OCHRONA PRYWATNOŚCI W CYBERPRZESTRZENI

z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji

Marcin Rojszczak

Wolters Kluwer

OCHRONA PRYWATNOŚCI W CYBERPRZESTRZENI

z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji

Marcin Rojszczak

Wolters Kluwer

WARSZAWA 2019

SERIA **MONOGRAFIE**

Stan prawny na 1 marca 2019 r.

Recenzent
Dr hab. Mariusz Jagielski

Wydawca
Monika Pawłowska

Redaktor prowadzący
Adam Choiński

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

Łamanie
Wolters Kluwer Polska

ISBN 978-83-8160-472-7
ISSN 1897-4392

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

„Starożytność była cywilizacją spektaklu:
Udostępnić wielkiej masie ludzi oglądanie niewielkiej liczby przedmiotów
– to zadanie rozwiązywała architektura świątyń, teatrów i cyrków.
W widowisku kulminowało życie publiczne, intensywność świąt,
zmysłowa bliskość.
Epoka nowoczesna odwraca problem:
Dostarczyć niewielu osobom, a nawet jednemu człowiekowi,
natychmiastowy wgląd w wielką masę ludzi.
W społeczeństwie, którego konstytutywnych elementów nie stanowi
już wspólnota ani życie na forum, ale prywatne jednostki z jednej,
a państwo z drugiej strony, relacje może regulować jedynie forma
będąca dokładną odwrotnością widowiska:
Przeto współczesności, stale rosnącemu wpływowi państwa,
jego z każdym dniem pogłębiającej się ingerencji we wszystkie szczegóły
i wszystkie relacje życia społecznego, przypadło w udziale,
aby poszerzać i ulepszać jej oddziaływanie, a to przez wykorzystywanie
i wdrażanie do tego wielkiego celu budowy i dystrybucji gmachów
służących równoczesnemu nadzorowaniu wielkiej masy ludzi".

Michel Foucault

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa 2002/21	–	dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z 7.03.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.Urz. WE L 108, s. 33)
dyrektywa 2002/58	–	dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. WE L 201, s. 37)
dyrektywa 2016/680	–	dyrektywa 2016/680 Parlamentu Europejskiego i Rady (UE) z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)
EKPC (lub europejska Konwencja)	–	Konwencja o ochronie praw człowieka i podstawowych wolności (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2018 r. poz. 1025 ze zm.)
k.k.	–	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2018 r. poz. 1600 ze zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)

konwencja 108	–	Konwencja nr 108 Rady Europy sporządzona w Strasburgu 28.01.1981 r.o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25 z uzup.)
k.p.c.	–	ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2018 r. poz. 1360 ze zm.)
k.p.k.	–	ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2018 r. poz. 1987 ze zm.)
KPP (lub Karta)	–	Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389)
MPPOiP	–	Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku 19.12.1966 r.(Dz.U. z 1977 r. Nr 38, poz. 167)
PDPC	–	Powszechna Deklaracja Praw Człowieka
pr. adw.	–	ustawa z 26.05.1982 r. – Prawo o adwokaturze (Dz.U. z 2018 r. poz. 1184 ze zm.)
pr. tel.	–	ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2018 r. poz. 1954 ze zm.)
RODO (lub ogólne rozporządzenie)	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE z 2016 r. C 202, s. 47)
TUE	–	Traktat o Unii Europejskiej (Dz.Urz. UE z 2016 r. C 202, s. 13)
TWE	–	Traktat ustanawiający Wspólnotę Europejską
u.o.d.o.2018	–	ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.)
u.o.d.o.1997	–	ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.; uchylona z dniem 6.02.2019 r.)
u.p.p.RPP	–	ustawa z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2017 r. poz. 1318 ze zm.)
u.s.i.o.z.	–	ustawa z 28.04.2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2019 r. poz. 408 ze zm.)
ustawa antyterrorystyczna	–	ustawa z 10.06.2016 r. o działaniach antyterrorystycznych (Dz.U. z 2018 r. poz. 452 ze zm.)

u.ś.u.d.e.	–	ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2019 r. poz. 123 ze zm.)

Czasopisma, publikatory, zbiory orzecznictwa

BPK	–	Biuletyn Prawa Karnego
BVerfGE	–	Entscheidungen des Bundesverfassungsgerichts (zbiór urzędowy orzeczeń niemieckiego Sądu Konstytucyjnego)
Dz.U.	–	Dziennik Ustaw
Dz.Urz. UE/WE	–	Dziennik Urzędowy Unii Europejskiej/Wspólnot Europejskich
EPS	–	Europejski Przegląd Sądowy
IKAR	–	internetowy Kwartalnik Antymonopolowy i Regulacyjny
MoP	–	Monitor Prawniczy
ONSA	–	Orzecznictwo Naczelnego Sądu Administracyjnego
OSNC	–	Orzecznictwo Sądu Najwyższego. Izba Cywilna
OSNKW	–	Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSNP	–	Orzecznictwo Sądu Najwyższego. Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych
OTK	–	Orzecznictwo Trybunału Konstytucyjnego
OTK-A	–	Orzecznictwo Trybunału Konstytucyjnego, Seria A
PiP	–	Państwo i Prawo
PME	–	Prawo Mediów Elektronicznych
POSAG	–	Przegląd Orzecznictwa Sądu Apelacyjnego w Gdańsku
PPKonst	–	Przegląd Prawa Konstytucyjnego
Prz.Sejm.	–	Przegląd Sejmowy
RPEiS	–	Ruch Prawniczy, Ekonomiczny i Socjologiczny

Inne

ABW	–	Agencja Bezpieczeństwa Wewnętrznego
AW	–	Agencja Wywiadu
CBA	–	Centralne Biuro Antykorupcyjne
CNIL	–	Commission nationale de l'informatique et des libertés
EIOD	–	Europejski Inspektor Ochrony Danych

EOG	–	Europejski Obszar Gospodarczy
ETPC	–	Europejski Trybunał Praw Człowieka
EWG	–	Europejska Wspólnota Gospodarcza
FTK	–	Federalny Trybunał Konstytucyjny RFN
GCHQ	–	Centrala Łączności Rządowej (Government Communications Headquarters) – agencja wywiadowcza Wielkiej Brytanii
GIODO	–	Generalny Inspektor Ochrony Danych Osobowych
ICANN	–	Internet Corporation for Assigned Names and Numbers
KE	–	Komisja Europejska
KPC	–	Komitet Praw Człowieka
MC	–	Minister Cyfryzacji
MSOP	–	Międzynarodowe Standardy Ochrony Prywatności
MSWiA	–	Minister Spraw Wewnętrznych i Administracji
NSA	–	Naczelny Sąd Administracyjny; również, w zależności od kontekstu (głównie w rozdziale 8), Agencja Bezpieczeństwa Wewnętrznego (National Security Agency) – agencja wywiadowcza Stanów Zjednoczonych
PE	–	Parlament Europejski
PNR	–	dane dotyczące pasażera (ang. *passenger name record*)
RE	–	Rada Europy
RPO	–	Rzecznik Praw Obywatelskich
SA	–	Sąd Apelacyjny
SKW	–	Służba Kontrwywiadu Wewnętrznego
SN	–	Sąd Najwyższy
TK	–	Trybunał Konstytucyjny
TSUE	–	Trybunał Sprawiedliwości Unii Europejskiej
UKE	–	Urząd Komunikacji Elektronicznej
UODO	–	Urząd Ochrony Danych Osobowych
WSA	–	Wojewódzki Sąd Administracyjny

PRZEDMOWA

Po niemal trzydziestu latach transformacji Polska w wielu obszarach zrównała się z rozwojem cywilizacyjnym państw Europy Zachodniej. W ten sposób marzenie poprzednich pokoleń o możliwości wychowywania swoich dzieci w kraju wolnym i demokratycznym stało się rzeczywistością. Miarą tego sukcesu jest akcesja do Unii Europejskiej oraz możliwość partnerskiego uczestnictwa w projekcie wspólnego społeczeństwa europejskiego, dla którego wolność i godność jednostki stanowi fundament, na bazie którego budowana jest wspólna przyszłość.

Prywatność jest emanacją wolności. Jednostka pozbawiona prywatności nie może być wolna. Przytoczony jako motto fragment dzieła M. Foucaulta[1] wskazuje na uniwersalny charakter tej myśli. J. Bentham, tworząc w XVIII w. koncepcję więzienia idealnego – Panoptykonu – nie mógł przewidzieć, że ponad sto pięćdziesiąt lat później jego wizja zostanie przedstawiona jako ogólna koncepcja kontroli społecznej, a jeszcze później – u progu XXI stulecia – stanie się trafnym opisem możliwości nadzoru realizowanego wobec całych społeczeństw w cyberprzestrzeni. Osiemnastowieczna koncepcja więzienia opisuje bliski nam model demokracji.

Zaprezentowane w niniejszej pracy poglądy są wyrazem moich przemyśleń i opinii, a także głębokiego przekonania, że każda forma zinstytucjonalizowanego nadzoru i kontroli wypacza ideały, które stanowią podstawę naszego społeczeństwa. Nic w tym zakresie nie straciły na

[1] Cytat za: M. Foucault, *Nadzorować i karać. Narodziny więzienia*, tłum. T. Komendant, Warszawa 1993, s. 260.

aktualności poglądy J. S. Milla, który wskazywał na wolność myśli jako jedną z fundamentalnych swobód człowieka: „żadne społeczeństwo, w którym swobody te nie są, na ogół biorąc, szanowane, nie jest wolne, bez względu na formę jego rządu; i żadne społeczeństwo nie jest całkowicie wolne, jeżeli nie są one w nim uznawane bez żadnych absolutnie zastrzeżeń”[2].

[2] J. S. Mill, *O wolności* [w:] *Utylitaryzm – O wolności*, tłum. A. Kurlandzka, Warszawa 2006, s. 106.

WPROWADZENIE

W uchwalonej w 1948 r. Powszechnej Deklaracji Praw Człowieka po raz pierwszy wyróżniono i nazwano potrzebę prawnej ochrony sfery prywatności jako jedno z podstawowych praw człowieka. Niemal siedemdziesiąt lat później, w 2018 r., w nauce prawa nadal nie wypracowano uniwersalnej i powszechnie akceptowanej definicji prywatności ani standardów jej ochrony. Pomimo przyjęcia licznych deklaracji, rezolucji i wytycznych gremiów międzynarodowych, nie wyłączając tak poważanych, jak Organizacja Narodów Zjednoczonych czy Rada Europy, nadal aktualny jest problem poszanowania prywatności, zarówno w relacjach wertykalnych, jak i horyzontalnych. Problematyka ta zyskuje na znaczeniu wraz z coraz powszechniejszym wykorzystywaniem nowoczesnych środków komunikacji i przetwarzania danych w kolejnych sferach życia. Fenomen cyberprzestrzeni i związany z nią brak terytorialności, pozorna anonimowość i łatwość w dystrybucji informacji skutkują potrzebą ponownej analizy, czy normy prawne ustanowione kilkadziesiąt lat wcześniej są wystarczające i adekwatne do ochrony prywatności w odniesieniu do nowych zagrożeń technologicznych.

Od połowy lat 70. XX w. rośnie ponadto znaczenie legislacji międzynarodowej dotyczącej przetwarzania danych osobowych. Przepisy stanowione w tym obszarze miały przeciwdziałać potencjalnym nadużyciom związanym z przetwarzaniem dużej ilości danych osobowych w systemach informatycznych. Aby cel ten mógł być osiągnięty, funkcja ochronna przepisów została uzupełniona o rozwiązania publicznoprawne i nadanie szeregu nowych praw podmiotom danych, dzięki czemu możliwa była lepsza kontrola nad realizowanymi procesami przetwarzania. O ile w przypadku ochrony prywatności normy międzynarodowe

miały prowadzić do ochrony przed arbitralnością władzy krajowej, o tyle w przypadku ochrony danych osobowych miały zapewnić stosowanie tych samych standardów i reżimów przetwarzania na płaszczyźnie ponadnarodowej. W ten sposób przeniesienie wiążących zobowiązań na grunt prawnomiędzynarodowy miało z jednej strony usunąć bariery w międzynarodowym transferze danych, a z drugiej – stworzyć bezpieczną przestrzeń do przetwarzania danych. Niestety cel ten nie został nigdy w pełni osiągnięty. Po części stało się tak z uwagi na odmienne rozumienie i definiowanie prywatności – różne w poszczególnych kręgach kulturowych. Ponadto, nawet jeśli uznawano prywatność za uniwersalną potrzebę człowieka, pojawiała się trudność w zdefiniowaniu granic potrzebnej ochrony, a w konsekwencji i sytuacji uzasadniających możliwą ingerencję. Odmienne spojrzenie na znaczenie prawa do prywatności skutkowało wprowadzaniem przepisów różnej rangi w poszczególnych systemach prawnych. Klasycznym przykładem może być odmienne spojrzenie na prywatność w amerykańskiej i europejskiej nauce prawa. W efekcie skoro w gronie państw demokratycznych, zbudowanych w oparciu o te same wartości i podstawy ustrojowe, nie sposób było osiągnąć zgodności co do rozpoznania prawa do prywatności jako jednego z podstawowych praw człowieka, jest oczywiste, że różnice te tylko narastały w odniesieniu do państw niedemokratycznych.

Upowszechnienie Internetu oraz dynamiczny rozwój technik przetwarzania informacji, w tym pojawienie się zupełnie nowych modeli przetwarzania, takich jak chmura obliczeniowa czy analizy *Big Data*, zwiększyło potrzebę wprowadzenia skutecznych mechanizmów ochrony praw w cyberprzestrzeni. Możliwość gromadzenia i przetwarzania dużych zbiorów danych, pozyskanych z wielu rozproszonych baz danych i ich swobodne, globalne przetwarzanie doprowadziło do powstania rynku brokerów danych – przedsiębiorców posiadających bazy danych na temat setek milionów osób, w których uwzględniono informacje na temat ich stanu zdrowia, indywidualnych preferencji, sytuacji finansowej czy przynależności do określonych mniejszości. Profilowanie – a więc budowanie opisu jednostki w oparciu o informacje pozyskiwane z wielu elektronicznych baz danych – stało się skuteczną techniką marketingu produktów i usług, ale również badania i przewidywania zachowań ludzi albo całych społeczności, a w wariancie bardziej rozbudowanym

– skutecznym narzędziem inwigilacji. W ten sposób już dzisiaj możliwe jest określenie, jaka część uczestników festiwalu muzycznego Open'er to kobiety starające się o dziecko, a jaka – przedstawiciele mniejszości seksualnych[1]. Z kolei amerykańska sieć handlowa Target może określać zaawansowanie ciąży swoich klientek, a także precyzyjnie przewidywać planowany termin porodu – i w ten sposób odpowiednio dobierać promowane produkty[2]. Wszystko to w oparciu o dane pozyskane dzięki nowoczesnym środkom przetwarzania danych, bez pytania osób zainteresowanych o konkretne fakty i zdarzenia z ich życia. W efekcie normy prawne i możliwości techniczne coraz częściej postrzegane są w kategoriach dychotomii, pozostawiając jednocześnie nierozstrzygniętymi formułowane wątpliwości etyczne i moralne. Jest to błędna diagnoza, pomijająca znaczenie nowoczesnych form przetwarzania informacji dla dalszej ewolucji w kierunku społeczeństwa opartego na wiedzy. Europejski Inspektor Ochrony Danych zauważył, że „nigdy wcześniej podstawowe prawa do prywatności i ochrony danych osobowych nie były tak istotne dla ochrony godności człowieka. Dają one człowiekowi możliwość rozwijania własnej osobowości, prowadzenia niezależnego życia, wykazywania się innowacyjnością oraz korzystania z innych praw i wolności. Technologia nie powinna narzucać wartości i praw, jednak relacji tej nie należy również sprowadzać do błędnej dychotomii. Z rewolucją cyfrową wiążą się obietnice korzyści w takich obszarach jak zdrowie, środowisko, międzynarodowy rozwój i efektywność ekonomiczna"[3].

Te same technologie, które prywatni przedsiębiorcy wykorzystują do swoich działań komercyjnych, władze państwowe starają się wykorzystywać w obszarze szeroko pojętego bezpieczeństwa narodowego. Analityka predykcyjna – termin określający możliwość typowania zdarzeń w oparciu o zaawansowane algorytmy i duże, wieloaspektowe zbiory danych – jest już dzisiaj wykorzystywana do wskazywania osób podejrzanych

[1] Szczegółowa analiza przypadku, wraz ze wskazaniem zastosowanych technologii oraz implikacji z punktu widzenia ochrony prywatności – zob. podrozdział 7.1. (s. 383).

[2] N. Richards, *The Dangers of Surveillance*, „Harvard Law Review" 2013/126, s. 1939–1940.

[3] Europejski Inspektor Ochrony Danych, *W kierunku nowej etyki cyfrowej: dane, godność i technologia*, Opinia 4/2015 z 11.09.2015 r., https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_pl.pdf, s. 4.

o najpoważniejsze przestępstwa. Ponieważ termin „najpoważniejsze przestępstwa" jest chętnie używany w deklaracjach i oświadczeniach politycznych, ale nie został zdefiniowany na gruncie norm prawnych w sposób powszechnie akceptowany, to w sposób oczywisty pojawia się poważne ryzyko nadużycia władzy. Ta sama technologia może zostać wykorzystana do gromadzenia informacji na temat przeciwników politycznych czy stworzenia stałego systemu nadzoru nad społeczeństwem. Stale rozbudowywane programy masowej inwigilacji, bazujące na gromadzeniu hurtowych i nieukierunkowanych informacji na temat wszystkich użytkowników sieci łączności elektronicznej każą ponownie zadać pytanie o skuteczność istniejących prawnych mechanizmów ochrony prywatności – krajowych, regionalnych oraz międzynarodowych. Problem ten został dostrzeżony także przez Parlament Europejski, który w odniesieniu do istniejących mechanizmów ochrony prywatności stwierdził, że „traktaty międzynarodowe oraz prawodawstwo UE i Stanów Zjednoczonych, a także krajowe mechanizmy nadzoru, nie zdołały zagwarantować niezbędnych kontroli i równowagi ani demokratycznej rozliczalności"[4].

W polskiej literaturze brakuje kompleksowego opracowania dotyczącego problematyki ochrony prywatności w cyberprzestrzeni. Dominują ujęcia ukierunkowane na przedstawienie prywatności jako elementu prawa międzynarodowego[5] lub systemów ochrony praw człowieka[6]. W ostatnich latach na skutek większego zainteresowania negatywnymi zjawiskami mającymi miejsce w cyberprzestrzeni publikowane są opracowania dotyczące cyberprzestępczości[7] oraz cyberbezpieczeństwa –

[4] Rezolucja Parlamentu Europejskiego z 12.03.2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI), P7_TA(2014)0230, pkt 9.

[5] A. Czubik, *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Kraków 2013.

[6] *Prawo prywatności jako reguła społeczeństwa informacyjnego*, red. K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak, Warszawa 2017.

[7] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013.

rozumianego głównie w wymiarze zapewnienia ochrony infrastruktury systemów i sieci przed atakami[8].

W krajowym prawodawstwie, z racji funkcjonowania Polski zarówno w systemie europejskiej konwencji, jak i członkostwa w Radzie Europy oraz Unii Europejskiej, funkcjonują trwałe i wielostopniowe mechanizmy prawnej ochrony prywatności. Powstaje jednak pytanie: na ile są to rozwiązania skuteczne i adekwatne do rodzajów ryzyka obecnych w cyberprzestrzeni? Czy brak granic, swoboda dostępu i wymiany informacji – różniąca cyberprzestrzeń od przestrzeni fizycznej – nie tworzy z praw i gwarancji wynikających z praw o krajowym lub regionalnym zakresie stosowania norm tworzących zaledwie pozory ochrony prywatności?

Oddzielnym zagadnieniem jest ocena rozwiązań prawnomiędzynarodowych wprowadzanych przez organizacje o zasięgu regionalnym, takie jak Unia Europejska czy Rada Europy. Przyczyną opracowania przez UE własnych regulacji związanych z ochroną prywatności oraz danych osobowych było przekonanie, że w przeciwnym przypadku nie powiedzie się projekt związany z budową nowoczesnego społeczeństwa opartego na informacji. Tylko zniesienie barier w swobodnej wymianie informacji może przyczynić się do nieskrępowanego rozwoju nowoczesnych usług świadczonych w sieciach takich, jak Internet. O ile więc projekt budowy europejskiego modelu ochrony danych można z dzisiejszego punktu widzenia ocenić jako udany, to w szerszej perspektywie jego sukces unaocznił ryzyka i niedoskonałości wynikające z braku wspólnych, ponadregionalnych regulacji związanych z badaną problematyką. Internet nie ma granic, w przeciwieństwie do prawodawstwa, w tym także stanowionego przez organizację ponadnarodową, taką jak UE. Problem ten trafnie podsumowała Grupa Robocza Art. 29, wskazując, że „zgodnie z prawem UE, prawo do ochrony danych osobowych to prawo podstawowe, podlegające ochronie na mocy art. 8 Karty Praw Podstawowych UE. W innych częściach świata potrzeba ochrony danych jest uznawana, niekoniecznie jednak ma status prawa podstawowego. UE i jej państwa członkowskie winny zagwarantować to podstawowe

[8] *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014.

prawo każdej osobie objętej ich jurysdykcją. W zglobalizowanym świecie oznacza to, że obywatele mogą również żądać ochrony, jeśli ich dane są przetwarzane poza terytorium UE”[9].

Pogląd o niepełnej skuteczności istniejących regulacji prawnych mających na celu ochronę przed zagrożeniami dla prywatności wynikającymi z nowoczesnych technik przetwarzania danych nie powinien prowadzić do mylnego przekonania, że głównym zagrożeniem dla ochrony prywatności jest postęp techniki. Jeżeli bowiem uznać taką hipotezę za prawdziwą, to w konsekwencji celem wprowadzanych norm prawnych powinno być przeciwdziałanie temu zjawisku, a więc *de facto* próba powstrzymania lub znacznego ograniczenia upowszechnienia się nowoczesnych technik przetwarzania informacji. Jest to podejście błędne, wynikające zapewne z pozanaukowego przekonania, że technologia może mieć cechy przypisywane działaniom ludzi. W rzeczywistości technika jest narzędziem o konkretnych możliwościach i funkcjach, bardziej lub mniej doskonałych – ale cały czas nie stanowi samodzielnego bytu w przestrzeni społecznej. To ludzie kształtują sposób, w jaki nowoczesna technika jest wykorzystywana. Sposobem ograniczania lub kontrolowania jej zastosowań jest między innymi wprowadzanie skutecznych norm prawnych. Celem prawodawcy nie powinno być hamowanie postępu techniki poprzez wprowadzanie archaicznych, niedopasowanych przepisów, ale kształtowanie go we właściwy sposób, zgodny z wartościami stojącymi u podstaw funkcjonowania współczesnych społeczeństw. Wprowadzanie tego typu regulacji – i to nie czekając na pojawienie się negatywnych skutków związanych z ich brakiem – jest zadaniem trudnym, zwłaszcza że obszary zastosowania niektórych technologii (np. *Big Data* czy IoT[10]) nie są jeszcze gruntownie rozpoznane. Nie zmienia to jednak faktu, że – jak zauważyła KE – tylko synergia pomiędzy normami prawnymi oraz rozwiązaniami technologicznymi

[9] Grupa Robocza Art. 29 i Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości, *Przyszłość prywatności. Wspólny wkład do Konsultacji Komisji Europejskiej w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych*, WP 168, pkt 22–23.

[10] Internet rzeczy (ang. *Internet of Things*).

może zaowocować pomyślną transformacją w kierunku społeczeństwa opartego na wiedzy i informacji[11].

Zakreślony powyżej problem badawczy jest złożony i wieloaspektowy. Jego badanie wykracza poza przestrzeń nauki prawa, nie może bowiem pomijać aspektów technicznych związanych z funkcjonowaniem cyberprzestrzeni i zagrożeń w niej występujących. Rozważania dotyczące skuteczności norm prawnych bez odniesienia i omówienia technologii, które normy te mają regulować, są obarczone ryzykiem, że przedstawione wnioski będą niepełne i wybiórcze. W efekcie duża część rozważań przedstawionych w niniejszej pracy służy omówieniu i wyjaśnieniu, dlaczego istniejące lub proponowane przepisy prawne są i będą nieskuteczne w odniesieniu do technologii, którą mają regulować. Rozstrzygając tę kwestię, podjęto także próbę wskazania warunków brzegowych, jakie powinny zostać spełnione i uwzględnione, aby będąca efektem prac umowa międzynarodowa prowadziła do skutecznej ochrony prywatności w cyberprzestrzeni.

Rozważając problem niedopasowania norm prawnych do zastosowań technicznych, które mają one regulować, wyróżnić może kilka problemów szczegółowych, wymagających odrębnej analizy:

- czy obecne normy prawnomiędzynarodowe – wynikające z systemów ochrony praw człowieka, ustanawiające przepisy ochronne w zakresie prawa do prywatności oraz ochrony danych osobowych – są wystarczające do regulowania zdarzeń oddziałujących na prywatność, a mających miejsce w cyberprzestrzeni?
- czy prawo unijne ma potencjał, by doprowadzić do standaryzacji w zakresie ochrony prywatności, a w efekcie do stworzenia bezpiecznej przestrzeni przetwarzania danych, wykraczającej poza granice państw członkowskich UE?
- czy niedoskonałości prawa ponadnarodowego mogą być uzupełnione na płaszczyźnie prawa krajowego; w szerszym ujęciu – jaka jest rola prawodawcy krajowego w badanym obszarze i czy w ogó-

[11] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia jednolitego rynku cyfrowego dla Europy*, COM (2015) 192 final, s. 10.

le krajowe normy ochronne mają praktyczne znaczenie z punktu widzenia sposobu funkcjonowania sieci Internet?
– wreszcie – czy jeśli wziąć pod uwagę techniczne aspekty związane z nowymi technikami przetwarzania informacji, klasyczne rozumienie „prywatności" jako wolności człowieka od ingerencji (zainteresowania) ze strony świata zewnętrznego jest nadal aktualne? W jaki sposób rozwiązać oczywiste niedopasowanie Internetu bez granic oraz terytorialności cechującej stanowione normy prawne?

Istotnym elementem pracy jest także analiza orzecznictwa, w tym międzynarodowych organów sądowych i kontrolnych. Z uwagi na znaczenie norm prawnomiędzynarodowych dla badanej problematyki szczególną uwagę poświęcono analizie orzecznictwa Europejskiego Trybunału Praw Człowieka oraz Trybunału Sprawiedliwości Unii Europejskiej. W pracy wykorzystano też informacje udostępnione przez krajowe organy władzy publicznej na podstawie przepisów ustawy o dostępie do informacji publicznej[12].

Próba odpowiedzi na pytanie o przyczyny nieskuteczności istniejących regulacji prawnych wymaga w pierwszej kolejności wprowadzenia i wyjaśnienia podstawowych pojęć i terminów – takich jak „prywatność" i związane z nią „prawo do prywatności", a także „cyberprzestrzeń" oraz wzajemna relacja pomiędzy ochroną danych osobowych a ochroną prywatności. Zagadnienia te zostały przedstawione w rozdziale 1. Szczególną uwagę zwrócono na wyjaśnienie uniwersalnej roli prywatności jako potrzeby warunkującej prawidłowy rozwój osobowości człowieka. Jest to kwestia o fundamentalnym znaczeniu, nadal bowiem – również w dyskursie prawniczym – spotyka się opinie sugerujące, że prywatność stanowi wytwór współczesnej cywilizacji państw wysoko rozwiniętych, a w efekcie próba przeniesienia mechanizmów jej prawnej ochrony na płaszczyznę ponadnarodową musi się spotkać z zarzutem narzucania innym własnych wartości.

[12] Ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2018 r. poz. 1330 ze zm.).

W rozdziale 2 przedstawiono analizę i omówienie najważniejszych systemów ochrony praw człowieka funkcjonujących w polskim porządku prawnym i wprowadzających normy ochronne związane z prawem do prywatności. Pokazano ewolucję postrzegania prywatności na gruncie prawodawstw różnych organizacji międzynarodowych (w szczególności Organizacji Narodów Zjednoczonych, Rady Europy i Unii Europejskiej). Rozważania dotyczące prawa materialnego uzupełniono analizą skuteczności środków ochrony prawnej – w szczególności powołanych organów kontrolnych i sądowych, a także znaczenia wydawanych przez nie rozstrzygnięć dla sytuacji prawnej jednostek na gruncie przepisów krajowych. W rozdziale tym przedstawiono również analizę najważniejszych norm konstytucyjnych mających wpływ na badaną problematykę, wraz z ich porównaniem ze standardami ochrony wynikającymi z traktatów międzynarodowych.

Rozdział 3 poświęcono przedstawieniu najważniejszych aktów prawnomiędzynarodowych, w większości o charakterze niewiążącym, wprowadzających wytyczne dotyczące ochrony danych osobowych. Regulacje te miały znaczący wpływ na ukształtowanie norm prawa krajowego wielu państw, ale również norm ponadnarodowych – takich jak prawo UE. Chociaż cechują się one o wiele bardziej szczegółowym i technicznym charakterem – zwłaszcza w porównaniu z ogólną treścią norm wynikających z systemów ochrony praw człowieka – to *de facto* w dużej części wpłynęły na ukształtowanie dzisiejszego europejskiego modelu ochrony danych.

W kolejnym, czwartym rozdziale przedstawiono najważniejsze akty prawne oraz obszary regulacji związane z prawem UE. Prawodawstwo unijne jest powszechnie uznawane za modelowe w zakresie podnoszenia standardów ochrony prywatności w cyberprzestrzeni. Jest też często przytaczane w literaturze przedmiotu jako przeciwieństwo podejścia funkcjonującego w systemie prawnym Stanów Zjednoczonych. Reforma unijnych przepisów o ochronie danych to doskonały moment nie tylko na ocenę, na ile wprowadzane oraz dyskutowane regulacje mogą stanowić kompleksowe rozwiązanie problemu ochrony prywatności w cyberprzestrzeni, ale również – na ile proponowany przez prawodawcę unijnego sposób budowania bezpiecznej przestrzeni przetwarzania

informacji w relacjach z państwami trzecimi (nienależącymi do UE/EOG) jest realny i możliwy do zastosowania.

W rozdziale 5 omówiono przepisy krajowe oraz rolę krajowego prawodawcy w obszarze ochrony prywatności w cyberprzestrzeni. Uwzględniając funkcjonowanie Polski w kilku systemach praw człowieka (MPPOiP, EKPC, KPP) oraz pamiętając o istotnej roli przepisów stanowionych przez UE w zakresie ochrony prywatności, interesujące było zbadanie, czy i w jakim zakresie krajowy prawodawca dysponuje przestrzenią do stanowienia dodatkowych regulacji kształtujących prawne granice prywatności. W ten sposób poza wskazaniem wniosków *de lege lata* i *de lega ferenda* przeprowadzono także ocenę istniejących rozwiązań prawnomiędzynarodowych, w szczególności ocenę ich skuteczności w przypadku, gdy władze publiczne nie realizują odpowiednio swoich pozytywnych lub negatywnych obowiązków wynikających z treści traktatów.

W kolejnych trzech rozdziałach omówiono wybrane zagadnienia dotyczące najważniejszych, zdaniem autora, problemów związanych z ochroną prywatności w cyberprzestrzeni. Każde z przedstawionych zagadnień nie tylko może posłużyć do zobrazowania różnych słabości istniejących modeli ochrony prywatności, ale także prowadzi do konieczności rozważenia, czy w ogóle przyjęte założenia doktrynalne leżące u podstaw prawnej ochrony prywatności i danych osobowych są prawidłowe i aktualne. W rozdziale 6 omówiono przetwarzanie informacji w modelu chmury obliczeniowej, w rozdziale 7 przeprowadzono analizę dużych zbiorów danych (*Big Data*), a w rozdziale 8 rozważono obecne możliwości władzy publicznej związane z prowadzeniem masowych programów inwigilacji. Wszystkie rozdziały części drugiej przygotowano w podobny sposób, w szczególności określono w nich podstawową terminologię, wyjaśniono technologie i zastosowania będące przedmiotem badania, a także dokonano analizy prawnej wraz z odwołaniem się w podsumowaniu i wnioskach do wpływu danej technologii na płaszczyznę ochrony prywatności użytkowników w cyberprzestrzeni. Jednocześnie w każdym z rozdziałów części drugiej przedstawiono analizowany problem z innej perspektywy, dając możliwość zrozumienia wieloaspektowości badanej problematyki.

Monografię kończy podsumowanie, w którym zebrano wnioski cząstkowe, na podstawie których określono, czy i w jaki sposób normy prawnomiędzynarodowe powinny tworzyć ramy ochronne i regulacyjne w zakresie prawa do prywatności w cyberprzestrzeni.

Część I

OCHRONA PRYWATNOŚCI: HISTORIA, TERAŹNIEJSZOŚĆ I PRZYSZŁOŚĆ

Rozdział 1

PRYWATNOŚĆ I CYBERPRZESTRZEŃ – ZAGADNIENIA PODSTAWOWE

1.1. Psychologiczne i socjologiczne rozumienie prywatności

Prywatność stosunkowo niedawno, bo w drugiej połowie XX w., stała się odrębnym przedmiotem badań nauk psychologicznych i socjologicznych. Wcześniej wiązano ją z innymi, lepiej poznanymi pojęciami – takimi, jak afiliacja, terytorializm, samotność czy izolacja[1]. W rezultacie prywatność, chociaż będąca terminem powszechnie używanym dla różnych form opisu relacji między jednostką a otaczającą ją społecznością, na gruncie badań naukowych do dzisiaj pozostaje zjawiskiem stosunkowo słabo poznanym. Dlatego przed rozpoczęciem rozważań na temat celu i zakresu prawnej ochrony prywatności, a także odniesienia środków prawnych do nowej płaszczyzny budowania relacji społecznych, jaką stanowi cyberprzestrzeń, konieczne jest odpowiednie przedstawienie poglądów nauki na sam fenomen prywatności, w szczególności w odniesieniu do prawidłowego rozwoju osobowości i wpływu na kształtowanie społeczeństwa.

Podstawowe pytanie, jakie należy w tym miejscu sformułować, dotyczy charakteru prywatności. Czy jest to potrzeba człowieka charakterystycz-

[1] K. Jędruszczak, *Prywatność jako potrzeba w ramach koncepcji siebie*, „Roczniki Psychologiczne" 2005/2, s. 112.

na dla wszystkich ludzi w sposób niezależny od wpływu środowiska i kręgu kulturowego? Czy raczej należy ją uznać za cechę osobowości, której nasilenie, objawiające się potrzebą różnych form izolacji, wyraża potrzebę określonej jednostki, ale nie jest wspólne dla ogółu ludzi? Odpowiedzi na te pytania, chociaż wykraczające poza sferę nauk prawnych, mają fundamentalne znaczenie dla określenia konieczności i celowości wprowadzania norm prawnych chroniących ten aspekt życia. Także wskazanie istnienia oraz stopnia zależności występowania potrzeby prywatności (jeżeli uznać prywatność za potrzebę)[2] od określonego kręgu kulturowego jest istotne dla rozważań związanych z uwzględnieniem jej ochrony w katalogu podstawowych praw człowieka. Jeżeli bowiem prywatność nie byłaby podobnie traktowana i interpretowana w różnych grupach społecznych czy kręgach kulturowych, wprowadzenie uniwersalnych rozwiązań prawnych służących jej ochronie mogłoby spotkać się z uzasadnionym zarzutem próby narzucania innym własnych wartości i wizji funkcjonowania społeczeństwa.

Jak wskazuje się w literaturze przedmiotu, w XX w. nastąpiła dynamiczna ekspansja fenomenu prywatności[3]. W efekcie tego sytuacje,

[2] Por. np. rozważania K. Jędruszczak na temat statusu prywatności (*Prywatność...*, s. 116).

[3] Kwestia rozumienia granic prywatności w różnych dziedzinach nauki oraz języku potocznym jest przedmiotem intensywnych badań. Interesujące wyniki w tym zakresie przedstawiła D. Kasper, która przeprowadziła analizę informacji publikowanych w amerykańskiej prasie na przestrzeni czternastu lat (1990–2003). Kwerenda dotyczyła tekstów, w których tytule lub akapicie wprowadzającym wymieniony został termin „naruszenie prywatności" (ang. *invasion of privacy*). W ten sposób wybrano ponad 3700 artykułów prasowych. Zakresem badań było objęte przeanalizowanie częstotliwości publikowanych wiadomości z podziałem na typ ingerencji (w tym celu D. Kasper wprowadziła podział na trzy kategorie: pozyskanie informacji, obserwacja lub wkroczenie) oraz określenie strony, która jest sprawcą oraz ofiarą naruszenia prywatności. Celem badań było ustalenie, czy w badanym okresie nastąpiła ewolucja rozumienia terminu „naruszenie prywatności" oraz opisanie zakresu tej zmiany. W ten sposób autorka ustaliła, że niezmiennie najczęściej występującą formą naruszenia jest pozyskanie informacji (średnio 60% badanych przypadków), na drugim miejscu znajduje się wkroczenie (średnio 21%), a najmniej przypadków dotyczyło obserwacji (18%). Badaczka zaprezentowała także szereg wniosków szczegółowych związanych z poszczególnymi typami naruszeń oraz analizą stron naruszających prywatność. Badanie zasługuje na uwagę z powodu wyboru nietypowej metody badawczej (analiza prasy), pozwalającej na prześledzenie trendów w dużej populacji (Stany Zjednoczone), a nie tylko w odniesieniu do ankietowanej,

które kilkadziesiąt lat wcześniej nie były interpretowane jako należące do sfery życia prywatnego, dzisiaj są już tak traktowane. Obserwowane jest jednak także zjawisko przeciwne – polegające na akceptowaniu ujawniania i wprowadzania do sfery publicznej informacji, które historycznie uznawane były za dotyczące sfery prywatności. Rozumienie prywatności jest zależne od kręgu kulturowego, ale i od wieku badanych osób, ich osobistych preferencji w zakresie nawiązywania relacji społecznych, pozycji zawodowej czy społecznej. Co więcej, ta sama osoba może w tym samym czasie (będąc w tym samym wieku) oceniać tę samą sytuację jako naruszającą jej poczucie prywatności lub nie – w zależności od kontekstu sytuacyjnego. Ciekawe wyniki badań przedstawił w tym zakresie A. Mednis, wskazując, że odpowiedzi ankietowanych dotyczące oceny sytuacji, w której byliby podglądani podczas mycia się, zmieniały się, jeżeli treść pytania została uzupełniona informacją, że osobą obserwującą jest dwuletnie dziecko[4]. Obserwacja ta prowadzi do wniosku, że oczekiwanie prywatności może się zmieniać w zależności od zrozumienia przez jednostkę całego kontekstu sytuacji. Wniosek ten ma szczególne znaczenie w odniesieniu do cyberprzestrzeni – która tworząc pozory anonimowości, ale jednocześnie dostarczając narzędzi nieskrępowanego wyrazu, może wpływać na zmianę granic prywatności jednostki, sprawiając, że te same sytuacje i zdarzenia będą przez nią inaczej interpretowane tylko dlatego, że nie zachodzą w przestrzeni fizycznej. Prywatność jest zatem zjawiskiem wieloaspektowym i złożonym, w badaniu którego istotna jest nie tylko jednostka (jej potrzeby, oczekiwania, światopogląd), ale również jej umiejscowienie w społeczeństwie. Stąd aspekt socjologiczny, obok psychologicznego, jest równie istotny w zrozumieniu prywatności.

stosunkowo niedużej grupy osób. Szczegóły: D. Kasper, *The Evolution (Or Devolution) of Privacy*, „Sociological Forum" 2005/1, s. 69–92.

[4] Tak wyniki i wnioski opisuje A. Mednis: „Aż 80% ankietowanych uznało podglądanie kogoś przy myciu za naruszenie prywatności. Jeśli podglądającym miałoby być dwuletnie dziecko, to tylko 43% uznałoby to za naruszenie, dla 47% nie jest to w tym wypadku ingerencja w prywatność. Poczucie naruszenia prywatności jest więc dla wielu osób silnie powiązane ze zdolnością rozumienia sytuacji przez podglądacza", A. Mednis, *Granice prywatności* [w:] A. Mednis, *Prawo do prywatności a interes publiczny*, Warszawa–Kraków 2006.

Marcin Rojszczak – doktor nauk prawnych; specjalista w zakresie bezpieczeństwa IT oraz ochrony prywatności w Internecie; ma wykształcenie informatyczne oraz prawnicze; od ponad 15 lat realizuje i nadzoruje projekty z obszaru bezpieczeństwa informacji, zarządzania usługami IT oraz ciągłości działania (DRP/BCP) w największych polskich firmach sektorów energetycznego, finansowego i produkcyjnego, a także urzędach administracji centralnej; w latach 2012–2015 członek Rady ds. Certyfikacji Polskiego Komitetu Normalizacyjnego.

W publikacji w przystępny sposób przedstawiono najważniejsze regulacje dotyczące ochrony prywatności i danych osobowych w odniesieniu do nowych form przetwarzania danych, takich jak *cloud computing* czy *big data*. Szczegółowej analizie poddano również zagadnienia prywatności w kontekście bezpieczeństwa publicznego, w tym podstawy prawne prowadzenia programów masowej inwigilacji obywateli.

Autor omawia zarówno istniejące, jak i planowane regulacje międzynarodowe, unijne i krajowe, w tym przyjmowane w związku z trwającą reformą europejskiego modelu ochrony danych.

Książka jest przeznaczona przede wszystkim dla prawników zajmujących się obszarem nowych technologii, inspektorów ochrony danych oraz oficerów bezpieczeństwa IT. Czytelnicy niemający wiedzy technicznej odnajdą w niej ponadto wprowadzenie do najistotniejszych pojęć związanych z nowoczesnymi formami przetwarzania danych.

9788381604727 W01P01

ISSN 1897-4392
ISBN 978-83-8160-472-7
9 788381 604727

CENA 129 ZŁ (W TYM 5% VAT)