mgr Katarzyna Bakalarczyk-Burakowska
Państwowa Szkoła Wyższa
im. Papieża Jana Pawła II w Białej Podlaskiej

dr Julia Nowicka*
Akademia Sztuki Wojennej
Wydział Wojskowy
*ORCID: 0000-0002-0778-0519

OCHRONA DANYCH OSOBOWYCH W CYBERPRZESTRZENI

PROTECTION OF PERSONAL DATA IN CYBERSPACE

Streszczenie
W artykule podjęto próbę przedstawienia problematyki ochrony prywatności, a zwłaszcza danych osobowych w erze cyfrowej, ze szczególnym uwzględnieniem ram organizacyjno – prawnych**.** Ochrona danych osobowych staje się istotnym elementem bezpieczeństwa cybernetycznego i stabilności w cyberprzestrzeni. Obecnie wszelkie strategie, polityki i przepisy dotyczące cyberbezpieczeństwa uwzględniają dane osobowe jako swoją integralną część, warunkującą osiąganie krajowych, regionalnych i międzynarodowych celów w tym zakresie. Trend konwergencji ochrony danych i bezpieczeństwa cybernetycznego jest widoczny w wielu różnych systemach prawnych na całym świecie. Cyberbezpieczeństwo w ogóle, a bezpieczeństwo danych osobowych w cyberprzestrzeni w szczególności, jest w obecnie jednym z największych wyzwań dla wszystkich administratorów. Stworzenie dobrej i efektywnej strategii bezpieczeństwa cybernetycznego nie jest łatwym zadaniem. Wymaga zaangażowania wielu zasobów: technologicznych, kadrowych, a przede wszystkim finansowych.

Słowa kluczowe: bezpieczeństwo, cyberprzestrzeń, cyberbezpieczeństwo, dane, ochrona

Abstract
The article attempts to highlight the issues of privacy protection, especially personal data in the digital age, with particular emphasis on the organizational and legal framework. Personal data protection is becoming an essential element of cybersecurity and stability in cyberspace. Currently, all cybersecurity strategies, policies and regulations include personal data as an integral part of achieving national, regional and international goals in this regard. The trend of data protection and cybersecurity convergence is visible in many different legal systems around the world. Cybersecurity in general, and the security of personal data in cyberspace in particular, is currently one of the greatest challenges for all

administrators. Creating a good and effective cybersecurity strategy is not an easy task. It requires the involvement of many resources: technological, human and, above all, financial.

Keywords: security, cyberspace, cybersecurity, data, protection

Wstęp

Ochrona danych osobowych staje się istotnym elementem bezpieczeństwa cybernetycznego i stabilności w cyberprzestrzeni. Obecnie wszelkie strategie, polityki i przepisy dotyczące cyberbezpieczeństwa uwzględniają dane osobowe jako swoją integralną część, warunkującą osiąganie krajowych, regionalnych i międzynarodowych celów w tym zakresie. Trend konwergencji ochrony danych i bezpieczeństwa cybernetycznego jest widoczny w wielu różnych systemach prawnych na całym świecie, zarówno w Europie, Azji czy Afryce.

Cyberprzestrzeń jeszcze kilka dekad nie była terminem powszechnie znanym. Kiedy w 1990 roku pojawił się Internet, tylko nieliczni uświadamiali sobie konsekwencje tego fenomenu. Wystarczył upływ zaledwie kilku lat, aby cyberprzestrzeń, na początku lat 90., za sprawą wojny w Zatoce Perskiej, wkroczyła do terminologii wojskowej jako piąte środowisko (obok lądu, przestrzeni morskiej, przestrzeni powietrznej i kosmosu) zmagań wojennych. Stała się tym samym specyficznym narzędziem polityki, a na początku XXI wieku na stałe zagościła w słownikach i encyklopediach[1].

Współcześnie niemal każdy aspekt życia indywidualnego i społecznego ulega szybkim przemianom w wyniku innowacyjnych sposobów gromadzenia, przetwarzania, analizowania, wykorzystywania i rozpowszechniania informacji w cyberprzestrzeni. Numery identyfikacyjne, numery ubezpieczenia społecznego, konta bankowe, karty kredytowe i smartfony umożliwiają identyfikację i śledzenie miejsc, w których dana osoba była bądź przebywa. Połączenie potężnych technik informatycznych i ogromnych ilości danych osobowych może prowadzić do naruszeń prywatności, a więc ewolucja technologiczna w cyberprzestrzeni drastycznie zmieniła pojęcie indywidualnej kontroli nad ujawnianiem i wykorzystywaniem danych osobowych.

W konsekwencji prywatność stała się przedmiotem dyskusji i obaw dotyczących zarządzania Internetem i cyberprzestrzenią. Postulat zwiększonej ochrony danych osobowych i prywatności w cyberprzestrzeni nie jest już kwestią tylko teoretyczną, jak to było wcześniej, ale został obudowany zestawem określonych przepisów i praktyk, które obejmują działania związane z gromadzeniem danych przez trzech głównych aktorów cyberprzestrzeni: rządów, przedsiębiorstw i społeczeństwa obywatelskiego. Ważną cezurę w procesie budowy bezpieczeństwa danych osobowych w cyberprzestrzeni stanowiło unijne Rozporządzenie o Ochronie Danych Osobowych (RODO – angielski skrót GDPR – *General Data Protection Re-*

[1] P. Sienkiewicz, *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", nr 13/2015, s. 96.

gulation), które weszło w życie w dniu 25 maja 2018 roku i w znacznym stopniu wpłynęło na system ochrony danych osobowych w Unii Europejskiej[2].

Pomimo wielu rozwiązań normatywnych i organizacyjnych, charakterystycznych zwłaszcza dla kilku ostatnich lat, cyberbezpieczeństwo, a szczególnie bezpieczeństwo danych osobowych w cyberprzestrzeni, jest obszarem obarczonym wieloma mankamentami, który wymaga zdecydowanych oraz skoordynowanych rozwiązań i działań, a także budowy wielostronnych mechanizmów ochronnych.

Ochrona prywatności człowieka – ramy prawne

Idea praw człowieka zrodziła się i rozwinęła w europejskim kręgu cywilizacyjnym, którego fundament tworzą etyka judeochrześcijańska, grecka estetyka i rzymska doktryna prawa[3]. Nie wchodząc w historyczny rozwój ochrony prawa do prywatności należy uwypuklić fakt, iż w tym długim procesie wyodrębniły się trzy generacje praw człowieka:

- pierwsza generacja – prawa fundamentalne, obywatelskie i polityczne;
- druga generacja – prawa ekonomiczne, społeczne i kulturalne;
- trzecia generacja – prawa kolektywne, prawa solidarności[4].

Istotną rolę w procesie kształtowania się nowych praw odegrał postęp technologiczny, a przede wszystkim rozwój fotografii prasowej. Powstał bowiem nowy nośnik informacji. Pojawienie się i rozwój prawnej ochrony prywatności to efekt poczucia zagrożenia wywołanego zbyt głęboką ingerencją w życie codzienne obywateli. Prezentowane w nauce prawa poglądy odnoszące się do sfery prywatności zyskały uznanie prawodawców i stały się podstawą do sformułowania odpowiednich przepisów.

Analiza dostępnej literatury pozwala dostrzec, iż używa się wiele terminów tożsamych z prywatnością człowieka, a mianowicie *sfera osobista człowieka, prawno-osobista sfera własna, sfera intymności czy obszar tajemnicy*[5]. Prawo związane ze sferą życia prywatnego zmieniało się w zależności od państwa, systemu prawnego, koncepcji naukowych czy też czynników kulturowo-religijnych. Prowadzi to do wniosku, że nie został wykształcony jeden uniwersalny system ochrony prywatności.

Prawo do prywatności zostało skodyfikowane na poziomie międzynarodowym między innymi w Powszechnej Deklaracji Praw Człowieka (PDPCz)[6], Mię-

---

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy* 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz. Urz. UE L z 2016 r. Nr 119, s. 1, ze zm.).

[3] R. Kuźniar, *Prawa człowieka. Prawo, instytucje, stosunki międzynarodowe,* Wydawnictwo Naukowe Scholar, Warszawa 2008, Wydanie trzecie uzupełnione, s. 20.

[4] Ibidem, s. 50.

[5] M. Pryciak, *Prawo do prywatności*, „Studia Erasmiana Wratislavensia", nr 4/2010, s. 213.

[6] *Powszechna Deklaracja Praw Człowieka*, Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana w dniu 10 grudnia 1948 r.

dzynarodowym Pakcie Praw Obywatelskich i Politycznych[7], Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[8]. Dla przykładu w Powszechnej Deklaracji Praw Człowieka sformułowano postulat, że *nie wolno ingerować samowolnie w czyjeś życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu*[9]. Z tym zapisem koresponduje art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych, który stanowi, że *1. Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię. 2. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami*[10].

Organizacja Narodów Zjednoczonych również angażowała się we wdrażanie praw do prywatności, w tym do prywatności w cyberprzestrzeni. Dwa wiodące przykłady to Rezolucja Zgromadzenia Ogólnego ONZ z 2014 r. dotycząca prawa do prywatności w erze cyfrowej oraz Rezolucja Rady Praw Człowieka ONZ z 2016 r. w sprawie promowania, ochrony i korzystania z praw człowieka w Internecie. W pierwszej rezolucji Zgromadzenie Ogólne ONZ potwierdziło, że *te same prawa, które mają ludzie offline, muszą być chronione online, w tym prawo do prywatności*[11]. W rezolucji z 2016 roku Rada Praw Człowieka potępiła naruszania praw człowieka popełnione przeciwko osobom w odniesieniu do realizacji praw człowieka i podstawowych wolności w Internecie oraz wezwała wszystkie państwa do zapewnienia kontroli w tym zakresie. Napiętnowała również środki służące do celowego uniemożliwiania lub utrudniania, z naruszeniem międzynarodowego ustawodawstwa dotyczącego praw człowieka, dostępu do lub rozpowszechniania informacji online. Zaapelowała do wszystkich państwa o powstrzymanie się i zaprzestanie wykorzystywania takich środków[12].

Z powyższych rozważań wynika, iż prawo do prywatności zostało sformalizowane na poziomie międzynarodowym, niezależnie od egzekwowania tego prawa w ramach krajowych jurysdykcji. W Polsce przez wiele lat regulacja dotycząca ochrony prywatności nie była wyrażona wprost w przepisach prawa, jednak doktryna i orzecznictwo powszechnie uznawały prywatność za jedno z dóbr osobistych, co umożliwiało ochronę tej sfery za pomocą prawa cywilnego. Na przestrzeni lat okazało się, iż obrona prywatności na gruncie prawa cywilnego jest

---

7 *Międzynarodowy Pakt Praw Obywatelskich i Politycznych* otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. 1977 nr 38 poz. 167.

8 *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. Dz.U.1993.61.284.

9 *Powszechna Deklaracja Praw Człowieka,* art. 12.

10 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych*, art. 17.

11 Rezolucja przyjęta przez Zgromadzenie Ogólne w dniu 18 grudnia 2013 roku, (68/167. *Prawo do prywatności w erze cyfrowej),* Opublikowana w dniu 21 stycznia 2014 r. Dostępna na: https://undocs.org/A/RES/68/167 [dostęp 09.10.2020].

12 Rezolucja przyjęta przez Radę Praw Człowieka 1 lipca 2016 r. (32/13) P*romowanie, ochrona i korzystania z praw człowieka w Internecie.* Opublikowana w dniu 18 lipca 2016 r. A/HRC/RES/32/13 Dostępna na: https://undocs.org/A/HRC/RES/32/13, [dostęp 09.10.2020].

niewystarczająca. Polskie prawo do prywatności ma swoje korzenie w Konstytucji RP z 2 kwietnia 1997 r., w szczególności w art. 47, który gwarantuje każdemu obywatelowi prawo do życia prywatnego: *Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym*[13]. Ponadto art. 49 Konstytucji gwarantuje wolność i ochronę tajemnicy komunikowania się zastrzegając, że ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej sprecyzowany[14] a artykuł 51 Konstytucji dotyczący zakazu obowiązku ujawniania informacji stanowi m.in., że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby oraz że każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. Ponadto każdy obywatel ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą[15].

Te zasady konstytucyjne doprecyzowano w art. 23 i 24 ustawy z dnia 13 kwietnia 1964 r. – Kodeks Cywilny, które chronią dobra osobiste osób fizycznych[16].

Reasumując, pod wpływem silnego nacisku społecznego na kontrolę informacji, postępowała powolna, ale systematyczna budowa ram prawnych dla ochrony danych osobowych jako warunku zachowania prywatności w cyberprzestrzeni. Niektóre pojęcia tradycyjnie związane z prywatnością, takie jak samotność, odosobnienie czy tajemnica – przekute na *prawo do bycia pozostawionemu w spokoju* – stworzyły przestrzeń dla nowych systemów, w których można gromadzić i wykorzystywać dane osobowe, o ile jest to zgodne z wolą właściciela i jego oczekiwaniami. Wprawdzie formalne zapisy i regulacje dotyczące udostępniania i ujawniania danych osobowych mogą być postrzegane jako antyteza prywatności, ale w istocie uwzględniając indywidulaną potrzebę decydowania o tym, co ma pozostać objęte ochroną, realizują główny z celów prywatności: strzegą indywidualizm i osobowość człowieka.

Prawne podstawy i zasady ochrony danych osobowych

Potrzeba ochrony danych osobowych powstała, jak podkreślono wcześniej, na gruncie prawa do prywatności oraz w związku z intensywnym rozwojem społeczeństwa informacyjnego. Po raz pierwszy problem ochrony danych osobowych dostrzegli dwaj amerykańscy sędziowie – S. D. Warren raz L.D. Brainders, autorzy

[13] Ustawa z dnia 2 kwietnia 1997 r. – *Konstytucja Rzeczypospolitej Polskiej* (Dz. U. z 1997 r. Nr 78, poz. 483), art. 47.

[14] Ibidem, art. 49.

[15] Ibidem, art. 51.

[16] Ustawa z dnia 23.04.1964 r. Kodeks cywilny. Tekst jednolity Dz.U.2020 poz.1740. Istotny jest tu artykuł 23, który stanowi: „*Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach*".

opublikowanego w 1890 roku artykułu *The Right to Privacy*. Dość szybko konieczność ochrony danych dostrzeżono w Europie. Po raz pierwszy kwestię tą uregulowano w Konwencji nr 108 Rady Europy z 1981 roku[17], a następnie w Dyrektywie 95/46 Parlamentu Europejskiego i Rady[18]. Pracę nad aktualnie obowiązującym RODO rozpoczęto w 2012 roku[19].

Definicję danych osobowych zawiera art. 4 pkt 1 przywoływanego już unijnego RODO, zgodnie z którym dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („*osobie, której dane dotyczą*"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: 1) imię i nazwisko, 2) numer identyfikacyjny, 3) dane o lokalizacji, 4) identyfikator internetowy, 5) jeden czynnik bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[20].

Wyróżnić można następujące kategorie danych:

- zwykłe dane osobowe;
- wrażliwe dane osobowe, czyli takie, na podstawie których możliwe jest poznanie pochodzenia rasowego bądź etnicznego, poglądów politycznych, przekonań religijnych, danych genetycznych oraz danych dotyczących zdrowia, orientacji seksualnej itp.;
- dane osobowe dotyczące wyroków skazujących i naruszeń prawa[21].

W przypadku drugiej grupy danych – wrażliwych danych osobowych (szczególnych danych osobowych) – RODO formułuje zakaz ich przetwarzania, przewidując tylko kilka wyjątkowych przypadków, kiedy takie przetwarzanie może mieć miejsce[22].

Nowe rozwiązania unijne zawarte w RODO, a w konsekwencji nowa ustawa o ochronie danych osobowych[23], pojawiły się dlatego, że ustawodawstwa krajowe państw, wchodzących w skład UE bardzo różnie podchodziły (i nadal podchodzą) do kwestii ochrony danych osobowych. Brakowało przejrzystości i pewności stosowania prawa w tym obszarze. Zaistniała potrzeba stworzenia przepisów gwarantujących równorzędny stopień ochrony danych osobowych na terenie całej Unii. Jeśli do tego dodamy kwestię swobodnego przepływu pracy, ludzi czy informacji (w tym także danych osobowych), jakie mają miejsce na obszarze UE, konieczność uregulowania ochrony danych osobowych stała się oczywista.

---

17 Konwencja Nr 108 Rady Europy z 1981 r. *o ochronie osób w związku z automatycznym* przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. z 2003 r. nr 3, poz. 25).

18 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. *w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych* (Dz. Urz. WE L 281 z 23.11.1995, tłumaczenie na język polski) – stosowana do 25 maja 2018 r.

19 A. Stępień, *Bezpieczeństwo danych osobowych w cyberprzestrzeni – Big Data*, „Przedsiębiorczość i Zarządzanie", nr 2/2018, s. 52.

20 RODO, art. 4 pkt. 1.

21 M. Gumularz (red.), *Ochrona danych osobowych w marketingu i sprzedaży*, Beck, Warszawa 2019, s. 4.

22 RODO, art. 9. Ust. 1 i 2.

23 Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* Dz.U. 2018 poz. 1000.

Nowe prawo wprowadziło m.in.:

- łatwiejszy dostęp do danych (zapewnienie większej liczby informacji na temat sposobu przetwarzania danych i zapewnienie, aby informacje były dostępne w przejrzysty i zrozumiały sposób);
- prawo do przenoszenia danych (ułatwia przesyłanie danych osobowych pomiędzy dostawcami usług);
- jaśniejsze prawo do usunięcia danych („prawo do bycia zapomnianym");
- prawo do bycia niezwłocznie poinformowanym w razie ataku hackerskiego na dane (podmioty będą także zobligowane zawiadomić odpowiednie organy nadzorcze ds. ochrony danych);
- technologie takie, jak pseudonimizacja i szyfrowanie.

RODO stanowi wiodący przykład spójnych norm dotyczących regulacyjnej ochrony danych osobowych. Co istotne, RODO jest wspierane solidnymi środkami administracyjnymi i cywilnymi, które ustanawiają jurysdykcję normatywną w zakresie praw osób, których dane dotyczą, nie tylko w granicach terytorialnych UE, ale także poza Unią.

Walorem nowych rozwiązań jest niewątpliwie precyzyjne określenie zasad przetwarzania danych osobowych. Co istotne, wskazano również wymagania, jakie powinny być spełnione przed przystąpieniem do procesu gromadzeniem danych osobowych. Przede wszystkim należy określić jakie dane mają być zbierane i przeanalizować czy rzeczywiście są potrzebne do celu przetwarzania, ocenić czy dane będą przekazywane lub czy przewiduje się ich przekazywanie do państwa (podmiotu) trzeciego. Potencjalni administratorzy winni upewnić się, że istnieje podstawa prawna do przetwarzania danych oraz zapewnić, że podczas zbierania danych osobom przekazuje się informacje wymagane prawem. Ponadto należy ocenić ryzyko dla prywatności (dla praw i wolności osób) związane z przetwarzaniem. Jeżeli to ryzyko będzie duże lub takie będzie się wydawać, dokonać pełnej oceny skutków dla ochrony danych. Wreszcie należy wdrożyć podstawowe mechanizmy zabezpieczenie danych.

W art. 5 ust 1 RODO określone zostały warunki zbierania danych. Dane osobowe muszą być gromadzone w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Pozyskiwane dane winny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych)[24].

Regulacje RODO gwarantują przetwarzania danych osobowych wyłącznie w ramach prawa. Takie prawne uzasadnienie celu przetwarzania określane jest w literaturze fachowej spełnieniem przesłanki legalności przetwarzania danych osobowych. Przetwarzanie jest zgodne z prawem wyłącznie w przypadku, gdy – i w takim zakresie jakim – spełniony jest co najmniej jeden z warunków przedstawionych w art. 6 RODO, tj.:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

[24] RODO, art. 5. ust. 1.

- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem[25].

Podmiot (organizacja) gromadząca dane osobowe musi wypełnić tak zwany obowiązek informacyjny, który polega na poinformowaniu osoby o szczegółach gromadzenia i przetwarzania jej danych osobowych[26]. Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą obejmują m.in.: tożsamość i dane kontaktowe administratora; cele przetwarzania danych osobowych; podstawę prawną przetwarzania; prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; informacje o odbiorcach danych osobowych lub o kategoriach odbiorców; informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej; okres przechowywania; informacje o prawie do dostępu do własnych danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; informacje o prawie wniesienia skargi do organu nadzorczego; informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Reasumując rozważania dotyczące zasad przetwarzania danych osobowych pamiętać należy, że prawo do ochrony danych osobowych zawarte w RODO, nie jest prawem bezwzględnym. Konieczne jest, aby było ono przestrzegane w kontekście funkcji społecznej, jakie pełni oraz aby było wyważone względem innych praw podstawowych, zgodnie z zasadami proporcjonalności. Przetwarzanie danych osobowych zawsze jest związane bowiem z ingerencją w prywatność osoby,

[25] RODO, art. 6. ust. 1.
[26] RODO, art. 13 i 14.

której dane są przetwarzane. Ingerencja ta jest jednak często konieczna z uwagi na potrzebę realizacji innych praw i wartości. Stopień tej ingerencji powinien każdorazowo być proporcjonalny do realizacji wyznaczonego celu[27].

Ochrona danych osobowych w cyberprzestrzeni

Analizę problemu należy rozpocząć od sprecyzowania czym jest cyberprzestrzeń. We współczesnym znaczeniu, z racji swojego niematerialnego charakteru, cyberprzestrzeń nie ma jednolitej, powszechnie uznanej definicji. W potocznym rozumieniu to wirtualna przestrzeń wykorzystywana do komunikacji przy wykorzystaniu sieci komputerowych i innych mediów cyfrowych. Na podstawie analizy różnych opisów cyberprzestrzeni można przyjąć, że w ujęciu funkcjonalnym tworzą ją:

- technologiczna infrastruktura (m. in. wszystkie elementy tworzące sieci komputerowe oraz sieci telekomunikacyjne – komputery, serwery, centrale, łącza, wraz z oprogramowaniem wyposażonym w interfejsy użytkownika);
- określone reguły prawne i niesformalizowane, rządzące zachowaniami w jej obszarze;
- aktywność i wzajemne interakcje użytkowników poruszających się po jej zasobach[28].

Konsekwencją takiego ujęcia może być określenie – przytaczane w licznych opracowaniach i źródłach Internetowych – że *„..cyberprzestrzeń jest obszarem społecznego doświadczenia podejmowanego za pośrednictwem technologii informatycznych – głównie komputerów z zainstalowanym oprogramowaniem, gdzie jednostki, z pominięciem geograficznych granic oraz wymiarów, mogą wzajemnie oddziaływać na siebie wywołując także określone (jak najbardziej rzeczywiste) skutki prawne*"[29].

Poszukując polskiej definicji cyberprzestrzeni należy stwierdzić, iż pierwszym dokumentem należącym do rodzimego porządku prawnego, w którym posłużono się pojęciem „*cyberprzestrzeń*", a jednocześnie zaprezentowano definicję tego terminu, stał się przygotowany pod auspicjami Ministerstwa Spraw Wewnętrznych i Administracji (wówczas jako ministerstwa właściwego do spraw informatyzacji) „*Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011*"[30]. Cyberprzestrzeń określono jako „*przestrzeń komunikacyjną tworzoną przez system powiązań internetowych*". Dokument został przyjęty w dniu 9 marca 2009 r. przez Komitet Stały Rady Ministrów w celu wzmocnienia ochrony infrastruktury krytycznej kraju przed atakami o charakterze terrorystycznym, w tym cyberterrorystycz-

[27] J. Taczkowska-Olszewska, M. Nowikowska, *Prawo do informacji publicznej, informacje niejawne i ochrona danych osobowych*, Wolters Kluwer, Warszawa 2019, s. 47.

[28] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne,* Praca doktorska napisana w Katedrze Prawa Karnego Uniwersytetu w Białymstoku 2017, s. 41.

[29] Ibidem, s. 41.

[30] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia,* Warszawa marzec 2009. Dostępny na: https://csirt.gov.pl/cer/publikacje/rzadowy-program-ochron/23,Rzadowy-program-ochrony-cyberprzestrzeni-RP-na-lata-2009-2011-zalozenia.html. [dostęp 09.10.2020].

nym. W zasadzie zdefiniowano w nim dwa pojęcia, a mianowicie „*cyberprzestrzeń*" oraz „*cyberprzestrzeń RP*". To drugie określono jako „*przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa*"[31].

Definicje te z uwagi na swoje niedostatki, zwłaszcza wątpliwe wydzielenie cyberprzestrzeni krajowej, zostały zmodyfikowane w kolejnej edycji tego samego programu na lata 2011-2016, który – z uwagi na przedłużające się prace legislacyjne – ostatecznie został wprowadzony w życie w formie dokumentu bezterminowego. W poprawionej wersji cyberprzestrzeń zdefiniowano jako „*cyfrową przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*"[32]. Natomiast definicja cyberprzestrzeni RP otrzymała brzmienie: „*Cyberprzestrzeń RP – cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe*"[33]. Warto podkreślić, iż identyczną definicję cyberprzestrzeni użyto w najnowszej „*Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*"[34].

Przechodząc do aktualnych rozwiązań ustawowych w Polsce należy stwierdzić, że cyberprzestrzeń nie jest zdefiniowana na gruncie ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[35]. Ustawodawca zdecydował się na umieszczenie i zdefiniowanie pojęcia cyberprzestrzeni w treści ustaw o stanach nadzwyczajnych, tj.:

- Ustawie z 29 lipca 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[36];
- Ustawie z 21 czerwca 2002 r. o stanie wyjątkowym[37];
- Ustawie z 18 kwietnia 2002 r. o stanie klęski żywiołowej[38].

Przez pojęcie cyberprzestrzeni, zgodnie z przyjętą na gruncie ustaw o stanach nadzwyczajnych definicją, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3

[31] Ibidem.
[32] *Rządowy program ochrony cyberprzestrzeni na lata 2011-2016*, Ministerstwo Spraw Wewnętrznych i Administracji Warszawa czerwiec 2010. Dostępny na: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp 09.10.2020].
[33] Ibidem.
[34] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Ministerstwo Cyfryzacji, Warszawa 2017, s. 28.
[35] Dz.U. z 2018 r. poz. 1560.
[36] Dz.U. z 2017 r. poz. 1932.
[37] Dz.U. z 2017 r. poz. 1928.
[38] Dz.U. z 2017 r. poz. 1897.

ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[39].

Najważniejszym dokumentem regulującym ochronę danych osobowych w cyberprzestrzeni jest szeroko omówione już rozporządzenie unijne RODO. Określa ono zasady, narzędzia, instrumenty oraz środki ochrony danych osobowych w cyberprzestrzeni. Wprowadziło ono kilka nowych elementów odnoszących się wprost do ochrony danych w cyberprzestrzeni. Jednym z nich jest prawo do „bycia zapomnianym", które gwarantuje zainteresowanej osobie możliwość usunięcia jej danych. Rozwiązanie to dokładnie reguluje prawa osób, których dane dotyczą, daje każdej osobie przywilej kontrolowania swoich danych oraz szerszej ochrony prawnej, w sytuacji, gdy dojdzie do naruszenia jej praw[40].

Kolejną ważną regulacją jest określenie ram prawnych profilowania. Przez profilowanie rozumie się „*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*"[41]. W RODO zawarto przepis, iż profilowanie co do zasady jest zakazane, o ile zainteresowana osoba nie wyraziła na nie zgody.

W przypadku przetwarzania danych w cyberprzestrzeni istotnym staje się rozwiązanie wprowadzone w artykule 32 RODO, a mianowicie wymóg szacowania ryzyka w przypadku wdrażania organizacyjnych oraz technicznych środków bezpieczeństwa przetwarzania danych. Jednoczenie zgodnie z art. 35 w przypadku, gdy dane są przetwarzane w szczególności z wykorzystaniem nowych technologii, co może powodować wysokie ryzyko naruszenia praw lub wolności osób, konieczne jest przeprowadzanie oraz udokumentowanie oceny skutków dla ochrony danych (ang. DPIA – Data Protection Impact Asessment)[42]. Podmioty przetwarzające dane osobowe zobligowane są nie tylko do wdrożenia technicznych środków bezpieczeństwa, ale również do zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń.

Do przetwarzania danych osobowych w cyberprzestrzeni odnoszą się również inne prawa, takie jak prawo dostępu do własnych danych, prawo sprostowania danych, prawo do ograniczenia przetwarzania, obowiązek powiadamiania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania czy też prawo do wniesienia skargi do organu nadzorczego.

---

[39] Art.3 pkt. 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publicznej definiuje system teleinformatyczny jako zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. Zob. Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm.).

[40] A. Stępień, *Bezpieczeństwo*..., op. cit., s. 52.

[41] RODO, art. 4 pkt. 4.

[42] RODO, art. 32 i 35.

Innymi ważnymi aktami prawnymi funkcjonującymi na gruncie prawa krajowego są:

- ustawa o krajowym systemie cyberbezpieczeństwa;
- ustawa o ochronie danych osobowych[43];
- ustawa o świadczeniu usług drogą elektroniczną[44];
- ustawa o usługach zaufania i identyfikacji elektronicznej[45];
- ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.

Ustawa o krajowym systemie cyberbezpieczeństwa uwzględnia ochronę danych osobowych. Nakłada na operatorów kluczowych usług oraz dostawców usług cyfrowych obowiązki, które są bardzo zbliżone do tych, wynikających z RODO. Podobieństwa odnoszą się zwłaszcza do bezpieczeństwa danych bazującego na ryzyku, wewnętrznej dokumentacji oraz na raportowaniu incydentów. Każdy operator usługi kluczowej, czyli takiej usługi, która ma znaczenie w działalności społecznej bądź gospodarczej, ma obowiązek zbudowania i wdrożenia systemu zarządzania bezpieczeństwem w systemie teleinformatycznym. Wykorzystywane w tym celu środki techniczne i organizacyjne mające na celu zarządzanie ryzykiem występującym na poziomie sieci oraz systemów informatycznych, muszą zapewniać dopasowany do tego ryzyka poziom bezpieczeństwa[46]. Uznać można więc, że cyberbezpieczeństwo to jeden z elementów szerszej regulacji, jaka odnosi się do ochrony danych osobowych w kontekście ochrony prywatności[47]. Gwarancja ochrony danych osobowych to jedno z zadań wchodzących w skład listy czynności skupionych na zagwarantowaniu cyberbezpieczeństwa.

Podsumowanie

Cyberprzestrzeń to miejsce, w którym dane osobowe przetwarzane są na niespotykaną w innych przestrzeniach skalę. Mają one dużą wartość dla różnych podmiotów, dzięki nim mogą przykładowo profilować klientów bądź dopasowywać oferty do konkretnych potrzeb. Dane osobowe, z pozoru nieistotne dla ich właścicieli, okazują się cenne dla innych podmiotów. Dzięki wiedzy na temat zachowania danej osoby oraz jej aktywności w sieci możliwe jest prognozowanie sposobu jej zachowania, aktywności, preferencji itp.

Internet to dziś ogromne źródło służące zarówno do pozyskiwania, jak i do przetwarzania danych. W cyberprzestrzeni każdego dnia tworzone są ogromne zbiory danych. Wiele z tych danych to dane wrażliwe. W praktyce dane te groma-

[43] Ustawa z 10 maja 2018 r. *o ochronie danych osobowych* (Dz.U. z 2018 r. poz. 1000 ze zm.).

[44] Ustawa z 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną* (Dz.U. z 2017 r. poz. 1219 ze zm.).

[45] Ustawa z 5 września 2016 r. *o usługach zaufania oraz identyfikacji elektronicznej* (Dz.U. z 2019 r. poz. 162).

[46] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Beck, Warszawa 2019, s. 52.

[47] T. Gwara, *Przepisy o cyberbezpieczeństwie mają wiele wspólnego z RODO*, https://www.prawo.pl/biznes/jak-wdrozyc-obowiazki-ktore-naklada-ustawa-o,295053.html, [dostęp 09.10.2020].

dzone są nadmiarze, bądź też są przechowywane dłużej, niż to konieczne. Wiele osób nie ma świadomości tego, jak szeroka jest skala nadużyć. Tymczasem zbiór danych osobowych pozwala na stworzenie takich algorytmów, dzięki którym firmy opracowują strategie swoich działań. Dane osobowe, podobnie jak wcześniej zasoby materialne czy informacje stały się towarem.

Wykorzystywanie danych osobowych stanowi ryzyko z punktu widzenia prywatności osób, których te dane dotyczą. Największe niebezpieczeństwo związane jest z łatwą oraz szybką utratą kontroli właścicieli nad swoimi danymi. Przez wiele lat dzięki tzw. profilowaniu możliwe było pozyskiwanie oraz profilowanie danych osobowych. Popularność Internetu sprawiła, że ludzie zaczęli wykazywać wzmożoną aktywność w sieci. Dzięki różnym usługom komunikacja stała się szybka i tania. Niestety, im większa aktywność w sieci, tym wyższe ryzyko bezprawnego wykorzystania danych osobowych.

Cyberbezpieczeństwo w ogóle, a bezpieczeństwo danych osobowych w cyberprzestrzeni w szczególności, jest w obecnie jednym z największych wyzwań dla wszystkich ich administratorów. Stworzenie dobrej i efektywnej strategii bezpieczeństwa cybernetycznego nie jest łatwym zadaniem. Wymaga zaangażowania wielu zasobów: technologicznych, kadrowych, a przede wszystkim finansowych. Wydaje się, że w warunkach polskich nie dostrzega w pełni, jak istotna jest właściwa polityka zarządzania cyberbezpieczeństwem w organizacji. Wiele podmiotów (instytucji, przedsiębiorców) podchodzi do tej kwestii jedynie w podstawowym zakresie. To głównie problem niskiej świadomości oraz sporych nakładów finansowych. Jednak o wiele większe koszty niesie za sobą lekceważenie inwestycji w ten obszar bezpieczeństwa. Przy bagatelizowaniu nakładów na zabezpieczenia, może dojść do realnych, wymiernych i niewymiernych strat.

Ważnym, a jednocześnie najsłabszym ogniwem systemu bezpieczeństwa w cyberprzestrzeni jest zawsze człowiek. Odpowiednia edukacja jest więc na pewno inwestycją o bardzo wysokiej stopie zwrotu. Gwarantuje ograniczenie późniejszych wydatków, czy to finansowych (naprawa systemów, z których wyciekły dane), czy czasowych (utrata gromadzonych danych, wstrzymanie działania danego podmiotu), a nawet wizerunkowych (utrata reputacji podmiotu, firmy na skutek skandalu po wycieku wrażliwych danych), a sama w sobie nie jest dużym wydatkiem.

Polska jest krajem, który dość dobrze, w wymiarze organizacyjno-prawnym, radzi sobie z cyfryzacją społeczeństwa oraz reagowaniem na wyzwania związane z nowymi technologiami i cyberzagrożeniami, czego dowodem jest uchwalona w 2018 r. ustawa o krajowym systemie cyberbezpieczeństwa. Państwo posiada dobrze rozbudowane prawodawstwo dotyczące ochrony danych osobowych. Istnieją jednak nadal mankamenty w egzekwowaniu tego prawa oraz dostosowaniu go do skutecznej ochrony prywatności obywateli przed cyberatakami.

Literatura:

1. Gumularz M. (red.), *Ochrona danych osobowych w marketingu i sprzedaży*, Beck, Warszawa 2019.
2. Gwara T., *Przepisy o cyberbezpieczeństwie mają wiele wspólnego z RODO*, https://www.prawo.pl/biznes/jak-wdrozyc-obowiazki-ktore-naklada-ustawa-o,295053.html.
3. Kitler W., Taczkowska-Olszewska J., Radoniewicz F., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Beck, Warszawa 2019, s. 52.
4. Kuźniar R., *Prawa człowieka. Prawo, instytucje, stosunki międzynarodowe*, Wydawnictwo Naukowe Scholar, Warszawa 2008, Wydanie trzecie uzupełnione.
5. Pryciak M., *Prawo do prywatności*, „Studia Erasmiana Wratislavensia", nr 2010/4.
6. Sienkiewicz P., *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", nr 13/2015.
7. Stępień A., *Bezpieczeństwo danych osobowych w cyberprzestrzeni – Big Data*, „Przedsiębiorczość i Zarządzanie", nr 2/2018.
8. Taczkowska-Olszewska J., Nowikowska M., *Prawo do informacji publicznej, informacje niejawne i ochrona danych osobowych*, Wolters Kluwer, Warszawa 2019.
9. Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Praca doktorska napisana w Katedrze Prawa Karnego Uniwersytetu w Białymstoku 2017.

Źródła prawa i materiały źródłowe:

10. Powszechna Deklaracja Praw Człowieka, Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana w dniu 10 grudnia 1948 r.
11. Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. 1977 nr 38 poz. 167.
12. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. Dz.U.1993.61.284.
13. Ustawa z dnia 2 kwietnia 1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz. U. z 1997 r. Nr 78, poz. 483).
14. Ustawa z dnia 23.04.1964 r. Kodeks cywilny. Tekst jednolity Dz.U.2020 poz.1740.
15. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych Dz.U. 2018 poz.1000.
16. Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560).
17. Ustawa z 29 lipca 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2017 r. poz. 1932).
18. Ustawa z 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2017 r. poz. 1928.)
19. Ustawa z 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2017 r. poz. 1897)
20. Rezolucja przyjęta przez Zgromadzenie Ogólne w dniu 18 grudnia 2013 roku, (68/167. Prawo do prywatności w erze cyfrowej).
21. Ustawa z dnia 23.04.1964 r. Kodeks cywilny. Tekst jednolity Dz.U.2020 poz.1740.
22. Konwencja Nr 108 Rady Europy z 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. z 2003 r. nr 3, poz. 25).
23. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych

oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, tłumaczenie na język polski) – stosowana do 25 maja 2018 r.
24. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz.Urz. UE L z 2016 r. Nr 119, s. 1, ze zm.).
25. Rezolucja przyjęta przez Radę Praw Człowieka 1 lipca 2016 r. (32/13) Promowanie, ochrona i korzystania z praw człowieka w Internecie. Opublikowana w dniu 18 lipca 2016 r. A/HRC/RES/32/.
26. Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, Warszawa marzec 2009.
27. Ministerstwo Cyfryzacji, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Warszawa 2017.