

Waldemar Perdion¹

Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie

https://doi.org/10.29316/9788368103359_6

OCRONA DANYCH OSOBOWYCH W CYBERPRZESTRZENI

PERSONAL DATA PROTECTION IN CYBERSPACE

Streszczenie

W dobie dynamicznego rozwoju technologii cyfrowych, temat ochrony danych osobowych nabiera szczególnego znaczenia. Nasza codzienność coraz silniej przenika się z cyberprzestrzenią – miejscem, gdzie wymiana informacji, komunikacja, zakupy, a nawet aktywność zawodowa odbywają się za pośrednictwem Internetu. W tym wirtualnym świecie niemal każda nasza aktywność wiąże się z przetwarzaniem danych – często bardzo wrażliwych. Ochrona danych osobowych to jedno z kluczowych wyzwań XXI wieku. W epoce, w której informacja stała się jedną z najcenniejszych walut, dane osobowe mogą być zarówno zasobem, jak i zagrożeniem. Ich niewłaściwe przetwarzanie, przechowywanie czy wykorzystywanie może prowadzić nie tylko do naruszenia prywatności jednostki, ale również do realnych strat finansowych, kradzieży tożsamości, manipulacji wyborczych, a nawet destabilizacji systemów państwowych. W tym kontekście ochrona danych nie jest już wyłącznie domeną specjalistów z zakresu informatyki czy prawa, ale staje się sprawą publiczną i społeczną, dotyczącą każdego użytkownika technologii

¹ <https://orcid.org/0000-0001-6956-8508>, e-mail: waldemar.perdion@uth.edu.pl

cyfrowych. Celem niniejszego opracowania jest podjęcie refleksji nad skutecznością obowiązujących regulacji prawnych dotyczących ochrony danych osobowych w warunkach rzeczywistości cyfrowej. Czy obecne przepisy są wystarczające, by zapewnić realne bezpieczeństwo użytkownikom Internetu? Czy są w stanie chronić nie tylko prywatność zwykłych obywateli, ale również interesy instytucji publicznych i bezpieczeństwo państwa? W dobie rosnącej liczby cyberataków, wycieków danych oraz nadużyć ze strony podmiotów komercyjnych, pytania te stają się nie tylko zasadne, ale wręcz palące. W niniejszej pracy postaram się przybliżyć istotę zagadnienia, wskazać najważniejsze wyzwania, a także zaprezentować aktualne ramy prawne i praktyczne rozwiązania, które mają służyć ochronie danych osobowych w cyberprzestrzeni.

Słowa kluczowe: dane osobowe, przestępczość, cyberprzestrzeń, bezpieczeństwo, informacje

Abstract

In an era of dynamic development in digital technologies, the issue of personal data protection is gaining particular importance. Our daily lives are increasingly intertwined with cyberspace – a place where information exchange, communication, shopping, and even professional activities take place online. In this virtual environment, almost every activity involves the processing of data – often highly sensitive data. Personal data protection is one of the key challenges of the 21st century. In a time where information has become one of the most valuable currencies, personal data can be both a resource and a threat. Improper processing, storage, or use of such data can lead not only to violations of individual privacy but also to tangible financial losses, identity theft, electoral manipulation, and even the destabilization of state systems. In this context, data protection is no longer the exclusive domain of IT or legal specialists; it has become a public and social issue that affects every user of digital technologies. The purpose of this study is to examine the effectiveness of existing legal regulations concerning personal data protection in the digital world. Are the current regulations sufficient to ensure real security for internet users? Can they protect not only the privacy of ordinary citizens, but also the interests of public institutions and state security? In an age of increasing cyberattacks, data leaks, and abuses by commercial entities, these questions have become not only relevant but even urgent. In this paper, I will seek to explore the essence of the issue, identify the key challenges, and present the current legal framework and practical solutions for protecting personal data in cyberspace.

Keywords: personal data, crime, cyberspace, security, information

Wstęp

Informacja to jeden z najcenniejszych zasobów współczesnego świata. W dobie społeczeństwa informacyjnego stanowi ona dobro strategiczne, które należy skutecznie chronić. Wiedza – rozumiana jako umiejętność pozyskiwania, analizowania i wykorzystywania informacji – jest dziś fundamentem podejmowania decyzji na wszystkich poziomach funkcjonowania społeczeństwa: od indywidualnych obywateli, przez przedsiębiorstwa, aż po instytucje publiczne. Posiadanie informacji ułatwia planowanie, przewidywanie zagrożeń oraz efektywną realizację działań.

Właściwe gospodarowanie informacją, a także jej ochrona, są nieodłącznym elementem sprawnego funkcjonowania państwa i bezpieczeństwa jego obywateli. Ustawowe objęcie ochroną niektórych kategorii informacji oraz prawne uregulowanie dostępu do nich potwierdzają, że informacja została przez ustawodawcę uznana za dobro prawnie chronione. Współczesne podejście do informacji obejmuje zarówno jej wymiar materialny, jak i niematerialny – może ona przybierać formę idei, myśli, gestu, dźwięku, symbolu, dokumentu, dzieła sztuki, a także zapisów umownych. W tym szerokim kontekście mieszczą się również dane osobowe, będące jedną z najważniejszych i najbardziej wrażliwych kategorii informacji (Taczowska-Olszewska, Chałubińska-Jentkiewicz, Nowikowska, 2019, s. 11).

Pojęcie danych osobowych zostało po raz pierwszy szerzej ujęte w 1980 roku w wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD), gdzie zaproponowano definicję, która – w zmodyfikowanej formie – funkcjonuje do dziś. Według niej dane osobowe to wszelkie informacje dotyczące osoby zidentyfikowanej lub możliwej do zidentyfikowania (Rojszczak, 2019, s. 150).

Z kolei zgodnie z obowiązującym w Unii Europejskiej Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), dane osobowe oznaczają: „Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to taka, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową

lub społeczną tożsamość osoby fizycznej” (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

W praktyce oznacza to, że każda informacja, która może prowadzić do identyfikacji konkretnej osoby, nawet jeśli wymaga połączenia kilku elementów, uznawana jest za daną osobową. Szczególną kategorię stanowią dane wrażliwe, które ze względu na swój charakter wymagają dodatkowej ochrony. Zostały one zdefiniowane w art. 27 ust. 1 nieobowiązującej już ustawy o ochronie danych osobowych, a obecnie ich katalog został przeniesiony do art. 107 ust. 1 RODO. Obejmuje on m.in. informacje ujawniające:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub filozoficzne,
- przynależność wyznaniową, partyjną lub związkową,
- dane o stanie zdrowia, dane genetyczne, biometryczne, nałogach lub życiu seksualnym,
- dane dotyczące wyroków skazujących, postępowań sądowych i administracyjnych (Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych).

Zarówno dane zwykłe, jak i wrażliwe są przedmiotem szczególnego zainteresowania prawodawcy, ponieważ ich ujawnienie lub niewłaściwe przetwarzanie może prowadzić do naruszenia prywatności, dyskryminacji, a nawet zagrożenia dla wolności i bezpieczeństwa jednostki.

Współcześnie obserwujemy niezwykle dynamiczny proces przenoszenia coraz większej liczby aktywności człowieka do przestrzeni wirtualnej, będącej integralną częścią cyberprzestrzeni. Funkcjonowanie w niej stało się nieodzownym elementem życia społecznego, gospodarczego i politycznego. Korzyści płynące z wykorzystania cyberprzestrzeni są niepodważalne, jednak towarzyszą im również poważne zagrożenia – w tym możliwość jej wykorzystania w sposób sprzeczny z interesem państwa i obywateli.

Zgodnie z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne oraz powiązania między nimi i ich relacje z użytkownikami (Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne).

Sednem tej definicji są dwa kluczowe pojęcia: informacja oraz systemy teleinformatyczne. Informacja – jako zasób strategiczny – została dostrzeżona jako dobro wymagające szczególnej ochrony. Współcześnie traktowana jest nie tylko jako nośnik wiedzy, lecz także jako potencjalna broń, wykorzystywana na piątym teatrze działań wojennych – obok lądu, morza, powietrza i przestrzeni kosmicznej – jakim stała się cyberprzestrzeń (Lakomy, 2015, s. 63).

To także odrębna przestrzeń społeczna, w której zachodzą procesy komunikacji i wymiany gospodarczej. Wymaga ona odpowiedniego zabezpieczenia ze względu na interesy jej użytkowników – zarówno w zakresie ochrony danych osobowych, jak i ochrony nieletnich czy przeciwdziałania przestępczości (Lubasz, 2013). Do charakterystycznych cech cyberprzestrzeni zalicza się jej:

- rozległość (globalny zasięg),
- zdolność do łączenia zasobów w ogromną bazę danych,
- złożoność,
- bezprzestrzenność – brak fizycznych granic i wymiarów, jakie znamy ze świata realnego (Wasilewski, 2015).

W literaturze przedmiotu można odnaleźć różne definicje cyberprzestrzeni. M. Rojszczak przywołuje tę sformułowaną przez Departament Obrony Stanów Zjednoczonych, według której cyberprzestrzeń to: „Domena związana z użyciem elektronicznych i elektromagnetycznych urządzeń w celu gromadzenia, modyfikowania i wymiany danych za pomocą systemów sieciowych oraz związanej z nimi infrastruktury fizycznej” (Rojszczak, 2019, s. 53).

Autor jednocześnie podkreśla, że w odniesieniu do koncepcji Internetu, cyberprzestrzeń to przede wszystkim przestrzeń zastosowań i możliwości technicznych, której fizyczny wymiar trudno jest jednoznacznie zdefiniować. M. Rojszczak proponuje również najszerszą definicję cyberprzestrzeni, zgodnie z którą obejmuje ona wszelkie urządzenia zdolne do komunikacji sieciowej – niezależnie od tego, czy są w danym momencie podłączone do sieci publicznej. Internet pozostaje jej dominującą częścią, umożliwiającą globalną wymianę treści (Rojszczak, 2019, s. 54).

A. Bartnicki z kolei ujmuje cyberprzestrzeń jako przestrzeń komunikacyjną tworzoną przez systemy powiązań internetowych, pozwalającą użytkownikom na komunikację i budowanie relacji w czasie rzeczywistym.

Jego zdaniem jest to środowisko wymiany informacji za pomocą sieci i systemów komputerowych, w którym wszelkie działania mają odmienny charakter niż te podejmowane w świecie fizycznym (Bartnicki, 2020, s. 145).

Rozwój tzw. globalnej „internetomanii” oraz szeroka dostępność usług sieciowych niosą ze sobą poważne zagrożenia. Jednym z kluczowych problemów pozostaje możliwość przechwytywania danych wrażliwych przez niepowołane podmioty. Informacje te, ze względu na swoją specyfikę, mogą prowadzić m.in. do kradzieży technologii, ujawnienia rozwiązań konstrukcyjnych, kompromitacji systemów obrony, a w konsekwencji – do osłabienia lub nawet destabilizacji gospodarczej podmiotów, a w skrajnych przypadkach – całych państw (Bartnicki, 2020, s. 147).

W tym kontekście istotne staje się pojęcie cyberprzestępczości, które zostało zdefiniowane m.in. przez X Kongres ONZ w sprawie zapobiegania przestępczości i traktowania przestępców. W ujęciu szerokim cyberprzestępcstwo obejmuje wszelkie działania popełnione z użyciem systemów komputerowych lub sieci, jak również te, które ich dotyczą. Obejmuje to m.in. nielegalne posiadanie, udostępnianie czy rozpowszechnianie informacji za pomocą narzędzi cyfrowych. Zjawisko cyberprzestępczości staje się coraz powszechniejsze, a jego rosnący poziom trudności wykrywania i przeciwdziałania wynika m.in. z relatywnej anonimowości sprawców oraz transgranicznego charakteru przestępstw cyfrowych (Bartnicki, 2020, s. 147).

Każda nasza aktywność w Internecie – wyszukiwanie informacji, korzystanie z mediów społecznościowych, dokonywanie zakupów online czy logowanie się do aplikacji – pozostawia po sobie cyfrowy ślad. Jest to zespół informacji, które świadomie lub nieświadomie pozostawiamy w środowisku cyfrowym. Cyfrowy ślad obejmuje zarówno dane jawne (np. zdjęcia profilowe, komentarze, posty), jak i ukryte (adresy IP, dane lokalizacyjne, czas logowania czy kliknięcia w linki). Konsekwencje istnienia cyfrowych śladów są wielowymiarowe. Z jednej strony umożliwiają one tworzenie spersonalizowanych usług i udoskonalanie doświadczenia użytkownika. Z drugiej – mogą prowadzić do nadużyć, takich jak profilowanie, sprzedaż danych stronom trzecim, manipulacja informacjami czy kradzież tożsamości. Warto podkreślić, że cyfrowy ślad ma również znaczenie prawne – jego analiza może posłużyć jako dowód w sprawach sądowych, ale też jako narzędzie inwigilacji lub represji w rękach autorytarnych reżimów. Świadomość jego istnienia oraz umiejętność zarządzania nim stają się niezbędnymi kompetencjami w świecie cyfrowym.

Kwestie związane z ochroną danych osobowych w Polsce regulowane są zarówno przez prawo unijne, jak i krajowe. Fundamentalnym aktem prawnym obowiązującym na poziomie Unii Europejskiej jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., znane szerzej jako RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). Rozporządzenie to zaczęło obowiązywać we wszystkich państwach członkowskich Unii Europejskiej 25 maja 2018 roku i ujednoliciło zasady przetwarzania danych osobowych w całej UE. Wraz z nim przyjęto Dyrektywę 2016/680, dotyczącą przetwarzania danych osobowych w związku z zapobieganiem przestępczości, wykrywaniem i ściganiem przestępstw.

Zgodnie z art. 4 pkt 1 RODO, dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osoba możliwa do zidentyfikowania to taka, której tożsamość można ustalić bezpośrednio lub pośrednio, zwłaszcza na podstawie takich danych jak: imię, nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających jej tożsamość fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

RODO wprowadza katalog zasad przetwarzania danych osobowych (art. 5), a także nowe prawa i obowiązki dla administratorów danych i osób, których dane są przetwarzane. RODO znacząco rozszerzyło katalog praw przysługujących osobom fizycznym, których dane osobowe są przetwarzane. Osoby te, zwane osobami, których dane dotyczą, mają obecnie większy wpływ na to, w jaki sposób ich dane są wykorzystywane. Do najważniejszych praw tych osób należą:

- Prawo dostępu do danych – osoba ma prawo dowiedzieć się, czy jej dane są przetwarzane, a jeśli tak – uzyskać do nich dostęp oraz informacje o celu i zakresie przetwarzania,
- Prawo do sprostowania danych – umożliwia poprawienie danych nieprawidłowych lub ich uzupełnienie,
- Prawo do usunięcia danych („bycia zapomnianym”) – daje możliwość żądania usunięcia danych, gdy nie są już potrzebne, zgoda została cofnięta lub przetwarzanie odbywa się niezgodnie z prawem,

- Prawo do ograniczenia przetwarzania – np. w sytuacji, gdy osoba kwestionuje prawidłowość danych,
- Prawo do przenoszenia danych – umożliwia otrzymanie danych w ustrukturyzowanym formacie i ich przekazanie innemu administratorowi,
- Prawo do sprzeciwu – można sprzeciwić się przetwarzaniu danych, np. w celach marketingu bezpośredniego,
- Prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu – chroni przed automatycznym profilowaniem, które może wywoływać skutki prawne (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Zgodnie z RODO, administrator danych osobowych to podmiot (osoba fizyczna, prawna, organ publiczny, jednostka lub inny organ), który decyduje o celach i sposobach przetwarzania danych osobowych. Na administratorach ciąży szereg obowiązków mających na celu zapewnienie zgodnego z prawem i bezpiecznego przetwarzania danych.

Do podstawowych obowiązków administratora należą:

- Zasada rozliczalności – administrator musi być w stanie wykazać, że przetwarza dane zgodnie z zasadami określonymi w RODO,
- Minimalizacja danych – przetwarzane mogą być tylko te dane, które są niezbędne do realizacji danego celu,
- Obowiązek informacyjny – administrator jest zobowiązany poinformować osobę, której dane dotyczą, o celach i podstawach przetwarzania danych, czasie ich przechowywania, a także o przysługujących jej prawach,
- Zapewnienie bezpieczeństwa danych – administrator powinien stosować środki techniczne i organizacyjne zapewniające odpowiedni stopień ochrony danych,
- Zgłaszanie naruszeń danych – administrator ma obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego nie później niż w ciągu 72 godzin od jego wykrycia (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Najważniejszym dokumentem regulującym ochronę danych osobowych w cyberprzestrzeni jest również rozporządzenie unijne RODO. Określa ono zasady, narzędzia, instrumenty oraz środki ochrony danych osobowych w cyberprzestrzeni. Wprowadziło ono również kilka elementów odnoszących się wprost do ochrony danych w cyberprzestrzeni. Jednym z nich jest wspomniane wyżej prawo do bycia zapomnianym (Bakalarczyk-Burakowska, Nowicka, 2020, s. 78). Kolejną ważną regulacją jest określenie ram prawnych profilowania, czyli dowolnego zautomatyzowanego przetwarzania danych osobowych pozwalającego ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Istotnym dla przetwarzania danych osobowych w cyberprzestrzeni jest również artykuł 32 RODO, określający wymóg szacowania ryzyka w przypadku wdrażania organizacyjnych oraz technicznych środków bezpieczeństwa przetwarzania danych. Z kolei art. 35 wskazuje, że w przypadku, gdy dane są przetwarzane w szczególności z wykorzystaniem nowych technologii, konieczne jest przeprowadzanie oraz udokumentowanie oceny skutków dla ochrony danych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). Na poziomie krajowym ochrona danych osobowych opiera się również na następujących aktach prawnych:

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 z późn. zm.) – reguluje zasady działania Prezesa Urzędu Ochrony Danych Osobowych (UODO) i uzupełnia postanowienia RODO na gruncie krajowym,
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 z późn. zm.) – ma na celu zapewnienie bezpieczeństwa sieci i systemów informatycznych używanych do świadczenia kluczowych usług,
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.) – dotyczy m.in. odpowiedzialności dostawców usług online w zakresie przetwarzania danych osobowych,

- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579 z późn. zm.) – odnosi się do kwestii podpisu elektronicznego, tożsamości cyfrowej i bezpieczeństwa transakcji elektronicznych,
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.) – reguluje zasady wprowadzania i stosowania technologii informacyjno-komunikacyjnych w instytucjach publicznych. Jej celem jest zapewnienie sprawnej, nowoczesnej i bezpiecznej realizacji zadań publicznych, m.in. poprzez ujednolicenie systemów teleinformatycznych, wdrożenie elektronicznej administracji, interoperacyjność systemów oraz dostęp obywateli do usług publicznych drogą elektroniczną.

Rozwój technologii informatycznych oraz powszechna cyfryzacja codziennego życia przyniosły wiele korzyści, ale również nowe zagrożenia dla prywatności. Dane osobowe użytkowników Internetu stały się cennym towarem, a ich przejęcie i wykorzystanie przez nieuprawnione podmioty może skutkować poważnymi konsekwencjami – od kradzieży tożsamości po szantaż czy oszustwa finansowe. W niniejszym rozdziale przedstawiono najczęstsze formy zagrożeń, z jakimi spotykają się użytkownicy sieci.

Phishing to jedna z najczęstszych form oszustwa internetowego, polegająca na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia danych osobowych, loginów, haseł czy danych karty płatniczej. Atakujący wykorzystują mechanizmy socjotechniki, czyli manipulacji psychologicznej, aby skłonić ofiarę do podjęcia określonego działania – np. kliknięcia w link, pobrania załącznika lub podania danych logowania. Przykładami mogą być fałszywe wiadomości e-mail rzekomo od banku, portalu społecznościowego lub firmy kurierskiej, w których użytkownik proszony jest o „weryfikację konta” lub „potwierdzenie przesyłki” (Hadnagy, Fincher, 2016, s. 28). Wzrost liczby ataków phishingowych potwierdzają coroczne raporty – wskazując, że każdy użytkownik e-mail prędzej czy później stanie się adresatem wiadomości phishingowej (Hadnagy, Fincher, 2016, s. 57).

Ataki hakerskie, czyli nieautoryzowane próby uzyskania dostępu do systemów informatycznych, są kolejnym poważnym zagrożeniem dla danych osobowych. Cyberprzestępcy wykorzystują luki w zabezpieczeniach

systemów firm i instytucji publicznych, aby uzyskać dane klientów, użytkowników czy pacjentów. Wycieki danych mogą mieć dramatyczne skutki – dane trafiają na czarne rynki (tzw. dark web), gdzie są sprzedawane lub wykorzystywane do dalszych oszustw. W ostatnich latach głośne były przypadki wycieków danych m.in. z serwisów społecznościowych, firm telekomunikacyjnych czy instytucji medycznych. Do popularnych technik hakerskich należą:

- ataki typu SQL injection – to podatność występująca w aplikacjach internetowych, umożliwiająca atakującemu „wstrzyknięcie” własnego zapytania SQL do bazy danych. Do ataku dochodzi w sytuacji, gdy aplikacja nie filtruje odpowiednio zapytań przesyłanych do bazy danych albo w ogóle tego nie robi. W efekcie aplikacja przekazuje do bazy danych zapytanie, które – wraz z dołączonym kodem – zostaje wykonane w całości. Skutecznie przeprowadzony atak może prowadzić do odczytu, modyfikacji, dodania lub usunięcia danych z bazy, a także obejścia mechanizmów zabezpieczających (Dymek, Nycz, Gerka, 2016, s. 27),
- wykorzystanie słabych haseł i braku uwierzytelnienia dwuskładnikowego,
- ataki typu zero-day, czyli wykorzystujące nieznane wcześniej luki bezpieczeństwa.

Malware (złośliwe oprogramowanie) to ogólna kategoria programów stworzonych w celu szkodenia użytkownikowi – kradzieży danych, śledzenia działań online, przejęcia kontroli nad komputerem. Szczególnie niebezpieczną odmianą jest ransomware, który szyfruje pliki użytkownika i żąda okupu za ich odszyfrowanie. Do najczęstszych sposobów infekcji należą: otwieranie podejrzanych załączników e-mail, pobieranie plików z niesprawdzonych źródeł czy korzystanie z niezaktualizowanego oprogramowania. Ransomware szczególnie uderza w firmy i instytucje, powodując przestoje i straty finansowe, ale także indywidualni użytkownicy są jego ofiarami (Diogenes, Ozkaya, 2023).

Media społecznościowe są miejscem, gdzie użytkownicy dobrowolnie udostępniają wiele informacji o sobie – często bez refleksji nad tym, kto i w jakim celu może z nich skorzystać. Dane zamieszczane na Facebooku, Instagramie czy TikToku mogą być wykorzystywane nie tylko przez

reklamodawców, ale także przez osoby trzecie do profilowania, manipulacji (np. politycznej) czy kradzieży tożsamości.

Najczęstsze zagrożenia związane z mediami społecznościowymi to:

- oszustwa tożsamościowe (tworzenie fałszywych profili),
- wyłudzenie informacji w ramach konkursów lub quizów,
- rozpowszechnianie fake newsów i dezinformacji,
- brak odpowiednich ustawień prywatności, umożliwiające dostęp do danych przez nieznajomych.

W kontekście RODO nadużycia te mogą prowadzić do naruszeń prawa do prywatności, a odpowiedzialność spoczywa nie tylko na użytkownikach, ale również na administratorach portali społecznościowych, którzy mają obowiązek wdrażania środków technicznych i organizacyjnych chroniących dane osobowe.

W obliczu rosnących zagrożeń cyfrowych ochrona danych osobowych nie może ograniczać się jedynie do przepisów prawnych. Równie istotna jest świadomość użytkowników oraz stosowanie konkretnych środków technicznych i organizacyjnych. Współczesna cyberprzestrzeń wymaga od każdego – zarówno osób prywatnych, jak i podmiotów przetwarzających dane – stosowania praktycznych i skutecznych metod zabezpieczeń, które minimalizują ryzyko wycieku lub nieuprawnionego wykorzystania informacji. W niniejszym rozdziale przedstawiono najważniejsze i najbardziej dostępne sposoby ochrony danych w codziennym użytkowaniu Internetu i technologii cyfrowych.

Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że te dodatkowe informacje przechowywane są osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). Wykorzystuje się ją w celu utrudnienia identyfikacji określonej osoby fizycznej. Polega na zastąpieniu danych osobowych dotyczących osoby fizycznej innymi danymi np. numerem identyfikacyjnym. Pseudonimizacji możemy dokonać za pomocą: zaciemniania lub maskowania liter, szyfrowania, tokenyzacji, zastępowania części danych ciągiem znaków, modyfikacji danych w taki sposób, by pokazywały przybliżone wartości.

Anonimizacja polega z kolei na nieodwracalnym usunięciu wszystkich informacji, które w jakikolwiek sposób umożliwiają identyfikację określonej osoby, której dane dotyczą, przez administratora danych lub osobę trzecią (Bartnicki, 2020).

Jednym z podstawowych filarów bezpieczeństwa cyfrowego pozostaje stosowanie silnych i unikalnych haseł do wszystkich kont i usług. Hasła powinny zawierać minimum 12 znaków i być kombinacją małych i wielkich liter, cyfr oraz znaków specjalnych. Należy unikać haseł łatwych do przewidzenia, takich jak daty urodzenia, imiona dzieci czy sekwencje liczb. Uzupełnieniem tej metody jest tzw. uwierzytelnianie dwuskładnikowe (2FA – Two-Factor Authentication), które znacząco podnosi poziom bezpieczeństwa, wymagając oprócz hasła dodatkowego potwierdzenia tożsamości – np. kodu SMS, aplikacji autoryzacyjnej lub klucza sprzętowego (Diogenes, Ozkaya, 2020, s. 406).

Szyfrowanie danych to jedna z najskuteczniejszych metod zabezpieczenia informacji przed dostępem osób trzecich. Dzięki niemu nawet w przypadku przechwycenia danych, ich treść pozostaje nieczytelna bez odpowiedniego klucza deszyfrującego. Szyfrowaniu powinny podlegać zarówno dane przechowywane na urządzeniach, jak i przesyłane przez sieć. W tym kontekście warto także wspomnieć o wirtualnych sieciach prywatnych (VPN – Virtual Private Network), które maskują adres IP użytkownika i szyfrują cały ruch internetowy. Korzystanie z VPN szczególnie zalecane jest podczas łączenia się z publicznymi sieciami Wi-Fi, które często stanowią łatwy cel dla cyberprzestępców (Diogenes, Ozkaya, 2020, s. 406).

Nawet najbardziej zaawansowane rozwiązania techniczne nie przyniosą oczekiwanych rezultatów, jeśli użytkownicy nie będą świadomi zagrożeń oraz zasad bezpiecznego korzystania z technologii. Dlatego tak ważna jest edukacja cyfrowa – zarówno wśród dzieci i młodzieży, jak i dorosłych użytkowników. Do podstawowych zasad należą: ostrożność przy otwieraniu załączników i linków w wiadomościach e-mail, unikanie podawania danych osobowych na nieznanych stronach internetowych, regularna aktualizacja oprogramowania i korzystanie z legalnych źródeł aplikacji. Równie istotne jest uświadamianie użytkowników na temat ich praw wynikających z RODO oraz możliwości reagowania w przypadku naruszenia ich danych osobowych.

Urządzenia mobilne – smartfony i tablety – stały się nieodłączną częścią codziennego życia, a wraz z nimi pojawiły się nowe wektory zagrożeń. Podstawą ochrony danych na tych urządzeniach jest zabezpieczenie ich ekranów hasłem, PIN-em lub biometrią, regularne instalowanie aktualizacji oraz ograniczenie dostępu aplikacji do danych wrażliwych. Podobnie korzystanie z tzw. chmur wymaga zachowania ostrożności. Użytkownicy powinni wybierać zaufanych dostawców usług chmurowych, korzystać z szyfrowania plików przed ich wysłaniem oraz regularnie monitorować, kto ma dostęp do konkretnych danych i dokumentów.

Ochrona danych osobowych nie kończy się na sformułowaniu zasad i przyjęciu odpowiednich dokumentów prawnych. Kluczową rolę odgrywa egzekwowanie tych przepisów – zarówno na poziomie organizacyjnym, jak i indywidualnym. RODO, jak również ustawa o ochronie danych osobowych z dnia 10 maja 2018 r., jasno określają obowiązki, sankcje oraz instytucje nadzorujące przestrzeganie przepisów. Zasadnicze obszary odpowiedzialności: firm i organizacji, przypadki naruszeń oraz znaczenie funkcji Inspektora Ochrony Danych.

Na mocy art. 24 i 32 RODO, administratorzy danych osobowych są zobowiązani do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zgodności przetwarzania z przepisami. Obejmuje to m.in. prowadzenie rejestrów czynności przetwarzania, ocenę skutków dla ochrony danych (DPIA), szyfrowanie, pseudonimizację, czy też zapewnienie ciągłości działania w razie incydentu (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679).

Firmy i organizacje, które nie wywiązują się z obowiązków, podlegają odpowiedzialności administracyjnej, cywilnej i karnej. Zgodnie z art. 83 RODO, wysokość administracyjnych kar pieniężnych może sięgnąć do 20 milionów euro lub 4% całkowitego rocznego obrotu z poprzedniego roku obrotowego – w zależności od tego, która kwota jest wyższa (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679). W polskim porządku prawnym kwestie te reguluje m.in.:

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, która uzupełnia postanowienia RODO na poziomie krajowym,
- Kodeks cywilny, który umożliwia dochodzenie roszczeń z tytułu naruszenia dóbr osobistych, takich jak prywatność (art. 23 i 24 KC).

W praktyce naruszenia ochrony danych obejmują:

- nieuprawnione udostępnienie danych osobom trzecim,
- niezabezpieczone formularze kontaktowe lub bazy danych,
- przetwarzanie danych bez odpowiednich podstaw prawnych,
- niedopełnienie obowiązku informacyjnego wobec osób, których dane dotyczą (Bielak-Jomaa, Lubasz, 2018, s. 263).

Jednym z kluczowych elementów systemu odpowiedzialności w organizacjach przetwarzających dane jest funkcja Inspektora Ochrony Danych (IOD). Zgodnie z art. 37-39 RODO, wyznaczenie IOD jest obowiązkowe dla:

- podmiotów publicznych,
- podmiotów, których główna działalność polega na przetwarzaniu danych na dużą skalę.

Zadania IOD obejmują:

- informowanie i doradzanie administratorowi danych w zakresie obowiązków wynikających z RODO,
- monitorowanie zgodności przetwarzania z przepisami,
- współpracę z organem nadzorczym (UODO),
- pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą.

W praktyce IOD pełni rolę niezależnego strażnika danych, który nie tylko nadzoruje zgodność działań firmy z przepisami, ale również uczy pracowników, opiniuje procedury i ocenia ryzyka związane z przetwarzaniem danych (Lubasz, 2020, s. 345).

Ochrona danych osobowych jest procesem dynamicznym, który musi nadążać za tempem postępu technologicznego i zmieniającymi się realiami społecznymi. Choć podstawy prawne zostały ugruntowane na poziomie Unii Europejskiej (RODO), a także w krajowych regulacjach, to coraz częściej wskazuje się na konieczność aktualizacji i elastyczności przepisów. Przyszłość ochrony danych osobowych wiąże się ściśle z takimi zjawiskami jak rozwój sztucznej inteligencji, upowszechnienie danych biometrycznych, globalizacja przepływu informacji oraz skutki pandemii COVID-19, które przyspieszyły cyfryzację wielu sektorów życia.

Jednym z największych wyzwań dla sztucznej inteligencji są przepisy o ochronie danych osobowych. Duża część zastosowań sztucznej inteligencji

dotycz osób fizycznych, a tym samym wiąże się z przetwarzaniem ich danych osobowych.

Aby zapewnić zgodność z prawem przetwarzania danych osobowych w projektach AI, należy traktować je tak jak każdy inny projekt przetwarzania danych osobowych i stosować do niego zasady opisane w RODO. Nie jest to łatwe, ponieważ sposób w jaki są tworzone i funkcjonują algorytmy AI stoi w kontrze do zadań ochrony danych osobowych. AI nie tworzy scentralizowanej bazy danych, o której mówią przepisy, a tylko w takich bazach danych łatwo jest zidentyfikować administratorów danych. Technologia blockchain, która opiera się na architekturze rozproszonych baz danych i niezmienności zapisanych w niej informacji utrudnia np. realizowanie praw osób, których dotyczą dane np. prawa do sprostowania danych czy ich usunięcia. Tym samym obecnie nie ma jednego uniwersalnego rozwiązania, które sprawiłoby, że każdy blockchain byłby zgodny z RODO (Wittbrodt, Brodecki, Dargas-Draganik, 2024, s. 211).

Sztuczna inteligencja (AI), zwłaszcza w obszarze przetwarzania danych i uczenia maszynowego, może generować poważne ryzyka dla prywatności jednostek. Algorytmy uczące się na podstawie dużych zbiorów danych mogą nie tylko nieświadomie utrzymywać uprzedzenia i dyskryminację, ale też naruszać zasadę minimalizacji danych czy ograniczenia celu ich przetwarzania (zgodnie z art. 5 RODO). Problemem staje się także tzw. „czarna skrzynka” algorytmów – brak przejrzystości i kontroli nad ich działaniem. Z tego względu coraz większego znaczenia nabierają zasady tzw. privacy by design oraz privacy by default, które nakładają obowiązek projektowania systemów z uwzględnieniem ochrony prywatności już na etapie ich tworzenia (Świerczyński, 2021).

Dane biometryczne, takie jak odciski palców, skan twarzy, głosu czy siatkówki oka, uznawane są za szczególną kategorię danych osobowych (art. 9 RODO). Ich przetwarzanie dopuszczalne jest tylko w ściśle określonych przypadkach, np. w kontekście bezpieczeństwa publicznego lub ochrony zdrowia. Jednocześnie są to dane niezwykle wrażliwe – ich utrata lub przejęcie może mieć nieodwracalne skutki, ponieważ w przeciwieństwie do hasła nie można ich zmienić. Z tego względu konieczne jest stosowanie najwyższych standardów bezpieczeństwa, w tym szyfrowania, a także prowadzenie ocen skutków dla ochrony danych (DPIA – Data Protection Impact Assessment).

Pandemia COVID-19 przyspieszyła cyfrową transformację – praca zdalna, e-usługi czy zdalna edukacja stały się powszechne. Wraz z tym wzrosła powierzchnia ataku cyberprzestępców. Wyzwania pojawiają się zarówno po stronie użytkowników indywidualnych (np. słabe zabezpieczenia domowych sieci Wi-Fi), jak i instytucji, które musiały błyskawicznie wdrażać nowe technologie. Ochrona danych w takim kontekście wymaga zintegrowanego podejścia do cyberbezpieczeństwa, w którym kluczowe są m.in. szkolenia, aktualizacje systemów, kontrola dostępu oraz świadomość zagrożeń. W świetle ustawy o krajowym systemie cyberbezpieczeństwa podmioty świadczące usługi kluczowe muszą spełniać konkretne obowiązki w zakresie zabezpieczenia informacji (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa).

Dane osobowe coraz częściej przekraczają granice państw - są przetwarzane na serwerach ulokowanych poza Unią Europejską, zwłaszcza w krajach, które nie zapewniają odpowiedniego poziomu ochrony (np. nie posiadają ekwiwalentnych regulacji jak RODO). W związku z tym unijne prawo (m.in. art. 44-49 RODO) przewiduje mechanizmy takie jak: decyzje o adekwatności Komisji Europejskiej, standardowe klauzule umowne czy wiążące reguły korporacyjne (BCR). Jednak globalizacja stawia pytania o skuteczność tych narzędzi, zwłaszcza wobec potęg technologicznych i państw, które gromadzą dane w celach nadzoru. Niezbędna wydaje się szersza współpraca międzynarodowa i harmonizacja standardów ochrony danych (Bielak-Jomaa, Lubasz, 2018, s. 905).

Podsumowanie

Upowszechnienie Internetu oraz dynamiczny rozwój technologii przetwarzania informacji – w tym nowych modeli, takich jak chmura obliczeniowa czy analizy Big Data - znacząco zwiększyły potrzebę wdrożenia skutecznych mechanizmów ochrony praw w cyberprzestrzeni. Cyberprzestrzeń, ze swoim pozbawionym granic charakterem, iluzoryczną anonimością i łatwością rozpowszechniania informacji, wymusza ponowną refleksję nad tym, czy obowiązujące normy prawne - często uchwalone w zupełnie innych realiach technologicznych – są dziś wystarczające i adekwatne wobec rosnących zagrożeń dla prywatności. Ochrona danych osobowych w cyberprzestrzeni to dziś nie tylko kwestia techniczna czy formalna – to

jeden z fundamentów zaufania społecznego oraz sprawnie funkcjonującego społeczeństwa informacyjnego. W dobie cyfrowej transformacji dane osobowe stały się walutą XXI wieku, a ich nadużycia prowadzą do poważnych konsekwencji zarówno dla jednostek, jak i całych instytucji. Podjęcie tematu w niniejszym opracowaniu miało na celu pokazanie złożoności zagadnienia, zwrócenie uwagi na najczęstsze zagrożenia, a także przybliżenie aktualnych rozwiązań prawnych i praktycznych metod ochrony danych:

- Dane osobowe stanowią dobro szczególnie chronione, a ich ochrona wpisuje się w konstytucyjne prawo do prywatności,
- Wprowadzenie RODO ujednoliciło zasady ochrony danych w krajach UE i znacznie zwiększyło odpowiedzialność podmiotów przetwarzających dane,
- W cyberprzestrzeni użytkownicy narażeni są na różnorodne formy ataków, takie jak phishing, wycieki danych, ransomware czy nadużycia w mediach społecznościowych,
- Ochrona danych wymaga zarówno narzędzi technologicznych (szyfrowanie, silne hasła, VPN), jak i ciągłego podnoszenia świadomości społecznej,
- Kluczową rolę pełnią firmy i organizacje – ich obowiązkiem jest nie tylko zabezpieczanie danych, ale także transparentne działania i edukacja użytkowników.

W dobie dzisiejszego świata, gdzie wykorzystywana jest sztuczna inteligencja (AI) i na niespotykaną skalę Internet, należy dążyć do zaleceń:

- Niezbędne jest prowadzenie szkoleń z zakresu cyberbezpieczeństwa – zarówno w sektorze publicznym, jak i prywatnym,
- Użytkownicy powinni korzystać z menedżerów haseł, dwuskładnikowego uwierzytelniania i unikać udostępniania danych na niesprawdzonych stronach,
- Instytucje powinny regularnie przeprowadzać audyty bezpieczeństwa oraz wdrażać polityki ochrony danych zgodne z RODO i ustawą krajową,
- Warto zwiększyć nakłady na edukację cyfrową – już od poziomu szkoły podstawowej – tak by kształtować kompetentnych i świadomych cyfrowo obywateli.

Bezpieczeństwo danych osobowych w dużej mierze zależy od decyzji podejmowanych przez samych użytkowników. To właśnie ich codzienne wybory – jak np. korzystanie z publicznych sieci Wi-Fi, nieaktualizowanie oprogramowania, kliknięcie w podejrzany link – mogą zadecydować o tym, czy dane pozostaną bezpieczne. W związku z tym, budowanie świadomości i odpowiedzialności cyfrowej powinno stać się jednym z priorytetów nie tylko polityki państwowej, ale także codziennego funkcjonowania w świecie on-line.

Literatura

1. Bakalarczyk-Burakowska, K., Nowicka, J. (2020). Ochrona danych osobowych w cyberprzestrzeni. W: Z. Ciekanowski (red.), *Współczesne zagrożenia bezpieczeństwa państwa. Część 1*. Państwowa Szkoła Wyższa im. Papieża Jana Pawła II, Biała Podlaska.
2. Bartnicki, A., Wojciechowski, Z., Zaskórski, P. (2020). *Analiza ryzyka i pseudonimizacja w systemie zabezpieczania danych osobowych cyberprzestrzeni, IV rewolucja przemysłowa. Mity, paradygmaty i zastosowania*, WAT, Warszawa.
3. Bielak-Jomaa, E., Lubasz, D. (2018). *Komentarz do RODO*, Wolters Kluwer, Warszawa.
4. Bielak-Jomaa, E., Lubasz, D. (2018). *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Wolters Kluwer, Warszawa.
5. Diogenes, Y., Ozkaya, E. (2023). *Cyberbezpieczeństwo. Strategie ataku i obrony*, Helion, Gliwice.
6. Dymek, M., Nycz, M., Gerka, A. (2016). *Analiza statycznych metod obrony przed atakami SQL Injection*, zeszyty Naukowe Politechniki Rzeszowskiej, Rzeszów.
7. Hadnagy, Ch., Fincher, M. (2016). *Mroczne oddechy phishingu. Nie daj się złowić!*, Helion, Gliwice.
8. Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Uniwersytet Śląski, Katowice.
9. Lubasz, D. (2020). *Ochrona danych osobowych. Komentarz do przepisów RODO*, Wolters Kluwer, Warszawa.

10. Lubasz, D. (2013). *Techniczne, ekonomiczne i prawne uwarunkowania handlu elektronicznego, Handel elektroniczny. Bariery prawne*, LexisNexis, Warszawa.
11. Rojszczak, M. (2019). *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Wolters Kluwer, Warszawa.
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
13. Świerczyński, M. (2021). *Sztuczna inteligencja a ochrona danych osobowych*, Przegląd Prawa Publicznego, Uniwersytet Wrocławski, Wrocław.
14. Taczkowska-Olszewska, J., Chałubińska-Jentkiewicz, K., Nowikowska, M. (2019). *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Wolters Kluwer, Warszawa.
15. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.).
16. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.).
17. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz. U. z 2018 r. poz. 1560 z późn. zm.).
18. Wasilewski, J. (2015). *Zarys definicyjny cyberprzestrzeni*, Zeszyty Naukowe (13/2025). Warszawska Wyższa Szkoła Informatyki, Warszawa.
19. Wittbrodt, E., Brodecki, Z., Dargas-Draganik, M. (2024). *Przedwiośnie ery sztucznej inteligencji technologia – zarządzanie – prawo. Tom 2*, Uniwersytet Gdański, Gdańsk.