Anna Pawlak
Akademia Ekonomiczno-Humanistyczna w Warszawie
Instytut Nauk Prawnych
a.pawlak@vizja.pl
ORCID ID: 0000-0001-6112-8743

PRAWO DO PRYWATNOŚCI W DOBIE SZTUCZNEJ INTELIGENCJI

THE RIGHT TO PRIVACY IN THE ERA OF ARTIFICIAL INTELLIGENCE

Streszczenie

Prawo do prywatności w dobie sztucznej inteligencji oznacza możliwość sprawowania kontroli nad własnym życiem prywatnym, w tym nad informacjami o sobie i swojej rodzinie. Solidne przepisy o ochronie prywatności są nieodzowne dla budowy i utrzymywania zaufania w świecie cyfrowym. Niezwykle istotne jest zapewnienie równowagi między należytą ochroną życia prywatnego a wspieraniem rozwoju nowych technologii i innowacji.

Artykuł przedstawia, czym jest prywatność w dobie sztucznej inteligencji, jakie zagrożenia dla prywatności płyną z rozwoju technologii, w jaki sposób gwarantowane i chronione jest prawo do prywatności (zarówno przez normy międzynarodowe, jak i polskie regulacje prawne). Autor dokonuje także oceny regulacji prawnych dotyczących gwarancji prawa do prywatności w świecie sztucznej inteligencji.

Abstract

Privacy in the era of artificial intelligence is the ability to exercise control over your private life, including information about yourself and your family. Robust privacy laws are essential to building and maintaining trust in a digital world. It is extremely important to ensure a balance between proper protection of private life and supporting the development of new technologies and innovation.

The article presents what privacy is in the era of artificial intelligence, what threats to privacy result from the development of technology, how the right to privacy is guaranteed and protected (both by international standards and Polish legal regulations). The author also assesses the legal regulations regarding the guarantee of the right to privacy in the AI world.

Słowa kluczowe: *prawo do prywatności, sztuczna inteligencja, e-prywatność, zgrożenia prywatności*

Keywords: *the right to privacy, artificial intelligence, e-privacy, threats to privacy*

Wprowadzenie

Człowiek to istota społeczna, a zatem do harmonijnego rozwoju wymaga interakcji ze społeczeństwem, którego jest częścią. Naturalną konsekwencją interakcji międzyludzkich są ograniczenia autonomii każdej istoty ludzkiej, które przybierają postać ograniczeń naturalnych (natury moralnej, obyczajowej, religijnej itd.), jak i normatywnych. Pozwalamy więc organizacji państwowej oraz innym ludziom wkraczać w sferę naszych wolności, po to by czerpać z tego wymierne korzyści (takie jak wygoda, bezpieczeństwo, ład, przewidywalność zachowań drugiego człowieka, samorozwój, bogactwo, sława, szybkość dostępu do informacji itd.). Wraz z rozwojem sztucznej inteligencji (dalej: SI) nasza wolność, w tym nasza prywatność, kurczy się w niespotykanym do tej pory tempie. Zaburzona zostaje relacja między dwoma aspektami człowieczeństwa – autonomią bytu jednostki oraz jednostką będącą częścią większej społeczności. Wraz z rozwojem technologii, społeczeństwa informatycznego nasza wolność, nasza prywatność kurczy się w niespotykanym do tej pory tempie. Co gorsza – człowiek zaczyna być wart tyle, ile warte są jego dane osobowe. W społeczeństwie informacyjnym informacja stała się kluczowym elementem społeczno-ekonomicznej działalności i zmian, a bogato rozwinięte środki komunikacji i przetwarzania informacji stanowią podstawę tworzenia większości dochodu narodowego i zapewniają źródła utrzymania wielu ludziom[1]. To wszystko sprawia, że jedną z ważniejszych wolności człowieka,

[1] K. Krzysztofek, M. Szczepański, *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2002, s. 170.

która współcześnie powinna stać się przedmiotem szczególnej ochrony, jest autonomia osoby ludzkiej i jej prywatność.

Artykuł ma na celu przedstawienie, czym jest prywatność w dobie sztucznej inteligencji, jakie zagrożenia dla prywatności płyną z rozwoju technologii, w jaki sposób gwarantowane i chronione jest prawo do prywatności (zarówno przez normy międzynarodowe, jak i polskie regulacje prawne) i czy jest to ochrona wystarczająca, biorąc pod uwagę zdefiniowane zagrożenia.

Różne ujęcia prywatności

Próby zdefiniowania prywatności podjęto już pod koniec XIX w. Wówczas to amerykańscy prawnicy – Samuel D. Warren i Louis D. Brandeis, zgodnie z charakterystyczną dla amerykańskiej myśli prawniczej koncepcją indywidualistyczną, określali prawo do prywatności jako „prawo do bycia pozostawionym w spokoju”[2]. Mniej więcej w tym samym czasie w europejskim kręgu kulturowym zaczęła rodzić się niemiecka koncepcja „prawa do osobowości”, z której następnie wywiedziono prawo do prywatności[3], definiowanej przez Josepha Kohlera w 1907 r. jako swoboda rozporządzania informacjami na swój temat[4].

W ujęciu wolnościowym prywatność definiuje się jako stan, w którym osoba poodejmuje decyzje bez ingerencji osób trzecich[5]. Prywatność może być definiowana również w sposób szeroki – jako „prawo jednostki do życia własnym życiem, układanym według własnej woli, z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej”[6]. W wąskim ujęciu zaproponowanym przez Johna Innesa prywatność ogranicza się do ochrony sfery intymnej człowieka[7]. Biorąc pod uwagę aspekt socjologiczny i psychologiczny, wskazuje się, że doświadczenie prywatności to zjawisko uniwersalne

[2] S.D. Warren, L.D. Brandeis, *The right to Privacy*, „Harward Law Review” 1890, nr 4, s. 193–200.
[3] J. Żołyński, *RODO. Prawo do zapomnienia w sferze zatrudnienia*, Wolters Kluwer, Warszawa 2018, s. 72.
[4] J. Braciak, *Prawo do prywatności*, [w:] B. Banaszak, A. Presiner (red.), *Prawa i wolności obywatelskie w Konstytucji RP*, C.H. Beck, Warszawa 2004, s. 291.
[5] Z. Mielnik, *Prawo do prywatności (wybrane zagadnienia)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 1996, nr 2, s. 29.
[6] A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego (Zagadnienia konstrukcyjne)*, „Studia Cywilistyczne” 1972, nr 20, s. 6.
[7] J.C. Innes, *Privacy, Intimacy, and Isolation*, Oxford University Press, Oxford 1992.

i niezależne kulturowo, jest ono związane z koncepcją samowyobrażenia jednostki[8]. Z kolei samowyobrażenie to może być uzależnione od kontekstu społecznego. Warta podkreślenia jest współczesna teoria integralności kontekstowej Helen Nissenbaun[9], w której autorka wskazuje, że istnieje wiele kontekstów społecznych, w których występują różne oczekiwania odnośnie do ochrony prywatności. Prywatność kładziona jest na szali z innymi wartościami (takimi jak wygoda czy dostęp do informacji) i przeważnie z nimi przegrywa – co pokazuje przykład: wolimy karty kredytowe, aplikacje w telefonie, a nawet mikrochipy pod skórą od gotówki, podobnie jak wybieramy zakupy w sieci – bez kolejek i z dostawą do domu, podając w zamian swoje dane osobowe, numer konta i adres zamieszkania.

Istnieje wiele koncepcji oraz definicji prawa do prywatności, w zależności od interpretacji i podkreślenia wybranego aspektu prywatności w różnych sferach życia (osobistej, rodzinnej, wolności słowa, finansów osobistych, danych osobowych czy prowadzenia działalności gospodarczej). Jak wskazuje Małgorzata Ciechomska: „Taka nieprecyzyjna konceptualizacja prywatności może okazać się konieczna, aby utrzymać elastyczność, która umożliwia rozpoznanie, zrozumienie i uwzględnienie nowego wymiaru prywatności, w celu skutecznego reagowania na szybki rozwój technologiczny"[10]. Rozumienie prywatności zmienia się wraz z postępem, zwłaszcza w pokoleniu, które dorasta w czasach, w których Internet jest powszechnie dostępny i mocno rozwija się trend internetowy oparty na Web 2.0, u podstaw którego leży dzielenie się informacjami w sieci.

[8] M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Wolters Kluwer, Warszawa 2019, s. 39.
[9] H. Nissenbaum, *Privacy in the context: technology, privacy and the integrity of social life*, Standford University Press, Stanford 2010, s. 67.
[10] M. Ciechomska, *E-usługi a RODO*, Wolters Kluwer, Warszawa 2021, s. 45.

Prawo do prywatności

Ingerencja zewnętrzna ograniczająca wolę jednostki jest w pewnym zakresie niezbędna, ochrona prawa do prywatności powinna jednak zapewniać, że będzie to ingerencja celowa i konieczna.

Prawo do prywatności po raz pierwszy zostało proklamowane w Powszechnej Deklaracji Praw Człowieka z 10 grudnia 1948 r., będącej rezolucją Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych, która w art. 12 stanowi, że „nikt nie może być poddany arbitralnemu ingerowaniu w jego życie prywatne, rodzinne, domowe lub korespondencję […]". W systemie uniwersalnym prawo to zostało przyznane także w art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych z dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167), którego treść jest zbieżna z regulacją Powszechnej Deklaracji Praw Człowieka.

Z kolei w reżimie prawnym Rady Europy proklamowano prawo do prywatności już w 1950 r., zapisując je w art. 8 Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.). Ustęp 1 tego aktu wskazuje że: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji", z kolei w ust. 2 podkreślono, iż: „niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób". Akt ten ma szczególne znaczenie z uwagi na skuteczny mechanizm kontroli przestrzegania przez państwa członkowskie postanowień Konwencji, w postaci podlegania orzecznictwu Europejskiego Trybunału Praw Człowieka (dalej: ETPC) z siedzibą w Strasburgu. Trybunał jest bowiem władny rozpatrywać skargi dotyczące nieprzestrzegania zapisów Konwencji przez państwa będące stronami Konwencji. Orzecznictwo ETPC w zakresie prawa do prywatności doczekało się bogatego dorobku. Trybunał stoi na stanowisku, że nie można zastosować wyczerpującej definicji prawnej prywatności z uwagi na jej

szeroki zakres definicyjny[11]; wskazuje on, że do chronionej sfery prywatności należy zaliczyć tożsamość, przynależność etniczną, orientację seksualną[12], identyfikację osoby (nazwisko, zdjęcie), integralność fizyczną i psychiczną[13], przepływ danych osobowych[14] czy też korespondencję (w tym za pośrednictwem komunikacji elektronicznej)[15]. Bogate orzecznictwo ETPC przyczyniło się do ukształtowania prawnego rozumienia zakresu, ale także granic oraz możliwości limitacji prawa do prywatności[16].

W ramach Rady Europy już od lat siedemdziesiątych XX w. były wydawane rezolucje i rekomendacje dotyczące ochrony prawa do prywatności danych osobowych, przy czym w latach siedemdziesiątych były to rezolucje dotyczące ochrony sfery prywatności osób fizycznych (Rezolucja Komitetu Ministrów 22 (73) dotycząca wykorzystywania elektronicznych banków danych w sektorze prywatnym, a także Rezolucja 29 (74) odnosząca się do sektora publicznego). Natomiast zaczynając od 1981 r. Komitet Ministrów wydał szereg rekomendacji dotyczących różnych aspektów ochrony danych osobowych. Wprawdzie rezolucje i rekomendacje Rady Europy nie mają wiążącego charakteru, ale bez wątpienia wyznaczają państwom członkowskim preferowany poziom ochrony.

Ważnym aktem prawnym dotyczącym ochrony prywatności oraz ochrony danych osobowych jest Konwencja 108 sporządzona w Strasburgu dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych uchwalona w reżimie Rady Europy. Konwencja ta ma szczególne znaczenie z uwagi na sporą liczbę państw, która ją ratyfikowała, oraz swój wiążący charakter dla państw stron[17]. Była ona wielokrotnie uzupełniana i dostosowywana do postępu technologicznego. 10 października 2018 r.

[11] Wyrok ETPC z 2 dnia września 2010 r. w sprawie Uzun v. Niemcy, 35623, § 43.
[12] Wyrok ETPC z dnia 17 lipca 2003 r. w sprawie Perry v. Wielka Brytania, 63737/00, § 36.
[13] Wyrok ETPC z dnia 7 lutego 2012 r. w sprawie von Hannover v Niemcy, 40660/08, § 95.
[14] Wyrok ETPC z dnia 6 czerwca 2006 r. w sprawie Segerstedt-Wiberg i in. v. Szwecja, 62332/00; Wyrok ETPC z dnia 4 grudnia 2008 r. w sprawie S. i Marper v. Wielka Brytania, 30562/04 i 30566/04.
[15] Wyrok ETPC z 3 kwietnia 2007 r. w sprawie Copland v Wielka Brytania, 62617/00.
[16] Więcej zob.: M. Rojszczak, dz. cyt., s. 92 i n.
[17] Lista państw dostępna na stronie: Chart of signatures and ratifications of Treaty 108, Council of Europe 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (dostęp: 2.05.2021).

podpisany został Protokół zmieniający Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108)[18].

Prawo do prywatności zyskało szczególną rangę w systemie prawnym Unii Europejskiej (dalej: UE) z uwagi na uznanie go za prawo podstawowe. Karta Praw Podstawowych Unii Europejskiej[19], która moc wiążącą uzyskała w 2009 r., w art. 7 zawiera regulację wskazującą, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, domu i komunikowania się. Natomiast art. 8 zawiera regulacje dotyczące ochrony danych osobowych. Oba te przepisy należy odczytywać razem, gdyż: „dane osobowe są chronione ze względu na ich szczególne znaczenie w życiu prywatnym i rodzinnym"[20]. Uznanie prawa do prywatności oraz prawa do ochrony danych osobowych za prawa podstawowe pokazuje, jak duże znaczenie aktualnie nadaje się temu zagadnieniu.

Prawa do prywatności oraz do ochrony danych osobowych zostały umieszczone w Tytule II Karty Praw Podstawowych, który nosi nazwę „Wolności". Michał Czerniawski podkreśla, że „w epoce społeczeństwa informacyjnego i Internetu na znaczeniu wydaje się zyskiwać […] aspekt „wolnościowy", kontrolowania dotyczących siebie informacji i rozporządzania dotyczącymi siebie informacjami, w tym własnymi danymi osobowymi"[21].

Jednak jeszcze przed proklamowaniem Karty Praw Podstawowych w strukturach unijnych powstawały akty normatywne mające na celu ochronę prawa do prywatności oraz jednego z jej aspektów – danych osobowych. Pierwszym, milowym krokiem poczynionym w kierunku standaryzacji i ujednolicenia zasad ochrony danych osobowych w ramach Unii Europejskiej było uchwalenie w 1995 r. 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 (OJ L 281 z 1995 r.). Po uchwaleniu tej dyrektywy w ramach UE wydanych zostało wiele

[18] Lista państw, które podpisały Protokół zmieniający: Chart of signatures and ratifictions of Treaty 223, Council od Europe 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (dostęp: 3.05.2021).

[19] Karta Praw Podstawowych Unii Europejskiej z 30 marca 2010 r. (Dz.Urz. UE C 202 z 7 czerwca 2016 r., s. 389).

[20] T. Jurczyk, *Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*, Oficyna, Warszawa 2009.

[21] M. Czerniawski, *Ochrona danych osobowych w prawie międzynarodowym*, [w:] D. Lubasz (red.), *Meritum. Ochrona danych osobowych*, Wolters Kluwer, Warszawa 2020, s. 21.

dyrektyw mających na celu standaryzację zasad ochrony szeroko pojętej prywatności. Między innymi z 2000 r. pochodzi dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady Wspólnoty Europejskiej, regulująca prawa i obowiązki usługodawców i usługobiorców społeczeństwa informacyjnego. Z kolei w 2002 r. wydano Dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej, zwana także dyrektywą o e-prywatności). Zobowiązuje ona państwa członkowskie do zapewnienia ekwiwalentnego stopnia ochrony prawa do prywatności w odniesieniu do przetwarzania danych osobowych w sektorze komunikacji elektronicznej, a także do zapewnienia swobodnego przepływu tych danych osobowych we Wspólnocie. Dyrektywa ta nadal obowiązuje, wymaga jednak szybkiej aktualizacji, by uwzględnić zmiany technologiczne i rynkowe, takie jak rozpowszechnienie telefonii internetowej oraz internetowych usług poczty i komunikacji elektronicznej oraz pojawienie się nowych technik śledzenia zachowań użytkowników w Internecie.

Unia Europejska swoimi regulacjami objęła także standardy w zakresie zatrzymywania pewnych danych przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności, tak by zapewnić w określonych sytuacjach wykorzystanie tych danych w celach wykrywania i ścigania poważnych przestępstw, określonych w przepisach krajowych (stanowi o tym Dyrektywa Parlamentu Europejskiego i Rady WE nr 2006/24/WE).

By przenieść ochronę prawa do prywatności z poziomu horyzontalnego na wertykalny, akt unijny, jakim są dyrektywy, jest środkiem niewystarczającym, a gwarancje prawa do prywatności winny znaleźć się w akcie prawnym mającym zastosowanie również między obywatelami państw członkowskich. W 2012 r. zaczęto prace nad reformą ochrony danych w UE. Prace nad nowymi przepisami zakończyły się uchwaleniem 27 kwietnia 2016 r. Rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 4 maja 2016 r., s. 1). Przepisy o ochronie danych osobowych zyskały formę rozporządzenia unijnego, co skutkuje ich bezpośrednim stosowaniem we wszystkich krajach członkowskich UE.

Ogólne rozporządzenie o ochronie danych weszło w życie 24 maja 2016 r., natomiast w państwach członkowskich zaczęło być stosowane od 25 maja 2018 r.

Unia Europejska pracuje także nad tzw. rozporządzeniem e-privacy, którego projekt został przedstawiony 10 stycznia 2017 r. Rozporządzenie to w pierwotnym założeniu miało wejść w życie razem z rozporządzeniem o ochronie danych osobowych i stanowić specjalną regulację w zakresie prywatności w Internecie (tzw. lex specialis do RODO). Negocjacje wciąż jednak trwają[22]. Rozporządzenie to ma na celu uchylenie Dyrektywy 2002/58/WE w sprawie prywatności i łączności elektronicznej.

W polskim porządku prawnym prawo do ochrony prywatności posiada rangę gwarancji konstytucyjnej. W art. 47 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.) uregulowano, iż: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Regulacja ta została uzupełniona o treść art. 51 Konstytucji RP odnoszącego się do ochrony danych osobowych, w którym wskazano m.in., iż nikt nie może być zobowiązany inaczej niż na postawie ustawy do ujawnienia informacji dotyczącej jego osoby (art. 51 ust. 1). W doktrynie wskazuje się, że oba te artykuły chronią tę samą wartość konstytucyjną, jaką jest prawo do prywatności[23]. Gwarancje te uzupełniono o przepisy szczegółowe regulujące takie obszary związane z prawem do prywatności jak: nietykalność i wolność osobista (art. 41), tajemnica korespondencji (art. 49), nienaruszalność mieszkania (art. 50), wolność sumienia i wyznania (art. 53) czy też ochrona konsumentów przed działaniami zagrażającymi ich prywatności (art. 76 Konstytucji RP).

[22] https://www.gov.pl/web/cyfryzacja/projekt-rozporzadzenia-ue-w-sprawie-prywatnosci-i-lacznosci-elektronicznej-rozporzadzenie-eprivacy (dostęp: 7.08.2021).
[23] M. Rojszczak, dz. cyt., s. 132.

Zagrożenia SI dla prywatności

Termin „sztuczna inteligencja" (SI, ang. *artificial intelligence*, AI) odnosi się do systemów, które wykazują inteligentne zachowanie poprzez analizę swojego otoczenia i na jej podstawie podejmowanie działań – z pewnym stopniem autonomii – w celu osiągnięcia określonych celów. Takie systemy mogą być oparte wyłącznie na oprogramowaniu, działając w świecie wirtualnym (np. cyfrowi asystenci w telefonach lub komputerach, oprogramowanie do analizy obrazu, wyszukiwarki internetowe, systemy rozpoznawania mowy i twarzy) lub stanowić część składową urządzeń (np. zaawansowane roboty używane w fabrykach, autonomiczne samochody, drony lub aplikacje internetowe przedmiotów)[24].

Co do zasady sztuczna inteligencja umożliwia systemom technicznym postrzeganie ich otoczenia, zebranie informacji i ich przegląd oraz rozwiązywanie problemów, mając na względzie osiągnięcie określonego rezultatu. A zatem system zbiera informacje (już przygotowane lub odebrane za pomocą określonego czytnika, np. czujników inteligentnej klimatyzacji czy kamery), przetwarza je i wdraża odpowiednie zachowanie.

Sztuczna inteligencja postrzegana jest jako jedna z najważniejszych technologii przyszłości oraz centralny element cyfrowej transformacji społeczeństwa. Niektóre technologie sztucznej inteligencji istnieją od kilkudziesięciu lat, jednakże to współczesna transformacja cyfrowa, a w szczególności rozwój w zakresie mocy obliczeniowej oraz algorytmów, a także dostępność dużej liczby danych, przyniosły wielkie osiągnięcia w tej dziedzinie. Przewiduje się, że przyszłe zastosowania sztucznej inteligencji będą miały ogromny wpływ na funkcjonowanie społeczeństwa – z prognoz International Data Corporation[25] wynika, że w roku 2024 inwestycje w sztuczną inteligencję osiągną wartość 110 mld USD, tj. wartość dwa razy wyższą od poziomu z roku 2020.

---

[24] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Sztuczna inteligencja dla Europy*, Bruksela, 25 kwietnia 2018 r. COM(2018) 237 final,https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018DC0237&from=RO (dostęp: 7.08.2021).

[25] International Data Corporation, *Worldwide Spending on Artificial Intelligence Is Expected to Double in Four Years, Reaching $ 110 Billion in 2024, According to New IDC Spending Guide*, 25 sierpnia 2020 r.

Sztuczna inteligencja używana jest w gadżetach i urządzeniach powszechnego użytku typu smart (smart-watch, smart-phone, smart-zabawka, smart-tv), które z założenia mają uprzyjemnić i ułatwić życie ich użytkownikom. Społeczeństwo masowo kupuje tego typu urządzenia, udostępniając za ich pomocą wiele informacji o sobie – pory snu i aktywności, nazwisko ulubionego aktora, dane rodziny i znajomych, wizerunek dziecka, a nawet aktualny poziom stresu czy ciśnienia tętniczego. Ponadto urządzenia powszechnego użytku, takie jak lodówki, czajniki, czy różnego rodzaju sensory, czujniki oraz kamery, często stanowiące składową tzw. inteligentnych budynków, po dołączeniu ich do sieci stanowią bardzo duże zagrożenie, przede wszystkim gdy sieć ta nie jest zabezpieczona. Stąd też w ostatnich latach pojawił się nowy rodzaj ochrony zasobów sieciowych, zwany ochroną Internetu rzeczy (ang. *Internet of Things* – IoT)[26].

Posługując się sztuczną inteligencją, świadomie lub – co gorsza – nieświadomie udostępniamy informacje, które następnie sztuczna inteligencja wykorzystuje np. w celach profilowania naszej osoby. Analiza pozostawionych przez nas danych pozwala na stworzenie naszego profilu, przyporządkowaniu go do określonych grup społecznych i proponowanie odpowiednio dopasowanych usług. Profilowanie, którego użytkownicy często nie są świadomi, kłóci się z istotą prywatności, w ramach której każdy człowiek ma prawo decydować o tym, jakie informacje o jego osobie są przekazywane dalej.

Rozwój sztucznej inteligencji, jeśli będzie nieograniczony i nieusystematyzowany, może stanowić duże zagrożenie dla poszanowania prawa do prywatności osób korzystających z SI.

Zagrożenia te według Marcina Rojszczak[27] można podzielić na:

- cyberprzestępstwa (w tym kradzież, zniszczenie danych, wyłudzenia tożsamości, nieuczciwa manipulacja, wprowadzenie w błąd, ale także bezpośredni lub pośredni nielegalny przymus);
- profilowanie (realizowane bez poszanowania praw człowieka, wbrew wiedzy i woli użytkownika systemu);
- cyberinwigilację (nieuprawniona obserwacja zarówno w formie zinstytucjonalizowanej – przez państwa, np. poprzez system rozpoznawania twarzy, ale także przez podmioty prywatne, np. geolokalizacja na cele

[26] W. Nowak, *Specyfika zagrożeń w cyberprzestrzeni*, [w:] C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo*, Wolters Kluwer, Warszawa 2020, s. 118.
[27] M. Rojszczak, dz. cyt., s. 75 i n.

marketingu czy też inwigilacja mieszkań za pomocą kamery zamontowanej w smart-zabawce);
- ujawnienie informacji (z uwagi na działania inne niż przestępcze, np. awarię systemu);
- utratę kontroli nad informacją (np. na skutek utraty kontroli nad zaprogramowaną maszyną).

Do powyższych zagrożeń należy dodać niezwykle niebezpieczny skutek nieumiejętnego lub nadmiernego korzystania ze sztucznej inteligencji w postaci zagrożeń dla niezależności psychicznej i zdrowia psychicznego. Jak wskazuje się w wytycznych w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji:

„Wszechobecny kontakt ze społecznymi systemami SI we wszystkich obszarach naszego życia (czy to w ramach edukacji, pracy, opieki czy rozrywki) może zmienić naszą koncepcję pośrednictwa społecznego lub wpłynąć na nasze relacje i przywiązania społeczne. Chociaż systemy SI mogą być wykorzystywane do podnoszenia umiejętności społecznych, mogą one również przyczynić się do ich pogorszenia. Może to również wpłynąć na stan zdrowia fizycznego i psychicznego ludzi. W związku z tym należy skrupulatnie monitorować i brać pod uwagę wpływ tych systemów"[28].

Systemy SI komunikują się z ludźmi i poprzez interakcje humanoidalnego robota lub awatarów w rzeczywistości wirtualnej symulują umiejętności społeczne, przez co systemy te mogą zmienić nasze zachowania społeczno-kulturowe i strukturę naszego życia społecznego. Z założenia interakcja z SI ma poprawiać kompetencje społeczne (np. finansowany ze środków unijnych projekt opracowania oprogramowania komputerowego opartego na SI, które pozwala na skuteczniejszą interakcję z dziećmi autystycznymi w trakcie sesji terapeutycznych prowadzonych przez człowieka, co przyczynia się do poprawy ich umiejętności społecznych i komunikacyjnych)[29]. Jednak interakcja osoby ze sztuczną inteligencją niesie ryzyko wystąpienia dezorientacji u człowieka czy też zmęczenia poznawczego.

---

[28] Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, Komisja Europejska, kwiecień 2019 r., s. 24, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60436 (dostęp: 8.08.2021).

[29] Informacje na ten temat na stronie: http://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/headlines/news/article_19_03_12_en.html?infocentre&item=Infocentre&artid=49968 (dostęp: 8.08.2021).

Istotnym zagrożeniem związanym z funkcjonowaniem sztucznej inteligencji jest także możliwość wykorzystania jej dla wzmocnienia asymetrii władzy lub informacji (relacje między pracownikiem a pracodawcą, przedsiębiorcą a konsumentem, państwem a obywatelem). Szczególnie ważne są legalność przetwarzania informacji o osobach przez rządy państw, jakość zabezpieczeń danych osób przewidzianych przez krajowe systemy czy konieczność zapewnienia skutecznych mechanizmów dochodzenia przez obywateli swoich praw w przypadku naruszenia prawa do prywatności przez przedstawicieli państwa.

Biorąc pod uwagę dotkliwość zagrożeń wynikających z korzystania ze sztucznej inteligencji za pomocą cyberprzestrzeni, Włodzimierz owak wymienia trzy najdotkliwsze kategorie zagrożeń:

- ataki z użyciem szkodliwego oprogramowania (tj. malware, wirusy, trojany, robaki, keyloggery itd.);
- kradzieże tożsamości, wyłudzenia, modyfikacje lub niszczenie danych;
- blokowanie dostępu do usług, działania socjotechniczne, wyłudzenia[30].

Powyższe incydenty mogą wystąpić wówczas, gdy SI połączona jest z siecią internetową w sposób bezpośredni lub za pośrednictwem sieci firmy czy sieci domowej.

Wskazane powyżej zagrożenia nie wyczerpują katalogu niebezpieczeństw płynących z użytkowania sztucznej inteligencji, których skutkiem może stać się naruszenie prywatności użytkowników SI.

Regulacje prawne dotyczące SI w kontekście ochrony prywatności i ich ocena

W związku z tak licznymi zagrożeniami płynącymi z użytkowania sztucznej inteligencji, które mogą dotkliwie ingerować w sferę prywatności ludzi, niezwykle istotne jest odpowiednie zabezpieczenie użytkowników SI i jasne określenie zasad odpowiedzialności w przypadku zaistnienia naruszenia. By tak się mogło stać, w pierwszej kolejności musi zostać stworzony system regulacji prawnych, które zabezpieczą prawa użytkowników, wskażą kierunki rozwoju

[30] W. Nowak, dz. cyt., s. 103.

sztucznej inteligencji i choć w pewnym zakresie pozwolą go kontrolować, tak by minimalizować ryzyko nieodpowiedniego wykorzystania SI.

Niestety przegląd wiążących regulacji prawnych dotyczących sztucznej inteligencji, gwarantujących ochronę prywatności człowieka, nie jest optymistyczny. Nie ma w tym zakresie odpowiednich regulacji ani w systemie międzynarodowym, ani w systemie prawa krajowego. Również patrząc z drugiej strony – nieliczne z przedstawionych regulacji prawnych statuujących prawo do prywatności wprost odnosi się do sztucznej inteligencji. Dzieje się tak głównie z tego powodu, że są to akty prawne, które powstawały w większości w XX w., kiedy to SI nie była powszechnie używana przez osoby prywatne.

Intensywne prace nad stworzeniem regulacji prawnych gwarantujących bezpieczny rozwój sztucznej inteligencji trwają w ramach Unii Europejskiej od 2018 r., kiedy to 25 kwietnia Komisja wydała komunikat *Sztuczna inteligencja dla Europy*[31]. Komunikat ten zakładał, iż pierwszym krokiem w kierunku rozwiązania problemów etycznych, w tym wpływu SI na prywatność, będzie opracowanie wytycznych dotyczących etyki używania sztucznej inteligencji, z należytym uwzględnieniem Karty Praw Podstawowych Unii Europejskiej. W czerwcu 2018 r. Komisja Europejska powołała niezależną grupę ekspertów wysokiego szczebla ds. SI, która opracowała wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji. Wytyczne zostały opublikowane w grudniu 2018 r., a następnie po uwzględnieniu ponad 500 konsultacji poprawiony dokument opublikowano w kwietniu 2019 r.[32]

W wytycznych w zakresie etyki wskazano, że system SI powinien być zgodny z siedmioma zasadami godnej zaufania sztucznej inteligencji. Są one następujące: 1) przewodnia i nadzorcza rola człowieka, 2) solidność techniczna i bezpieczeństwo, 3) ochrona prywatności i zarządzanie danymi, 4) przejrzystość, 5) różnorodność, niedyskryminacja i sprawiedliwość, 6) dobrostan społeczny i środowiskowy oraz 7) odpowiedzialność. A zatem jedną z nadrzędnych zasad etycznej SI jest zapewnienie ochrony prywatności (zasada nr 3).

---

[31] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Sztuczna inteligencja…*, dz. cyt.

[32] Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, Bruksela, 10 kwietnia 2019, dostęp: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_PL.pdf (dostęp: 8.08.2021).

Wytyczne wskazują, że systemy SI muszą gwarantować ochronę prywatności i danych przez cały swój cykl życia. Dotyczy to informacji podanych początkowo przez użytkownika, a także informacji wygenerowanych na temat użytkownika w trakcie jego interakcji z systemem. Dzięki cyfrowym rejestrom zachowań ludzkich systemy SI mogą ustalać nie tylko indywidualne preferencje użytkowników, ale również ich orientację seksualną, wiek, płeć, poglądy religijne lub polityczne. Aby użytkownik mógł zaufać procesowi gromadzenia danych, należy zapewnić, aby zbierane dane dotyczące jego osoby nie były wykorzystywane do jego dyskryminowania, w sposób niesprawiedliwy lub niezgodny z prawem. W omawianych wytycznych wskazano na środki mające na celu zwiększenie ochrony prywatności, do których zaliczyć należy szyfrowanie, anonimizację i agregację.

Na wskazane wytyczne powołał się także Parlament Europejski, w rezolucji z dnia 12 lutego 2019 r. w sprawie kompleksowej europejskiej polityki przemysłowej w dziedzinie sztucznej inteligencji i robotyki[33]. Rezolucja Parlamentu podkreśla, że przejrzysta i oparta na założeniach etycznych sztuczna inteligencja i robotyka mogą wzbogacić nasze życie i poszerzyć nasze możliwości zarówno na poziomie jednostek, jak i ogółu, a coraz częstsze stosowanie robotyki w systemach ludzkich wymaga zdecydowanych wytycznych politycznych dotyczących sposobów maksymalizacji korzyści i minimalizacji ryzyka społecznego oraz zapewnienia bezpiecznego i sprawiedliwego rozwoju sztucznej inteligencji. Rezolucja Parlamentu Europejskiego poświęca dział 4.2 na omówienie zagadnienia danych osobowych i prywatności. Podkreśla się w niej, że należy zapewnić wysoki poziom bezpieczeństwa, ochrony i prywatności w odniesieniu do danych wykorzystywanych w komunikacji między ludźmi a robotami i sztuczną inteligencją, dlatego też niezbędne jest uwzględnianie zasad bezpieczeństwa i ochrony prywatności już na etapie projektowania sztucznej inteligencji (pkt 125). W rezolucji przypomniano także, że prawo do prywatności proklamowane w Karcie Praw Podstawowych UE ma zastosowanie do wszystkich obszarów robotyki i sztucznej inteligencji (pkt 126). Parlament wezwał do przeglądu norm prawa krajowego pod kątem zasad i kryteriów

[33] Rezolucja Parlamentu Europejskiego z dnia 12 lutego 2019 r. w sprawie kompleksowej europejskiej polityki przemysłowej w dziedzinie sztucznej inteligencji i robotyki (2018/2088(INI)), https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_PL.html (dostęp: 8.08.2021).

dotyczących korzystania z kamer i czujników, robotyki i odnoszących się do sztucznej inteligencji (pkt 127). W sposób wyraźny w Rezolucji wskazano, że prawo do prywatności musi być zawsze respektowane, a osoby fizyczne nie mogą być rozpoznawalne. Jeśli tak miało by się dziać, to projektant sztucznej inteligencji powinien zawsze otrzymać wyraźne, jednoznaczne i świadome przyzwolenie i to projektanci ponoszą odpowiedzialność za przestrzeganie procedur w zakresie ważnej zgody, poufności, anonimowości, sprawiedliwego traktowania i należytego postępowania; podkreśla się, że projektanci muszą stosować się do każdego wniosku o zniszczenie lub usunięcie jakichkolwiek powiązanych danych z wszelkich zestawów danych.

Kolejnym krokiem w kierunku opracowania unijnych regulacji dotyczących bezpiecznego rozwoju sztucznej inteligencji było wydanie 19 lutego 2020 r. przez Komisję Europejską Białej księgi w sprawie sztucznej inteligencji[34]. W księdze tej zauważa się, że UE dysponuje rygorystycznymi ramami prawnymi zapewniającymi m.in. ochronę danych osobowych i prywatności. W odniesieniu do danych osobowych funkcjonuje rozporządzenie o ochronie danych osobowych z 2016 r., natomiast ciągle jeszcze trwają prace nad rozporządzeniem o e-prywatności, a obecnie bezpieczeństwo prywatności w systemach informatycznych regulowane jest aktem prawnym o randze dyrektywy z 2002 r., co nie może być oceniane jako stan zadowalający. Obowiązująca obecnie dyrektywa o e-prywatności z 2002 r. wymaga aktualizacji, tak by uwzględniała zmiany technologiczne i rynkowe, takie jak rozpowszechnienie telefonii internetowej oraz internetowych usług poczty i komunikacji elektronicznej oraz pojawienie się nowych technik śledzenia zachowań użytkowników w Internecie. Trwają zatem nad tym prace, natomiast należy mieć na uwadze, że wdrożenie projektowanych regulacji w krajach członkowskich będzie wymagało wielu miesięcy przygotowań, podobnie jak to było w przypadku RODO.

Aktualnie Parlament UE pracuje nad projektem przedstawionym 21 kwietnia 2021 r. Komisji Europejskiej dotyczącym przekształcenia Europy w globalne centrum wiarygodnej sztucznej inteligencji[35]. W strukturach unijnych trwają

[34] Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania. Komisja Europejska, Bruksela, 19 lutego 2020 r., COM(2020) 65 final, tekst Księgi: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pl.pdf (dostęp: 8.08.2021).

[35] Więcej: https://www.europarl.europa.eu/news/pl/headlines/society/20201015STO89417/regulacje-ws-sztucznej-inteligencji-oczekiwania-parlamentu (dostęp: 8.08.2021).

intensywne prace nad wdrożeniem pakietu przepisów dotyczących cyberbezpieczeństwa[36].

W polskim systemie prawnym nie ma aktualnie odrębnych i szczegółowych regulacji w przedmiocie technologii SI. Stworzenie spójnej regulacji w zakresie nowej rzeczywistości cyfrowej jest dużym wyzwaniem legislacyjnym, w szczególności ze względu na nieustanny rozwój technologii. Warto podkreślić, że pod koniec grudnia 2020 r. Rada Ministrów uchwaliła *Politykę dla rozwoju sztucznej inteligencji w Polsce od roku 2020*[37], która w założeniu ma wskazać kierunek działaniom mającym na celu wspieranie rozwoju sztucznej inteligencji w Polsce, m.in. w administracji publicznej i gospodarce. Uchwała Rady Ministrów powołuje się na zasady etyczne SI zawarte w wytycznych grupy ekspertów Komisji Europejskiej. Pierwszą informację o realizacji działań w ramach polityki SI minister właściwy do spraw informatyzacji miał przedstawić Radzie Ministrów do dnia 1 września 2021 r.

Podsumowanie

Gwarancja prawa do prywatności w dobie sztucznej inteligencji w rzeczywistości oznacza zobowiązanie do umożliwienia obywatelowi sprawowania jeszcze większej kontroli nad własnym życiem prywatnym, w tym nad informacjami o nim i jego rodzinie. Co jest istotne – początkowo gdy w latach siedemdziesiątych ubiegłego wieku zaczęto proklamować prawo do prywatności, chodziło głównie o zapewnienie jak najmniejszej ingerencji w życie człowieka przez struktury państwowe. Współcześnie, dzięki rozwijającej się sztucznej inteligencji, biznes, a także osoby prywatne mają podobne do struktur państwowych, a niejednokrotnie i większe, możliwości ingerowania w prywatność drugiego człowieka (co uzależnione jest od zasobów finansowych danego sektora). Dlatego też ochrona prawa do prywatności nie może mieć jedynie wymiaru wertykalnego, ale także horyzontalny. By przenieść ochronę

[36] Na stronie: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-cyber-security-package znajduje się tzw. pociąg legislacyjny z 47 wagonami dotyczącymi różnych sfer cyberbezpieczeństwa, z których to zdecydowania większość „wagonów" znajduje się na etapie projektowania.

[37] Uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020" (M.P. 2020, poz. 23).

prywatności z poziomu wertykalnego na horyzontalny Unia Europejska pracuje nad rozporządzeniem e-privacy, które ma uchylić przestarzałą w odniesieniu do zagadnień SI obowiązującą dyrektywę w sprawie prywatności i łączności elektronicznej. Rada Unii Europejskiej na początku 2021 r. wydała czternastą wersję projektu rozporządzenia, co pokazuje, jak trudne jest ujednolicenie regulacji prawnych dotyczących prywatności w sieci we wszystkich krajach Unii Europejskiej.

Solidne przepisy o ochronie prywatności są nieodzowne dla budowy i utrzymywania zaufania w świecie cyfrowym. Niezwykle istotne jest zapewnienie równowagi między należytą ochroną życia prywatnego a wspieraniem rozwoju nowych technologii i innowacji. Natomiast aktualny stan regulacji prawnych nie może być oceniany w tym zakresie entuzjastycznie. W strukturach unijnych funkcjonują ogólne regulacje dotyczące prawa do prywatności, przestarzała dyrektywa dotycząca e-prywatności, a także wiele dokumentów niewiążących odnoszących się bezpośrednio do sztucznej inteligencji, które w pewnym zakresie dotyczą problemu prawa do prywatności. Obecnie problematyczne jest ustalenie, kto ponosi odpowiedzialność za naruszenie prywatności osoby fizycznej przez system SI. Dlatego też bardzo ważne jest zakończenie prac nad rozporządzeniem unijnym o e-prywatności, jednak jest to proces, na którego efekty musimy jeszcze poczekać. Wieloletnie negocjacje nad projektem rozporządzenia dotyczącego e-prywatności pokazują, jak trudny jest to temat, a jednocześnie podważają wiarę w możliwość szybkiego reagowania na zmieniającą się rzeczywistość i galopujący rozwój sztucznej inteligencji.

Bibliografia

Braciak J., *Prawo do prywatności*, [w:] B. *Banaszak, A.* Presiner (red,), *Prawa i wolności obywatelskie w Konstytucji RP*, C.H. Beck, Warszawa 2004.

Ciechomska M., *E-usługi a RODO*, Wolters Kluwer, Warszawa 2021.

Czerniawski M., *Ochrona danych osobowych w prawie międzynarodowym*, [w:] D. *Lubasz (red.), Meritum. Ochrona danych osobowych*, Wolters Kluwer Warszawa 2020, s. 21.

Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, Bruksela, 10 kwietnia 2019 r., *https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_PL.pdf (dostęp: 8.08.2021).*

Innes J.C., *Privacy, Intimacy and Isolation*, Oxford University Press, Oxford 1992.

International Data Corporation, *Worldwide Spending on Artificial Intelligence Is Expected to Double in Four Years, Reaching $110 Billion in 2024, According to New IDC Spending Guide*, 25 sierpnia 2020 r.

Jurczyk T., *Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*, C.H. *Beck, Warszawa 2009.*

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Sztuczna inteligencja dla Europy*, Bruksela, 25 kwietnia 2018 r., COM(2018) 237 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?*uri=CELEX:52018DC0237&from=RO (dostęp: 7.08.2021).*

Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego (Zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1972, nr 20.

Krzysztofek K., Szczepański M., *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2002.

Mielnik Z., *Prawo do prywatności (wybrane zagadnienia)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 2.

Nissenbaum H., *Privacy in the context: technology, privacy and the integrity of social life*, Standford University Press, Standford 2010.

Nowak W., *Specyfika zagrożeń w cyberprzestrzeni*, [w:] C. *Banasiński, M.* Rojszczak (red.), *Cyberbezpieczeństwo*, Wolters Kluwer, Warszawa 2020.

Rezolucja Parlamentu Europejskiego z dnia 12 lutego 2019 r. w sprawie kompleksowej europejskiej polityki przemysłowej w dziedzinie sztucznej inteligencji i robotyki (2018/2088(INI)), https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_PL.html (dostęp: 8.08.2021).

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Wolters Kluwer, Warszawa 2019.

Warren S.D., Brandeis L.D., *The right to Privacy, „Harward Law Review" 1890, nr 4.*

Żołyński J., *RODO. Prawo do zapomnienia w sferze zatrudnienia, Wolter Kluwers, Warszawa 2018.*

Źródła prawa

Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania, Komisja Europejska, Bruksela, 19 lutego 2020 r. *COM(2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pl.pdf (dostęp: 8.08.2021).*

Chart of signatures and ratifications of Treaty 108, Council of Europe 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (dostęp: 2.05.2021).

Chart of signatures and ratifictions of Treaty 223, Council od Europe 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (dostęp: 3.05.2021).

Karta Praw Podstawowych Unii Europejskiej z 30 marca 2010 r. (Dz.Urz. *UE C 202 z 7 czerwca 2016 r.,* s. 389).

Uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020" (M.P. *2020, poz.* 23).

Orzecznictwo

Wyrok ETPC z dnia 17 lipca 2003 r. w sprawie Perry v. *Wielka Brytania, 63737/00, § 36.*

Wyrok ETPC z dnia 6 czerwca 2006 r. w sprawie Segerstedt-Wiberg i in. *v.* Szwecja, 62332/00.

Wyrok ETPC z dnia 3 kwietnia 2007 r. w sprawie Copland v. *Wielka Brytania, 62617/00.*

Wyrok ETPC z dnia 4 grudnia 2008 r. w sprawie S. *i Marper v.* Wielka Brytania, 30562/04 i 30566/04.

Wyrok ETPC z dnia 2 września 2010 r. w sprawie Uzun v. *Niemcy, 35623, § 43.*

Wyrok ETPC z dnia 7 lutego 2012 r. w sprawie von Hannover v. *Niemcy, 40660/08, § 95.*