akt prawny nie zagwarantuje bezpieczeństwa danych w systemach sztucznej inteligencji, dopóki nie będzie możliwa pełna kontrola ich działania (Jędrzejczak 2024).

Omawiając relację AI Act i RODO warto także zwrócić uwagę na możliwość kolizji między tymi dwoma aktami. Przykładowo taka sytuacja może wystąpić w przypadku nakładania sankcji administracyjnej na dany podmiot, ponieważ

kary pieniężne za naruszenie przepisów RODO i AI Act mają podobną konstrukcję. Wobec tego pojawia się wątpliwość, czy w przypadku systemów wykorzystujących sztuczną inteligencję, które przetwarzają dane osobowe, istnieje możliwość nałożenia dwóch administracyjnych kar pieniężnych na podstawie obu aktów prawnych za to samo naruszenie (Stępień 2024). W doktrynie, jeszcze przed wejściem w życie AI Act, wskazywano na ryzyko tzw. "*overlappingu*", czyli nakładania się regulacji dotyczących sztucznej inteligencji z innymi obowiązującymi aktami prawnymi (Dobosz 2022, s. 133). Jako przykład sytuacji, w której mogłoby dojść do naruszenia zarówno RODO, jak i AI Act, można wskazać przypadek niedozwolonego scoringu społecznego. Taka sytuacja mogłaby wystąpić, gdy pracodawca wykorzystywałby systemy sztucznej inteligencji do analizy kandydatów do pracy na podstawie ich aktywności w mediach społecznościowych, podejmując decyzje o zatrudnieniu w oparciu o czynniki niezwiązane z wydajnością pracy, takie jak poglądy polityczne, przekonania religijne czy przynależność do określonych grup społecznych (Stępień 2024). W takim przypadku system sztucznej inteligencji naruszałby zarówno art. 5 ust. 1 lit. c AI Act, jak i art. 9 ust. 2 RODO, ponieważ przetwarzałby dane szczególnej kategorii bez odpowiedniej podstawy prawnej (Stępień 2024). Prawodawca unijny również dostrzegł ryzyko naruszenia zasady *ne bis in idem*, wskazując w motywie 168 AI Act na konieczność zapewnienia jej poszanowania. Jednocześnie w art. 2 ust. 7 AI Act podkreślono, że powinien on być stosowany bez uszczerbku dla przepisów RODO, choć takie zapewnienia mogą okazać się niewystarczające (Stępień 2024).

W świetle powyższego można stwierdzić, że rozporządzenie o ochronie danych osobowych oraz AI Act wzajemnie się uzupełniają, mimo różnic w zakresie przedmiotu regulacji. Unijny prawodawca wzorował się na RODO przy tworzeniu AI Act, jednak nie zawsze udało się w pełni osiągnąć zamierzony cel. Jest to szczególnie widoczne w przypadku zasady przejrzystości systemów sztucznej inteligencji, gdzie ze względu na fakt, że działanie AI nie jest w pełni wyjaśnialne, nie jest możliwe zapewnienie pełnej transparentności, jak to ma miejsce w przypadku przetwarzania danych osobowych

DEFINICJA SYSTEMÓW AI I ICH KLASYFIKACJA W AI ACT

Istotna dla zastosowania AI Act jest definicja systemów AI, ponieważ to właśnie te systemy są przedmiotem regulacji rozporządzenia (Flisak 2024). Zgodnie z definicją zawartą w art. 3 pkt. 1 AI Act system AI jest to:

> "system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który - na potrzeby wyraźnych lub dorozumianych celów - wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne".

Definicja ta jest krytykowana przez praktyków. Przykładowo T. Zalewski wskazuje, że pojęcie systemu AI powinno być jasno zdefiniowane, aby zapewnić pewność prawa (zgodnie z motywem 12 AI Act). Jego zdaniem to założenie nie zostało spełnione, ponieważ definicja ta została skonstruowana niezgodnie z zasadami tworzenia definicji legalnych i może być ona interpretowana na wiele wzajemnie wykluczających się sposobów (Zalewski 2025). T. Zalewski zwraca uwagę, że wszystkie cechy systemu AI wymienione w definicji, z wyjątkiem "wnioskowania", mogą być również spełnione przez tradycyjne programy komputerowe - co może utrudniać precyzyjne określenie, które systemy rzeczywiście można zakwalifikować jako systemy AI (Zalewski 2025).

Komisja Europejska opracowała wytyczne dotyczące definicji systemu AI, w których wyróżniła siedem kluczowych elementów tego pojęcia: oparcie o operacje maszynowe, autonomię, zdolność adaptacji, cele wyraźne lub dorozumiane, wnioskowanie, dane wyjściowe mogące wpływać na środowisko fizyczne lub wirtualne oraz interakcję z otoczeniem (Komisja Europejska 2024a).

"Oparcie o operacje maszynowe" oznacza, że systemy AI działają z wykorzystaniem maszyn (Komisja Europejska 2024a). We wcześniejszej wersji pojęcia systemu AI wskazywano, że są one oprogramowaniem (Kozłowski 2024). Trzeba wskazać, że wobec braku definicji "maszyny" nie jest jasne, jaki jest ostateczny zakres tej cechy systemu AI (Zalewski 2025). Przykładowo w słowniku języka polskiego PWN wskazano, że: "maszyna to urządzenie zawierające mechanizm lub zespół współdziałających mechanizmów, służące do przetwarzania energii albo do wykonywania określonej pracy" (Słownik Języka Polskiego PWN). Zdaniem T. Zalewskiego:

> "właściwość systemów AI polegająca na byciu systemami maszynowymi nie jest kluczową cechą systemów AI, która pozwala odróżnić je od tradycyjnego oprogramowania tworzonego przez ludzi. Wręcz przeciwnie - każdy program komputerowy będzie miał taką cechę, a zatem będzie spełniał tę część definicji systemu AI" (Zalewski 2025).

"Autonomia" odnosi się do projektowania systemów AI w taki sposób, aby funkcjonowały one z pewnym stopniem niezależności działań od zaangażowania

człowieka i możliwości działania bez jego interwencji (Komisja Europejska 2024a). Poziom autonomii, o którym mowa w art. 3 pkt 1 AI Act, teoretycznie może być minimalny, chociaż gdyby autonomia działania systemu była tak niska, że praktycznie pomijalna, to nie spełniałaby ona wymogów określonych w przepisie, co wynika z zasady zakazu wyprowadzania absurdalnych wniosków z przepisów (Spałek, Rzymowski 2024).

"Zdolność adaptacji" wskazuje na to, że system AI może wykazywać zdolności adaptacyjne po wdrożeniu. Należy zwrócić uwagę, że prawodawca unijny posługuje się w tej definicji słowem "może". Oznacza to, że system może, ale niekoniecznie musi, posiadać zdolność adaptacji lub samouczenia się po wdrożeniu, aby stanowić system AI (Komisja Europejska 2024a).

Według motywu 12 AI Act: "Odniesienie do wyraźnych lub dorozumianych celów podkreśla, że systemy AI mogą działać według jasno określonych lub dorozumianych celów. Cele systemu AI mogą różnić się od przeznaczenia systemu AI w określonym kontekście". Wyraźne cele odnoszą się do jasno określonych celów, które są bezpośrednio zakodowane przez dewelopera w systemie (Komisja Europejska 2024a). Z kolei cele dorozumiane można wywnioskować z podstawowych założeń systemów (Komisja Europejska 2024a). W wyjaśnieniach do definicji systemu AI OECD jako przykład podano regułę obowiązującą przy jeździe samochodem: "Jeśli światło jest czerwone, zatrzymaj się", w której ukrytym celem jest przestrzeganie prawa oraz zapobieganie wypadkom (Zalewski 2025). Ponadto warto podkreślić, że cel systemu AI może być znany dopiero po zastosowaniu systemu np. w przypadku systemów rekomendacji uczących się na podstawie interakcji z użytkownikami (Zalewski 2025).

Kolejna cecha systemu AI "wnioskowanie" odnosi się do tego, że musi on wywnioskować z otrzymanych danych wejściowych dane wyjściowe (Komisja Europejska 2024a). "Wnioskowanie" obejmuje etap tworzenia systemu AI oraz etap wykorzystywania systemu AI po jego wdrożeniu (Zalewski 2025).

Termin "Dane wyjściowe mogące wpływać na środowisko fizyczne lub wirtualne" podkreśla, że systemy AI mogą wywoływać skutki w środowisku fizycznym lub wirtualnym (Komisja Europejska 2024a). Odniesienie to podkreśla, że wpływ systemu sztucznej inteligencji może dotyczyć zarówno namacalnych, fizycznych obiektów, jak i środowisk wirtualnych, w tym przestrzeni cyfrowych, przepływów danych i ekosystemów oprogramowania (Komisja Europejska 2024a).

Ostatni element definicji systemu AI "interakcja z otoczeniem" oznacza, że systemy te aktywnie oddziałują na środowisko, w którym są stosowane

(Komisja Europejska 2024a). Interakcja może dotyczyć świata wirtualnego lub fizycznego (Komisja Europejska 2024a). "Systemy AI, które wchodzą w interakcję ze światem cyfrowym, to systemy, które mogą bezpośrednio wprowadzać zmiany w tym świecie, takie jak wykonywanie czynności prawnych w formie elektronicznej" (Zalewski 2020, s. 13). Z kolei "systemy AI, które wchodzą w interakcję ze światem fizycznym, to systemy, które mogą oddziaływać na otoczenie fizyczne, na przykład poprzez poruszanie się czy wprowadzanie zmian w rzeczywistości fizycznej" (Zalewski 2020, s. 13).

Należy także zwrócić uwagę, że nie wszystkie elementy definicji są elementami koniecznymi dla uznania, że dany system można zakwalifikować jako system AI w rozumieniu art. 3 pkt 1 AI Act. "Zdolność adaptacji" oraz "wpływ na środowisko fizyczne lub wirtualne" nie będą kluczowe dla wskazania, czy dany system jest systemem AI, ponieważ prawodawca używa przy nich słowa "może". Oznacza to, że cechy te są jedynie potencjalnymi, a nie koniecznymi elementami systemu AI. Kluczowe znaczenie będą miały inne elementy definicji, które ustawodawca określił jako obligatoryjne. "Elementy konieczne to: system maszynowy, zaprojektowany do działania z różnym poziomem autonomii, wnioskuje na potrzeby wyraźnych lub dorozumianych celów, jak generować wyniki takie jak predykcje, treści, zalecenia lub decyzje na podstawie danych wejściowych" (Zalewski 2025).

Warto również zauważyć, że intencją prawodawcy było to, aby w rozporządzeniu AI Act wyodrębnić cztery kategorie systemów AI: systemy zakazane, systemy wysokiego ryzyka, systemy ograniczonego ryzyka oraz systemy minimalnego ryzyka . W tym akcie wprost wyjaśniono, czym są zakazane praktyki (w art. 5 ust. 1 AI Act) oraz systemy wysokiego ryzyka (w art. 6 ust. 1 i ust. 2 AI Act). Wątpliwości budzi zakres systemów cechujących się „ograniczonym" oraz „minimalnym" ryzykiem, ponieważ w AI Act nie użyto takich sformułowań (Kozłowski 2024). Wskazuje się, że systemy o ograniczonym ryzyku podlegają podstawowym wymogom przejrzystości (Flisak 2024). Z kolei w przypadku systemów minimalnego ryzyka nie przewidziano żadnych szczególnych obowiązków.

WYKORZYSTYWANIE SZTUCZNEJ INTELIGENCJI PRZEZ PRACODAWCÓW

Warto zwrócić uwagę, że rozwój sztucznej inteligencji sprawia, że coraz więcej przedsiębiorstw decyduje się na automatyzację etapu rekrutacyjnego. Jest to proces używania nowoczesnych technologii i narzędzi, które mają na celu usprawnienie i przyspieszenie różnych etapów zatrudniania (Ffsolutions, 2024).

Niektóre z wykorzystywanych przez pracodawców systemów ATS (Applicant Tracking System) potrafią być wsparciem przy całym procesie rekrutacji. System może zasugerować, na jakim portalu najlepiej opublikować ogłoszenie, uwzględniając preferencje i konkretne kwalifikacje, których poszukuje u potencjalnego pracownika. Sztuczna inteligencja może również przygotować zadania rekrutacyjne dla kandydatów na stanowisko. Często pracodawcy powierzają systemowi wstępną selekcję CV i innych dokumentów potencjalnych pracowników. System AI może także przeprowadzać rozmowę kwalifikacyjną z kandydatami poprzez chatboty. Na jej podstawie istnieje możliwość dokonania analizy zachowań i emocji danej jednostki (Małobęcka-Szwast i in. 2025, s. 220). Narzędzie może podjąć zautomatyzowaną decyzję co do zatrudnienia kandydata lub jego rekomendacji do następnego etapu rekrutacji (porównując profil rekrutujących osób z profilem idealnego pracownika) (Małobęcka-Szwast i in. 2025, s. 220). Na koniec system AI może przygotować projekt umowy. Z powyższego przeglądu przykładowych zastosowań sztucznej inteligencji w procesie rekrutacji wynika, że jej wykorzystywanie może być szerokie. Cel jej użycia jest zależny od potrzeb pracodawcy.

Trzeba także wskazać, że w środowisku pracy sztuczna inteligencja może być cennym wsparciem w codziennych zadaniach, takich jak np. dobór pracowników do odpowiednich działów na podstawie zgodności ich charakterów. Może ona również dopasowywać czynności do kompetencji zespołu oraz wydawać sprecyzowane polecenia dotyczące kolejności zadań.

Zastosowanie systemów AI sprawia, że niektórzy pracodawcy mogą dążyć do zwiększenia kontroli nad swoimi pracownikami. Przykładowo w 2018 r. Amazon rozważało wprowadzenie elektronicznych opasek śledzących ruch pracowników magazynu w czasie rzeczywistym. Pozwalałyby one na analizę położenia osoby, na której nadgarstku znajduje się opaska. Jeśli pracownik magazynu podniósłby niewłaściwą paczkę, opaska zaczęłaby wibrować, co informowałoby, że powinien on skierować się do innego miejsca (Money 2018). Z kolei PKO Bank Polski we współpracy z producentem oprogramowania wdrożyło narzędzie liczące uśmiechy pracowników i klientów. Bank ogłosił, że za każdy zarejestrowany uśmiech zostanie przekazana kwota na cel charytatywny (Media PKO Bank Polski, 2019). Mimo, że celem wprowadzenia tego rozwiązania nie była kontrola pracowników, to zastanawiano się nad prawdziwymi intencjami spółki. Bank przewidział system nagród dla osób zatrudnionych, które się uśmiechały. Należy również uwzględnić, że pracodawcy mogą dążyć do monitorowania aktywności pracowników w sposób ingerujący w ich prywatność, na przykład poprzez analizę liczby

interakcji z interfejsem komputera, w tym liczby kliknięć. Wobec tego sztuczna inteligencja w środowisku pracy nie wiąże się wyłącznie z korzyściami dla przedsiębiorstw, ale również z ogromnymi zagrożeniami.

Wykorzystanie systemów AI w procesie rekrutacji może prowadzić do podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, czyli dokonywanych za pomocą środków technicznych bez bezpośredniego udziału człowieka (Małobęcka-Szwast i in. 2025, s. 227). W motywie 71 RODO podkreślono, że elektroniczne metody rekrutacji bez interwencji ludzkiej mogą znacząco wpływać na osobę, której dane dotyczą. Motyw ten nie tylko wskazuje na ryzyko związane z decyzjami podejmowanymi w sposób zautomatyzowany, ale przede wszystkim określa pożądany stan prawny, zgodnie z którym osoby fizyczne powinny być chronione przed skutkami takich decyzji.

Decyzja jest uznawana za opartą wyłącznie na zautomatyzowanym przetwarzaniu, jeśli administrator danych nie potrafi wyjaśnić powodów decyzji zaproponowanej przez system AI i zaakceptowanej przez człowieka lub jeśli osoba formalnie podejmująca decyzję nie ma realnej możliwości jej zmiany bądź odrzucenia rekomendacji systemu (Czerniawski 2018, s. 566). W art. 22 ust. 1 RODO zaznaczono, że osoba, której dane dotyczą, ma prawo do tego, by nie podlegać takiej decyzji, jeżeli wywołuje ona wobec tej jednostki skutki prawne lub w podobny sposób istotnie na nią wpływa. Uprawnienie to stanowi element szeroko pojmowanego prawa do ochrony danych osobowych i ma na celu przeciwdziałanie negatywnym skutkom automatyzacji procesów przetwarzania danych, które mogą stwarzać zagrożenie dla osób, których dane są przetwarzane (Fajgielski 2022, s. 332).

Negatywne konsekwencje, jakie wynikać mogą ze zautomatyzowanego przetwarzania danych, dotyczą często odmowy przyznania określonych korzyści podmiotowi danych (Fajgielski 2022, s. 333). W przypadku rekrutacji takim skutkiem jest niezatrudnienie osoby. Zgodnie z art. 22 ust. 2 RODO podejmowanie decyzji opartych wyłącznie o zautomatyzowane działanie jest możliwe w jednym z poniższych przypadków:

- gdy jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem danych,
- gdy jest to dozwolone prawem Unii Europejskiej lub prawem państwa członkowskiego, któremu podlega administrator danych i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą,
- kiedy opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W procesie rekrutacji decyzje podejmowane przy użyciu algorytmów nie zawsze wymagają zgody kandydata. Przykładowo, w swoich wytycznych Grupa Robocza Art. 29 ds. ochrony danych podkreśla, że przesłanką legalizującą przetwarzanie danych może być niezbędność do zawarcia umowy (Grupa Robocza art. 29 ds. Ochrony Danych 2017b). Taka sytuacja ma miejsce, gdy, z powodu dużej liczby zgłoszeń, pracodawca decyduje się na wykorzystanie systemu AI w celu odfiltrowania zgłoszeń, które są nieistotne (Grupa Robocza art. 29 ds. Ochrony Danych 2017b). W takim przypadku zautomatyzowane podejmowanie decyzji jest uzasadnione w celu sporządzenia krótkiej listy potencjalnych kandydatów, z zamiarem zawarcia umowy z osobą, której dane dotyczą (Grupa Robocza art. 29 ds. Ochrony Danych 2017b).

W kontekście tematyki zautomatyzowanego podejmowania decyzji warto również zwrócić uwagę na profilowanie. Zgodnie z definicją legalną zawartą w art. 4 pkt 4 RODO: "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".

W powyższej definicji podkreślono, że czynność ta koncentruje się na ocenie niektórych czynników osobowych osoby fizycznej, w szczególności analizie lub prognozie niektórych jej aspektów. Wobec tego należy zaznaczyć, że nie każda czynność zautomatyzowanego przetwarzania danych będzie profilowaniem (np. automatyczne rejestrowanie czasu pracy nie będzie stanowiło profilowania) (Czaplińska, Sakowska-Baryła, 2021). Pracodawcy powinni pamiętać, że profilowanie opiera się na modelach statystycznych, stąd jest ono obarczone marginesem błędu (Szymielewicz, Walkowiak 2014). Może ono skutkować ocenami nieuwzględniającymi indywidualnej sytuacji osoby, na przykład z powodu niepełnych danych wyjściowych.

Należy także wspomnieć, że wykorzystywanie sztucznej inteligencji w środowisku pracy może być obarczone ryzykiem dyskryminacji. Zjawisko to jest niedopuszczalne przez regulacje prawa unijnego (Tlatlik 2022, s. 25). Zakaz dyskryminacji został także uregulowany w przepisach krajowych - mowa o nim w ustawie z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania oraz w art. 18^3a kodeksu pracy. Ponadto kwestia dyskryminacji stanowi jedną z głównych wątpliwości etycznych związanych z szerokim zastosowaniem systemów AI. Słusznie wskazuje się, że modele mogą

faworyzować określone grupy lub podejmować decyzje na podstawie nieprawidłowych danych szkoleniowych (np. źle dobranych lub celowo zniekształconych) (Dolniak i in. 2024, s. 199). Zjawisko to znane jest pod pojęciem *algorithm bias* (Techtarget 2024). Powody powstania uprzedzeń są różne - najczęściej wskazuje się na wadliwy sposób zbierania danych szkoleniowych, a także nieprawidłowe ich dobranie do konkretnego systemu (Dolniak i in. 2024, s. 199).

W świetle powyższych rozważań należy stwierdzić, że pracodawcy powinni szczególnie dbać o to, aby stosowane przez nich systemy AI były zaprojektowane w sposób gwarantujący prawidłowość oraz niedyskryminacyjny charakter przetwarzania danych, a także minimalizowanie negatywnego wpływu takich procesów, w szczególności nieobiektywnego podejmowania decyzji, na prawa i wolności osób, których dane dotyczą (Jędrzejczak 2024).

MONITORING PRACOWNIKÓW

Niewątpliwie rozwój sztucznej inteligencji ma wpływ na sposoby monitorowania pracowników w miejscu pracy. Należy zwrócić uwagę, że prawodawca unijny wyodrębnił wśród systemów wysokiego ryzyka systemy AI wykorzystywane do monitorowania osób zatrudnionych . Kwestia monitoringu została również uregulowana w RODO. Ponadto art. 88 ust. 1 RODO umożliwia państwom członkowskim wprowadzenie bardziej szczegółowych przepisów dotyczących ochrony danych osobowych pracowników w kontekście zatrudnienia. W polskim porządku krajowym kwestię tę doprecyzowano w kodeksie pracy, w którym m.in. uregulowano wymogi dotyczące zasad wprowadzania monitoringu pracowników.

Zgodnie z art. 22^2 §1 kodeksu pracy monitoring definiuje się jako "szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu". Brzmienie wyżej wskazanego przepisu wskazuje, że pracodawca może wprowadzić monitoring, gdy jest to niezbędne dla zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić go na szkodę. Pracodawca nie powinien obejmować monitoringiem pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tego typu pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika. Ustawodawca zdecydował się na ograniczenie nadzoru w pewnych przestrzeniach ze względu na ochronę prywatności osób zatrudnionych (Jaśkowski, Maniewska 2025). Co więcej monitoring nie może dotyczyć pomieszczeń udostępnionych

zakładowej organizacji związkowej - od tego zakazu nie ma wyjątków. Takie uregulowanie odzwierciedla zasadę wolności i niezależności związków zawodowych (Jaśkowski, Maniewska 2025). Zgodnie z art. 22^2 §7 kodeksu pracy "nagrania z monitoringu pracodawca może przetwarzać wyłącznie do celów, dla których zostały zebrane, i przechowywać przez okres nie dłuższy niż 3 miesięcy od dnia nagrania". Pracodawcy nie mogą wprowadzać do swoich organizacji tzw. "ukrytego monitoringu". Artykuł 22^2 §7 kodeksu pracy nakłada na pracodawcę obowiązek powiadomienia pracowników o wprowadzeniu tego typu nadzoru nie później niż 2 tygodnie przed jego uruchomieniem. Do obowiązków pracodawcy należy także wskazanie celu, zakresu oraz sposobu zastosowania monitoringu, co wynika z art. 22^2 §6 kodeksu pracy. Ponadto pracodawca musi oznaczyć pomieszczenia i teren monitorowany w sposób widoczny i czytelny (Jaśkowski, Maniewska 2025).

Warto także podkreślić, że w art. 5 RODO określono ogólne zasady przetwarzania danych osobowych tj. zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności. Z kolei przepisy Kodeksu pracy dotyczące szczegółowych kwestii monitoringu w kontekście zatrudnienia są zgodne z zasadami wynikającymi z RODO, które stanowią podstawę dla wprowadzenia takich regulacji. Przykładowo określenie celu tej formy nadzoru jest zgodne z zasadą ograniczenia celu wskazaną w RODO. Z kolei zasada minimalizacji nakazuje pracodawcy zawężenie obszaru monitorowania do niezbędnego zasięgu.

Administrator danych osobowych przetwarzanych na potrzeby monitoringu musi wywiązać się ze swojego obowiązku informacyjnego wobec osoby obserwowanej, co wynika z art. 13 RODO. Ukryty nadzór pracowników to kwestia, która bywa przedmiotem zainteresowania pracodawców. Przepisy RODO, tak jak przepisy kodeksu pracy, nie pozwalają na nieprzekazanie osobom zatrudnionym w danym przedsiębiorstwie, informacji o wprowadzeniu takiej formy kontroli. Zgodnie ze wskazówkami Prezesa Urzędu Ochrony Danych Osobowych stosowanie ukrytych kamer może zostać uznane za nadmiarową formę przetwarzania danych. Co więcej uprawnienia do prowadzenia niejawnego monitorowania mają jedynie służby porządkowe i specjalne prowadzące czynności na podstawie ustaw regulujących ich działalność (Urząd Ochrony Danych Osobowych 2018).

Niejawny monitoring stanowił przedmiot niedawnej decyzji Prezesa Urzędu Ochrony Danych Osobowych. Centrum medyczne nie poinformowało swoich pacjentów i pracowników o wdrożeniu tej formy nadzoru. Z tego powodu została na nie nałożona kara pieniężna w wysokości 687.534,75 zł. Druga kara w kwocie 458.356,50 zł została wymierzona placówce za brak wdrożenia odpowiednich

środków bezpieczeństwa - technicznych i organizacyjnych, które zapobiegłyby ryzyku wycieku danych z kart pamięci urządzeń monitorujących (Urząd Ochrony Danych Osobowych 2025a). Rozstrzygnięcie podkreśla, jak ważna jest transparentność w stosowaniu monitoringu w miejscu pracy. Pracodawca, który nie przestrzega obowiązku dotyczącego informowania pracowników o tym nadzorze, może ponieść tego surowe konsekwencje.

Inną formą nadzoru w miejscu pracy może być monitoring poczty elektronicznej. Aby taka kontrola była legalna musi być to niezbędne dla zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz zapewnienia właściwego użytkowania udostępnionych pracownikowi narzędzi prac. Nakazy informacyjne pracodawcy są tożsame z obowiązkami związanymi z monitoringiem wizyjnym. Stosuje się je odpowiednio do charakteru tych czynności kontrolnych. Wskazać należy, że:

> „pracownicy powinny być jednak wyraźnie poinformowani, czy monitoring dotyczy wyłącznie faktu wysyłania lub odbierania wiadomości, czy też kontrolowana jest również treść wiadomości, co powinno być jednak stosowane wyjątkowo i sporadycznie, jeżeli nie mamy do czynienia z konkretnym podejrzeniem działania niezgodnego z prawem, które samo w sobie niweczy właściwe wykorzystanie służbowego sprzętu służbowego" (Dörre-Kolasa 2024, s. 385).

Europejski Trybunał Praw Człowieka zajmował się kwestią tej formy kontroli w środowisku pracy. Przykładowo w sprawie *Bărbulescu przeciwko Rumunii* podkreślono, że zakaz używania komunikatora do celów prywatnych nie jest równoznaczny z poinformowaniem pracowników monitorowaniu korespondencji (Europejski Trybunał Praw Człowieka 2017).

Trzeba wskazać, że przepisy dotyczące monitoringu poczty elektronicznej stosuje się do innych sposobów nadzoru, niewymienionych w kodeksie pracy. W przedsiębiorstwie może być także stosowany monitoring GPS umieszczony w pojazdach służbowych. Jest to zgodne z prawem, ale również wymaga spełnienia obowiązku informacyjnego wobec pracowników. Nakaz ten obejmuje również powiadomienie osoby zatrudnione o tym, że urządzenie rejestruje wszystkie ruchy wykonywane przez nich w trakcie korzystania z pojazdu (Grupa Robocza art. 29 ds. Ochrony Danych 2017a). Pracodawcy decydują się na wdrożenie takiej formy nadzoru, aby kontrolować tankowania i wydatki na paliwo, czy też w celu kontroli, czy samochód służbowy nie jest wykorzystywany do celów prywatnych. Zgodnie ze stanowiskiem Grupy Roboczej Art. 29 pracodawca nie powinien postrzegać tego typu monitoringu jako urządzenie monitorowania pracowników (Grupa Robocza art. 29 ds. Ochrony Danych 2017a).

Należy zaznaczyć, że wszystkie formy monitoringu łączy to, że mogą być one wspomagane przez sztuczną inteligencję. Zaawansowane algorytmy są w stanie przedstawiać obraz w stanie rzeczywistym, analizować zgromadzone dane, a także przewidywać zachowania pracowników. Osoby, które chcą wdrożyć w swojej organizacji monitoring oparty o sztuczną inteligencję, muszą pamiętać o przestrzeganiu obowiązków wynikających z rozporządzenia AI Act. Przykładowo powinni oni wiedzieć o tym, że zgodnie z art. 5 ust. 1 lit. f. systemy AI przeznaczone do wykorzystania przy rozpoznawaniu emocji w miejscu pracy są zakazaną praktyką. Według wytycznych Komisji Europejskiej dotyczących zakazanych praktyk w zakresie sztucznej inteligencji pojęcie miejsca pracy w kontekście tego zagadnienia należy rozumieć szeroko. Odnosi się ono do każdej fizycznej lub wirtualnej przestrzeni, w której są wykonywane obowiązki wyznaczone przez organizację. Może się ono różnić w zależności od charakteru danej pracy. Jest to niezależne od statusu pracownika, wykonawcy, stażysty, wolontariusza itp. Ponadto pojęcie "miejsca pracy" wskazane w art. 5 ust. 1 lit. f. AI Act należy odnosić także do procesu rekrutacji. Wynika to z faktu, że istnieje wtedy dysproporcja w uprawnieniach stron, a analiza emocji o inwazyjnym charakterze może być stosowana już na etapie zatrudniania (Komisja Europejska 2024b).

Powyższe rozważania wskazują, że pracodawcy planujący wdrożenie monitoringu w swojej organizacji muszą zapewnić zgodność z prawem, informując pracowników o zakresie, celu i sposobie zastosowania monitoringu. Powinni również pamiętać, że wykorzystanie technologii rozpoznawania emocji w miejscu pracy może naruszać prywatność pracowników, co stanowi niedopuszczalną ingerencję w ich sferę osobistą.

Wykorzystywanie sztucznej inteligencji przez pracowników

Sztuczna inteligencja w środowisku pracy to nie tylko spore ułatwienie dla pracodawcy, ale również dla jego pracowników. Systemy AI mogą ułatwiać wykonywanie codziennych żmudnych zadań. Przykładowo znajdują one zastosowanie przy wprowadzaniu dużej ilości danych do systemu, generowania faktur, czy przygotowywania zestawień. Dzięki temu pracownicy mogą skupić się na kreatywnych i bardziej wymagających czynnościach. Ponadto systemy AI bywają wykorzystywane do przygotowywania krótkich postów na portale społecznościowe, czy sprawdzania dokumentów pod kątem błędów w pisowni. Jednakże trzeba podkreślić, że pracownicy nie powinni korzystać z narzędzi opartych o sztuczną inteligencję bez wiedzy pracodawcy. Niewłaściwe użycie sztucznej inteligencji

w miejscu pracy może wiązać się ze sporym ryzykiem. Największe zagrożenie może wynikać z korzystania przez pracowników z generatywnej sztucznej inteligencji, która służy do tworzenia nowych treści, takich jak obrazy czy teksty, za pomocą specjalnych algorytmów i modeli opartych na nauce. Najpopularniejsze narzędzia tego typu to np. *ChatGPT, Microsoft Copilot* czy *Midjourney*. Wprowadzanie do tego typu modeli treści prywatnych czy danych osobowych stwarza ryzyko powielania tych informacji w wynikach innych osób. Może to w sposób niezamierzony ujawnić wrażliwe dane poszczególnych osób. Co więcej tworzenie promptów, które są wulgarne, agresywne lub dyskryminujące wobec jakiejkolwiek osoby lub grupy społecznej, może prowadzić do generowania stronniczych wyników.

Wobec tego pracodawcy powinni zadbać o to, aby pracownicy wiedzieli, jak bezpiecznie korzystać ze sztucznej inteligencji. Należy informować ich o takich kwestiach jak ograniczenie wprowadzania danych do AI, unikanie wprowadzania informacji poufnych oraz danych, które mogą naruszać prawo. Pracownicy nie powinni również wykorzystywać służbowych narzędzi do celów prywatnych. Przedsiębiorstwa mogą organizować cykliczne szkolenia na temat praktyk pracy z systemami AI oraz potencjalnych zagrożeń, aby podkreślić znaczenie odpowiedniego ich wykorzystywania. Warto także rozważyć stworzenie wewnętrznej polityki używania systemów AI.

PODSUMOWANIE

Podsumowując, w artykule przedstawiono relację między regulacjami dotyczącymi ochrony danych osobowych a przepisami rozporządzenia AI Act, które mają na celu uregulowanie stosowania systemów sztucznej inteligencji na terenie Unii Europejskiej. Analiza koncentruje się na trudnościach związanych z wdrożeniem systemów AI w środowisku pracy, zwłaszcza w kontekście ich wpływu na organizację pracy oraz interakcje z pracownikami. Niewątpliwie, wykorzystanie tych systemów budzi duże zainteresowanie ze strony pracodawców i pracowników ze względu na potencjał poprawy wydajności, rentowności oraz redukcji kosztów operacyjnych.

Należy pamiętać, że pomimo licznych zalet, wdrożenie systemów AI wiąże się z wyzwaniami, które pracodawcy muszą uwzględnić, takimi jak: dostosowanie się do wymogów dotyczących transparentności, monitorowania oraz minimalizowania ryzyk, które stanowią fundament AI Act. Nie jest to proste zadanie, ponieważ analiza przepisów AI Act napotyka trudności. Akt ten dotyczy systemów, których

działanie nie zawsze jest w pełni jasne i które nie mogą być całkowicie kontrolowane. Z tego względu, mimo starań prawodawcy, AI Act może nie spełniać swojego celu, jakim jest zminimalizowanie ryzyka związanego z używaniem systemów AI. Dopóki nie będzie możliwa pełna kontrola nad funkcjonowaniem systemów AI, zapewnienie bezpieczeństwa użytkowników oraz skutecznego monitorowania ryzyk związanych z ich stosowaniem pozostanie istotnym problemem.

W kontekście przyszłych zmian regulacji dotyczących sztucznej inteligencji, prawodawca powinien uwzględniać stopień "czarnej skrzynki" systemów AI, szczególnie w zakresie ujawniania algorytmów i metodologii ich funkcjonowania. Z uwagi na to, że wiele systemów AI działa w sposób trudny do pełnego zrozumienia i przewidzenia, istnieje potrzeba wprowadzenia bardziej szczegółowych wymogów dotyczących przejrzystości, które pozwolą użytkownikom na lepszą weryfikację ich wyników.

BIBLIOGRAFIA

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. U. UE. L. z 2016 r. Nr 119, str. 1 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 (akt w sprawie sztucznej inteligencji) Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. 1974 nr 24 poz. 141).

Literatura

Barzycka-Banaszczyk, M.

2025 Wykładnia oświadczeń woli, w: Prawo pracy wobec nowych technologii, red. M. Gersdorf, E. Maniewska, Warszawa.

Czaplińska, M., Sakowska-Baryła, M.
2021 Zgoda na przetwarzanie danych osobowych i profilowanie. Uwagi na tle wyroku Trybunału Sprawiedliwości UE z dnia 1 października 2019 r. w sprawie C-673/17, Studia Prawno-Ekonomiczne, T. CXXI.

Czerniawski, M.
2018 RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz.

Dobosz, K.
2022 Akt o sztucznej inteligencji w przestrzeni unijnego prawa regulacyjnego, [w:] Nauka prawa a praktyka prawnicza. Księga Jubileuszowa z okazji czterdziestolecia Okręgowej Izby Radców Prawnych w Krakowie, red. M. Araszkiewicz, M. Krok, M. Sala-Szczypiński, Kraków.

Dolniak, P., Kuźma, T., Ludwiński, A., Wasik, K.
2024 Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami, Warszawa.

Dörre-Kolasa, D.
2024 Prawo pracy, red. K. Baran, Warszawa.

Fajgielski, P.
2022 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. II, Warszawa.

Flisak, D.
2024 Akt w sprawie sztucznej inteligencji, komentarz praktyczny.

Gudowska-Natanek, E., Kuca, G.
2024 Prawo ochrony danych osobowych i prawo do informacji publicznej, Warszawa.

Jaśkowski, K., Maniewska, E.
2025 Komentarz aktualizowany do Kodeksu pracy.

Jędrzejczak, M.
2024 Protection of Personal Data Processed in Artificial Intelligence Systems, Gdańskie Studia Prawnicze, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk.

Konarski, X.
2024 Aktualności - dane osobowe i prywatność. Wzajemna relacja Aktu w sprawie sztucznej inteligencji oraz RODO, Prawo Nowych Technologii, nr 2.

Kozłowski, J.
2024 Akt o w sprawie sztucznej inteligencji – charakterystyka unijnej regulacji opartej na ryzyku, EPS, nr 12.

Małobęcka-Szwast, I.
2025 Wykorzystanie systemów AI w rekrutacji – wyzwania dla ochrony danych osobowych, w: Prawo pracy wobec nowych technologii, red. M. Gersdorf, E. Maniewska, Warszawa.

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

Rzymowski, J.
2024 Poziomy ryzyka na gruncie RODO, PPP, nr 5.

Spałek, D., Rzymowski, J.
2024 Jak nie stosować AI Act na podstawie definicji systemu sztucznej inteligencji, Prawo Nowych Technologii, nr 2.

Stępień, A.
2024 Zasada ne bis in idem a nakładanie administracyjnych kar pieniężnych na gruncie RODO i AI Act, Monitor Prawniczy, Dodatek do nr 11/2024.

Szymielewicz, K., Walkowiak, A.
2014 Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem, Monitor Prawniczy.

Tlatlik, J.
2022 Pojęcie dyskryminacji w prawie Unii Europejskiej, w: Zakaz dyskryminacji na etapie nawiązywania stosunku pracy, Warszawa.

Zalewski, T.
2020 Rozdział I. Definicja sztucznej inteligencji, w: Prawo sztucznej inteligencji, red. L. Lai, M. Świerczyński, Warszawa, Wydawnictwo C.H. Beck.

2025 Wokół definicji systemu AI w unijnym rozporządzeniu w sprawie sztucznej inteligencji, Prawo Nowych Technologii, nr 4, Warszawa.

Orzecznictwo

Urząd Ochrony Danych Osobowych
2025 Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 stycznia 2025 r. (DKN.5131.4.2024)

Europejski Trybunał Praw Człowieka
2017 Wyrok Europejskiego Trybunału Praw Człowieka z dnia 5 września 2017 r., Skarga nr 61496/08

Wytyczne:

Grupa Robocza art. 29 ds. Ochrony Danych
2017a Opinia 2/2017 na temat przetwarzania danych w miejscu pracy, Pobrane z: https://archiwum.giodo.gov.pl/pl/1520344/10395 (26.02.2025)
2017b Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, Pobrane z: https://www.uodo.gov.pl/data/filemanager_pl/908.pdf (26.02.2025)

Komisja Europejska
2024a Wytyczne dotyczące zakazanych praktyk w zakresie sztucznej inteligencji zgodnie z rozporządzeniem (UE) 2024/1689 (ustawa o sztucznej inteligencji), Pobrane z: https://digital-strategy.ec.europa.eu/pl/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act (26.02.2025)
2024b Wytyczne Komisji w sprawie definicji systemu sztucznej inteligencji ustanowionego rozporządzeniem (UE) 2024/1689 (ustawa o sztucznej inteligencji), Pobrane z: https://digital-strategy.ec.europa.eu/pl/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (26.02.2025)

AI Act, Pobrane z: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (02.04.2025)

Urząd Ochrony Danych Osobowych
2025b Poradnik Urzędu Ochrony Danych Osobowych dotyczący naruszeń ochrony danych osobowych (Pobrane z: https://uodo.gov.pl/pl/138/3561) (24.02.2025)

2018 Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, Pobrane z: https://uodo.gov.pl/data/filemanager_pl/1200.pdf (24.02.2025)

Źródła internetowe

Ffsolutions,
2024 Jak automatyzacja ułatwia proces rekrutacji, Pobrane z: https://ffsolutions.pl/rekrutacja-pracownikow-jak-automatyzacja-ulatwia-proces-rekrutacji/ (26.02.2025)

Konarski, X.
2024 Wzajemna relacja RODO i Aktu w sprawie sztucznej inteligencji. 10 najważniejszych informacji. Pobrane z: https://www.traple.pl/wzajemna-relacja-rodo-i-aktu-w-sprawie-sztucznej-inteligencji-10-najwazniejszych-informacji-2/ (26.02.2025)

Media PKO Bank Polski
2019 PKO Bank Polski i Quantum CX policzą uśmiechy klientów, Pobrane z: https://media.pkobp.pl/70981-pko-bank-polski-i-quantum-cx-policza-usmiechy-klientow (24.02.2025)

Money,
2018 Nowy sposób Amazona na kontrolę pracowników. Elektroniczna opaska, Pobrane z: https://www.money.pl/gospodarka/wiadomosci/artykul/nowy-sposob-amazona-na-kontrole-pracownikow,24,0,2397464.html (24.02.2025)

Słownik Języka Polskiego PWN, maszyna
https://sjp.pwn.pl/slowniki/maszyna.html (01.04.2025)

Techtarget,
2024 What is machine learning bias (AI bias)? https://www.techtarget.com/searchenterpriseai/definition/machine-learning-bias-algorithm-bias-or-AI-bias (31.03.2025)

ARTIFICIAL INTELLIGENCE IN THE WORK ENVIRONMENT IN THE AGE OF GDPR AND AI ACT

Abstract: The increasing use of artificial intelligence in the workplace raises new legal and ethical challenges, particularly in the area of personal data protection. Artificial intelligence is used to support recruitment processes, monitor employees, and automate routine tasks. The GDPR, which regulates the processing of personal data, requires compliance with transparency and security standards, of which employers should be aware. Additionally, the EU AI Act introduces new obligations for various entities involved in the implementation and use of AI systems. The aim of the chapter is to identify the key legal challenges arising from the deployment of AI tools by employers and to analyze their impact on how work is performed. The analysis shows that the lack of full control over the functioning of AI systems makes it impossible to ensure effective protection against the potentially negative consequences of their use in the workplace.

Key words: artificial intelligence, labour law, personal data protection, AI Act, workplace ethics

AGNIESZKA SZYMCZAK

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

OCHRONA DANYCH OSOBOWYCH W ERZE AI – WYZWANIA PRAWNE I TECHNOLOGICZNE

Streszczenie: Artykuł podejmuje analizę zbiegu regulacji RODO i AI Act w kontekście ochrony danych osobowych w dobie dynamicznego rozwoju systemów sztucznej inteligencji. Punktem wyjścia jest omówienie kluczowych wyzwań prawnych i technologicznych związanych z przetwarzaniem danych przez systemy AI, ze szczególnym uwzględnieniem obowiązków dostawców wynikających z AI Act (2024/1689). Autorzy omawiają zasady transparentności, ocenę ryzyka (DPIA), minimalizację danych, nadzór człowieka nad automatycznymi decyzjami oraz wymogi certyfikacyjne jako filary nowoczesnej ochrony prywatności. Zwrócono uwagę na konflikty interpretacyjne między AI Act a RODO oraz ryzyko kumulacji sankcji. Artykuł kończy się postulatami harmonizacji przepisów, wzmacniania mechanizmów compliance oraz edukacji decydentów i użytkowników. W konkluzji podkreślono, że skuteczna ochrona danych w erze AI wymaga synergii między technologią a elastycznym, lecz precyzyjnym systemem regulacyjnym.

Słowa kluczowe: RODO, AI Act, ochrona danych osobowych, systemy sztucznej inteligencji,

1. WPROWADZENIE – KONTEKST OCHRONY DANYCH W ERZE AI

Ochrona danych osobowych stanowi proces o złożonych uwarunkowaniach, w którym administrator danych musi polegać na rygorystycznych regułach wyznaczonych przez RODO oraz krajowe przepisy, takie jak ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. W ostatnich latach obserwujemy jednak dynamiczny rozwój technologii sztucznej inteligencji, który przynosi ze sobą nowe wyzwania zarówno o charakterze technologicznym, jak i prawnym. W odpowiedzi na te wyzwania, do grona aktów prawnych regulujących kwestie

przetwarzania danych osobowych dołączyło 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), znane jako AI Act (Dz.U.UE.L.2024.1689 z dnia 2024.07.12.). Metodologia badawcza oparta została na metodzie dogmatyczno-prawnej koncentrującej się na analizie literatury przedmiotu, studium przypadku oraz porównaniu regulacji, co pozwala na kompleksowe ujęcie omawianych zagadnień.

Znaczenie ochrony danych osobowych w erze AI jest szczególnie widoczne w kontekście rosnącej roli tych danych w działalności reklamowej oraz w zagrożeniach związanych z kradzieżą tożsamości czy innymi przestępstwami. Dlatego analiza wyzwań technologicznych i prawnych, wynikających z implementacji AI Act, jest kluczowa dla zrozumienia, jak nowa regulacja może przyczynić się do zwiększenia bezpieczeństwa i ochrony praw osób fizycznych. Niniejszy wywód podejmuje próbę omówienia tych zagadnień, koncentrując się na interakcji między przepisami AI Act a tradycyjnymi zasadami ochrony danych osobowych.

2. AI ACT W PRAKTYCE – KLUCZOWE WYMOGI DOTYCZĄCE OCHRONY DANYCH

Geneza AI Act sięga okresu poprzedzającego gwałtowną popularyzację narzędzi takich jak *ChatGPT*. Unijny prawodawca, zainspirowany rosnącym zainteresowaniem zarówno środowisk naukowych, jak i opinii publicznej, rozpoczął prace legislacyjne już na długo przed 2023 rokiem. Inicjatywy takie jak rezolucje Parlamentu Europejskiego oraz publikacje Komisji stanowiły pierwsze kroki w kierunku stworzenia kompleksowych regulacji, które miały nie tylko przeciwdziałać potencjalnym zagrożeniom, ale również umożliwiać elastyczną adaptację przepisów do dynamicznie zmieniających się technologii (Kozłowski 2024, s. 20). Wśród zalet AI Act należy wymienić jego innowacyjne, oparte na analizie ryzyka podejście. Dzięki temu rozwiązaniu możliwe jest precyzyjne wyodrębnienie systemów o wysokim potencjale negatywnego wpływu na prawa podstawowe oraz bezpieczeństwo użytkowników. Nowa regulacja umożliwia wdrażanie specjalistycznych środków nadzoru oraz mechanizmów kontroli, co przyczynia się do budowania zaufania do technologii AI. Jednakże, metoda ta nie jest pozbawiona wad. Wśród najpoważniejszych zastrzeżeń wskazuje się trudności

związane z jednoznacznym określeniem kategorii ryzyka oraz interpretacją niektórych kluczowych pojęć, co może skutkować rozbieżnościami w praktyce stosowania przepisów. Takie niedoskonałości wymagają dalszych usprawnień oraz interpretacji, aby zapewnić spójność całego systemu regulacyjnego (Róg-Dyrda, Wierzbowski 2022).

2.1 TRANSPARENTNOŚĆ PRZETWARZANIA DANYCH

Transparentność przetwarzania danych w kontekście systemów AI polega na udostępnianiu jasnych informacji o sposobie przetwarzania danych oraz mechanizmach podejmowania decyzji przez algorytmy. Oznacza to, że zarówno użytkownicy, jak i organy regulacyjne mają możliwość zrozumienia i monitorowania procesów operacyjnych, co jest kluczowe dla ochrony danych osobowych oraz budowania zaufania do technologii (Flisak 2024).

Regulacje AI Act nakładają na dostawców systemów obowiązek informowania użytkowników o zastosowaniu AI (art. 52) oraz zapewnienia przejrzystości działania systemów wysokiego ryzyka, co umożliwia ocenę zgodności algorytmów z obowiązującymi przepisami (art. 13). W praktyce wymaga to sporządzania szczegółowej dokumentacji technicznej oraz regularnych audytów, które mają potwierdzić, że systemy działają zgodnie z wymogami prawnymi. Mechanizmy te są szczególnie istotne w systemach wykorzystujących zdalną identyfikację biometryczną czy deepfake, gdzie ryzyko nadużyć jest szczególnie wysokie (Jagielski i in. 2023). Pomimo licznych mechanizmów zapewniających transparentność, wdrażanie tych rozwiązań napotyka na wyzwania, takie jak konflikt między obowiązkiem ujawniania logiki działania a ochroną tajemnic handlowych oraz trudności techniczne w wyjaśnianiu złożonych modeli, zwanych „czarnymi skrzynkami". Konieczne jest wypracowanie równowagi między przejrzystością a ochroną prywatności, co stanowi fundament etycznej i bezpiecznej implementacji systemów AI.

2.2 OCENA RYZYKA I DPIA

Ocena ryzyka w kontekście systemów sztucznej inteligencji (AI) to proces systematycznej analizy potencjalnych zagrożeń, które mogą naruszać prawa i wolności osób fizycznych. W praktyce oznacza to identyfikację oraz ocenę możliwości wystąpienia szkód wynikających z zastosowania AI oraz wdrożenie środków, które pozwolą zminimalizować te zagrożenia. Kluczowe znaczenie ma to nie tylko dla bezpieczeństwa użytkowników, ale również dla ochrony danych osobowych,

co umożliwia podjęcie działań korygujących już na etapie projektowania i wdrażania systemu (Róg-Dyrda, Wierzbowski 2022).

AI Act wprowadza trójstopniową klasyfikację systemów AI, opartą na poziomie ryzyka, jakie mogą one generować. Do kategorii systemów niedopuszczalnego ryzyka zalicza się rozwiązania wykorzystujące techniki podprogowe czy systemy scoringu społecznego, które ze względu na swój potencjalnie szkodliwy wpływ na wolności jednostki, są zakazane. Systemy wysokiego ryzyka, stosowane m.in. w sektorach medycznym i finansowym, muszą spełniać rygorystyczne wymogi dotyczące zarządzania ryzykiem, w tym przeprowadzenia oceny skutków dla ochrony danych (DPIA). Z kolei systemy o ograniczonym lub minimalnym ryzyku wymagają jedynie podstawowych obowiązków informacyjnych, co umożliwia ich swobodne stosowanie przy zachowaniu minimalnego poziomu zagrożeń (Flisak 2024).

Wdrożenie systemów AI wysokiego ryzyka nakłada na dostawców obowiązek przeprowadzenia kompleksowej oceny ryzyka oraz DPIA, czyli oceny skutków przetwarzania danych dla praw osób fizycznych. Proces ten obejmuje zarówno identyfikację zagrożeń, jak i wdrożenie odpowiednich środków technicznych i organizacyjnych, które mają na celu ograniczenie potencjalnych szkód. Równocześnie, zgodność z AI Act nie zwalnia podmiotów z obowiązków wynikających z RODO, co tworzy komplementarne ramy prawne w zakresie ochrony danych osobowych (Jagielski i in. 2023).

Praktyczne zastosowanie oceny ryzyka i DPIA jest szczególnie widoczne przy wdrażaniu systemów AI w procesach rekrutacyjnych czy zarządzaniu danymi medycznymi, gdzie niedostateczna kontrola może prowadzić do naruszenia praw jednostki oraz narażenia organizacji na poważne sankcje. W takich przypadkach kluczowe jest nie tylko techniczne zarządzanie ryzykiem, ale również ciągły nadzór ludzki oraz uwzględnienie aspektów etycznych, które pozwalają na monitorowanie działania systemów i wdrażanie korekt w razie wystąpienia nieprzewidzianych zagrożeń (Małobęcka-Szwast 2025).

2.3 OCHRONA DANYCH JUŻ NA ETAPIE PROJEKTOWANIA

Ochrona danych osobowych już na etapie projektowania to podejście, które zakłada wdrażanie zabezpieczeń i mechanizmów minimalizujących ryzyko naruszenia prywatności już podczas fazy tworzenia systemów AI. W ramach regulacji AI Act projektanci systemów muszą uwzględniać aspekty ochrony danych poprzez implementację środków technicznych i organizacyjnych, takich jak ograniczenie

zakresu przetwarzanych danych, mechanizmy audytu oraz systemy monitoringu, które pomagają zidentyfikować i wyeliminować potencjalne zagrożenia dla praw i wolności osób fizycznych. Taka strategia, znana jako privacy by design, umożliwia nie tylko spełnienie wymogów prawnych, ale również budowanie zaufania użytkowników do technologii, gdyż już na wczesnym etapie rozwoju systemu kładzie się nacisk na integralność przetwarzanych danych osobowych. (Kozłowski 2024, s. 22; Flisak 2024; Jagielski i in. 2023).

2.4 NADZÓR CZŁOWIEKA NAD AUTOMATYCZNYMI DECYZJAMI

AI Act kładzie nacisk na zachowanie kontroli ludzkiej nad decyzjami podejmowanymi przez systemy sztucznej inteligencji. Mimo automatyzacji procesów decyzyjnych, dostawcy i operatorzy systemów są zobowiązani do wdrożenia mechanizmów umożliwiających ciągły nadzór, który pozwala na interwencję w razie wykrycia błędów lub nadużyć. Taki model, czyli „*human-in-the-loop*", gwarantuje, że logika działania algorytmów jest monitorowana, a decyzje są sprawdzalne przez odpowiedzialnych operatorów, co umożliwia szybkie korygowanie potencjalnych zagrożeń dla praw i wolności osób fizycznych. Rozwiązanie to wzmacnia ochronę danych osobowych, wspierając jednocześnie przestrzeganie zasad wynikających z RODO (Stefanicki 2023, s. 7-8).

2.5 CERTYFIKACJA I MECHANIZMY COMPLIANCE

Certyfikacja i mechanizmy compliance stanowią fundament budowania zaufania zarówno do systemów sztucznej inteligencji, jak i do sposobów przetwarzania danych osobowych. Certyfikacja polega na przeprowadzeniu niezależnej oceny, która ma na celu potwierdzenie, że dany produkt czy system AI spełnia ustalone normy techniczne i prawne, w tym wymogi określone przez AI Act (m.in. art. 42 i 44) oraz RODO (art. 42). Proces ten, często realizowany przez uprawnione jednostki certyfikujące, umożliwia wykrycie potencjalnych nieprawidłowości i zapewnia, że systemy wysokiego ryzyka są wdrażane zgodnie z najwyższymi standardami ochrony danych. Mechanizmy compliance natomiast obejmują wewnętrzne procedury i systemy kontrolne wdrażane przez organizacje, które mają na celu stałe monitorowanie przestrzegania obowiązujących regulacji. Dzięki nim możliwe jest szybkie reagowanie na ewentualne naruszenia oraz wprowadzanie korekt, co minimalizuje ryzyko naruszenia praw jednostki wynikających z przetwarzania danych osobowych. W rezultacie, certyfikacja oraz

mechanizmy compliance nie tylko wspierają ochronę danych osobowych poprzez systematyczną weryfikację zgodności z przepisami, ale także przyczyniają się do budowania pewności prawnej i zwiększenia konkurencyjności na rynku nowych technologii (Kozłowski 2024, s. 22).

2.6 MINIMALIZACJA DANYCH I ZAPEWNIENIE ICH JAKOŚCI

Minimalizacja danych i zapewnienie ich jakości to kluczowe filary współczesnej ochrony informacji, których celem jest nie tylko zabezpieczenie prywatności jednostek, ale również podniesienie wiarygodności systemów opartych na sztucznej inteligencji. Zasada minimalizacji danych, wyrażona w art. 5 lit. c RODO, nakłada obowiązek, aby przetwarzane dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia określonych celów. Innymi słowy, organizacje mają obowiązek zbierania jedynie takich informacji, które są konieczne, co minimalizuje ryzyko nieuprawnionego wykorzystania nadmiarowych danych (Fajgielski 2022).

W kontekście unijnej regulacji dotyczącej sztucznej inteligencji, AI Act podchodzi do kwestii minimalizacji danych na dwóch płaszczyznach. Art. 10 AI Act zobowiązuje dostawców systemów AI do implementowania rozwiązań umożliwiających ograniczenie zbierania danych do absolutnego minimum, które jest niezbędne dla realizacji zamierzonych funkcji systemu. Natomiast art. 12 kładzie szczególny nacisk na jakość przetwarzanych danych – systemy muszą być zasilane danymi, które są nie tylko ograniczone ilościowo, ale przede wszystkim charakteryzują się wysoką dokładnością, aktualnością i reprezentatywnością. Takie podejście ma na celu ograniczenie ryzyka błędnych interpretacji, uprzedzeń oraz niezamierzonych konsekwencji wynikających z niewłaściwej jakości danych.

Integracja zasad minimalizacji danych z wymogami dotyczącymi jakości informacji tworzy spójny model ochrony, w którym zbieranie danych jest ściśle powiązane z koniecznością utrzymania ich najwyższych standardów. Dzięki temu nie tylko chroniona jest prywatność osób fizycznych, ale również zwiększa się efektywność i wiarygodność systemów AI, co w konsekwencji buduje zaufanie zarówno użytkowników, jak i instytucji nadzorczych (Kozłowski 2024, s. 23).

3. WYZWANIA TECHNOLOGICZNE W SYSTEMACH AI

Systemy sztucznej inteligencji, choć stanowią przełom w analizie i wykorzystaniu danych, niosą ze sobą szereg wyzwań technologicznych, które mają

bezpośredni wpływ na ochronę danych osobowych. Jednym z głównych problemów technicznych jest przetwarzanie ogromnych zbiorów danych – wymagają one nie tylko zaawansowanych narzędzi do ich gromadzenia i analizy, ale także skutecznych metod integracji oraz skalowania, by operacje odbywały się w sposób bezpieczny i efektywny. W ramach wyzwań technologicznych warto wyróżnić kilka kluczowych zagadnień tj. zarządzanie dużymi zbiorami danych, pseudonimizacja, bezpieczeństwo danych, zapewnienie ich jakości oraz trudności jakie wiążą się z automatyzacją i algorytmicznym podejmowaniem decyzji.

Zarządzanie dużymi zbiorami danych polega na stosowaniu systemów umożliwiających efektywne magazynowanie, sortowanie oraz analizę ogromnych ilości informacji, co minimalizuje ryzyko utraty lub niewłaściwej interpretacji danych. Pseudonimizacja natomiast jest to technika ochrony danych, w której identyfikatory umożliwiające bezpośrednią identyfikację osoby są zastępowane pseudonimami, co pozwala na zachowanie funkcjonalności analitycznej systemów AI przy jednoczesnym zwiększeniu poziomu ochrony prywatności (Tlatlik 2022). Z kolei bezpieczeństwo danych wymaga wdrożenia kompleksowych rozwiązań zabezpieczających, takich jak systemy szyfrowania czy mechanizmy monitorujące, które chronią przed nieautoryzowanym dostępem oraz atakami cybernetycznymi. W kontekście wyzwań technologicznych związanych z systemami AI istotne jest zapewnienie jakości danych. Oznacza to utrzymanie wysokiej rzetelności, aktualności i kompletności zbieranych informacji. Jakość danych jest niezbędna dla prawidłowego funkcjonowania algorytmów, gdyż niskiej jakości dane mogą prowadzić do błędnych wyników i nieadekwatnych decyzji. Wiele wyzwań technologicznych wiąże się również z automatyzacją i algorytmicznym podejmowaniem decyzji. Automatyzacja zwiększa efektywność operacyjną, ale jednocześnie rodzi problemy z przejrzystością procesów decyzyjnych, utrudniając identyfikację potencjalnych błędów czy uprzedzeń w działaniu algorytmów (Prabucki i Grajewski 2024). W odniesieniu do przepisów, AI Act podkreśla konieczność wdrożenia rozwiązań minimalizujących ryzyko związane z przetwarzaniem danych przez systemy AI, a RODO – poprzez zasadę ograniczenia przetwarzanych informacji – wskazuje, że gromadzone dane muszą być adekwatne i niezbędne do realizacji określonych celów. Integracja tych podejść ma na celu nie tylko zabezpieczenie praw osób, ale także budowanie zaufania do technologii, która operuje na coraz większych i bardziej złożonych zbiorach danych (Kozłowski 2024, s. 24).

4. WYZWANIA PRAWNE I REGULACYJNE

Implementacja AI Act napotyka szereg problemów prawnych, wynikających zarówno z dynamicznego rozwoju technologii, jak i z niejasności interpretacyjnych przepisów. Po pierwsze, elastyczność regulacji musi równoważyć precyzję norm, co skutkuje sporami interpretacyjnymi i trudnościami w określeniu zakresu odpowiedzialności podmiotów stosujących systemy AI. Dodatkowo, nakładające się obowiązki wynikające z AI Act oraz RODO mogą prowadzić do ryzyka podwójnego nakładania sankcji, co stwarza niepewność prawną oraz zwiększa obciążenia regulacyjne dla przedsiębiorstw działających w obszarze nowych technologii. Kwestia odpowiedzialności w kontekście równoczesnego stosowania obu aktów jest szczególnie złożona – trudność polega na jednoznacznym określeniu, czy i w jakim zakresie sankcje powinny być wymierzane na podstawie AI Act, RODO czy obu tych instrumentów jednocześnie. W związku z tym, kluczowe znaczenie ma wypracowanie spójnych mechanizmów prawnych, które pozwolą na uniknięcie dublowania kar, jednocześnie zapewniając skuteczną ochronę danych osobowych.

Rola organów nadzoru, takich jak krajowe instytucje ochrony danych (np. Prezes UODO) oraz europejskie struktury koordynacyjne (EROD), jest nieoceniona w procesie wdrażania nowych regulacji. Organy te nie tylko monitorują przestrzeganie przepisów, ale również pełnią funkcję doradczą dla podmiotów rynkowych, ułatwiając interpretację norm oraz koordynując działania na poziomie międzynarodowym, co jest kluczowe w obliczu globalnego przepływu danych (Makowski 2018).

Międzynarodowy transfer danych w erze AI stanowi kolejne wyzwanie – globalny charakter systemów opartych na sztucznej inteligencji powoduje, że dane osobowe często przekraczają granice państw. Różnice w systemach prawniczych i standardach ochrony danych poza obszarem UE mogą prowadzić do niejednolitych rozwiązań, co utrudnia zapewnienie jednolitej ochrony i wymusza ciągłą współpracę między organami regulacyjnymi.

Takie wyzwania prawne i regulacyjne wskazują na konieczność dalszej harmonizacji przepisów oraz wzmożonej koordynacji działań między państwami członkowskimi, aby skutecznie chronić dane osobowe w dobie rozwoju technologii AI (Kozłowski 2024, s. 24).

5. PRZYSZŁOŚĆ OCHRONY DANYCH W ERZE AI – REKOMENDACJE I PERSPEKTYWY

Przyszłość ochrony danych w erze AI będzie kształtowana przez dynamiczny rozwój zarówno regulacji, jak i technologii, co otwiera nowe możliwości, ale jednocześnie stawia przed ustawodawcami i przedsiębiorstwami szereg wyzwań. Prognozy wskazują, że ramy prawne – w szczególności AI Act – będą stopniowo dostosowywane do szybko zmieniającego się krajobrazu technologicznego. Możliwe scenariusze implementacji obejmują zarówno model etapowego wdrażania obowiązkowych standardów, jak i hybrydowy system, w którym podstawowe normy uzupełniane są dobrowolnymi kodeksami postępowania, umożliwiając elastyczność i adaptację do specyfiki poszczególnych sektorów gospodarki (Stefanicki 2023, s. 9-10).

W kontekście rekomendacji, przedsiębiorstwa powinny zainwestować w rozwój systemów zarządzania ryzykiem oraz w szkolenia z zakresu ochrony danych, co pozwoli na bieżące monitorowanie zgodności z regulacjami. Równocześnie organy nadzoru, takie jak Prezes UODO i EROD, powinny intensyfikować współpracę międzynarodową i wymianę doświadczeń, aby wypracować spójne standardy interpretacyjne i egzekucyjne. Kluczowym elementem strategii ochrony danych jest także edukacja – zarówno użytkowników, jak i decydentów – w zakresie zagadnień prawnych i technologicznych, co przyczyni się do budowania zaufania i zwiększenia efektywności systemów AI.

W rezultacie, przyszłość ochrony danych w erze AI będzie zależała od synergii pomiędzy innowacyjnymi rozwiązaniami technologicznymi a elastycznym, aczkolwiek precyzyjnym systemem regulacji, który z jednej strony umożliwi rozwój nowych technologii, a z drugiej skutecznie zabezpieczy prawa jednostek (Kozłowski 2024, s. 24).

6. PODSUMOWANIE I WNIOSKI

Uchwalenie AI Act miało istotny wpływ na ochronę danych osobowych w Unii Europejskiej. Wprowadzenie obowiązkowych ocen skutków dla praw podstawowych oraz wdrożenie rygorystycznych procedur analizy ryzyka umożliwiło podniesienie standardów ochrony prywatności. Nowa regulacja, ściśle powiązana z wymaganiami RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz.U.UE.L.2016.119.1 z dnia 2016.05.04.), zmusza podmioty wykorzystujące systemy AI do przestrzegania wysokich norm bezpieczeństwa, co przyczynia się do lepszej ochrony danych osobowych obywateli. W rezultacie, AI Act stanowi ważny element unijnego systemu ochrony praw podstawowych, choć nadal pozostaje obszarem, w którym dalsze modyfikacje legislacyjne mogą być konieczne, aby w pełni zharmonizować przepisy dotyczące przetwarzania danych (Kozłowski 2024, s. 25).

BIBLIOGRAFIA

Fajgielski, P.
2022 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. II, Warszawa, art. 5.

Flisak, D.
2024 Akt w sprawie sztucznej inteligencji, LEX/el. (dostęp 2025-03-02 13:17).

Jagielski, M.
2023 Prawo sztucznej inteligencji i nowych technologii 3, red. B. Fischer et al., Warszawa.

Kozłowski, J.
2024 Akt w sprawie sztucznej inteligencji w praktyce – charakterystyka unijnej regulacji opartej na ryzyku, Europejski Przegląd Sądowy, nr 12.

Makowski, P.
2018 RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa, art. 64.

Małobęcka-Szwast, I.
2025 DPIA, w: Prawo pracy wobec nowych technologii, red. M. Gersdorf, E. Maniewska, Warszawa.

Prabucki, R. T., Grajewski, O.
2024 Procedura ochrony przechowywanych lub przekazywanych danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, LEX.

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

Stefanicki, R.
2023 Sztuczna inteligencja tworzona przez człowieka, ukierunkowana na osobę ludzką i przez nią kontrolowana, Przegląd Prawa Handlowego, nr 1, s. 4–15.

Tlatlik, J.
2022 Pseudonimizacja danych osobowych, w: Zakaz dyskryminacji na etapie nawiązywania stosunku pracy, Warszawa.

PERSONAL DATA PROTECTION IN THE AI ERA – LEGAL AND TECHNOLOGICAL CHALLENGES

Abstract: The chapter explores the intersection of the GDPR and the AI Act in the context of personal data protection amidst the rapid development of artificial intelligence systems. It begins with an analysis of key legal and technological challenges arising from data processing in AI systems, focusing on the obligations introduced by Regulation (EU) 2024/1689 (AI Act). The study discusses core concepts such as transparency, risk assessment (DPIA), data minimization, human oversight of automated decisions, and certification requirements as essential pillars of modern data protection. Attention is drawn to interpretative conflicts between the AI Act and the GDPR and the risk of overlapping sanctions. The chapter concludes with recommendations for regulatory harmonization, strengthening compliance mechanisms, and increasing stakeholder education. Ultimately, it emphasizes that effective data protection in the AI era depends on a synergy between innovation and a flexible yet coherent legal framework.

Key words: GDPR, AI Act, personal data protection, artificial intelligence systems,

KINGA PARCHEM

WYŻSZA SZKOŁA ADMINISTRACJI I BIZNESU
IM. EUGENIUSZA KWIATKOWSKIEGO W GDYNI

BEZPIECZEŃSTWO DANYCH GENETYCZNYCH W POLSKIM PORZĄDKU PRAWNYM

Streszczenie: Rozwój technologii wspiera dynamiczny postęp w badaniach genetycznych, co jednocześnie zwiększa konieczność skutecznej ochrony danych genetycznych, mający na celu przeciwdziałanie ryzyku naruszenia prywatności i potencjalnej dyskryminacji. Celem niniejszego rozdziału jest ukazanie kluczowych wyzwań związanych z ochroną danych genetycznych w polskim porządku prawnym, ze szczególnym uwzględnieniem luk prawnych i wynikających z nich ryzyk. Dane genetyczne wymagają szczególnej ochrony ze względu na ich unikalny charakter i potencjalne ryzyko naruszenia praw pacjenta. Polski system prawny nie zabezpiecza w wystarczającym stopniu danych genetycznych. Problematyka poruszanego tematu obejmuje szczególnie zlecanie przetwarzania danych genetycznych podmiotom zagranicznym, co skutkuje utratą kontroli nad ich bezpieczeństwem oraz brak skutecznych instrumentów prawnych umożliwiających egzekwowanie odpowiedzialności za ich nieuprawnione przetwarzanie. Przeprowadzone badania opierają się na dogmatycznoprawnej analizie obowiązujących regulacji, w tym przepisów RODO, ustawy o ochronie danych osobowych oraz ustaw szczególnych dotyczących ochrony zdrowia. Uwzględniono również podejście komparatystyczne, analizując wybrane regulacje międzynarodowe. Wskazano na konieczność dostosowania regulacji prawnych do specyfiki danych genetycznych. Podkreślono, że wypracowanie spójnych i kompleksowych mechanizmów prawnych jest kluczowe dla minimalizacji ryzyka naruszeń oraz wzmocnienia ochrony praw pacjentów.

Słowa kluczowe: dane genetyczne, rodo, biobankowanie, ochrona praw pacjenta

1. WPROWADZENIE

Współczesna nauka uznaje genetykę za fundament nowoczesnej medycyny, a testy genetyczne za narzędzie zarówno w diagnostyce, jak i prognozowaniu schorzeń. Dzięki poznaniu pełnej sekwencji ludzkiego genomu w XXI wieku oraz określeniu funkcji poszczególnych genów, możliwe stało się precyzyjne określanie predyspozycji zdrowotnych i indywidualnych cech organizmu. Osiągnięcia te przyczyniły się do dynamicznego rozwoju medycyny spersonalizowanej, umożliwiając dostosowanie metod leczenia do genotypu pacjenta, co zwiększa skuteczność terapii i minimalizuje ryzyko działań niepożądanych (Pręgowska 2019, s. 114-115). Nie bez znaczenia pozostaje również rozróżnienie pomiędzy danymi genetycznymi a danymi biometrycznymi. Choć oba te rodzaje informacji mogą służyć identyfikacji osoby fizycznej, różnią się one zarówno pod względem charakteru i zakresu zastosowania, jak i potencjalnych zagrożeń związanych z ich gromadzeniem, przetwarzaniem oraz ochroną. Właściwa klasyfikacja i regulacja tych danych stanowi element zapewnienia zgodności z normami prawa ochrony danych osobowych oraz ochrony prywatności.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) w przepisie art. 4 pkt 13–14 *expressis verbis* definiuje te dane oraz kwalifikuje je jako szczególne kategorie danych osobowych (tzw. dane wrażliwe), które ze względu na swój charakter podlegają szczególnemu reżimowi prawnemu oraz zaostrzonym standardom ochrony.

Dane genetyczne w świetle przepisu art. 4 pkt.13 RODO oznaczają „dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej". Innymi słowy, danymi genetycznymi są między innymi sekwencje DNA, wyniki testów genetycznych wskazujące na predyspozycje chorobowe, mutacje genów czy profile DNA. Natomiast dane biometryczne zgodnie z przepisem art. 4 pkt. 14 RODO 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". Te dane wykorzystywane są przede wszystkim w celach identyfikacyjnych, obejmujących m.in. zastosowanie w systemach kontroli dostępu, rejestrach kryminalistycznych czy dokumentach tożsamości, poprzez analizę unikalnych cech fizjologicznych jednostki, takich jak odciski palców,

wizerunek twarzy czy struktura tęczówki oka. Natomiast dane genetyczne zawierają informacje odnoszące się do wewnętrznych właściwości biologicznych organizmu, w tym do predyspozycji zdrowotnych oraz cech dziedzicznych, co czyni je szczególnie wrażliwymi z punktu widzenia ochrony prywatności i bezpieczeństwa danych osobowych.

Ochrona danych genetycznych w Polsce opiera się głównie na ogólnych regulacjach dotyczących ochrony danych osobowych i prywatności, w tym na RODO oraz ustawach sektorowych, takich jak ustawa o ochronie danych osobowych, ustawa o prawach pacjenta czy ustawa o zawodzie lekarza. Zgodnie z brzmieniem przepisu art. 9 ust. 1 RODO, dane genetyczne należą do szczególnych kategorii danych, których przetwarzanie jest co do zasady zakazane, z wyjątkami, o których mowa w przepisie art. 9 ust. 2 RODO, tj. m.in. w przypadku konieczności diagnostycznej lub terapeutycznej, pod warunkiem zachowania tajemnicy zawodowej lub uzyskania wyraźnej zgody pacjenta. W doktrynie wskazuje się, że niedopuszczalne jest wyrażenie zgody na przetwarzanie danych wrażliwych w sposób dorozumiany, z uwagi na to, że prawodawca wymaga wyraźnego oświadczenia, co jest podyktowane chęcią zapewnienia silniejszej ochrony (Fajgielski 2018). Sankcja za naruszenie tej regulacji została ujęta w przepisie art. 107 ust. 2 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie – bez uprawnienia – danych szczególnie wrażliwych, takich jak informacje dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, przynależności związkowej, danych genetycznych, biometrycznych służących identyfikacji osoby fizycznej, a także danych o stanie zdrowia, życiu seksualnym lub orientacji seksualnej, podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do trzech lat.

W przepisie art. 30 Kodeksu Etyki Lekarskiej z dnia 18 maja 2024 r. zobowiązano do zapewnienia poufności informacji, które mogą być odczytane z materiału genetycznego pacjenta i członków jego rodziny. Obowiązek ochrony danych genetycznych rozciąga się również na osoby współpracujące z lekarzem, w szczególności na tych, którzy w ramach swojej działalności zawodowej mają bezpośredni dostęp do materiału genetycznego, prowadzą jego analizę oraz przeprowadzają badania genetyczne. Lekarze specjalizujący się w tej dziedzinie, ze względu na zakres dostępu do materiału oraz możliwość pozyskania z niego szerokiego spektrum informacji, ponoszą szczególną odpowiedzialność za zapewnienie odpowiedniego poziomu ochrony tych danych (Kubiak 2025, s. 266-267). W związku z tym są zobowiązani do stosowania podwyższonych

standardów zabezpieczeń, adekwatnych do charakteru przetwarzanych informacji i wynikających zarówno z przepisów prawa, jak i zasad deontologii lekarskiej.

W sektorze medycznym dane genetyczne traktowane są jako część dokumentacji medycznej i podlegają standardowym regulacjom dotyczącym ochrony danych o stanie zdrowia. Brakuje jednak szczegółowych przepisów dostosowanych do specyfiki informacji genetycznych. *De lege lata* w Polsce nie istnieje kompleksowa ustawa regulująca kwestie testów genetycznych i ochrony danych genetycznych, mimo wielokrotnie zgłaszanych postulatów. Najwyższa Izba Kontroli w raporcie z 2018 r. wskazała na brak regulacji dotyczących poradnictwa genetycznego, bankowania materiału biologicznego oraz bezpieczeństwa danych genetycznych (Raport NIK 2018). Wyraźnie uwypukliła brak skutecznego mechanizmu kontroli jakości i akredytacji laboratoriów genetycznych, co umożliwia prowadzenie działalności w tym zakresie bez odpowiedniego nadzoru. W konsekwencji pacjenci narażeni są na ryzyko nieuprawnionego przetwarzania i niewłaściwego przechowywania danych, zwłaszcza w przypadku podmiotów komercyjnych oferujących testy genetyczne w modelu *direct to consumer* (DTC). Usługi te, świadczone bez nadzoru organów regulacyjnych, często wiążą się z brakiem kontroli nad dalszym wykorzystywaniem danych genetycznych, w tym możliwością ich sprzedaży lub transferu do podmiotów trzecich, co rodzi istotne zagrożenia dla prywatności i bezpieczeństwa osób korzystających z takich badań (RM Hendricks-Sturrup RM, CY Lu 2019, s. 3-7).

Mimo powołania w 2016 r. zespołu w Ministerstwie Zdrowia, prace nad ustawą nie zostały ukończone. W konsekwencji pacjenci pozostają bez skutecznej ochrony przed nieuczciwymi praktykami przedsiębiorstw oferujących testy DNA – brak jest norm dotyczących jakości badań, kwalifikacji wykonujących je osób oraz zasad przechowywania i zabezpieczania materiału genetycznego.

Przetwarzanie danych genetycznych w Polsce opiera się na ogólnych regulacjach prawnych, w szczególności na przepisach RODO, ustawie o działalności leczniczej oraz ustawie o medycynie laboratoryjnej. W sektorze ochrony zdrowia warto ponownie podkreślić, że dane te kwalifikowane są jako szczególna kategoria danych wrażliwych, a ich przetwarzanie dopuszczalne jest wyłącznie w wyjątkowych sytuacjach, takich jak diagnostyka lub terapia, przy zachowaniu obowiązku uzyskania wyraźnej zgody pacjenta.

W obszarze identyfikacji kryminalistycznej, która jest rezultatem badawczym (Czeczot, Tomaszewski 1999, s. 213), dane genetyczne stanowią jedynie proces badania śladów kryminalistycznych (Hołyst 2004, s. 580). Profilowanie DNA osób podejrzanych oraz prowadzeniem bazy danych DNA odbywa się na

podstawie przepisu art. 21 (a) ustawy o Policji z dnia 6 kwietnia 1990 r, jednak brak szczegółowych regulacji dotyczących retencji oraz zakresu dostępu do tych danych budzi istotne wątpliwości w kontekście ochrony prywatności.

2. LUKI PRAWNE W ZAKRESIE DANYCH GENETYCZNYCH

W prawoznawstwie pojęcie luki prawnej odnosi się do sytuacji, w której w obowiązującym porządku prawnym brak jest normy regulującej istotny stan faktyczny, mimo że jego uregulowanie jest społecznie i prawnie oczekiwane. Luka może wynikać zarówno z pominięcia ustawodawczego, jak i z opóźnienia legislacyjnego wobec dynamicznych zmian społecznych i technologicznych. W przypadku ochrony danych genetycznych mamy do czynienia z luką rzeczywistą – ustawodawca nie przewidział kompleksowych regulacji w tej materii, co prowadzi do niepewności prawnej i braku jednolitych standardów ochrony. W efekcie organy stosujące prawo zmuszone są do posługiwania się przepisami ogólnymi, analogią prawną lub zasadami ogólnymi, co nie zawsze zapewnia skuteczną ochronę danych genetycznych.

W Polsce, jak podkreślono powyżej, brak kompleksowej regulacji ustawowej w zakresie genetyki, której powoduje, że działalność związana z przeprowadzaniem testów DNA funkcjonuje w stanie regulacyjnej luki. Pomimo że wiele państw członkowskich Unii Europejskiej już na początku XXI wieku przyjęło szczegółowe rozwiązania legislacyjne z zakresu bioetyki i prawa genetycznego, polski ustawodawca ograniczył się jedynie do implementacji ogólnych norm prawa unijnego, w szczególności wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz aktów pochodnych, które jednak nie uwzględniają w wystarczającym stopniu specyfiki problematyki danych genetycznych.

Brak precyzyjnych regulacji dotyczących zasad wykonywania badań genetycznych, przechowywania materiału biologicznego (w tym próbek DNA), jak również przetwarzania i zabezpieczania informacji o charakterze genetycznym, stwarza istotne ryzyko zarówno dla systemu organizacyjnego jednostek wykonujących tego rodzaju badania, jak i dla ochrony danych osobowych pacjentów (Raport NIK 2018). Regulacje bioetyczne w tym kontekście odnoszą się do norm prawnych i etycznych mających na celu zapewnienie ochrony godności osoby ludzkiej w związku z postępem biotechnologicznym i medycznym, w szczególności w zakresie badań genetycznych, terapii genowych oraz wykorzystania danych biologicznych. Ich zadaniem jest wyznaczanie granic ingerencji w integralność

cielesną i informacyjną człowieka, z uwzględnieniem zasady świadomej zgody, ochrony informacji wrażliwych oraz niedyskryminacji. Brak takich regulacji w prawie krajowym skutkuje nie tylko niedostateczną ochroną praw jednostki, ale również pogłębia niepewność prawną wśród podmiotów prowadzących działalność diagnostyczną i badawczą w zakresie genetyki.

Istotny problem zdaje się stanowić interpretacja badań, które otrzymuje pacjent bez wyjaśnienia ich znaczenia medycznego. Nieprawidłowa interpretacja wyników może prowadzić do błędnych decyzji zdrowotnych, zwłaszcza w przypadku wyników fałszywie negatywnych. Ustawa o zawodach lekarza i lekarza dentysty z dnia 5 grudnia 1996 r. w przepisie art. 31 przewiduje wymóg świadomej zgody pacjenta na badania diagnostyczne, jednak nie precyzuje standardów interpretacji testów genetycznych. Zapewnienie pacjentowi nie tylko możliwości wyrażenia świadomej zgody na przeprowadzenie diagnostyki, ale również dostarczenie mu pełnej i zrozumiałej interpretacji uzyskanych wyników. Brak właściwego omówienia rezultatów badań może prowadzić do błędnych decyzji zdrowotnych, zwłaszcza gdy pacjent samodzielnie interpretuje wyniki, nie posiadając odpowiedniej wiedzy medycznej. Zgodnie z przepisem art. 31 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, pacjent ma prawo do wyrażenia świadomej zgody na przeprowadzenie badań diagnostycznych. Jednakże przepis ten nie precyzuje standardów dotyczących interpretacji wyników tych badań. W przypadku testów genetycznych, gdzie wyniki mogą mieć daleko idące implikacje dla zdrowia pacjenta oraz jego rodziny, konieczne jest, aby proces uzyskiwania świadomej zgody obejmował nie tylko zgodę na samo badanie, ale również zapewnienie pacjentowi profesjonalnej interpretacji wyników oraz omówienie ich potencjalnych konsekwencji.

Niedostateczna interpretacja wyników badań genetycznych została również podkreślona w raporcie Najwyższej Izby Kontroli z 2018 roku, gdzie wskazano na brak kompleksowych regulacji prawnych dotyczących wykonywania badań genetycznych oraz konieczność zapewnienia pacjentom odpowiedniego poradnictwa genetycznego (Raport NIK 2018).

Ponadto, zgodnie z art. 9 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, pacjent ma prawo do pełnej informacji o swoim stanie zdrowia, w tym o wynikach przeprowadzonych badań. Brak profesjonalnej interpretacji wyników badań genetycznych może naruszać to prawo, prowadząc do sytuacji, w której pacjent nie jest w pełni świadomy swojego stanu zdrowia oraz potencjalnych zagrożeń.

W polskim ustawodawstwie nie funkcjonuje również żadna szczególna regulacja dotycząca tworzenia i funkcjonowania biobanków, które powstają w celu przechowywanie tkanek, komórek i organów ludzkich (Krekora-Zając 2012, s. 64-77). W efekcie materiał biologiczny może być przechowywany i wykorzystywany w sposób nieuregulowany, w tym do celów komercyjnych bez wyraźnej zgody klienta. Ustawa o działalności leczniczej z dnia 15 kwietnia 2011 r. zawiera jedynie ogólne przepisy dotyczące ochrony danych medycznych, nie odnosząc się bezpośrednio do specyfiki biobankowania.

Inne obowiązujące przepisy, w tym ustawa o Policji, nie precyzują, jak długo mogą być przechowywane profile DNA osób podejrzanych lub skazanych. Brak ustawowego obowiązku okresowego przeglądu i usuwania takich danych budzi poważne wątpliwości w kontekście ochrony praw jednostki. Trybunał Sprawiedliwości Unii Europejskiej (TSUE, wyrok C-207/16) uznał podobne praktyki w innych krajach za sprzeczne z prawem Unii Europejskiej, co sugeruje konieczność dostosowania polskiego prawa.

Polski ustawodawca nie wprowadził na przykład zakazu żądania testów genetycznych przez pracodawców czy ubezpieczycieli. Wprawdzie ogólne przepisy RODO i prawa pracy pośrednio chronią przed takimi praktykami (dane genetyczne to dane o zdrowiu, więc pracodawca nie może ich przetwarzać bez podstawy prawnej, a ubezpieczyciel może co najwyżej pytać o stan zdrowia w zakresie adekwatnym do ryzyka), jednak brak jest jednoznacznego zakazu dyskryminacji genetycznej. Dla porównania – w wielu krajach istnieją przepisy expressis verbis zakazujące towarzystwom ubezpieczeniowym wykorzystywania informacji o mutacjach genetycznych klienta przy kalkulacji składki . W Polsce taka sytuacja nie była dotąd uregulowana szczególnie, co stanowi potencjalną lukę. Podstawowymi kryteriami determinującymi zawarcie umowy ubezpieczenia wraz z warunkami polisy ubezpieczeniowej, a w konsekwencji wysokość składki należnej ubezpieczycielowi, są między innymi: wiek osoby ubiegającej się o ochronę ubezpieczeniową, jej aktualny stan zdrowia oraz oszacowane prawdopodobieństwo wystąpienia określonych schorzeń (Kozieska 2015, s. 16-19). Dane te umożliwiają towarzystwom ubezpieczeniowym dokonanie kalkulacji ryzyka ubezpieczeniowego, co bezpośrednio przekłada się na wysokość świadczeń oraz warunki ochrony ubezpieczeniowej oferowanej danej osobie (Kubiak 2025, s. 267).

Co prawda można wskazać na międzynarodowe unormowania zakazujące dyskryminowania w szczególności odnosząc się do przepisu art. 11 Konwencji o prawach człowieka i biomedycynie przyjęta w dniu 19 listopada 1996 r. czy też

przepisu art. 6 Powszechnej Deklaracji UNESCO o genomie ludzkim i prawach człowieka z 11 listopada 1997 r.

Ochrona praw pacjentów poddających się testom genetycznym opiera się również na przepisach ustawy o zawodzie lekarza i lekarza dentysty, ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz ustawy o działalności leczniczej. Lekarz, zlecając badanie genetyczne, musi uzyskać świadomą zgodę pacjenta, zgodnie z przepisem art. 31 ustawy o zawodzie lekarza, a laboratoria diagnostyczne podlegają ogólnym regulacjom dotyczącym jakości badań, wynikającym z przepisów Ministerstwa Zdrowia w zakresie standardów laboratoryjnych z dnia 16 lipca 2024 r. Niemniej jednak obecne przepisy nie odnoszą się do specyficznych problemów związanych z genetyką, takich jak informowanie członków rodziny o wynikach mogących mieć wpływ na ich zdrowie czy zgody na dalsze wykorzystanie próbek do badań naukowych.

W sektorze konsumenckim, zwłaszcza w przypadku wspomnianych testów genetycznych *direct to consumer* (DTC), stosowane są ogólne przepisy ustawy o prawach konsumenta oraz ustawy o świadczeniu usług drogą elektroniczną, jednak nie przewidują one szczególnych wymagań dotyczących zakresu informacji przekazywanych klientowi o badaniu genetycznym. Podmiotami potencjalnie zainteresowanymi uzyskaniem dostępu do danych genetycznych są przede wszystkim pracodawcy, zakłady ubezpieczeń oraz szeroko rozumiane podmioty sektora prywatnego. Kwestia ta została dostrzeżona przez ELSI (Ethical, Legal and Social Issues), która w swoich wytycznych dotyczących ochrony genomu zwróciła uwagę na wynikające z tego zagrożenia. Przedmiotowa problematyka została syntetycznie omówiona w niniejszej monografii w kontekście analizy art. 7 Deklaracji w sprawie genomu (Zieliński 2023, roz. 6).

W efekcie przedsiębiorstwa mogą promować swoje usługi w sposób mogący wprowadzać konsumentów w błąd, sugerując możliwość wykrycia wszystkich predyspozycji do nowotworów, mimo że testy genetyczne nie dają tak jednoznacznych wyników. Jak wskazuje prof. Michał Witt, brak szczegółowych regulacji oznacza, że przedsiębiorstwa nie są zobowiązane do zapewnienia rzetelnej interpretacji wyników testów (Witt 2016). Warto dodać, że współczesny rynek diagnostyki molekularnej szacowany jest na około 5 miliardów dolarów amerykańskich, co stanowi około 11% wartości całego sektora diagnostyki medycznej. (Zieliński 2023, roz. 6). Molekularne badania diagnostyczne charakteryzują się roczną dynamiką wzrostu na poziomie 12% (Witt 2016, s.73).

W odniesieniu do potencjalnych naruszeń prawa, przepisy Kodeksu cywilnego (dalej: k.c.) oraz Kodeksu karnego (dalej: k.k.) mogą zapewnić ochronę

jednostkom przed bezprawnym przetwarzaniem ich danych genetycznych. Przepisy art. 23 i 24 k.c. przewidują możliwość dochodzenia roszczeń z tytułu naruszenia dóbr osobistych, w tym prawa do prywatności i ochrony danych genetycznych jako elementu integralności osobistej. Ponadto przepis art. 267 k.k. penalizuje bezprawne uzyskanie informacji, co w określonych przypadkach mogłoby znaleźć zastosowanie do nieautoryzowanego pozyskania i analizy czyjegoś DNA. W praktyce jednak tego rodzaju postępowania należą do rzadkości, a polskie sądy nie wykształciły jeszcze spójnej linii orzeczniczej w zakresie ochrony prywatności genetycznej. Brak szczególnej ustawy regulującej ochronę danych genetycznych powoduje, że obecny system prawny opiera się na fragmentarycznych przepisach, które nie zawsze zapewniają wystarczającą ochronę przed nadużyciami.

3. RYZYKA NARUSZEŃ ZWIĄZANE Z DANYMI GENETYCZNYMI

W literaturze przedmiotu przyjęto pogląd, wedle którego nie można zdefiniować ryzyka bez określenia zbioru opisującego go cech, co oznacza, że brak jest uniwersalnej definicji pojęcia. Cechami dookreślającymi ryzyko jest źródło ryzyka, jego przedmiot i skutki realizacji wystąpienia ryzyka (Jedynak, Szydło 1997, s. 14). Przyjmując kryterium skutku wystąpienia ryzyka, wyróżnia się ryzyko rozumiane jako możliwość poniesienia szkody oraz ryzyko rozumiane jako możliwość odchylenia od zamierzonego rezultatu, negatywne albo pozytywne (Jajuga, Jajuga 1998, s. 99). W analizie ryzyka zgodnie z RODO przyjmuje się, że naruszenie dotyczące takich danych wiąże się z wysokim prawdopodobieństwem negatywnych konsekwencji dla praw i wolności osoby. Wyróżnić zatem można trzy skale ryzyka: niskie, średnie i wysokie.

Ryzyka prawne związane z ochroną danych genetycznych w Polsce wynikają przede wszystkim z nieuprawnionego dostępu do informacji, niewłaściwego wykorzystania, przetwarzania bez zgody, międzynarodowego transferu. W kontekście nieuprawnionego dostępu kluczowym problemem jest możliwość przejęcia lub wycieku informacji zawierających profile DNA pacjentów. Dane genetyczne są szczególnie wrażliwe, ponieważ ujawniają informacje nie tylko o jednostce, ale także o jej rodzinie, co może prowadzić do naruszenia prywatności wielu osób jednocześnie. Zgodnie z wytycznymi Europejskiej Rady Ochrony Danych (EROD) oraz art. 9 ust. 1 RODO, ich przetwarzanie wymaga szczególnych zabezpieczeń, a każde naruszenie powinno być zgłaszane do organu nadzorczego, jeśli istnieje wysokie ryzyko naruszenia praw i wolności osób fizycznych (European Data Protection Board 2021).

Kontrola nadzorcza zgodności z RODO należy do Prezesa Urzędu Danych Osobowych. W zakres jego kompetencji wchodzi wskazywanie na środki naprawcze, które mogą przybrać formę upomnień lub ostrzeżeń. Organ nadzorczy dysponuje kompetencją do wydania ostrzeżenia administratorowi danych o potencjalnym ryzyku naruszenia przepisów RODO, jak również do zobowiązania go do dostosowania procesów przetwarzania danych do obowiązujących norm prawnych. W określonych sytuacjach może również udzielać zezwoleń oraz pełnić funkcję doradczą w zakresie zgodności przetwarzania z wymogami ochrony danych osobowych. Warto podkreślić, że wskazane środki nie wykluczają możliwości nałożenia administracyjnych kar pieniężnych, które mogą zostać zastosowane równolegle do środków naprawczych (Mednis 2020).

Kolejnym istotnym ryzykiem jest niewłaściwe wykorzystanie danych genetycznych, co oznacza ich przetwarzanie poza zakresem, dla którego zostały pierwotnie zgromadzone. Może to obejmować przypadki, w których próbki DNA, pobrane w celach medycznych, są wykorzystywane do badań naukowych lub komercyjnych bez wyraźnej zgody pacjenta. Przykładem może być sytuacja, w której laboratoria przechowują i analizują próbki po zakończeniu pierwotnych badań w celu budowania baz danych dla przyszłych projektów badawczych, co bez odpowiedniej zgody narusza zasadę ograniczenia celu przetwarzania (art. 5 ust. 1 lit. b RODO). Trybunał Sprawiedliwości Unii Europejskiej w swoich orzeczeniach wielokrotnie podkreślał, że dane o stanie zdrowia, w tym genetyczne, wymagają szczególnej ochrony, a ich nieautoryzowane wykorzystanie może prowadzić do odpowiedzialności administracyjnej oraz cywilnej, w tym do roszczeń o zadośćuczynienie za naruszenie prawa do prywatności (TSUE, C-311/18 Schrems II, 2020). Europejski Trybunał Praw Człowieka w sprawie S. i Marper z dnia 4 grudnia 2008 r. przeciwko Wielkiej Brytanii orzekł, że przechowywanie próbek DNA osób, wobec których nie postawiono zarzutów, narusza prawo do prywatności chronione przepisem art. 8 Europejskiej Konwencji Praw Człowieka. Co w konsekwencji ukazuje, że nadmierna retencja danych genetycznych może stanowić naruszenie praw podstawowych (ETPCz, 2008).

Transfer danych genetycznych do państw trzecich stanowi kolejne ryzyko, zwłaszcza w kontekście braku decyzji Komisji Europejskiej o adekwatnym poziomie ochrony dla wielu państw spoza Europejskiego Obszaru Gospodarczego. W praktyce wiele przedsiębiorstw, które oferują testy DNA w modelu *direct to consumer* (DTC), wysyła próbki i wyniki analiz do laboratoriów w Stanach Zjednoczonych, Chinach czy Indiach, gdzie poziom ochrony danych może być niższy niż w Unii Europejskiej. Orzeczenie TSUE w sprawie *Schrems II* unieważniło

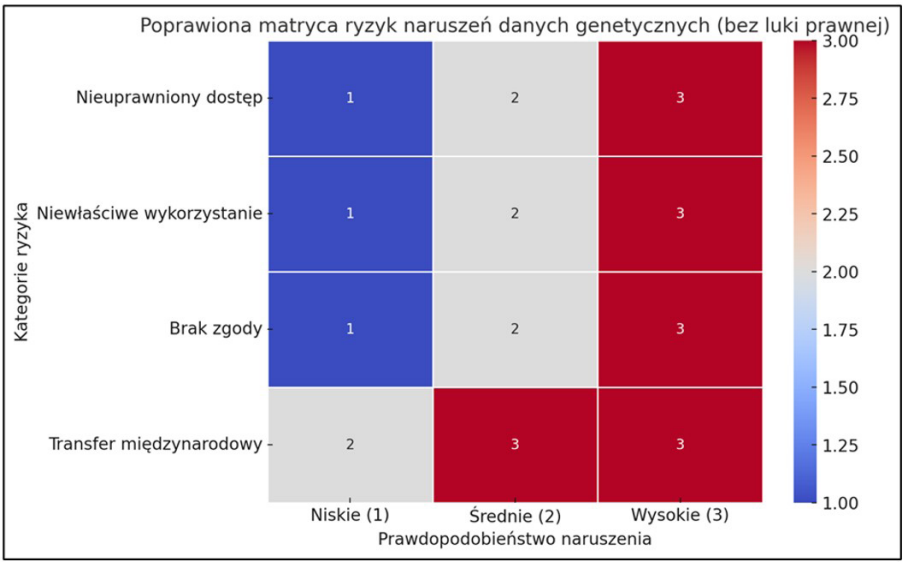
decyzję *Privacy Shield*, która wcześniej regulowała transfery do USA, co oznacza, że obecnie każde przedsiębiorstwo przekazujące dane genetyczne za granicę musi stosować dodatkowe zabezpieczenia, np. standardowe klauzule umowne (TSUE, C-311/18, 2020). W przypadku Chin sytuacja jest jeszcze bardziej problematyczna, ponieważ chińskie przepisy dotyczące ochrony danych genetycznych mogą pozwalać na dostęp do takich informacji przez władze państwowe, co rodzi poważne ryzyko niekontrolowanego wykorzystania profili DNA obywateli Unii Europejskiej. Raport NIK wskazuje, że w Polsce brakuje skutecznych mechanizmów nadzoru nad tym, jakie podmioty przekazują dane genetyczne poza granice kraju, co powoduje, że pacjenci mogą nawet nie zdawać sobie sprawy, że ich genom jest analizowany w laboratoriach o nieznanych standardach ochrony prywatności (Raport NIK 2018).

Na gruncie prawa niemieckiego obowiązuje ustawa o badaniach genetycznych (*Gendiagnostikgesetz*), która precyzyjnie określa warunki wykonywania testów DNA, obowiązki informacyjne oraz zakazy wykorzystania informacji genetycznych przez ubezpieczycieli i pracodawców. We Francji istnieje ustawa bioetyczna, która wprowadza ścisłe ograniczenia dotyczące analizy DNA oraz jasno określa rolę państwowego nadzoru nad badaniami genetycznymi (Kozielewicz 2018, s. 19-28). Polska pozostaje w tyle za tymi rozwiązaniami, co potwierdzają raporty ekspertów i wnioski Rzecznika Praw Obywatelskich, który wielokrotnie wskazywał na konieczność uchwalenia regulacji chroniących dane genetyczne na poziomie krajowym. Luka legislacyjna zwiększa ryzyko dowolności w interpretacji obowiązujących przepisów, a także osłabia skuteczność egzekwowania ochrony danych osobowych w kontekście postępującej komercjalizacji badań genetycznych.

Poniżej znajduje się propozycja matrycy ryzyk dla naruszeń danych genetycznych, która przedstawia skalę naruszeń od niskiego do wysokiego, zaznaczona liczbami odpowiednio od 1 do 3. Transze oznaczone kolorem niebieskim oznaczają niższe ryzyko, a czerwone wskazują na zagrożenia wymagające pilnych działań zaradczych. Interpretacja skali:

1. Niskie ryzyko – sytuacje, w których naruszenie nie powoduje bezpośrednich negatywnych skutków dla osób (np. dane są zaszyfrowane lub odpowiednio zabezpieczone).
2. Średnie ryzyko – sytuacje, w których naruszenie może wpłynąć na prywatność osób, ale nie prowadzi do natychmiastowej szkody (np. dane trafiły do niewłaściwego odbiorcy, ale nie zostały wykorzystane).

3. Wysokie ryzyko– sytuacje, które mogą prowadzić do poważnych skutków, takich jak ujawnienie pełnego profilu DNA osobom trzecim, co może skutkować dyskryminacją genetyczną, utratą prywatności lub nieodwracalnymi konsekwencjami prawnymi.



Rysunek 1 matryca ryzyk naruszeń danych genetycznych, opracowanie własne na podstawie Wytycznych 01/2021EDPB oraz Poradnika dotyczącego naruszeń danych osobowych UODO z 25.02.2025 r.

Warto również wskazać na konkretny przypadek naruszenia, który można wyczytać ze skali.

Przykład:

Załóżmy, że przedsiębiorstwo biotechnologiczne działająca w Polsce oferuje testy DNA klientom, przekazując dane genetyczne do laboratorium w Chinach. W tym kontekście prawdopodobieństwo wystąpienia naruszenia oceniane jest jako wysokie (3), co oznacza, że istnieje duże ryzyko zaistnienia incydentu związanego z nieuprawnionym przetwarzaniem danych. Ocena ta nie odnosi się jedynie do hipotetycznej możliwości naruszenia, lecz opiera się na analizie praktyki rynkowej, częstotliwości takich transferów oraz poziomu zabezpieczeń po stronie odbiorcy danych. W przypadku przekazywania informacji genetycznych poza Europejski Obszar Gospodarczy – zwłaszcza do państw, które nie zapewniają równoważnego poziomu ochrony, takich jak Chiny – wzrasta ryzyko ingerencji ze strony władz publicznych, braku przejrzystości procedur dostępowych oraz

ograniczenia skuteczności egzekwowania praw osób, których dane dotyczą.

Jednocześnie, konsekwencje takiego naruszenia również oceniane są jako wysokie (3), ponieważ niekontrolowane ujawnienie danych genetycznych może prowadzić do istotnych skutków dla osób fizycznych, w tym do naruszenia prywatności, dyskryminacji genetycznej, wykorzystania danych w celach komercyjnych lub populacyjnych oraz do nieodwracalnych konsekwencji prawnych. W rezultacie, przypadek ten mieści się w najwyższej kategorii ryzyka – oznaczonej kolorem czerwonym w matrycy – i wymaga wdrożenia natychmiastowych środków zaradczych. Wśród rekomendowanych działań należy wskazać na konieczność stosowania mechanizmów zwiększających bezpieczeństwo przetwarzania, takich jak szyfrowanie danych, ich pseudonimizacja lub anonimizacja, a także wybór partnerów przetwarzających dane wyłącznie w ramach jurysdykcji państw członkowskich UE, gdzie możliwe jest zapewnienie zgodności z przepisami RODO. Brak wdrożenia adekwatnych środków może skutkować nie tylko naruszeniem praw osób, których dane dotyczą, ale również wysokimi karami administracyjnymi dla administratora danych.

Reasumując, ryzyka prawne związane z ochroną danych genetycznych w Polsce obejmują szeroki zakres zagrożeń, od naruszeń poufności, przez niewłaściwe wykorzystanie, brak zgodności z regulacjami, aż po systemowe luki w przepisach. Ochrona tych danych wymaga zarówno skuteczniejszych mechanizmów nadzoru, jak i dostosowania krajowych regulacji do standardów unijnych, aby zagwarantować pełną zgodność z wymogami RODO oraz zapewnić odpowiednie zabezpieczenia przed nadużyciami.

4. PODSUMOWANIE

Rozdział przedstawia kompleksową analizę zagadnienia ochrony danych genetycznych w polskim porządku prawnym, ze szczególnym uwzględnieniem istniejących luk normatywnych oraz zagrożeń wynikających z braku spójnych i całościowych regulacji w tym zakresie. Przyjęta metodologia badawcza – obejmująca podejście dogmatycznoprawne oraz komparatystyczne – umożliwiła identyfikację kluczowych deficytów legislacyjnych, jak również sformułowanie postulatów *de lege ferenda* w kierunku harmonizacji prawa krajowego z obowiązującymi standardami międzynarodowymi.

Na szczególne podkreślenie zasługuje zarys ryzyk związanych z przetwarzaniem danych genetycznych bez odpowiednich podstaw prawnych, w tym

w szczególności brak jednoznacznych unormowań w zakresie biobankowania, nieprecyzyjne regulacje dotyczące przechowywania i retencji próbek biologicznych oraz zagrożenie ich wykorzystania do celów komercyjnych. Uwzględnienie dorobku orzeczniczego Trybunału Sprawiedliwości Unii Europejskiej oraz problematyki transferu danych do państw trzecich nadaje analizie wymiar praktyczny. W konkluzji słusznie wskazano na konieczność ustanowienia szczegółowych regulacji prawnych, które nie tylko implementowałyby standardy unijne, lecz również zapewniałyby adekwatny poziom ochrony przed negatywnymi skutkami komercjalizacji testów genetycznych. Cennym uzupełnieniem opracowania jest zaprezentowana matryca ryzyka, umożliwiająca przeprowadzenie oceny prawdopodobieństwa i skali wystąpienia potencjalnych naruszeń.

BIBLIOGRAFIA

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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2024 r. poz. 145 z późn. zm.).

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

Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz. U. z 2025 r. poz. 450).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061 z późn. zm.).

Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz. U. z 2024 r. poz. 1287 z późn. zm.).

Orzeczenia

Wyrok ETPCz z dnia 4 grudnia 2008 r., S. i Marper przeciwko Zjednoczonemu Królestwu, skarga nr 30562/04 i 30566/04,

Wyrok TSUE z dnia 2 października 2018 r., 2018 Ministerio Fiscal, sprawa C-207/16, ECLI:EU:C:2018:788.

Wyrok TSUE z dnia 16 lipca 2020 r., Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, sprawa C-311/18, ECLI:EU:C:2020:559

Literatura

Bach-Golecka D., Stankiewicz R. (red.)
2020 Organizacja systemu ochrony zdrowia. System Prawa Medycznego, t. 3, Warszawa.

Czeczot Z., Tomaszewski T.
1999 Kryminalistyka ogólna, Toruń.

Hendricks-Sturrup R. M., Lu C. Y.
2019 Direct-to-Consumer Genetic Testing Data Privacy: Key Concerns and Recommendations Based on Consumer Perspectives, Journal of Personalized Medicine, 9(2), 25. https://doi.org/10.3390/jpm9020025 (dostęp: 06.04.2025 r.)

Hołyst B.
2004 Kryminalistyka, Warszawa.

Jajuga K., Jajuga T.
1998 Inwestycje. Instrumenty finansowe, ryzyko finansowe, inżynieria finansowa, Warszawa.

Jedynak P., Szydło S.
1997 Zarządzanie ryzykiem, Wrocław.

Kapelańska-Pręgowska J.
2019 Prawo wobec rozwoju genetyki, [w:] System Prawa Medycznego, t. II, cz. 1, Regulacja prawna czynności medycznych, red. M. Boratyńska, P. Konieczniak, Warszawa.

Kozielewicz B.
2019 Komercjalizacja ciała ludzkiego we Francji. Wybrane zagadnienia prawne, Przegląd Prawniczy Uniwersytetu Warszawskiego, nr 2.

Krekora-Zając D.
2012 O konieczności regulacji prawnej biobanków, Państwo i Prawo, nr 7.

Kubiak R.
2025 Kodeks Etyki Lekarskiej. Komentarz, red. R. Tymiński, Warszawa, art. 30.

Mednis A.
2018 Ochrona danych genetycznych jako danych osobowych, Warszawa.

Przyłuska J.
2015 Bezpieczeństwo finansowe w ubezpieczeniach na życie, [w:] Społeczno-gospodarcze aspekty bezpieczeństwa Polski – wyzwania i zagrożenia, rozdz. Ekonomiczne aspekty bezpieczeństwa Polski, Lublin

Witt M.
2016 Czy genetyka kliniczna jest bezpieczna?, Warszawa.

Zieliński P.
2023 Deklaracje bioetyczne UNESCO jako źródło prawa biomedycznego, Warszawa.

Komentarze i opracowania prawne

Fajgielski P.
2018 Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Lex/el., komentarz do art. 9 RODO, teza 16

Dokumenty i raporty

European Data Protection Board (EDPB)
2021 Wytyczne 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych, wersja 2.0, dostęp: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_pl.pdf. (dostęp: 06.04.2025 r.)

Najwyższa Izba Kontroli
2018 Raport NIK, dostęp: https://www.nik.gov.pl/plik/id,16680,vp,19234.pdf. (dostęp: 06.04.2025 r.)

Urząd Ochrony Danych Osobowych
2025 Poradnik dotyczący naruszeń danych osobowych, dostęp: https://uodo.gov.pl/pl/138/3561. (dostęp: 06.04.2025 r.)

Źródła internetowe

https://bip.brpo.gov.pl/pl/content/minister-zdrowia-o-koniecznosci-prawnej-regulacji-testow-genetycznych-i-biobankowania (dostęp: 06.04.2025).

https://bip.brpo.gov.pl/pl/content/testy-genetyczne-prawa-człowieka-seminarium-rpo-w-gdańsku (dostęp: 06.04.2025).

https://cowzdrowiu.pl/aktualnosci/post/prof-olga-haus-na-braku-ustawy-o-genetyce-medycznej-tracimy-wszyscy (dostęp: 06.04.2025).

https://www.theguardian.com/australia-news/article/2024/sep/10/australia-insurance-company-discrimination-genetic-testing? (dostęp: 06.04.2025).

https://www.theguardian.com/australia-news/article/2024/may/12/life-insurance-industry-customers-genetic-tests-ban? (dostęp: 06.04.2025).

GENETIC DATA SECURITY IN THE POLISH LEGAL ORDER

Abstract: Technological advancement enables the rapid development of genetic research, which simultaneously increases the need for effective protection of genetic data due to the risk of privacy breaches and potential discrimination. This chapter analyzes the challenges related to the protection of genetic data within the Polish legal framework, highlighting existing legal gaps and the associated risks. Particular attention is given to the issue of transferring genetic data to foreign entities and the lack of effective legal instruments for ensuring control and accountability. The analysis is based on current regulations (including the GDPR, the Personal Data Protection Act, and sector-specific health laws) and adopts a comparative approach by examining selected international regulations. The study emphasizes the need to develop comprehensive and tailored legal mechanisms to address the specific nature of genetic data and to strengthen the protection of patients' rights.

Keywords: genetic data, GDPR, biobanking, patient rights protection

ALEKSANDRA PAWEŁEK

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

OCHRONA DANYCH OSOBOWYCH W MIĘDZYNARODOWYCH BADANIACH KLINICZNYCH I LECZENIU PACJENTÓW ZA GRANICĄ

Streszczenie: Współczesna medycyna coraz częściej przekracza granice państw, zarówno w kontekście badań klinicznych, jak i leczenia pacjentów w krajach innych niż te, w których są oni obywatelami lub w których pierwotnie rozpoczęto ich terapię. Taka międzynarodowa współpraca medyczna niesie za sobą wiele korzyści, ale także wymaga szczególnej uwagi w zakresie ochrony danych osobowych pacjentów. W artykule omówiono najważniejsze wymogi prawne związane z przetwarzaniem i przekazywaniem danych w takich sytuacjach, ze szczególnym uwzględnieniem regulacji europejskiego Rozporządzenia o Ochronie Danych Osobowych (RODO), wytycznych Światowej Organizacji Zdrowia (WHO), takich jak Guidance on the Ethical Conduct of Public Health Surveillance, Decyzje Schrems II (TSUE, Sprawa C-311/18) oraz innych kluczowych dokumentów i przepisów prawa europejskiego i międzynarodowego. Przedstawiono podstawowe zasady ochrony danych, w tym konieczność uzyskania świadomej zgody pacjenta, stosowania odpowiednich zabezpieczeń takich jak szyfrowanie czy pseudonimizacja, które są kluczowe dla zapewnienia poufności wrażliwych informacji. Szczególną uwagę poświęcono specyfice danych medycznych jako kategorii szczególnie chronionej oraz wyzwaniom technicznym i prawnym, jakie mogą wystąpić podczas ich przekazywania do innych państw. W artykule opisano także wybrane regulacje spoza Europy, takie jak amerykańska HIPAA, które mają istotne znaczenie w międzynarodowej współpracy medycznej, zwłaszcza w kontekście badań klinicznych obejmujących wiele krajów. Omówiono też w celu komparatystyki krajowe regulacje. Na konkretnych przykładach przeanalizowano najczęstsze problemy, z którymi mogą zetknąć się młodzi specjaliści, studenci i badacze, takie jak sposoby legalnego transferu danych do państw trzecich, identyfikacja potencjalnych ryzyk oraz metody ich minimalizowania. Celem publikacji jest nie tylko przedstawienie aktualnych regulacji prawnych oraz innych istotnych źródeł pozaprawnych, ale również przybliżenie ich praktycznego zastosowania w sposób przystępny i zrozumiały.

Słowa kluczowe: Ochrona danych osobowych, rodo, międzynarodowa współpraca medyczna, dane medyczne, przekazywanie danych, badania kliniczne, hipaa, prywatność pacjenta, pseudonimizacja, zgoda pacjenta, bezpieczeństwo informacji, prawo międzynarodowe, decyzja schrems II

WPROWADZENIE

Współczesna medycyna, z uwagi na rozwój technologii oraz globalizację, coraz częściej przekracza granice państwowe. Oznacza to, najprościej podejmując temat, że pacjenci mogą być leczeni w krajach innych niż te, w których mają obywatelstwo lub gdzie rozpoczęto ich terapię. Tego typu międzynarodowa współpraca staje się coraz powszechniejsza, szczególnie w kontekście badań klinicznych i dostępu do nowych terapii. Dzięki temu pacjenci mają możliwość skorzystania z nowoczesnych metod leczenia, które mogą być dostępne tylko w innych częściach świata, a badania kliniczne zyskują na jakości, ponieważ angażują uczestników z różnych regionów, co zwiększa reprezentatywność wyników. Ponadto, wymiana doświadczeń i wiedzy między lekarzami i badaczami z różnych krajów pozwala na wypracowywanie nowych, skuteczniejszych sposobów leczenia, a także na szybszy rozwój innowacji medycznych.

Nie można również zająć się tematem leczenia poza granicami państwa zamieszkania nie poruszając zjawiska turystyki medycznej (Niezgoda, Kowalska 2015 s. 2).

Turystyka medyczna, będąca jednym z wyrazów globalizacji opieki zdrowotnej, zyskuje na znaczeniu na całym świecie (Lunt, Carrera 2010). Coraz więcej osób decyduje się na podróże międzynarodowe w poszukiwaniu wysokiej jakości usług medycznych, które jednocześnie pozwalają na korzystanie z atrakcji turystycznych oferowanych przez miejsce docelowe (Iordache i wsp. 2013). Rynek turystyki medycznej rozwija się dynamicznie, stając się istotnym segmentem globalnej gospodarki. W krajach rozwiniętych, gdzie obserwuje się wzrost liczby osób starszych, zmiany demograficzne mają bezpośredni wpływ na popyt na usługi medyczne, co jednocześnie sprzyja rozwojowi prezentowanego zjawiska. Z wiekiem rośnie zapotrzebowanie na opiekę zdrowotną, a tym samym na usługi, które łączą leczenie z możliwością zwiedzania i odpoczynku, co czyni ten trend jeszcze bardziej widocznym w społeczeństwach starzejących się.

Międzynarodowa współpraca w medycynie wiąże się jednak także z pewnymi wyzwaniami, zwłaszcza w obszarze ochrony danych osobowych pacjentów. Przesyłanie danych medycznych przez granice państwowe może rodzić ryzyko ich nieautoryzowanego ujawnienia lub wykorzystania. Różne państwa mają bowiem różne regulacje dotyczące ochrony prywatności, co może prowadzić do trudności w zapewnieniu zgodności z obowiązującymi przepisami prawa, takimi jak unijne RODO (Parlament Europejski i Rada UE, 2016). Dodatkowo, pacjenci mogą mieć obawy co do tego, czy ich dane osobowe będą odpowiednio chronione

w ramach międzynarodowej współpracy medycznej. Z tego powodu konieczne jest, aby międzynarodowe projekty medyczne zapewniały odpowiednią ochronę danych osobowych, stosując najnowsze technologie zabezpieczające i przestrzegając międzynarodowych standardów ochrony prywatności, co pomoże zbudować zaufanie pacjentów i zapewnić bezpieczeństwo informacji.

AKTY PRAWNE REGULUJĄCE DANE OSOBOWE PACJENTÓW

Prawną sytuacje pacjentów decydujących się na leczenie poza państwem zamieszkania precyzuje dyrektywa parlamentu europejskiego w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Parlament Europejski i Rada UE, 2011) - dalej nazywana „dyrektywą transgraniczną". Reguluje ona prawa pacjentów korzystających z opieki zdrowotnej w innym kraju Unii Europejskiej. W dokumencie opisano zasady, według których pacjenci mogą leczyć się za granicą i ubiegać się o zwrot kosztów leczenia, przy zachowaniu przepisów obowiązujących w ich kraju. Ważnym elementem dyrektywy jest również współpraca państw członkowskich w wymianie informacji medycznych oraz wprowadzanie wspólnych standardów w ochronie zdrowia. Szczególny nacisk położono na ochronę danych osobowych pacjentów, aby zapewnić ich prywatność i bezpieczeństwo, co jest szczególnie ważne w przypadku przekazywania danych między różnymi krajami. Przepisy te są zgodne z zasadami RODO, co pozwala na bezpieczną wymianę informacji i ochronę praw pacjentów. Dyrektywa ta jest podstawą prawną, która umożliwia rozwój transgranicznej opieki zdrowotnej w UE i zwiększa dostępność wysokiej jakości leczenia.

Rozporządzenie Parlamentu Europejskiego i Rady, znane jako RODO, jest fundamentalnym aktem prawnym, który reguluje ochronę danych osobowych na terenie Unii Europejskiej. Wprowadzone 25 maja 2018 roku, zastąpiło Dyrektywę 95/46/WE, oferując jednolite i bardziej rygorystyczne zasady przetwarzania danych, w tym danych szczególnie wrażliwych, takich jak informacje medyczne. Celem RODO jest nie tylko zwiększenie poziomu ochrony prywatności obywateli UE, ale także ułatwienie wymiany danych w obrębie wspólnego rynku przy jednoczesnym zapewnieniu bezpieczeństwa i zgodności z prawem.

Artykuł 9 RODO wprowadza ogólny zakaz przetwarzania danych szczególnej kategorii, do których należą dane dotyczące zdrowia. Zakaz ten może zostać uchylony wyłącznie w określonych przypadkach, takich jak konieczność przetwarzania danych w celu zapewnienia opieki zdrowotnej, diagnostyki, leczenia czy zarządzania systemami opieki zdrowotnej. Warunkiem dopuszczalności

przetwarzania jest jednak zapewnienie, że dane są obsługiwane przez osoby objęte tajemnicą zawodową lub inne podmioty zobowiązane do zachowania poufności. Przepis ten podkreśla szczególną wrażliwość danych medycznych i konieczność ich odpowiedniej ochrony.

Przepisy dotyczące przekazywania danych osobowych do państw trzecich określają szczegółowe wymagania mające na celu zapewnienie ciągłości ochrony danych. Zgodnie z artykułem 44 i kolejnymi, transfer danych poza granice Unii Europejskiej jest możliwy jedynie pod warunkiem, że kraj odbiorcy gwarantuje odpowiedni poziom ochrony, co może być potwierdzone decyzją Komisji Europejskiej. Alternatywnie, dopuszczalne jest stosowanie innych mechanizmów ochronnych, takich jak standardowe klauzule umowne czy wiążące reguły korporacyjne. W przypadku danych medycznych szczególny nacisk kładzie się na ich bezpieczeństwo, co obejmuje nie tylko ochronę przed nieuprawnionym dostępem, ale także zapewnienie integralności i poufności w całym procesie przetwarzania.

RODO wprowadza także obowiązek stosowania odpowiednich zabezpieczeń technicznych i organizacyjnych, które minimalizują ryzyko naruszeń ochrony danych. Artykuł 32 zobowiązuje administratorów i podmioty przetwarzające do wdrażania takich środków, jak szyfrowanie, pseudonimizacja czy systemy monitorowania naruszeń. W sektorze medycznym zabezpieczenia te odgrywają kluczową rolę, ponieważ dane dotyczące zdrowia są nie tylko szczególnie wrażliwe, ale również często wykorzystywane w kontekście współpracy międzynarodowej i złożonych procesów diagnostycznych.

Przyznanie osobom, których dane dotyczą, szerokich praw w zakresie ochrony ich informacji jest istotnym elementem regulacji RODO. Na mocy artykułu 15 pacjenci mogą uzyskać szczegółowe informacje o sposobie, celu i zakresie przetwarzania swoich danych. Artykuł 17 umożliwia z kolei żądanie ich usunięcia w określonych sytuacjach, przy czym w przypadku danych medycznych ograniczenia wynikają m.in. z konieczności ich przetwarzania w celu realizacji obowiązków prawnych lub ochrony zdrowia publicznego. Przepisy RODO dotyczące danych medycznych tworzą spójne i kompleksowe ramy prawne, które umożliwiają zarówno ich bezpieczne przetwarzanie, jak i efektywną wymianę w granicach UE oraz poza nimi. Ochrona danych pacjentów jest tu priorytetem, a szczegółowe regulacje, takie jak artykuły 9, 32 i 44, stanowią wyraźne wytyczne dla administratorów i podmiotów przetwarzających, wspierając zrównoważony rozwój systemów ochrony zdrowia w zglobalizowanym świecie.

Dyrektywa transgraniczna oraz RODO, choć odnoszą się do różnych obszarów prawnych, mają wiele wspólnych elementów, które łączą je w kontekście

ochrony danych osobowych i międzynarodowej wymiany informacji. Oba akty prawne koncentrują się na ochronie praw jednostek, transparentności przetwarzania danych oraz zapewnieniu, że dane są przetwarzane w sposób zgodny z przepisami prawa. Jednocześnie oba dokumenty szczególną uwagę poświęcają kwestiom związanym z danymi medycznymi, które uznawane są za dane wrażliwe wymagające szczególnej ochrony. Podstawowym wspólnym elementem tych regulacji jest ochrona prywatności oraz dbałość o bezpieczeństwo przetwarzania danych osobowych. RODO, jako ogólno-unijna regulacja dotycząca ochrony danych, wprowadza zasady i mechanizmy, które mają zastosowanie do wszystkich sektorów, w tym opieki zdrowotnej. W tym kontekście art. 9 RODO, zakazujący przetwarzania danych szczególnej kategorii, w tym danych dotyczących zdrowia, z wyjątkiem przypadków przewidzianych w rozporządzeniu, znajduje bezpośrednie odzwierciedlenie w zasadach współpracy między państwami członkowskimi określonych w Dyrektywie transgranicznej. Nakłada ona wymóg przestrzegania rygorystycznych norm ochrony danych osobowych pacjentów, takich jak poufność, ograniczenie celu przetwarzania oraz minimalizacja zakresu przetwarzanych danych. Oba akty kładą duży nacisk na zapewnienie, że dane medyczne są przetwarzane w sposób bezpieczny i wyłącznie w uzasadnionych celach. Dyrektywa transgraniczna w swoich przepisach wskazuje na konieczność ochrony danych pacjentów podczas ich wymiany między państwami członkowskimi, co jest kluczowe w kontekście transgranicznej opieki zdrowotnej. RODO z kolei precyzuje, że przetwarzanie danych w takich sytuacjach wymaga zastosowania odpowiednich zabezpieczeń technicznych i organizacyjnych, co określono w art. 32 rozporządzenia. W tym zakresie oba akty prawne wzajemnie się uzupełniają, podkreślając wagę wdrażania takich środków jak pseudonimizacja, szyfrowanie oraz inne technologie zapewniające integralność i poufność danych osobowych. Wspólnym mianownikiem obu regulacji jest także konieczność transparentności w przetwarzaniu danych. RODO, w szczególności w art. 12, wymaga, aby osoby, których dane dotyczą, miały pełną świadomość, tego w jaki sposób ich dane są wykorzystywane. Dyrektywa 2011/24/UE odnosi się do tego poprzez promowanie przejrzystości w systemach opieki zdrowotnej i wymiany informacji medycznych, co jest kluczowe dla budowania zaufania pacjentów do transgranicznej opieki zdrowotnej.

Kolejnym istotnym aspektem łączącym oba dokumenty jest ustanowienie mechanizmów współpracy międzynarodowej w zakresie wymiany informacji medycznych. Dyrektywa transgraniczna wprowadza ramy prawne umożliwiające państwom członkowskim dzielenie się danymi pacjentów w celu zapewnienia

dostępu do odpowiedniej opieki zdrowotnej. RODO z kolei reguluje, w jaki sposób takie transfery danych mogą być realizowane zgodnie z zasadami ochrony danych, szczególnie w przypadkach, gdy dane przekazywane są poza granice Unii Europejskiej. Przepisy dotyczące transferów danych określone w artykułach 44 do 49 RODO uzupełniają cele dyrektywy, zapewniając, że dane medyczne pacjentów pozostają chronione nawet w kontekście międzynarodowej wymiany informacji. Oba akty prawne przewidują również odpowiedzialność podmiotów przetwarzających dane za przestrzeganie zasad ochrony danych. W RODO wyraźnie wskazano na odpowiedzialność administratorów danych i konieczność wdrożenia odpowiednich środków w celu ochrony danych osobowych, co znajduje odzwierciedlenie w zasadach określonych w Dyrektywie transgranicznej, które nakładają na państwa członkowskie obowiązek stosowania odpowiednich regulacji w zakresie wymiany danych medycznych.

Kolejnym istotnym elementem legislacji jest Dokument „*Guidance on the Ethical Conduct of Public Health Surveillance*" (World Health Organization 2017) opracowany przez Światową Organizację Zdrowia (WHO). Odgrywa on kluczową rolę w kształtowaniu standardów etycznych w zakresie transgranicznego przekazu danych medycznych. Jego wytyczne, oparte na zasadach ochrony praw człowieka, bezpieczeństwa danych oraz przejrzystości procesów przetwarzania, mają szczególne znaczenie w kontekście globalnych działań na rzecz zdrowia publicznego. Wymiana danych medycznych pomiędzy państwami członkowskimi, szczególnie w ramach działań związanych z nadzorem epidemiologicznym, wymaga przyjęcia jednolitych zasad etycznych i organizacyjnych, co podkreślają założenia tego dokumentu.

Jednym z najważniejszych elementów wytycznych WHO jest zasada proporcjonalności i minimalizacji danych (pojawiające się już w powyżej wspominanych dyrektywach). Podkreśla się, że przekazywane dane powinny być ograniczone wyłącznie do tych informacji, które są niezbędne do realizacji jasno określonych celów zdrowotnych, takich jak monitorowanie chorób zakaźnych, zarządzanie kryzysami zdrowotnymi czy ocena ryzyka. Taki sposób postępowania nie tylko zapewnia ochronę prywatności osób, których dane dotyczą, ale także zmniejsza ryzyko potencjalnych naruszeń wrażliwych informacji. Zasada ta, zgodna z postanowieniami art. 5 ust. 1 RODO, stanowi podstawę etycznego przetwarzania danych w kontekście międzynarodowym. WHO zwraca również uwagę na konieczność zastosowania odpowiednich zabezpieczeń technicznych i organizacyjnych w procesie transgranicznego przekazu danych. Dokument szczegółowo omawia środki takie jak szyfrowanie, pseudonimizacja oraz ograniczenie dostępu wyłącznie do

upoważnionych podmiotów. W kontekście międzynarodowej współpracy, gdzie poziom ochrony danych może się różnić w zależności od kraju, środki te mają kluczowe znaczenie dla zapewnienia integralności i poufności danych medycznych. Warto podkreślić, że wytyczne WHO wpisują się w standardy określone w art. 32 RODO, który nakłada na administratorów obowiązek wdrażania zabezpieczeń odpowiednich do ryzyka. Dokument podkreśla także, że transgraniczny przepływ danych medycznych powinien odbywać się w sposób transparentny, z poszanowaniem prawa do prywatności i integralności osób, których dane dotyczą. WHO rekomenduje, aby pacjenci byli informowani o zakresie, celu oraz podstawie prawnej przetwarzania ich danych, co koresponduje z art. 12 RODO, dotyczącym obowiązku transparentności wobec osób fizycznych. Chociaż w sytuacjach kryzysowych, takich jak epidemie, możliwe jest przetwarzanie danych bez zgody osób, których dotyczą, wytyczne WHO podkreślają, że takie działania powinny być jasno uzasadnione nadrzędnym interesem zdrowia publicznego oraz ograniczone w czasie.

Ważnym aspektem, na który zwraca uwagę WHO, jest odpowiedzialność państw i instytucji uczestniczących w procesie wymiany danych za zapewnienie zgodności swoich działań z zasadami etycznymi i prawnymi. Dokument zaleca regularne monitorowanie i ocenę skuteczności oraz zgodności procedur przetwarzania danych z obowiązującymi standardami. Postulat ten jest spójny z wymogami RODO dotyczącymi odpowiedzialności i rozliczalności, wyrażonymi w art. 24 i art. 30, które nakładają na administratorów i podmioty przetwarzające obowiązek prowadzenia rejestrów działań związanych z przetwarzaniem danych oraz oceny ryzyka. Wytyczne WHO podkreślają także znaczenie solidarności i współpracy międzynarodowej w zakresie nadzoru zdrowia publicznego. Transgraniczny przepływ danych medycznych, szczególnie w kontekście globalnych zagrożeń zdrowotnych, takich jak pandemie, wymaga zaufania między państwami oraz wspólnego podejścia do ochrony danych. Przekazywanie informacji wrażliwych powinno odbywać się na podstawie jasno określonych ram prawnych, które uwzględniają różnorodność systemów prawnych i standardów ochrony danych w poszczególnych krajach.

Zalecenia zawarte w „*Guidance on the Ethical Conduct of Public Health Surveillance*" nie tylko uzupełniają regulacje takie jak RODO, ale również stanowią istotny wkład w budowanie globalnego systemu ochrony danych medycznych. Ich wdrożenie przyczynia się do zapewnienia, że międzynarodowe działania w zakresie zdrowia publicznego są prowadzone w sposób zgodny z zasadami etyki, praw człowieka oraz ochrony prywatności.

Równie istotnym dokumentem, na który warto zwrócić uwagę jest, *Health Insurance Portability and Accountability Act* (HIPAA) (U.S. Department of Health and Human Services 1996), uchwalony w Stanach Zjednoczonych. Jest to jeden z kluczowych aktów rangi ustawy regulujących przetwarzanie danych medycznych. Jego celem jest zapewnienie prywatności oraz ochrony danych zdrowotnych pacjentów, a także ustanowienie standardów dotyczących ich przetwarzania i wymiany, szczególnie w kontekście rosnącej cyfryzacji systemów opieki zdrowotnej. HIPAA wprowadza liczne mechanizmy kontrolne, mające na celu zabezpieczenie danych, zarówno w obrocie krajowym, jak i w kontekście międzynarodowym. Choć akt ten jest ograniczony terytorialnie do jurysdykcji Stanów Zjednoczonych, jego regulacje mają istotne znaczenie również dla transgranicznego transferu danych medycznych, szczególnie w przypadku współpracy międzyinstytucjonalnej czy badawczej.

W kontekście transgranicznego transferu poufnych danych medycznych, HIPAA określa zasady ochrony danych zdrowotnych poprzez wymóg przestrzegania standardów prywatności i bezpieczeństwa określonych w *Privacy Rule* oraz *Security Rule*. *Privacy Rule* definiuje, w jaki sposób chronione dane zdrowotne (ang. *Protected Health Information*, PHI) mogą być wykorzystywane i ujawniane, zarówno w celach leczniczych, jak i badawczych. Z kolei Security Rule ustanawia obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie elektronicznych danych zdrowotnych (ang. ePHI). W odniesieniu do transferu danych poza granice Stanów Zjednoczonych, HIPAA w sposób pośredni reguluje tę kwestię, wymagając, aby podmioty objęte przepisami (ang. *covered entities*) oraz ich partnerzy biznesowi (ang. *business associates*) zapewniali zgodność z obowiązującymi standardami niezależnie od lokalizacji.

Istotnym elementem HIPAA jest zasada minimalizacji danych, która wymaga, aby przekazywane dane zdrowotne były ograniczone do informacji niezbędnych do realizacji danego celu. W przypadku międzynarodowej wymiany danych ma to szczególne znaczenie, gdyż redukuje ryzyko nieuprawnionego ujawnienia wrażliwych informacji. Ponadto, HIPAA nakłada na podmioty przetwarzające obowiązek monitorowania i raportowania ewentualnych naruszeń danych, co pozwala na szybką reakcję w przypadku incydentów bezpieczeństwa. W kontekście transferu transgranicznego szczególnie ważna jest także konieczność zawierania odpowiednich umów, tzw. *Business Associate Agreements* (BAA), które określają obowiązki i odpowiedzialność stron w zakresie ochrony danych zdrowotnych.

Porównując HIPAA do RODO, zauważyć można zarówno podobieństwa, jak i różnice w podejściu do ochrony danych medycznych. Oba akty prawne podkreślają znaczenie prywatności oraz wdrażania odpowiednich zabezpieczeń technicznych i organizacyjnych w przetwarzaniu danych zdrowotnych. Zarówno RODO, jak i HIPAA wymagają minimalizacji danych, transparentności oraz ograniczenia celu przetwarzania. Jednocześnie, RODO stosuje bardziej uniwersalne podejście, obejmując wszystkie rodzaje danych osobowych i definiując szczegółowe zasady dotyczące transferów danych poza Europejski Obszar Gospodarczy, co wyrażone jest m.in. w artykułach 44-50 rozporządzenia. Różnice między tymi regulacjami wynikają głównie z zakresu ich stosowania oraz charakteru. HIPAA jest specyficznym aktem prawnym, skoncentrowanym na ochronie danych zdrowotnych w Stanach Zjednoczonych, i nie odnosi się bezpośrednio do innych kategorii danych osobowych. Natomiast RODO wprowadza kompleksowe regulacje dotyczące ochrony danych we wszystkich sektorach, w tym także w obszarze medycznym. Co więcej, RODO przewiduje bardziej szczegółowe mechanizmy dotyczące zgody osoby, której dane dotyczą, oraz środków ochrony praw jednostek w przypadku naruszenia ich prywatności, takie jak możliwość zgłoszenia skargi do organu nadzorczego czy prawo do bycia zapomnianym.

W praktyce, w sytuacjach wymagających transgranicznego transferu danych medycznych między Stanami Zjednoczonymi a państwami Unii Europejskiej, konieczne jest pogodzenie wymagań wynikających zarówno z HIPAA, jak i z RODO. Proces ten wymaga uwzględnienia specyfiki obu regulacji, takich jak zawieranie odpowiednich umów transferowych zgodnie z RODO czy przestrzeganie zasad określonych w BAA. Tym samym, chociaż HIPAA i RODO różnią się w wielu aspektach, oba akty prawne mają wspólny cel: zapewnienie wysokiego poziomu ochrony danych zdrowotnych wrażliwych, niezależnie od granic geograficznych.

SCHREMS II

Kluczowym punktem w międzynarodowej legislacji dotyczącej medycznych danych osobowych jest decyzja Trybunału Sprawiedliwości Trybunału Europejskiego (TSUE) w sprawie *Schrems II* (wyrok Trybunału Sprawiedliwości UE (TSUE) w sprawie C-311/18). Orzeczenie z lipca 2020 roku znacząco zmieniło zasady międzynarodowego transferu danych osobowych, w tym danych medycznych, które wymagają szczególnej ochrony ze względu na ich wrażliwy charakter. Unieważnienie mechanizmu *Privacy Shield* pomiędzy UE a USA oraz

ograniczenia dotyczące stosowania standardowych klauzul umownych (SCC) w sytuacjach, gdy ochrona danych w państwach trzecich jest niewystarczająca, nałożyły na administratorów i podmioty przetwarzające nowe obowiązki. Decyzja ta wymaga gruntownej oceny zgodności transferów z przepisami RODO oraz wdrożenia dodatkowych zabezpieczeń, takich jak pseudonimizacja, szyfrowanie czy inne środki techniczne i organizacyjne. W artykule omówiono kluczowe konsekwencje prawne orzeczenia *Schrems II* dla sektora ochrony zdrowia, analizując ryzyka wynikające z międzynarodowych przepływów danych oraz przedstawiając praktyczne rozwiązania i rekomendacje pozwalające na dostosowanie procesów do nowych wymogów prawnych. Orzeczenie wprowadziło istotne zmiany w zasadach regulujących międzynarodowy transfer danych osobowych. Unieważnienie decyzji Komisji Europejskiej dotyczącej programu *Privacy Shield*, który stanowił podstawę przesyłania danych osobowych między Unią Europejską a Stanami Zjednoczonymi, podważyło bezpieczeństwo transferów danych do państw trzecich. Jednocześnie Trybunał utrzymał w mocy standardowe klauzule umowne (SCC), jednak uzależnił ich stosowanie od przeprowadzenia przez administratorów szczegółowej analizy przepisów obowiązujących w państwie odbiorcy danych i wdrożenia dodatkowych zabezpieczeń w przypadku braku odpowiedniego poziomu ochrony. Dla sektora ochrony zdrowia, który w dużej mierze opiera się na transgranicznych przepływach danych w ramach badań klinicznych, współpracy międzynarodowej czy zdalnych usług medycznych, skutki tej decyzji są szczególnie doniosłe. Dane medyczne, będące szczególną kategorią danych osobowych w rozumieniu RODO, wymagają najwyższego poziomu ochrony. Wyrok *Schrems II* stawia przed podmiotami przetwarzającymi dane konieczność wnikliwej analizy warunków prawnych w państwach trzecich oraz wdrażania zaawansowanych mechanizmów zabezpieczeń, takich jak pseudonimizacja, szyfrowanie czy przechowywanie danych wyłącznie na serwerach zlokalizowanych w Unii Europejskiej.

Ocena zgodności z RODO wymaga również prowadzenia szczegółowych analiz ryzyka, takich jak *Transfer Impact Assessment*, które uwzględniają lokalne przepisy dotyczące ochrony danych i możliwość niekontrolowanego dostępu służb publicznych do przesyłanych informacji. W państwach takich jak Stany Zjednoczone, gdzie przepisy takie jak FISA 702 dopuszczają szeroki dostęp do danych przez organy państwowe, wdrożenie dodatkowych zabezpieczeń staje się kluczowe dla zapewnienia ochrony prywatności osób, których dane są przetwarzane. Decyzja ta wymusza także weryfikację istniejących umów dotyczących przetwarzania danych oraz audyt obecnych mechanizmów zabezpieczeń.

Administratorzy danych oraz podmioty przetwarzające są zobowiązane do zapewnienia, że partnerzy biznesowi w państwach trzecich spełniają standardy wynikające z przepisów unijnych, co nierzadko wymaga renegocjacji umów lub zmiany stosowanych praktyk. Niedostosowanie się do wymogów wynikających z decyzji *Schrems II* może prowadzić do poważnych konsekwencji, takich jak wysokie kary administracyjne, odpowiedzialność cywilna czy utrata reputacji. Jednocześnie przestrzeganie tych standardów, choć kosztowne i skomplikowane, pozwala na budowanie zaufania oraz wzmacnianie ochrony praw podstawowych osób, których dane są przetwarzane. Dla sektora medycznego oznacza to nie tylko konieczność dostosowania się do zmieniających się wymogów prawnych, ale również szansę na wzmocnienie pozycji w globalnym obiegu danych dzięki transparentnym i zgodnym z prawem procesom zarządzania danymi.

ŚWIADOMA ZGODA

Agencja badań medycznych (Agencja Badań Medycznych 2023c) definiuje świadomą zgodę jako „niezależne i dobrowolne wyrażenie przez uczestnika swojej woli udziału w konkretnym badaniu klinicznym, po uzyskaniu informacji o wszystkich aspektach badania, które mają znaczenie dla decyzji uczestnika o udziale, lub – w przypadku małoletnich i uczestników niezdolnych do wyrażenia zgody – zezwolenie lub zgoda ich wyznaczonych zgodnie z prawem przedstawicieli na objęcie ich badaniem klinicznym." (Agencja Badań Medycznych 2023b). Definicja ta może być rozbita na kilka kluczowych elementów, które stanowią fundament procesu uzyskiwania świadomej zgody, zarówno w badaniach klinicznych, jak i w szerszym kontekście ochrony praw pacjentów. Pierwszym i najistotniejszym elementem w definicji jest „niezależne i dobrowolne wyrażenie woli przez uczestnika". Oznacza to, że zgoda musi być wyrażona w sposób, który nie jest obarczony żadnym przymusem, naciskiem ani podstępem. Uczestnik musi mieć pełną swobodę decyzji, zarówno jeśli chodzi o wyrażenie zgody, jak i jej późniejsze wycofanie, bez obawy o jakiekolwiek negatywne konsekwencje. Przymus – czy to w postaci presji ze strony personelu medycznego, czy też z innych powodów – czyni zgodę nieważną, ponieważ podważa jej dobrowolność, co jest kluczowym aspektem w prawie ochrony danych osobowych i praw pacjentów (Kubiak 2022) .

Kolejnym ważnym elementem jest „uzyskanie informacji o wszystkich aspektach badania, które mają znaczenie dla decyzji uczestnika" (Agencja Badań Medycznych, „Świadoma zgoda na udział w badaniu", Pacjent w badaniach

klinicznych, dostęp 10 kwietnia 2025). Świadoma zgoda nie może zostać udzielona bez pełnej informacji na temat badania, w które pacjent ma zamiar się zaangażować. Uczestnik musi zostać poinformowany o celu badania, jego metodzie, potencjalnych ryzykach i korzyściach, a także wszelkich innych kwestiach, które mogą wpłynąć na jego decyzję o udziale. Warto podkreślić, że obowiązek informacyjny w kontekście badań klinicznych ma charakter szczególny na tle ogólnego prawa pacjenta do informacji – zakres i szczegółowość przekazywanych danych są znacznie szersze (Ustawa z dnia 6 listopada 2008 r). Co istotne, przekazywana informacja powinna być nie tylko kompletna, ale także dostosowana do indywidualnych potrzeb konkretnego pacjenta, z uwzględnieniem jego stanu zdrowia, wieku, wykształcenia oraz sytuacji rodzinnej, co wynika zarówno z zasad etyki medycznej, jak i wytycznych GCP (Dobrej Praktyki Klinicznej) (ICH-GCP 2016). Konieczność przekazania tej informacji w sposób jasny, zrozumiały i kompletny jest fundamentem etycznym i prawnym procesu uzyskiwania zgody, a jej brak może prowadzić do naruszenia praw pacjenta.

W przypadku „małoletnich i uczestników niezdolnych do wyrażenia zgody", zgoda musi być uzyskana przez ich przedstawicieli prawnych – rodziców, opiekunów prawnych lub inne osoby uprawnione do podejmowania decyzji w imieniu osoby niepełnoletniej lub niezdolnej do wyrażenia zgody. Dzieci, małoletni i osoby niepełnosprawne umysłowo, nie mogą wyrazić w pełni świadomej zgody z powodu wieku lub stanu zdrowia, dlatego też przedstawiciel prawny staje się istotnym uczestnikiem procesu uzyskiwania zgody. Zgoda przedstawiciela musi być także oparta na pełnej informacji o badaniu, a decyzja powinna uwzględniać najlepszy interes osoby, której zgoda dotyczy.

Świadoma zgoda pacjenta stanowi podstawę zarówno w etyce, jak i prawie, szczególnie w kontekście badań naukowych oraz leczenia. Zgodnie z polskim prawem, obowiązek uzyskania świadomej zgody wynika przede wszystkim z ustawy o zawodach lekarza i lekarza dentysty (Ustawa z dnia 5 grudnia 1996 r.). Art. 34 ust. 1 stanowi, że lekarz jest zobowiązany uzyskać zgodę pacjenta na udzielenie świadczeń zdrowotnych, chyba że przepisy stanowią inaczej (Kos, Furtak-Niczyporuk 2018). Ponadto, w przypadku, gdy świadczenie zdrowotne wiąże się z badaniami naukowymi, konieczność uzyskania zgody wynika z przepisów dotyczących ochrony praw osób biorących udział w badaniach medycznych, jak wskazuje m.in. art. 37 ust. 1 ustawy o badaniach klinicznych produktów leczniczych stosowanych u ludzi (Ustawa z dnia 9 marca 2023 r.). Nakłada on obowiązek uzyskania świadomej zgody pacjenta przed przeprowadzeniem badań (Świderska 2019).

W kontekście badań naukowych, zwłaszcza transgranicznych, uzyskanie świadomej zgody pacjenta staje się szczególnie istotne, ponieważ wymagania prawne różnią się w zależności od jurysdykcji. Zgodnie z RODO, art. 9 ust. 2 przetwarzanie danych osobowych dotyczących zdrowia jest dozwolone tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na to wyraźną zgodę. Zgoda ta musi być dobrowolna, świadoma, jednoznaczna i udzielona na piśmie lub za pomocą innej formy - np. protokołowanej, która zapewnia zapis zgody pacjenta. Warto podkreślić, że RODO szczegółowo reguluje również zasady dotyczące przechowywania, udostępniania oraz transferu danych poza terytorium UE, wskazując w artykule 44 na konieczność stosowania odpowiednich zabezpieczeń, gdy dane osobowe są przekazywane do krajów trzecich.

Sytuacja, gdy leczenie lub badania są przeprowadzane poza granicami państwa, stanowi wyzwanie związane z uzyskaniem świadomej zgody na leczenie. W takich przypadkach może zachodzić konieczność dostosowania formularzy zgody do lokalnych regulacji prawnych oraz zapewnienia, że pacjent lub uczestnik badania w pełni rozumie przekazywane mu informacje o przewidzianych działaniach. Zgodnie z art. 3 RODO, przepisy rozporządzenia stosują się do przetwarzania danych osobowych osób znajdujących się na terytorium Unii Europejskiej, niezależnie od tego, czy administrator danych ma siedzibę w Unii, czy poza nią. Oznacza to, że w przypadku transgranicznego transferu danych medycznych, podmioty przetwarzające te dane muszą przestrzegać przepisów ochrony danych osobowych, nawet jeśli badania odbywają się w kraju spoza UE. W praktyce oznacza to konieczność zawarcia odpowiednich umów transferowych lub zapewnienia adekwatnego poziomu ochrony danych zgodnie z art. 46 RODO.

Ochrona danych osobowych jest bezpośrednio powiązana z procesem uzyskiwania świadomej zgody, ponieważ dane zdrowotne pacjenta są klasyfikowane jako dane wrażliwe. Zgodnie z art. 9 ust. 1 RODO, przetwarzanie danych dotyczących zdrowia jest zabronione, chyba że zachodzą określone wyjątki, takie jak zgoda osoby, której dane dotyczą. Dlatego też zapewnienie bezpieczeństwa danych podczas ich przetwarzania, zwłaszcza w kontekście badań transgranicznych, wymaga stosowania odpowiednich środków ochrony, takich jak pseudonimizacja, szyfrowanie czy kontrola dostępu. Przepisy RODO nakładają na podmioty przetwarzające obowiązek wprowadzenia odpowiednich środków technicznych i organizacyjnych, jak wskazuje art. 32, który wymaga, aby środki te były dostosowane do ryzyka związanego z przetwarzaniem danych osobowych.

W literaturze przedmiotu omawia się, że proces uzyskania świadomej zgody na leczenie nie powinien być traktowany jako formalność, lecz jako element

budowania zaufania między pacjentem a instytucją medyczną (Podgórniak, Piróg, Putowski i in. 2016). Zgoda pacjenta jest wyrazem poszanowania jego autonomii i prywatności. Zgoda pacjenta wyznacza zakres ingerencji w sferę jego prywatności, a jej udzielenie musi odbywać się po rzetelnym poinformowaniu o celach, metodach oraz ryzyku związanym z leczeniem lub badaniem.

Uzyskanie świadomej zgody pacjenta w kontekście badań naukowych i leczenia, zwłaszcza realizowanych poza granicami państwa, wymaga szczególnej uwagi na przepisy prawne oraz zasady ochrony danych osobowych. Niezależnie od miejsca przeprowadzania badań, proces ten musi spełniać wymogi prawne dotyczące zgody oraz ochrony danych, zarówno w krajach członkowskich Unii Europejskiej, jak i poza nią. Wymaga to uwzględnienia różnic kulturowych, językowych oraz dostosowania procedur do lokalnych regulacji, przy jednoczesnym zapewnieniu odpowiedniego poziomu ochrony danych pacjentów.

SPOSOBY ZABEZPIECZENIA DANYCH MEDYCZNYCH

W kontekście transgranicznego transferu danych medycznych, zastosowanie odpowiednich środków ochrony, takich jak szyfrowanie i pseudonimizacja, jest nie tylko zalecane, ale wręcz wymagane przez obowiązujące przepisy prawne.

Szyfrowanie to proces polegający na przekształcaniu danych w formę nieczytelną dla osób nieuprawnionych, za pomocą zaawansowanych algorytmów kryptograficznych, takich jak AES (*Advanced Encryption Standard*) czy RSA (*Rivest–Shamir–Adleman*) (Katarzyna Nocuń 2024). Dzięki temu nawet w przypadku przechwycenia zaszyfrowanych informacji przez osoby trzecie ich treść pozostaje niedostępna. Klucz deszyfrujący, będący integralnym elementem szyfrowania, umożliwia odwrócenie tego procesu wyłącznie uprawnionym podmiotom. Takie rozwiązanie znajduje szczególne zastosowanie podczas przesyłania danych między instytucjami medycznymi w różnych krajach, gdzie ryzyko przechwycenia informacji podczas transmisji jest znaczące.

Z kolei pseudonimizacja to metoda przetwarzania danych osobowych, w ramach której dane identyfikujące są zastępowane wartościami zastępczymi, które same w sobie nie pozwalają na ustalenie tożsamości osoby. Definicja tego procesu została zawarta w art. 4 pkt 5 RODO i wskazuje, że jest to mechanizm mający na celu zmniejszenie ryzyka związanego z przetwarzaniem danych. Pseudonimizacja znajduje zastosowanie w badaniach naukowych i analizach statystycznych, gdzie pełna identyfikacja osób fizycznych nie jest konieczna. Na przykład w badaniach klinicznych każdy uczestnik może zostać oznaczony unikalnym identyfikatorem,

takim jak "Uczestnik_001", przy czym dane pozwalające na identyfikację osoby są przechowywane oddzielnie i odpowiednio zabezpieczone.

Istotne różnice między szyfrowaniem a pseudonimizacją wynikają z ich zastosowania i efektów działania. Szyfrowanie koncentruje się na ochronie poufności danych podczas ich przesyłania i przechowywania, czyniąc je całkowicie nieczytelnymi bez klucza deszyfrującego. Pseudonimizacja natomiast zmniejsza ryzyko naruszenia prywatności, utrudniając powiązanie danych z konkretną osobą fizyczną, lecz pozostaje procesem odwracalnym, co umożliwia administratorowi danych przywrócenie oryginalnej formy informacji w uzasadnionych przypadkach.

Oba narzędzia, choć różnią się funkcją, są komplementarne. Szyfrowanie jest niezbędne w sytuacjach wymagających ochrony danych przed nieuprawnionym dostępem podczas transmisji, na przykład gdy dane pacjentów są przesyłane w ramach międzynarodowych konsultacji medycznych. Pseudonimizacja natomiast znajduje zastosowanie po zakończeniu przesyłu, w kontekście dalszego przetwarzania danych, szczególnie w celach badawczych. Dla przykładu dane medyczne po zaszyfrowaniu podczas transferu mogą zostać pseudonimizowane po dotarciu do miejsca przeznaczenia, aby zapewnić ich dalsze przetwarzanie w sposób zgodny z zasadą minimalizacji danych wynikającą z art. 5 ust. 1 RODO (Mednis 2022).

Pomimo różnic w zastosowaniu i mechanizmie działania, zarówno szyfrowanie, jak i pseudonimizacja pełnią istotną rolę w ochronie danych osobowych. W kontekście transgranicznego transferu danych medycznych stosowanie obu tych środków zapewnia zgodność z wymogami prawnymi oraz minimalizuje ryzyko związane z przetwarzaniem informacji o szczególnym charakterze wrażliwości, takich jak dane dotyczące zdrowia. Właściwe wdrożenie tych metod wymaga jednak nie tylko stosowania odpowiednich narzędzi technicznych, ale także procedur organizacyjnych, które uwzględniają specyfikę przetwarzanych danych oraz kontekst ich wykorzystania.

PODSUMOWANIE

Ochrona danych osobowych stanowi obecnie kwestię o fundamentalnym znaczeniu, szczególnie w kontekście postępującej digitalizacji i globalizacji procesów przetwarzania informacji. Dane pacjentów, jako jedne z najbardziej wrażliwych i poufnych, wymagają szczególnej troski oraz zastosowania najwyższych standardów bezpieczeństwa. Zapobieganie ich nieuprawnionemu ujawnieniu czy wyciekowi jest nie tylko obowiązkiem prawnym, ale również moralnym

i społecznym, który wymaga najwyższego stopnia zaangażowania oraz środków o najwyższej skuteczności.

Szczególna uwaga powinna być poświęcona wymianie danych o charakterze transgranicznym, która stwarza dodatkowe wyzwania wynikające z różnorodności systemów prawnych, uwarunkowań kulturowych oraz kontekstów politycznych w różnych państwach. Rozbieżności w przepisach dotyczących ochrony danych osobowych mogą prowadzić do niejednoznaczności interpretacyjnych, a w konsekwencji – do zagrożeń dla integralności i poufności danych. Wobec tego konieczne jest zapewnienie harmonizacji procedur, ścisłego przestrzegania międzynarodowych standardów oraz monitorowania, aby wymiana informacji odbywała się w sposób zgodny z prawem oraz respektujący prawa pacjentów.

Naszych praw- jako że prawie każdego człowieka, tym bardziej obywatela Unii Europejskiej, można uznać za podmiot prawa medycznego- pomagają strzec liczne, szczegółowe regulacje. Obejmują one zarówno przepisy krajowe, jak i unijne, a także regulacje poszczególnych państw, w których podmioty publiczne lub prywatne mogą mieć dostęp do naszych poufnych danych. Akty prawne, takie jak RODO czy dyrektywa transgraniczna, stanowią rozbudowane przez co ciężkie w odbiorze regulacje. Ich złożoność wynika jednak z konieczności precyzyjnego uregulowania kwestii dotyczących ochrony wrażliwych danych, które mają kluczowe znaczenie dla zachowania prywatności i bezpieczeństwa obywateli.

Najważniejsze zasady, takie jak świadoma zgoda oraz szyfrowanie danych, mogą wydawać się pozornie niejasne. Ich rola jednak zdecydowanie przewyższa potencjalne trudności związane z ich wdrożeniem. Proces implementacji tych zasad jest dodatkowo wspierany przez szczegółowe akty prawne oraz interpretacje prawnicze, które ułatwiają ich stosowanie w praktyce.

BIBLIOGRAFIA

Literatura

Bertinato, L., Busse, R., Fahy, N., Legido-Quigley, H. et al.
2005 Cross-Border Health Care in Europe, Copenhagen: WHO on behalf of the European Observatory on Health Systems and Policies.

Iordache, C., Ciochină, I., Roxana, P.
2013 Medical tourism – between the content and socio-economic development goals. Development strategies, Romanian Journal of Marketing, nr 1, s. 31–42.

Kos, M., Furtak-Niczyporuk, M.
2018 Świadoma zgoda pacjenta na leczenie szpitalne, Teka Komisji Prawniczej PAN Oddział w Lublinie, 11(1), s. 169–182.

Kubiak, R.
2022 Prawo medyczne, Warszawa: Wolters Kluwer, s. 163.

Lunt, N., Carrera, P.
2010 Medical tourism: Assessing the evidence on treatment abroad, Maturitas, 66(1), s. 27–32.

Mednis, A.
2022 Ochrona danych osobowych w praktyce, Warszawa: C.H. Beck.

Niezgoda, A., Kowalska, K.
2015 Turystyka medyczna – istota, zakres i konsekwencje rozwoju zjawiska, Rozprawy Naukowe Akademii Wychowania Fizycznego we Wrocławiu, 49, s. 126–134.

Nocuń, K.
2024 Nasze dane medyczne trafią do chmury. Kluczowy będzie ich operator, dostępne online: https://www.prawo.pl/zdrowie/ehds-czyli-dane-medyczne-w-chmurze%2C526964.html (dostęp: 10.04.2025).

Podgórniak, M., Piróg, M., Putowski, M., Padała, O. et al.
2016 Rola świadomej zgody pacjenta w procesie diagnostyki i leczenia = The role of patient informed consent in the process of diagnosis and treatment, Journal of Education, Health and Sport, 6(4), s. 103–114.

Świderska, M.
2019 Zgoda pacjenta na zabieg medyczny, Toruń: Dom Organizatora.

Raporty

Agencja Badań Medycznych
2023a Proces uzyskiwania świadomej zgody: Rekomendacje dla badaczy, Warszawa.
2023b Świadoma zgoda na udział w badaniu. Pacjent w badaniach klinicznych, dostępne online: https://pacjentwbadaniach.abm.gov.pl/pwb/moj-udzial-w-badaniu/swiadoma-zgoda-na-udzial-w-badaniu.html (dostęp: 10.04.2025).

2023c Świadoma zgoda na udział w badaniu. Pacjent w badaniach klinicznych, dostępne online: https://pacjentwbadaniach.abm.gov.pl/pwb/moj-udzial-w-badaniu/swiadoma-zgoda-na-udzia/196,Swiadoma-zgoda-na-udzial-w-badaniu.html (dostęp: 10.04.2025).

Akty prawne i dokumenty urzędowe

Parlament Europejski i Rada UE (2011). Dyrektywa 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej. Dziennik Urzędowy UE, L 88, 4 kwietnia 2011. [Online] Available at: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32011L0024 [Accessed 10 Apr. 2025].

Parlament Europejski i Rada UE (2016). Rozporządzenie (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). Dziennik Urzędowy UE, L 119, 4 maja 2016. [Online] Available at: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679 [Accessed 10 Apr. 2025].

Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty. Dz.U. 1997 nr 28 poz. 152 z późn. zm.

Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Dz.U. 2023 poz. 1545, art. 9 w zw. z art. 25.

Ustawa z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi. Dz.U. 2023 poz. 605.

WHO (2017). WHO guidelines on ethical issues in public health surveillance. Geneva: World Health Organization. Licence: CC BY-NC-SA 3.0 IGO.

U.S. Department of Health and Human Services (1996). Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Assistant Secretary for Planning and Evaluation. [Online] Available at: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996 [Accessed 23 Apr. 2025].

ICH-GCP (2016). Guideline for Good Clinical Practice E6(R2). International Council for Harmonisation of Technical Requirements for

Pharmaceuticals for Human Use, section 4.8.7.

Trybunał Sprawiedliwości Unii Europejskiej (2020). Wyrok w sprawie C-311/18 - Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillianowi Schremsowi.

PERSONAL DATA PROTECTION IN INTERNATIONAL CLINICAL TRIALS AND CROSS-BORDER PATIENT TREATMENT

Abstract: Modern medicine increasingly transcends national borders, both in the context of clinical research and the treatment of patients in countries other than their country of citizenship or where their therapy originally began. Such international medical cooperation brings many benefits but also requires special attention to the protection of patients' personal data. This chapter discusses the key legal requirements related to the processing and transfer of data in such situations, with particular emphasis on the European General Data Protection Regulation (GDPR), World Health Organization (WHO) guidelines (such as the Guidance on the Ethical Conduct of Public Health Surveillance), the Schrems II decision (CJEU, Case C-311/18), and other crucial European and international legal instruments. The chapter presents the fundamental principles of data protection, including the necessity of obtaining informed patient consent and implementing appropriate safeguards such as encryption and pseudonymization, which are essential to ensuring the confidentiality of sensitive information. Special attention is given to the unique nature of medical data as a particularly protected category, and the technical and legal challenges that may arise when transferring such data across borders. The chapter also reviews selected non-European regulations, such as the U.S. HIPAA, which play a significant role in international medical cooperation, especially in multinational clinical trials. For comparative purposes, national regulations are also discussed. Real-life examples illustrate common challenges faced by young professionals, students, and researchers — such as lawful data transfers to third countries, identifying potential risks, and methods of mitigating them. The aim of this publication is not only to present current legal regulations and relevant non-legal sources but also to explain their practical application in a clear and accessible way.

Keywords: personal data protection, GDPR, international medical cooperation, medical data, data transfer, clinical trials, HIPAA, patient privacy, pseudonymization, patient consent, information security, international law, Schrems II decision

MGR **MIKOŁAJ RESZKOWSKI**

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU

BIOBANKI I OCHRONA DANYCH OSOBOWYCH

Streszczenie: Celem rozdziału jest analiza ram prawnych regulujących działalność biobanków w Polsce w kontekście ochrony danych osobowych, ze szczególnym uwzględnieniem przepisów RODO. Początkowo, praca definiuje pokrótce biobanki, a następnie analizuje krajowe oraz unijne ramy prawne, które mogą mieć zastosowanie do działalności biobanków. Analiza obejmuje takie zagadnienia jak podstawy przetwarzania danych osobowych, metodyka zabezpieczeń zbieranych danych, a także sposób ustalania okresu przetwarzania danych osobowych. Rozdziałodnosi się również do kwestii traktowania materiałów zbieranych przez biobank jako danych osobowych, mając na względzie kryterium identyfikowalności osoby fizycznej. Praca wykazuje również braki regulacyjne oraz potrzebę stworzenia kompleksowych przepisów dedykowanych działalności biobanków. Wskazuje również na ryzyko, jakie niesie zbyt ogólne podejście do ochrony danych w kontekście badań naukowych opartych na materiale biologicznym. W końcowej części pracy postuluje się stworzenie jasnych, szczegółowych ram prawnych, które zapewnią równowagę pomiędzy rozwojem biobankowości a ochroną praw jednostki.

Słowa kluczowe: biobank, RODO, dane osobowe, ochrona prywatności

WSTĘP

Rozwój współczesnej technologii, w szczególności tej związanej z lepszym poznawaniem organizmu człowieka wymaga analizowania ogromnych ilości informacji. Większy przepływ danych umożliwia dokładniejsze zrozumienie tego, jakie czynniki mogą wpływać na nasz organizm, z uwzględnieniem wielu zmiennych, jak na przykład lokalizacja, klimat, czy tryb życia. Tego typu nowoczesne metody wymagają jednak ogromnych nakładów finansowych i organizacyjnych, a także wsparcia w reżimie obowiązujących norm prawnych. Nie bez znaczenia pozostają tu przyjęte za elementarne standardy prawne i etyczne, chociażby te związane z zakazem handlu częściami ludzkiego ciała (Pawlikowska,

Pawlikowski, Krekora-Zając 2023, s. 154). Innymi słowy, środowisko prawne przyjazne dla nowoczesnych metod badawczych jest istotnym elementem postępu w medycynie – braki regulacyjne, czy też zbyt ogólne normy, mogą stanowić jedynie blokadę.

Tym samym, zważając na istotność zagadnienia, konieczne jest przeanalizowanie obecnych ram prawnych w Polsce, które odnoszą się do funkcjonowania nowoczesnych rozwiązań umożliwiających rozwój współczesnej medycyny, w szczególności w odniesieniu do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (ogólne rozporządzenie o ochronie danych, cyt. dalej jako RODO). Dogłębna analiza poszczególnych metod badawczych w naukach związanych ze zdrowiem wychodziłaby poza ramy artykułu naukowego, dlatego też publikacja ta skupi się na prawnych aspektach funkcjonowania biobanków, z uwzględnieniem regulacji funkcjonujących na poziomie Polski oraz Unii Europejskiej. Celem rozdziau jest dojście do wniosków, czy obecny ekosystem prawny umożliwia rzeczywisty rozwój biobankowości, z uwzględnieniem zabezpieczenia praw osób przekazujących im materiały biologiczne.

DEFINICJA BIOBANKU

Definicje biobanku nie są jednolite – w większości wypadków skupiają się jednak na wspólnym mianowniku, czyli oczywiście na kolekcjonowaniu materiału biologicznego w celach badawczych, w szczególności pochodzących od człowieka komórek, organów, czy tkanek, z różnym poziomem zorganizowania i systematyzowania tych danych. Biobankiem będzie zwłaszcza podmiot zajmujący się badaniami naukowymi, w ramach którego przechowywane są materiały od osób zdrowych oraz chorych (por. Kozera et al. 2018, s. 13-14). Komisja Europejska w swym dokumencie 25 rekomendacji dotyczących etycznych, prawnych i społecznych implikacji badań genetycznych biobank określa jako ”same zbiory próbek biologicznych plus powiązane z nimi bazy danych, dopuszczające pewien poziom dostępności, osiągalności i wymiany dla celów naukowych”. Biobanki można też podzielić, w zależności od tego, czy działają samodzielnie lub też w ramach konkretnych jednostek badawczych, czy też w zależności od tego, jakie rodzaje próbek (czy też w jakim celu) zbierają – na przykład *The Swedish Twin Registry* zbierający próbki pochodzące od bliźniaków (por. Mascalzoni 2015, s. 15-16). Brak jest obecnie legalnej definicji biobanku w polskim prawie.

RAMY PRAWNE W POLSCE

W dyskusji o fundamentalnych zasadach funkcjonowania biobankowości trzeba wspomnieć o wartościach konstytucyjnych – stanowią one przedpole do dyskusji o ewentualnych regulacjach szczegółowych. Art. 47 Konstytucji RP tworzy gwarancję poszanowania prawa jednostki do prywatności, z którego wywnioskować można takie elementy jak konieczność pozyskania świadomej zgody na pobranie materiałów od dawcy, prawo do żądania usunięcia danych z biobanku oraz prawo do informacji, w jaki sposób materiały i dane z nimi związane są wykorzystywane – innymi słowy, skupiając się na ochronie danych osobowych (Obara 2017, s. 115). Z art. 51 ust. 2 Konstytucji RP, pomimo tego że stanowi przede wszystkim wytyczną dla władzy, wynika również podmiotowe prawo jednostki do autonomii informacyjnej, tj. możliwość samodzielnego decydowania o ujawnianiu podmiotom trzecim informacji o swojej osobie (por. np. wyroki Trybunału Konstytucyjnego o sygn. SK 40/01 i K 45/02, K 25/13).

Odnosząc się do mniej abstrakcyjnych norm prawnych, w kwestii ochrony danych osobowych, jako regulację mającą tu prymat jest RODO, które swym zasięgiem obejmuje również Polskę. Poszczególne aspekty zastosowania RODO do biobankowości poddane zostaną analizie w dalszej części publikacji, biorąc pod uwagę wysoki poziom skomplikowania zagadnienia, w dużej mierze wynikający z ogólnego charakteru RODO.

Zwrócić należy uwagę na regulacje odnoszące się do działalności podmiotów leczniczych. Bycie związanym konkretnymi przepisami sektorowymi możemy rozpatrywać dwutorowo. Pierwszym z nich jest sytuacja, w której biobank jest podmiotem prowadzącym działalność leczniczą czy też jednostką organizacyjną takiego podmiotu i w ramach tejże działalności kolekcjonuje i analizuje materiał biologiczny. Wtedy dane osobowe pozyskiwane przez ten podmiot i służące do badań związane mogą być z udzielaniem świadczeń zdrowotnych. Tym samym, obok przepisów RODO, będą miały również art. 13, 14 oraz art. 23–30a ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta – np. objęcie przechowywanych danych tajemnicą zawodową czy też stosowanie odpowiednich przepisów związanych z tworzeniem i udostępnianiem dokumentacji medycznej. W pozostałym jednak zakresie, same badania medyczne, nie wspominając już o tak wąskiej tematyce jak biobankowość, nie są uregulowane w sposób szczegółowy i całościowy w ustawie o działalności leczniczej czy też ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta – w dużej mierze, konieczne jest oparcie się na ogólnych zasadach prawa (Osiejewicz 2023, s. 585-586, 589-590). Brak jest w Polsce jednolitego

aktu prawnego nakierowanego na usystematyzowanie tego, jak biobanki powinny działać, a nawet same przepisy dot. badań medycznych są bardzo fragmentaryczne, odnosząc się m.in. do takich kwestii jak eksperymenty medyczne w przepisach ustawy o zawodzie lekarza i lekarza dentysty.

Dojść można do wniosku, że na poziomie prawa krajowego jedynymi normami mającymi zastosowanie do biobanków są wartości konstytucyjne mające nieostry i abstrakcyjny charakter. Problem braków regulacyjnych może momentami być rozwiązany stosowaniem regulacji sektorowych (np. dot. działalności podmiotów leczniczych), ale nie zawsze będą one odpowiednio dostosowane do specyfiki funkcjonowania biobanków. Nie oznacza to oczywiście, że biobanki w praktyce funkcjonują w sposób całkowicie swobodny i niezapewniający stosownych standardów. W obrocie funkcjonuje szereg wytycznych i zaleceń odnoszących się do działalności biobanków, np. utworzone przez BBMRI (*Biobanking and BioMolecular resources Research Infrastructure*) „Standardy jakości dla biobanków polskich" (Matera-Witkiewicz et. al. 2021). Dokument ten, w części odnoszącej się do zarządzania procesami przetwarzania danych osobowych, ma charakter ogólnikowy, aczkolwiek samo jego istnienie należy ocenić pozytywnie. Dokument podkreśla konieczność poszanowania prywatności uczestników programów biobanków na każdym etapie. Jego autorzy wskazują na konieczność udostępniania dokumentacji dot. ochrony danych, formularzy zgody oraz szczegółowych materiałów informacyjnych przed pobraniem materiału biologicznego. Standardy akcentują również prawo uczestnika do wycofania zgody na różnych etapach badania, obowiązek informowania o wynikach badań istotnych klinicznie oraz konieczność zapewnienia prawa do niewiedzy o wynikach badań i stanie własnego zdrowia. Dokument określa zasady postępowania z materiałem biologicznym osób niezdolnych do wyrażenia zgody oraz wymogi formalne dotyczące pozyskiwania i dokumentowania świadomej zgody

ZASTOSOWANIE RODO DO FUNKCJONOWANIA BIOBANKÓW

RODO jest regulacją o bardzo ogólnym charakterze – ustawodawca unijny sam określa ten akt jako „neutralny technicznie" (por. motyw 15 RODO). Założeniem jest stworzenie przepisów, które nie wymagają stałej aktualizacji i doprecyzowywania, aby nadążyć za rozwojem nowoczesnych technologii. Podejście to oczywiście należy uznać za zasadne, aczkolwiek w wielu wypadkach ogólnikowość może utrudniać funkcjonowanie wysoce wyspecjalizowanych organizacji.

RODO ma zastosowanie w sytuacji, gdy konkretny podmiot, decydujący o celach i sposobach przetwarzania danych („administrator") przetwarza „dane osobowe", czyli wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przypadku biobanków, za dane osobowe, które wynikają z przechowywanego materiału biologicznego, można uznać m.in. informacje o trybie życia, dane genetyczne czy też dane z badań przeprowadzonych na konkretnych próbkach (Hallinan 2021, s. 135). Warto nadmienić, że sporne jest to, czy sam materiał biologiczny (np. próbka krwi) będzie stanowił dane osobowe, czy też taki przymiot dopiero nadać należy informacjom wydedukowanym z tego materiału w wyniku badań (Hallinan 2021, s. 136). Zdania na ten temat są podzielone. Część przedstawicieli doktryny przyjmuje, że definicję danych osobowych należy zawężać, biorąc pod uwagę rozwój technologii umożliwiających daleko idącą dedukcję, nawet z bardzo ograniczonych informacji. Sprawiałoby to, że dane anonimowe niemalże zanikną – wszystko będzie uznawane za dane osobowe. Innymi słowy, jedynie nieodwracalne uczynienie danych nieidentyfikowalnymi dla kogokolwiek będzie mogło być uznane za niepodlegające pod RODO. Takie podejście dostrzec można np. w Decyzji Wykonawczej Komisji Europejskiej nr 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz.U. L 199 z 7.6.2021). Z drugiej strony, pojawiają się głosy przeciwne, wskazujące na zasadność stosowania mniej rygorystycznych kryteriów niż kompletna niemożliwość identyfikacji (por. Schneider 2022, s. 180-183). Orzecznictwo nie jest w tej materii bogate. Na gruncie nieobowiązującej już ustawy o ochronie danych osobowych z 1997 r., w wyroku z dnia 7 czerwca 2013 r., (sygn. akt II SA/Wa 666/13) Wojewódzki Sąd Administracyjny w Warszawie przyjął rygorystyczne podejście i stwierdził, że „nie ulega wątpliwości, że wyizolowana próbka DNA jest nośnikiem informacji genetycznej, a także zawiera informacje o stanie zdrowia. Każda próbka materiału genetycznego będzie oznaczona specjalnym kodem, który umożliwi skarżącej pełną i jednoznaczną identyfikację osoby fizycznej poprzez powiązanie próbki z danymi osobowymi klienta, w których posiadaniu będzie skarżąca." Pomimo tego, że ustawa o ochronie danych osobowych z 1997 r. już nie obowiązuje, można przyjąć, że wyrok nie stracił na aktualności – definicja danych osobowych w ustawie z 1997 r. oraz RODO jest w praktyce identyczna (Mednis 2018, s. 92). Tym samym, pomimo sporu w literaturze, dojść można do wniosku, że przy ocenie, czy mamy styczność z danymi osobowymi, prymat ma kryterium przyjmujące, że rzadko będziemy mieli do czynienia z procesowaniem

informacji niemających charakteru danych osobowych, które jest podejściem bardzo rygorystycznym. Niestety, to w gestii administratora jest ostateczne uznanie, w jakim zakresie musi on dostosować swoje działania do wymogów wynikających z RODO poprzez przyjęcie, że przetwarza lub nie przetwarza danych osobowych (Shabani, Chassang, Marelli 2021, s. 50).

PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

Przetwarzanie danych osobowych wymaga odpowiedniej podstawy prawnej – zgodnie z zasadą zgodności z prawem przewidzianą w art. 5 ust. 1 lit. a) RODO. Kluczowym zagadnieniem jest w tym wypadku przetwarzanie „danych osobowych szczególnej kategorii" (potocznie często nazywane „danymi wrażliwymi") przez biobank – RODO określa je poprzez enumeratywne wymienienie generalnych kategorii danych, wliczając w to istotne dla biobanków „dane genetyczne" oraz „dane dotyczące zdrowia". Dane genetyczne dookreślone zostały w art. 4 pkt 13 RODO, natomiast dane odnoszące się do zdrowia - w art. 4 pkt 15 RODO. Art. 9 RODO w ust. 1 ustanawia generalny zakaz przetwarzania danych osobowych szczególnej kategorii, z wyłączeniem sytuacji przewidzianych w ust. 2 tego artykułu. Nie wszystkie będą miały oczywiście zastosowanie do funkcjonowania biobanków – najistotniejsze, w ocenie autora, będą tu podstawy prawne wskazane w art. 9 ust. 2 lit. a), h) oraz j) RODO, tzn. odpowiednio wyraźna zgoda osoby na przetwarzanie jej danych, przetwarzanie dla celów szeroko pojętego zdrowia oraz przetwarzanie w celach badawczych i archiwalnych. W literaturze istnieją dwie sprzeczne koncepcje co do relacji pomiędzy art. 6 oraz art. 9 RODO. Pierwszy pogląd wskazuje na to, że art. 9 RODO stanowi *lex specialis* wobec art. 6 i tworzy samodzielne podstawy przetwarzania danych, zaś zgodnie z podejściem odmiennym, dopiero spełnienie odpowiedniej przesłanki z art. 6 umożliwia dalsze badanie spełnienia komplementarnych przesłanek z art. 9 (Schneider 2022, s. 195). Na potrzeby analizy przedstawionej w dalszej części pracy, autor przyjmie pierwszą z omawianych koncepcji, dokonując szczegółowej interpretacji właściwych fragmentów art. 9 ust. 2 RODO oraz oceny możliwości zastosowania wskazanych tam podstaw prawnych do przetwarzania danych osobowych w ramach działalności biobanku.

Pierwszą przesłanką, która legalizowałaby przetwarzanie danych wrażliwych, jest wyraźna zgoda osoby, której dane dotyczą. Zgoda ta nie może być dorozumiana (musi stanowi skonkretyzowane oświadczenie), a także musi być udzielona bez przymusu, z uwzględnieniem brak nierówności pomiędzy sytuacją

administratora i podmiotu danych (Schneider 2022, s. 196). W praktyce funkcjonowania funkcjonowaniu biobanków, istotne jest odpowiednie udokumentowanie takiej zgody (zgodnie z wymogiem wskazanym bezpośrednio w art. 7 ust. 1 RODO) oraz zadbanie o spełnienie wszystkich przesłanek konstytuujących ważną zgodę, za definicją z art. 4 pkt 11 RODO. Grupa Robocza ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych powołana na mocy art. 29 Dyrektywy 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. (powszechnie określana jako „Grupa Robocza Art. 29") zaleca w wytycznych nr 17/ENWP259, aby zgoda przyjmowała formę pisemnego oświadczenia, w celu pewnego spełnienia kryterium „wyraźnej" (*explicit*); tylko bowiem wówczas będzie spełniała kryteria wyraźnej. Wymóg pozyskania wyraźnej zgody na przetwarzanie danych osobowych dotyczących zdrowia (zgodnie z art. 9 ust. 2 lit. a) RODO) stanowi odpowiedni mechanizm, realizujący wartości konstytucyjne omówione wcześniej, tj. zasadę autonomii informacyjnej jednostki. Zakładając oczywiście, że administrator zadba o to, aby proces wyrażania zgody przez podmiot danych spełniał przewidziane prawem kryteria. Z drugiej jednak strony, zgoda uznawana jest w literaturze za przesłankę niewystarczającą dla prowadzenia działań badawczych, w szczególności ze względu na problemy z rozszerzaniem operacji przetwarzania (np. obejmując też nimi metody badawcze). Zwracając uwagę na to, że zgoda powinna być udzielana w konkretnych celach (por. Schneider 2022, s. 199). Podkreślić w tym miejscu należy, że zgoda na pobranie materiału genetycznego (wliczając w to ewentualne przeprowadzanie na nim badań i inne przewidziane przez biobank operacje), jest zgodą oddzielną od tej wyrażanej w odniesieniu do przetwarzania danych osobowych (Guarda, Bincoletto 2023, s. 373).

Biorąc pod uwagę, że w związku z badaniami na przechowywanym w biobanku materiale genetycznym może dojść do uzyskania przez analizujących ten materiał informacji o stanie zdrowia dawcy, które mogłyby okazać się dla niego istotne (np. o występowaniu konkretnej choroby) zastanowić się należy, czy biobank miałby tu podstawy prawne do udzielania dawcy próbek takiej informacji. Odpowiedzi zdaje się udzielać art. 9 ustawy o prawach pacjenta i Rzeczniku praw pacjenta. Jak się przyjmuje w literaturze, osoba wykonująca zawód medyczny, która pozyska informacje mające dla pacjenta znaczenie, powinna je mu przekazać (Krekora-Zając 2019, s. 177-178), co potwierdza tez orzecznictwo

(tak: Wyrok Sądu Apelacyjnego w Szczecinie z dnia 11 sierpnia 2016 r., sygn. akt I ACa 300/16), pomimo tego, że literalne brzmienie przepisu nie wskazuje na to jednoznacznie.

Zastosowanie podstawy prawnej określonej w art. 9 ust. 2 lit. h) oraz j) RODO (odpowiednio realizacji świadczeń zdrowotnych lub też przetwarzania dla celów archiwalnych) stanowiłoby dla biobanków znacznie mniej uciążliwe rozwiązanie praktyczne niż pozyskiwanie zgody na podstawie art. 9 ust. 2 lit. a). Należy jednak podkreślić, że możliwość wykorzystania przesłanek z lit. h) oraz j) jest ściśle uzależniona od istnienia odpowiednich przepisów prawa Unii Europejskiej lub ustawodawstwa krajowego państwa członkowskiego, które by taką ewentualność dopuszczały. W kontekście polskim można argumentować, że niektóre aspekty świadczeń zdrowotnych realizowanych w ramach działalności biobanków znajdują oparcie w istniejących przepisach sektorowych regulujących działalność leczniczą (przykładowo w ustawie o działalności leczniczej czy ustawie o prawach pacjenta). Jednakże przepisy te nie uwzględniają w pełni specyfiki funkcjonowania biobanków, które łączą w sobie elementy działalności klinicznej, badawczej oraz archiwizacyjnej. Brak dedykowanych regulacji prawnych dostosowanych do złożonej natury biobanków znacząco ogranicza możliwość wykorzystania ich pełnego potencjału naukowego i medycznego. W rezultacie, obie omawiane podstawy prawne (lit. h i j) mogą znaleźć zastosowanie jedynie w wybranych aspektach działalności biobanków, nie zapewniając kompleksowych ram prawnych dla całokształtu procesów przetwarzania danych osobowych w tych instytucjach.

Istnienie tzw. miękkiego prawa, chociażby jak przywołane powyżej zalecenia BBMRI, nie kształtuje realnie tego, na jakich zasadach biobanki mogłyby przetwarzać dane osobowe w kontekście posiadania odpowiednich przesłanek legalizujących. Tego typu wytyczne i zalecenia nie tworzą podstaw prawnych przetwarzania danych ani też nie wyznaczają konkretnych okresów retencji danych – co oczywiście wynika z braku przymiotu powszechnie obowiązującego prawa. Tym samym, opierając się jedynie na generalnych regułach tworzonych przez RODO, biobanki mogą napotykać istotne problemy związane z ustaleniem podstawy przetwarzania, która realizuje prawa jednostki, ale też zapewnia pewną swobodę działania biobanku i realizację jego misji. Pewne wsparcie zapewnia motyw 33 RODO wskazujący, że osoby, których dane dotyczą, powinny mieć możliwość (w sytuacji, w której ich dane są przetwarzane w celach badawczych) wyrażenia zgody na niektóre obszary badań naukowych, o ile te badania są uznawane za etyczne. Tym samym, biobank może w praktyce przyjąć mechanizm, który zakłada, że zgoda wyrażana będzie na pewne rodzaje badań. Nie zwolni to jednak

administratora z obowiązku zadbania o poinformowanie podmiotu danych (na ile to możliwe) o planowanych metodach przetwarzania danych.

ZABEZPIECZENIA

Zadaniem administratora na gruncie RODO jest odpowiednie zarządzanie wewnętrznymi procesami, tak aby w dopasowany do czynności przetwarzania sposób zadbać o bezpieczeństwo danych osobowych. W praktycznym wymiarze, oczywistym jest konieczność dostosowania zabezpieczeń (zwłaszcza informatycznych) w biobanku do kryteriów wynikających z art. 32 RODO. Jedynie odpowiednie środki techniczne i organizacyjne pozwolą odpowiednio zarządzać ryzykiem związanym z przetwarzanymi przez biobank informacjami. Wspierają w tym administratora takie dokumenty jak analiza ryzyka czy też rejestr czynności przetwarzania, uregulowany w art. 30 RODO. Tworzenie odpowiedniej dokumentacji, jakkolwiek stanowiące obciążenie, jest istotnym mechanizmem, który umożliwia administratorowi realizację zasady rozliczalności, wynikającą z art. 5 ust. 2 RODO, a także odpowiednio zarządzać ryzykiem w swojej organizacji i odpowiednio rozplanować poszczególne czynności przetwarzania, mając na względzie wynikające z nich zagrożenia.

USTALENIE OKRESU PRZETWARZANIA DANYCH OSOBOWYCH

Jedną z podstawowych zasad wyrażonych w art. 5 ust. 1 lit. e) RODO jest obowiązek administratora do ograniczenia przechowywania danych. Administrator, ustalając cel przetwarzania danych, zobligowany jest jednocześnie zweryfikować, jak długo musi przetwarzać dane w ramach tego celu, aż do jego osiągnięcia. Jednocześnie nie może on ustalić okresu przetwarzania, który byłby „nieskończony" (Fajgielski 2022). Bardzo trudne jest jednakże zastosowanie tej reguły do działalności badawczej, a w szczególności podmiotów, których zadaniem jest przeprowadzanie badań na dużych ilościach materiałów biologicznych, umożliwiając porównania pomiędzy poszczególnymi próbkami (czy też zbiorami informacji odnoszących się do tych próbek) (Cippitani, 2023, s. 186-187). Brak szczegółowej regulacji, która ustalałaby jasne ramy okresów retencji danych osobowych jest tu istotnym utrudnieniem dla działalności biobanków.

ANONIMIZACJA I PSEUDONIMIZACJA

Biobanki stosują różnorodne systemy przechowywania i udostępniania informacji innym organizacjom i badaczom. Jedną z praktycznych metod jest zastępowanie danych osobowych dawcy kodami, które uniemożliwiają badaczowi identyfikację źródła próbki (Kogut-Czarkowska 2023, s. 33). Powstaje pytanie, czy takie podejście faktycznie prowadzi do anonimizacji danych. Rozwiązanie, które mogłoby ograniczyć stosowanie przepisów RODO – szczególnie w kontekście problemu ograniczenia czasu przetwarzania danych – opierałoby się na uznaniu, że biobank skutecznie przeprowadził anonimizację, czyli przetworzył informacje w sposób uniemożliwiający powiązanie ich z konkretną osobą fizyczną. Należy podkreślić, że pseudonimizacja, czyli technika przetwarzania danych, w której informacje można powiązać z osobą przy użyciu dodatkowych danych, nie jest wystarczająca. Dane pseudonimizowane nadal klasyfikowane są jako dane osobowe i podlegają regulacjom RODO (Ho 2017, s. 96-97).

Próbując zrozumieć pojęcie „anonimizacji" warto odnieść się do motywu 26 RODO, który wskazuje na konieczność kierowania się rozsądnymi kryteriami przy ustaleniu, czy przetwarzane dane umożliwiają zidentyfikowanie osoby fizycznej, nie podając tutaj jednak bardziej szczegółowych kierunków. Z kolei Wytyczne 05/2014 Grupy Roboczej Art. 29 (obecnie: Europejskiej Rady Ochrony Danych) w sprawie technik anonimizacji z 10 kwietnia 2014 r. mogą stanowić doprecyzowanie tego podejścia, aczkolwiek przyjmujące bardzo wysoki standard anonimizacji. Konkretyzując EROD przyjął, że anonimizacja następuje, gdy identyfikacja jest „realistycznie niemożliwa" (ang. „*reasonably impossible*" – znaczenie anglojęzycznego tekstu wytycznych zdaje się sugerować „zdroworozsądkową" niemożliwość).

Można więc dojść do wniosku, że podobnie jak utrudnione jest jednoznaczne ustalenie momentu granicznego pomiędzy przyznaniem danej próbce/informacji przymiotu danych osobowych a uznaniem jej za informacje niemające przymiotu danych osobowych, tak samo niejasne jest zastosowanie pojęcia anonimizacji danych. Przyjęcie tak rygorystycznego kryterium anonimizacji, zakładając, że ją właśnie chciałby osiągnąć biobank, utrudniałoby przekazywanie pacjentom/dawcom informacji odnoszących się do analizowanych materiałów biologicznych ich dotyczących, np. w sytuacji wykrycia u nich incydentalnie rzadkiej choroby. Tym samym doszłoby do pozbawienia dawcy możliwości uzyskania wiadomości dotyczących stanu zdrowia, co może mieć przełożenie na żywotne interesy podmiotu danych (Kogut-Czarkowska 2023, s. 36).

WYCOFANIE ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

Zgodnie z art. 7 ust. 3 RODO, osobie, której dane dotyczą, przysługuje prawo do wycofania zgody na przetwarzanie jej danych osobowych. Przepis ten ma zastosowanie zarówno do „zwykłej" zgody wyrażonej w trybie art. 6 ust. 1 lit. a) jak i również wcześniej przywołanej wyraźnej zgody, opartej na art. 9 ust. 2 lit. a) (Fajgielski 2022). RODO wskazuje jednocześnie, że wycofanie zgody nie ma wpływu na przetwarzanie danych, które nastąpiło przed wycofaniem zgody. Stosowanie się do tej regulacji może jednak budzić wątpliwości praktyczne. Najbardziej dostrzegalnym problemem jest ciągłość badań przeprowadzanych przy użyciu materiału biologicznego osoby wycofującej zgodę. Przy braku szczególnej regulacji, która tworzyłaby inną podstawę prawną przetwarzania danych niż zgoda podmiotu danych, zastosowanie ma dosyć rygorystyczne podejście wynikające z art. 7 ust. 3 RODO. Konieczne jest wtedy całkowite zaprzestanie dalszego przetwarzania danych osobowych, wliczając w to zakończenie dalszych badań w odniesieniu do konkretnej próbki materiału biologicznego (por. Colcelli 2023, s. 141-143).

ZAKOŃCZENIE

Biobanki to wyspecjalizowane organizacje, których głównym obszarem działalności jest zbieranie dużych ilości materiału biologicznego, analizowanie go i wyciąganie z niego wniosków (lub też udostępnianie przechowywanych materiałów w tych celach badaczom). Tego typu wyspecjalizowana działalność wymaga stabilnych ram prawnych – ogólnikowe regulacje nie są niestety wystarczające. Niniejszy rozdział wskazuje na kluczowe problemy dotyczące biobanków: niejednoznaczny status próbek biologicznych jako danych osobowych w rozumieniu RODO, praktyczne trudności z wdrożeniem skutecznej anonimizacji spełniającej wymogi prawne przy zachowaniu wartości naukowej oraz problematyczność określania konkretnych okresów retencji danych wymaganych przez RODO w kontekście długoterminowych badań.

Obecnie, tematyka biobankowości została zepchnięta przez ustawodawcę na dalszy plan. Jest to podejście, które należy ocenić negatywnie. Niniejszy rozdział w wielu miejscach podkreślał, że obecne ramy prawne nie są wystarczające dla zapewnienia sprawnego funkcjonowania oraz rozwoju biobanków. Wiele z wątpliwości wynikających z braków w przepisach mogłoby być należycie rozwiązanych kompleksową regulacją odnoszącą się do badań medycznych oraz

biobanków. Sama luka w prawie zdaje się być dostrzeżona przez polskie władze, aczkolwiek nie spotkała się ona do tej pory z konkretną reakcją. Jak wskazuje Uchwała nr 10 Rady Ministrów z dnia 4 lutego 2020 r. w sprawie przyjęcia programu wieloletniego pn. Narodowa Strategia Onkologiczna na lata 2020-2030 (M.P.2022.814 t.j. z dnia 19 sierpnia 2022 r.), problemami dla współczesnej biobankowości jest rozproszona struktura, ograniczony zakres działania i braki w przepisach, w tym odnoszących się do zgód pacjentów i regulowania dostępu do danych. Tym samym, konieczne jest przez ustawodawcę polskiego stworzenie konkretnych ram prawnych dla działalności biobanków – RODO samo w sobie nie jest tu wystarczające.

BIBLIOGRAFIA

Colcelli, V.
2023 Consent Withdrawal. What is the procedure if consent will later be withdrawn, w: GDPR Requirements for Biobanking Activities Across Europe, red. V. Colcelli et al., Springer.

Cippitani, R.
2023 Ethical Principles and Legal Provisions. What ethical principles apply to biobanking activities?, w: GDPR Requirements for Biobanking Activities Across Europe, red. V. Colcelli et al., Springer.

Fajgielski, P.
2022 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. II, Warszawa, art. 9, LEX.

Guarda, P., Bincoletto, G.
2023 Scientific Research and the Biomedical Sector. Requirements and Methods for Planning and Managing a "Data Protection by Design" Project, w: GDPR Requirements for Biobanking Activities Across Europe, red. V. Colcelli et al., Springer.

Hallinan, D.
2021 Protecting Genetic Privacy in Biobanking through Data Protection Law, Oxford University Press.

Ho, C.
2017 Challenges of the EU General Data Protection Regulation for Biobanking and Scientific Research, Journal of Law, Information and Science, 84 (JlLawInfoSci 5).

Kogut-Czarkowska, M.
2023 Anonymisation: The Trap for Biobanking (Part II). Why the Anonymisation Could Be a Trap for the Biobanking Activity? Can There Really Be Anonymisation in the Research Biobanks?, w: GDPR Requirements for Biobanking Activities Across Europe, red. V. Colcelli et al., Springer.

Kozera, Ł.
2018 Biobankowanie ludzkiego materiału biologicznego dla celów naukowych w Polsce i w Europie, Studia Iuridica, nr 73.

Krekora-Zając, D.
2019 Legal aspects of biobanking HBS for scientific purposes in Poland, Studia Prawnicze, nr 4 (220).

Mascalzoni, D.
2015 Ethics, Law and Governance of Biobanking. National, European and International Approaches, Springer.

Mednis, A.
2018 Ochrona danych genetycznych jako danych osobowych, Studia Iuridica, nr 73.

Obara, P.
2017 Ochrona danych genetycznych w ramach prawa do prywatności dawców – uwagi na tle regulacji o ochronie danych osobowych, Przegląd Prawniczy TBSP UJ, nr 2.

Osiejewicz, J.
2023 Poland, w: GDPR Requirements for Biobanking Activities Across Europe, red. V. Colcelli et al., Springer.

Pawlikowska, J., Pawlikowski, J., Krekora-Zając, D.
2023 Biobanking of human biological material and the principle of non-commercialisation of the human body and its parts, Bioethics, Vol. 37(2).

Schneider, G.
2022 Health Data Pools Under European Data Protection and Competition Law. Health as a Digital Business, vol. 17, Springer.

Shabani, M., Chassang, G., Marelli, L.
2021 The Impact of the GDPR on the Governance of Biobank Research, w: GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe, red. S. Slokenberga, O. Tzortzatou, J. Reichel, Springer.

BIOBANKS AND THE PROTECTION OF PERSONAL DATA

Abstract: The purpose of this chapter is to analyze the legal framework governing the activities of biobanks in Poland in the context of personal data protection, with particular emphasis on the provisions of the GDPR. Initially, the paper briefly defines biobanks, and then analyzes the national and EU legal frameworks that may apply to the activities of biobanks. The analysis covers such issues as: the grounds for processing of personal data, the methodology for securing the collected data, and methods of determining the appropriate data retention period. The chapter also addresses the issue of treating materials collected by a biobank as personal data, bearing in mind the criteria of identifiability of an individual. The work also demonstrates regulatory shortcomings and the need for comprehensive laws dedicated to the activities of biobanks. It also points out the risks posed by an overly general approach to data protection in the context of scientific research based on biological material. The work is concluded by presenting arguments for the creation of a clear, detailed legal framework that strikes a balance between the development of biobanking and the protection of individual rights.

Keywords: biobank, GDPR, personal data, privacy protection

Niniejsza publikacja porusza różnorodne aspekty prawne związane z ochroną danych osobowych, analizując je na gruncie administracji publicznej, cyberbezpieczeństwa, sztucznej inteligencji oraz medycyny. Autorzy, reprezentujący środowisko akademickie wielu polskich uczelni, w sposób kompleksowy i interdyscyplinarny omawiają najważniejsze problemy i wyzwania prawne, przed jakimi stoją współczesne społeczeństwa informacyjne.

ISBN **978-83-68410-16-7**