STUDIA PRAWA PUBLICZNEGO
2023 • NR 3 (43) ISSN 2300-3936
https://doi.org/10.14746/spp.2023.3.43.6

II. KOMENTARZE, OPINIE, POLEMIKI

Katarzyna Cłapińska*

Prywatność vs. świat wirtualny: ochrona praw jednostki w dobie Internetu

Wprowadzenie

Rozwój zagadnienia prawa do ochrony prywatności w dużej mierze łączy się z rozwojem osiągnięć cywilizacyjnych. Początkowo głównym źródłem naruszeń były gazety, publikujące artykuły bez wiedzy osób, które często nie chciały, aby jakaś informacja została upubliczniona. Jednocześnie pojawiał się inny problem – wolności prasy i prawa do informacji publicznej. Wraz z rozwojem telewizji kwestia ta stała się jeszcze bardziej widoczna. Programy docierały często do większej liczby odbiorców oraz mogły być powtarzane z dużą częstotliwością. Prawdziwą rewolucją okazało się powstanie Internetu oraz dostęp dużej liczby użytkowników z całego globu do międzynarodowej sieci. W styczniu 2023 r. zanotowano rekordową liczbę aktywnych użytkowników Internetu wynoszącą 5,16 miliarda osób, z czego 4,76 miliarda to użytkownicy mediów społecznościowych[1]. Każdego dnia użytkownicy udostępniają ponad 2,5 kwintyliona bitów danych, w tym około 527 760 zdjęć w aplikacji Snapchat, 46 740 zdjęć w aplikacji Instagram i 456 000 postów

* Katarzyna Cłapińska, mgr, Université de Poitiers (Francja), e-mail: katarzynaclapinska@gmail.com, https://orcid.org/0000-0002-7233-3977.

[1] Raport opublikowany na stronie Meltwater – firmy zajmującej się monitorowaniem mediów społecznościowych i przepływem danych osobowych w Internecie, *New report: Time spent online falls to pre-pandemic levels, while social media use increases*, Meltwater, 26 I 2023, https://tinyurl.com/bd7ch9yx (dostęp: 4 V 2023).

SPP 3(43), 2023: 153–165. © The Author(s). Published by: Adam Mickiewicz University Press, 2023.

w aplikacji Twitter[2]. W wyniku rozwoju portali społecznościowych przesunęła się granica potrzeby ochrony prywatności w jej pierwotnym znaczeniu, czyli chęci nieujawniania sfery duchowo-intelektualnej. Dziś częściej i chętniej udostępniane są w Internecie prywatne zdjęcia czy przemyślenia. Współcześnie można zauważyć pojawienie się wielu innych, nowych problemów związanych z przechwytywaniem danych jednostki, które mogą być przetrzymywane przez nieograniczony czas oraz łatwo rozsyłane innym podmiotom. Problematyczne okazały się również inne zagadnienia, takie jak: zbyt długie przechowywanie danych, które utraciły znaczenie (*Google Spain v. Mario Costeja Gonzalez*[3]), przechwytywanie danych przez państwa trzecie (*Big Brother Watch i inni v. Wielkia Brytania*[4]) czy profilowanie informacji przekazywanych odbiorcom na podstawie ich danych (sprawa *Cambridge Analytica*[5]).

Celem artykułu jest wskazanie najważniejszych problemów związanych z ochroną prywatności jednostki w Internecie, a także wskazanie najważniejszych orzeczeń Trybunału Sprawiedliwości Unii Europejskiej oraz Europejskiego Trybunału Praw Człowieka dotyczących prawa do prywatności.

1. Geneza pojęcia prawa do prywatności

Pojęcie *prywatności* wywodzi się z amerykańskiej doktryny prawnej końca XIX w., a za jego twórców uznaje się S.D. Warrena i L.D. Brandeisa, którzy w 1890 r. opublikowali artykuł *The right to privacy* w „Harvard Law Review". Autorzy przeanalizowali orzecznictwo sądów angielskich i amerykańskich, próbując znaleźć odpowiedź na pytanie, czy w aktualnym stanie prawnym istnieje zasada, na którą można się powołać w celu ochrony prywatności, oraz jaki jest jej potencjalny charakter i zakres[6]. Swoje rozważania oparli na zasadzie prawa zwyczajowego. Zgodnie

[2] B. Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, Forbes, 21 V 2018, https://tinyurl.com/bdccef2h (dostęp: 4 V 2023).

[3] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 13 V 2014 r., C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

[4] Wyrok Europejskiego Trybunału Praw Człowieka z 25 V 2021 r., 58170/13 i in., *Big Brother Watch i inni v. Zjednoczone Królestwo*.

[5] Wyrok High Court of Justice w Wielkiej Brytanii z 17 IV 2019 r., [2019] EWHC 954 (Ch) w sprawach: CR-2018-006683, CR-2018-006687, CR-2018-006713, CR-2018-006709, CR-2018-006701, CR-2018-006696; decyzja amerykańskiej federalnej komisji handlu nr 182 3107 z 18 XII 2019 r.

[6] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, nr 4(5), s. 213.

z nim każdy człowiek ma prawo do określenia, w jakim stopniu jego myśli, uczucia i emocje mają być upublicznione. Prywatność powinna więc chronić strefę duchowo-intelektualną człowieka wiążącą się z jego wyglądem, wyrażaniem poglądów, pomysłami czy relacjami. Prawo to nie jest jednak absolutne. Musi być zestawione z prawem do informacji publicznej oraz interesem ogólnym.

Dwa lata przed publikacją artykułu *The right to privacy* sędzia T. McIntyre Cooley użył wyrażenia *The right to be let alone*, mającego podkreślić rozgraniczenie na sferę publiczną i prywatną człowieka, ta ostatnia miała być niedostępna dla innych, wolna od ingerencji osób trzecich. Według założeń sędziego udostępnianie faktów i zdarzeń zależało tylko od woli człowieka. Zadaniem prawa do kontrolowania informacji była ochrona jednostki przed niechcianym rozgłosem[7].

Doktryna prawa europejskiego również wykształciła mechanizmy, które służyły ochronie prywatności. Doktryna niemiecka w XIX w. stworzyła pojęcie *Individualrechte*, na które składało się szereg praw, m.in. prawo do dobrego imienia, nazwiska czy organizacji życia prywatnego bez ingerencji osób trzecich. W doktrynie prawa francuskiego końca XIX w. pojawiły się *droits de la personnalité*, czyli prawa przypisane do osoby, do których zaliczano ochronę człowieka, jego nazwisko czy wizerunek[8].

Dziś prawo do ochrony prywatności jest wymieniane przez większość najważniejszych konwencji praw człowieka, m.in. Konwencję o ochronie praw człowieka i podstawowych wolności[9] (art. 8), Międzynarodowy pakt praw obywatelskich i politycznych, oraz Kartę Praw Podstawowych[10] (art. 7 i art. 8). Prawo to stanowi ważny element prawa unijnego regulowanego przez dyrektywy.

2. Prawo do prywatności a prawo polskie

Na gruncie polskiej Konstytucji[11] prawo do ochrony prywatności znajduje swoje odzwierciedlenie w art. 47. Analizując artykuł, należy zauważyć,

[7] A. Sakowicz, *Prywatność jako samoistne dobro (per se)*, „Państwo i Prawo" 2006, nr 1, s. 17.

[8] Z. Mielnik, *Prawo do prywatności (zagadnienia wybrane)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 58(2), s. 30.

[9] Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 XI 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, dalej „Konwencja" lub „Europejska konwencja praw człowieka".

[10] Karta Praw Podstawowych Unii Europejskiej z dnia 7 XII 2000 r.

[11] Konstytucja Rzeczypospolitej Polskiej z dnia 2 IV 1997 r. (Dz.U. 1997 Nr 78, poz. 483 ze zm.), dalej „Konstytucja".

że konstytucyjnej ochronie podlegają cztery elementy prywatności: życie prywatne, życie rodzinne, cześć i dobre imię. Nie można jednak uznać, że tworzą one katalog zamknięty. Z art. 47 należy wyróżnić dwa rodzaje praw: prawo do prawnej ochrony prywatności oraz prawo do decydowania o swoim życiu osobistym. Pierwsze prawo nakłada na ustawodawcę obowiązek utworzenia norm mających na celu ochronę jednostki, drugie natomiast – obowiązek nieingerencji i „pozostawienia w spokoju jednostki"[12]. Innym proponowanym przez doktrynę podziałem jest wyodrębnienie dwóch sfer – sfery życia politycznego, w której obowiązkiem ustawodawcy jest zapewnienie przepisów ochronnych, i sfery życia społecznego, która ma charakter „wolności" wykluczającej wszelkie nieuzasadnione ingerencje[13].

Normami o charakterze szczegółowym względem art. 47 są art. 49 i art. 51 Konstytucji. Wolność komunikowania się, którą przewiduje art. 49 Konstytucji, obejmuje swoim zakresem ochrony nie tylko obywateli polskich, lecz także cudzoziemców i bezpaństwowców. Norma z jednej strony zobowiązuje ustawodawcę do stworzenia warunków mających na celu zabezpieczenie komunikacji jednostki przed niepożądanym działaniem osób trzecich, w tym przechwytywaniem i agregowaniem danych osobowych, numerów telefonów, adresów stron internetowych czy adresów IP lub IMEI[14]. Z drugiej strony nakłada obowiązek nieingerowania w tę wolność przez ograny władzy publicznej poprzez niepozyskiwanie i nieujawniane treści konwersacji[15]. Podążając za linią orzeczniczą (TK 23/11[16]), należy uznać, że ochroną objęta jest komunikacja zarówno bezpośrednia, jak i ta przeprowadzana na odległość.

Z art. 51 Konstytucji wywodzi się prawo do ochrony danych osobowych, które nakazuje organom władzy publicznej powstrzymanie się od zbierania i udostępniania danych osobowych, czyli danych zawierających indywidualne informacje oraz zbiór cech danej osoby[17]. Prawo to nie ma jednak charakteru nieograniczonego i może być limitowane

---

[12] M. Florczak-Wątor, *Art. 47*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. P. Tulei, Warszawa 2019, s. 167.

[13] P. Sarnecki, *Art. 47*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. L. Garlickiego, M. Zubika, t. 2, wyd. 2, Warszawa 2016, s. 248.

[14] IMEI to indywidualny numer identyfikacyjny telefonu komórkowego. Używany jest on przez sieć GSM w celu identyfikowania telefonów.

[15] M. Florczak-Wątor, *Art. 49*, w: *Konstytucja…*, pod red. P. Tulei, s. 172.

[16] Wyrok Trybunał Sprawiedliwości (TK) z 30 VII 2014 r., sygn. akt K 23/11 (Dz.U. 2014, poz. 1055).

[17] P. Sarnecki, *Art. 51*, w: *Konstytucja…*, pod red. L. Garlickiego, M. Zubika, s. 267.

przez ustawę chociażby ze względu na bezpieczeństwo publiczne. Inną kwestią nasuwającą się przy tym artykule jest pytanie: co zrobić, jeśli jednostka dobrowolnie zgodzi się na udostępnienie swoich danych osobowych, po czym bezpowrotnie utraci nad nimi kontrolę?

3. Prawo do prywatności a prawo Unii Europejskiej i Europejskiej konwencji praw człowieka

Problem ochrony prawa do prywatności został dostrzeżony na płaszczyźnie zarówno międzynarodowej, jak i unijnej. Art. 8 Europejskiej konwencji praw człowieka przewiduje prawo do poszanowania życia prywatnego i rodzinnego, którego ograniczenie może nastąpić jedynie w ściśle określonych przypadkach – ze względu na ochronę: bezpieczeństwa państwowego, bezpieczeństwa publicznego lub dobrobytu gospodarczego kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Norma ta obejmuje swoim zakresem bardzo szeroką problematykę. Zaczynając od spraw dotyczących dostępu do akt osobowych (*Gaskin v. Wielka Brytania*[18]), przez publikację zdjęć zrobionych z ukrycia ukazujących osobę publiczną w chwili opuszczania szpitala ze swoim nowo narodzonym dzieckiem (*Dupate v. Łotwa*[19]), kończąc na masowej inwigilacji komunikacji (*Brother Watch i inni v. Zjednoczone Królestwo*).

Analogiczną normę można odnaleźć w art. 7 Karty Praw Podstawowych dotyczącym poszanowania życia prywatnego i rodzinnego oraz uzupełniającym go art. 8 mówiącym o ochronie danych osobowych. Tematyka spraw rozstrzyganych przez Trybunał Sprawiedliwości Unii Europejskiej często dotyczy problematyki danych telekomunikacyjnych. Warto przytoczyć tutaj chociażby sprawę *H.K.* z 2 marca 2021 r.[20] Dotyczyła ona dostępu służb państwa do danych telekomunikacyjnych. Trybunał stwierdził, że kontrolę nad danymi powinien sprawować niezależny sąd lub wyszczególniony organ administracji. Każdorazowo powinien on analizować zakres ingerencji, odnośnie do której

[18] Wyrok Europejskiego Trybunału Praw Człowieka z 7 VII 1989 r., 10454/83 i in., *Gaskin v. Zjednoczone Królestwo*.

[19] Wyrok Europejskiego Trybunału Praw Człowieka z 19 XI 2020 r., 18068/11, *Dupate v. Łotwa*.

[20] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 2 III 2021 r., C-746/18, *H.K., Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*.

prowadzone jest rozpoznanie lub postępowanie. Kontrola powinna zostać pozostawiona bezstronnemu organowi administracyjnemu, który nie jest bezpośrednio zaangażowany w sprawę oraz zajmuje neutralną pozycję wobec stron postępowania[21]. Wcześniej do kwestii zgodności art. 7 i art. 8 Karty z prawem unijnym, a konkretniej dyrektywy 2006/24/WE dotyczącej retencji danych telekomunikacyjnych, Trybunał odniósł się w wyroku z 8 kwietnia 2014 r., w połączonych sprawach *Kärntner Landesregierung* i *Digital Rights Ireland Ltd*[22]. Sędziowie wskazali, że dyrektywa nie definiuje jasnych i precyzyjnych reguł określających zakres ingerencji we wskazane prawa podstawowe oraz nie nakłada obowiązku ustanowienia takich norm przez państwa członkowskie, a tym samym przekracza granice ustanowione przez zasadę proporcjonalności.

Oprócz Karty Praw Podstawowych na poziomie Unii Europejskiej funkcjonują dyrektywy mające na celu ochronę prywatności. Jedną z ważniejszych regulacji jest rozporządzenie o ochronie danych osób – RODO[23] (ang. General Data Protection Regulation, GDPR) dotyczące osób fizycznych. Rozporządzenie zostało przyjęte w 2016 r. i weszło w życie po ponad 2-letnim okresie przejściowym. W Polsce na skutek implementacji rozporządzenia utworzono nowy organ – Prezesa Urzędu Ochrony Danych Osobowych, który zastąpił urzędującego dotychczas Generalnego Inspektora Danych Osobowych. Rozporządzenie wprowadziło wiele zmian, m.in. konieczność umieszczania jasnych informacji o przetwarzaniu danych czy prawo do usunięcia danych – prawo do bycia zapomnianym. Regulacja łączy szeroko rozumianą ochronę praw jednostki przy jednoczesnym ułatwieniu swobodnego przepływu danych na jednolitym rynku cyfrowym. Jednym z jego zadań jest sprzyjanie rozwojowi działalności gospodarczej i biznesowi. Rozporządzenie proponuje liczne metody i środki realizujące cele aktu prawnego, tak aby administrator mógł odpowiednio zastosować je według własnego

[21] J. Kudła, *Dostęp służb do danych telekomunikacyjnych. Omówienie wyroku TS z dnia 2 marca 2021 r., C-746/18 (Prokuratuur)*, Lex/el. 2021.

[22] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 8 IV 2014 r., w połączonych sprawach C-293/12 i C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in*.

[23] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 IV 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).

uznania i własnych potrzeb[24]. Według RODO obowiązek uzyskania zgody na przetwarzanie danych leży po stronie firmy pozyskującej dane i to ona musi wykazać, że zgodę taką otrzymała. Zgoda musi być dobrowolna, konkretna, świadoma, a jej wycofanie powinno być łatwe[25].

Rozporządzenie RODO w art. 17 skodyfikowało zasadę *prawa do bycia zapomnianym*. Jeszcze przed wejściem rozporządzenia w życie Trybunał wypowiedział się na temat tej zasady w wyroku C-131/12 (*Google Spain v. Mario Costeja Gonzalez*). Skarżący, obywatel Hiszpanii, wniósł do tamtejszej agencji zajmującej się ochroną danych skargę przeciwko lokalnemu wydawcy dziennika oraz przeglądarce Google. Mężczyzna zauważył, że po wpisaniu w wyszukiwarkę swojego imienia i nazwiska pojawiał się link odsyłający do gazety, na stronie której widniała informacja o licytacji jego nieruchomości, w związku z zaległymi należnościami. Skarżący argumentował, że informacja ta dawno straciła na aktualności i nie powinna być dostępna publiczne. Sprawa trafiła do Trybunału Sprawiedliwości Unii Europejskiej, który orzekł, że operator jest zobowiązany do usunięcia danych, które godzą w dobre imię oraz nazwisko osoby trzeciej, a sam operator wyszukiwarki jest administratorem danych – odpowiedzialnym za ich przetwarzanie.

4. Zagrożenia związane z rozwojem Internetu

Pomimo licznych regulacji nie udaje się całkowicie wyeliminować zagrożeń związanych z funkcjonowaniem przestrzeni internetowej, a w szczególności związanych z cyberprzestępstwami. Jako główne zagrożenia należy wymienić: cyberprzestępstwa związane z kradzieżą danych, profilowaniem informacji czy cyberinwigilacją[26]. Innym zagrożeniem jest przechowywanie danych w chmurze . Jest to rozwiązanie, z którego często korzystają zarówno osoby prywatne (np. zapisywanie zdjęć), jak i duże korporacje. Wynika to z faktu, że koszt utrzymania serwerów i baz danych jest bardzo wysoki. Dużo popularniejszym

[24] D. Lubasz, *Art. 1*, w: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, pod red. E. Bielak-Jomaa, D. Lubasza, Warszawa 2018, s. 105–118.

[25] Ł. Olejnik, *RODO, zgoda i przetwarzanie danych – analiza*, Prywatnik.pl, 8 I 2018, https://prywatnik.pl/2018/01/08/analiza-rodo-zgoda-przetwarzanie-danych/ (dostęp: 6 V 2023).

[26] M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 50.

rozwiązaniem jest dzierżawa serwerów lub właśnie przenoszenie danych do chmury[27]. Jednym z zagrożeń związanych z funkcjonowaniem chmury jest wyciek danych dotyczący ujawnienia tajemnic handlowych, informacji finansowych, własności intelektualnej czy danych osobowych. Jako przykłady można wymienić dwa ataki na portal Linkedln i kradzież 167 milinów haseł w 2012 r. czy zawłaszczenie danych ok. 500 milinów kont w kwietniu 2021 r.[28] Niestety, częstą praktyką jest nieinformowanie użytkowników o wycieku ich danych, wskutek czego nie mają oni możliwości dowiedzenia się o ataku na ich prywatność.

Innym stosunkowo nowym zjawiskiem jest cryptojacking[29], czyli nielegalne kopalnie kryptowalut. Polega ono na użyciu ogromnej ilość mocy obliczeniowej w celu przełamania kodu i kradzieży kryptowaluty. Należy podkreślić, że nielegalne kopalnie nie są ukierunkowane na grabież jedynie dużych przedsiębiorstw, ale również indywidualnych osób. Hakerzy nakłaniają do kliknięcia w nieautoryzowany, złośliwy link, w efekcie czego na konto użytkownika pobierany jest kod cryptominingu, który pracuje w tle, znacznie spowolniając pracę komputera. W 2018 r. ofiarą cryptojackingu padła Tesla. Jak zapewnił zarząd firmy, szybko udało się namierzyć złośliwe oprogramowanie, co pomogło zapobiec nadmiernemu wyciekowi danych[30].

Kolejnym problemem jest funkcjonowanie APT (Advanced Persistent Threat), czyli grup hackerskich wynajmowanych przez państwo w celu sabotażu innego państwa lub firmy strategicznej.

Jedną z największych afer drugiej dekady XXI w. była sprawa Cambridge Analytic – firmy, założonej w 2013 r. w Londynie, zajmującej się politycznym konsultingiem. Zakupiła ona aplikację mydigitallife, którą pobrało ponad 270 tysięcy użytkowników Facebooka. Dzięki niej firma mogła inwigilować nie tylko użytkowników aplikacji, lecz także ich

---

[27] *Największe zagrożenia bezpieczeństwa związane z chmurą*, TyrantsThem, 2019, https://tyrantsthem.com/pl/artykuly/zagrozenia-bezpieczenstwa-chmura/ (dostęp: 6 V 2023).

[28] M. Dudzik, *Kolejny ogromny wyciek danych – tym razem z LinkedIn*, Tabletowo, 9 IV 2021, https://www.tabletowo.pl/linkedin-wyciekly-dane-ponad-500-milionow-kont/ (dostęp: 6 V 2023).

[29] Cryptojacking to zjawisko, którym określany jest nieautoryzowany dostęp do urządzenia w celu wydobywania internetowej waluty – tzw. kryptowaluty.

[30] L.H. Newman, *Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency*, Wired, 28 II 2018, https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/ (dostęp: 6 V 2023).

znajomych[31]. Dane te pozwalały tworzyć profile psychologiczne użytkowników, do których trafiały spersonalizowane informacje. Wcześniej prowadzono długie badania mające wykazać korelacje między osobowością użytkowników a odwiedzanymi przez nich stronami w Internecie. Firma została wynajęta przez sztab wyborczy Donalda Trumpa, który ubiegał się o fotel prezydenta Stanów Zjednoczonych w 2016 r. Szacuje się, że dzięki jej pracy poparcie dla D. Trumpa w tzw. swinging states[32] wzrosło od 1% do 3%[33].

5. Działanie państwowych służb specjalnych a kontrola jednostki

Nie tylko prywatne firmy i hakerzy stanowią zagrożenie dla prywatności. Sprawy dotyczące naruszeń ochrony prywatności przez państwowe służby specjalne stanowiły przedmiot licznych spraw sądowych, na gruncie zarówno europejskim, jak i krajowym.

W dniu 30 lipca 2014 r. Trybunał Konstytucyjny wydał wyrok (K 23/11) dotyczący katalogu zbieranych informacji za pomocą środków technicznych przez służby specjalne oraz zasady niszczenia zdobytych informacji. Zaskarżone przepisy miały zezwalać Policji, Straży Granicznej, Żandarmerii Wojskowej, Centralnemu Biuru Antykorupcyjnemu, Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego i Służbie Celnej na pozyskiwanie danych od operatorów i dostawców usług telekomunikacyjnych bez należytej kontroli[34]. TK przychylił się do zarzutów wnioskodawców – Rzecznika Praw Obywatelskich i Prokuratora Generalnego, którzy zakwestionowali i warunki dostępu do danych i samą procedurę ich udostępniania. Rażącym naruszeniem Konstytucji był brak wykreowanych niezależnych mechanizmów kontroli. Wyrok

[31] M. Madejski, *Cambridge Analytica – czym jest firma, która pokazała Trumpowi i komuś z Polski twojego Facebooka*, Bezprawnik, 21 III 2018, https://bezprawnik.pl/cambridge-analytica/ (dostęp: 6 V 2023).

[32] Stany, w których liczba osób głosujących na republikanów i demokratów jest zbliżona. Zazwyczaj głosy tych stanów są rozstrzygające w wyborach.

[33] S. Czubkowska, *Afera Cambridge Analytica. Facebook wybrał Amerykanom prezydenta. Czy nam też wybierze? I jeszcze na tym zarobi*, Gazeta Wyborcza, 24 III 2018, https://wyborcza.pl/7,156282,23182834,afera-cambridge-analytica-facebook-wybral-amerykanom.html (dostęp: 6 V 2023).

[34] J. Podkowik, *Niezależna kontrola udostępniania danych telekomunikacyjnych*, „Przegląd Legislacyjny" 2015, nr 2(92), s. 24.

odroczono o 18 miesięcy, aby ustawodawca miał czas na przygotowanie odpowiednich rozwiązań legislacyjnych[35].

Na gruncie międzynarodowym przełomowym momentem okazało się ujawnienie tajnych raportów amerykańskich służb specjalnych przez E. Snowdena w 2013 r. Były pracownik CIA upublicznił m.in. fakt, że amerykańskie służby podsłuchiwały tysiące rozmów dziennie (wewnątrzkrajowych i międzynarodowych) oraz zobowiązywały dostawców danych do przekazywania metadanych rozmówców. E. Snowden wyjawił też istnienie brytyjskiego systemu Tempora, który miał masowo podsłuchiwać międzynarodowe rozmowy i szpiegować internautów.

Na skutek ujawnienia tych informacji ponad 16 wnioskodawców, w tym 14 organizacji pozarządowych, postanowiło wnieść do Europejskiego Trybunału Praw Człowieka skargę, zarzucając Wielkiej Brytanii naruszenie art. 8 i art. 10 Konwencji. Skarżący wnosili m.in., że Intelligence Services Act, Security Services Act i Regulation of Investigatory Powers Act są niezgodne z Konwencją, ponieważ dopuszczają do trzech rodzajów bezprawnej inwigilacji w postaci: masowego przechwytywania komunikacji, wymiany wywiadowczej z obcymi państwami oraz przekazywania przez dostawców usług telekomunikacyjnych danych osobowych służbom specjalnym. Kolejnym podnoszonym zarzutem była groźba daleko idącego naruszenia tajemnicy dziennikarskiej w postaci ujawnienia źródeł dziennikarzy. Taka sytuacja mogła wywołać efekt mrożący. Informatorzy mogliby obawiać się, że ich dane będą ujawnione.

Trybunał orzekł, że zaskarżone przepisy naruszają postanowienia Konwencji, ponieważ nie przewidują odpowiednich mechanizmów chroniących prywatność. Zaznaczył natomiast, że sama w sobie wymiana informacji wywiadowczych nie stanowi naruszenia prawa międzynarodowego. Wciąż aktualne są groźby ataków terrorystycznych, a jednym ze sposobów zapobiegania im jest inwigilacja ze strony służb specjalnych.

Podsumowanie

Pojęcie prawa do ochrony prywatności w dobie cyfrowej stało się jednym z ważniejszych. Powszechność dostępu do Internetu znacznie

[35] B. Grabowska-Moroz, *Ochrona gromadzonych danych telekomunikacyjnych i zasady ich udostępniania na tle Konstytucji RP i prawa Unii Europejskiej. Glosa do wyroku TS z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12 oraz do wyroku TK z dnia 30 lipca 2014 r., K 23/11*, „Europejski Przegląd Sądowy" 2016, nr 1, s. 34.

zmieniła skalę problemów związanych z ochroną danych. W związku z rosnącą rolą portali społecznościowych ilość informacji, jakimi dzielą się na nich użytkownicy, znacząco wzrasta. Wyzwanie, przed którym stoją organy krajowe i międzynarodowe, polega na możliwości zapewnienia jednostce maksymalnej ochrony w Internecie, uwzględniając przy tym świadomą i pełną kontrolę nad udostępnianymi przez nią danymi i treściami. Pomimo coraz bardziej rozbudowanych regulacji na płaszczyźnie unijnej nadal nie udaje się w pełni powstrzymać cyberprzestępców przed kradzieżą danych osobowych. Użytkownicy nieświadomi zagrożeń z łatwością udostępniają swoje dane w sieci. Często też nie wiedzą, że padli ofiarą hakerów albo są manipulowani poprzez udostępnianie im profilowanych informacji. Przełomową regulacją, która wpłynęła nie tylko na zwiększenie ochrony danych, lecz także na zwrócenie większej uwagi społecznej na problem prywatności, okazało się być rozporządzenie o ochronie danych osobowych – RODO. Dzięki niemu wprowadzono m.in. konieczność umieszczania jasnych informacji o przetwarzaniu danych czy prawo do usunięcia danych – prawo do bycia zapomnianym. Należy jednak mieć na uwadze, że w wielu krajach dopiero wypracowywane są mechanizmy kontroli, mające zapobiec przed nieograniczonym dostępem do danych przez służby specjalne. Skutkuje to często nadużyciami w masowej inwigilacji komunikacji, o czym wielokrotnie rozstrzygał Europejski Trybunał Praw Człowieka (chociażby w sprawie *Brother Watch i inni v. Zjednoczone Królestwo*). Społeczne przyzwolenie na masową inwigilację ze strony państwa znacznie zwiększyło się po atakach 11 września 2001 r. na Word Trade Center i zdaje się nie słabnąć w obliczu nadal aktualnych gróźb ataków terrorystycznych.

PRIVACY AND THE VIRTUAL WORLD: PROTECTING INDIVIDUAL RIGHTS IN THE INTERNET AGE

Summary

The article aims to indicate the most important issues facing an individual wishing to protect his or her privacy on the Internet. It also describes the evolution of the concept of the right to privacy, which over the years has become one of the most important subjective rights reflected both in the Polish Constitution and in the legal acts of the Council of Europe and the European Union. The text also demonstrates the approach to the issue of the right to privacy taken by both the Polish constitutional and international judiciary. The European Court of Human Rights

in Strasbourg, in the cases of *Dupate v. Latvia* and *Brother Watch and others v. United Kingdom*, dealt with both the publication of photographs of a public figure taken surreptitiously in a private situation and mass surveillance. The Court of Justice of the European Union in Luxembourg, in its judgments, has often referred to the issue of the protection of telecommunications data, including the question of access by state services to such data (*H.K* case) and the rights and obligations created by Articles 7 and 8 of the Charter (*Kärntner Landesregierung and Digital Rights Ireland Ltd case*). The European Union authorities, reacting to the increasingly widespread problem of data flows on the Internet, decided to enact the General Data Protection Regulation (GDPR). The article describes the most important objectives and tasks to be fulfilled by this legal act. In addition, the main problems associated with the use of new technologies such as cybercrimes, cyber surveillance, data theft, as well as cryptojacking and the functioning of APTs (Advanced Persistent Threat), i.e. skilled hacking groups, are also indicated.

Keywords: right to privacy – Internet – personal data

BIBLIOGRAFIA

Czubkowska S., *Afera Cambridge Analytica. Facebook wybrał Amerykanom prezydenta. Czy nam też wybierze? I jeszcze na tym zarobi*, Gazeta Wyborcza, 24 III 2018, https://wyborcza.pl/7,156282,23182834,afera-cambridge-analytica-facebook-wybral-amerykanom.html (dostęp: 6 V 2023).

Dudzik M., *Kolejny ogromny wyciek danych – tym razem z LinkedIn*, Tabletowo, 9 IV 2021, https://www.tabletowo.pl/linkedin-wyciekly-dane-ponad-500-milionow-kont/ (dostęp: 6 V 2023).

Florczak-Wątor M., *Art. 47*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. P. Tulei, Warszawa 2019, s. 167.

Florczak-Wątor M., *Art. 49*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. P. Tulei, Warszawa 2019, s. 172–175.

Grabowska-Moroz B., *Ochrona gromadzonych danych telekomunikacyjnych i zasady ich udostępniania na tle Konstytucji RP i prawa Unii Europejskiej. Glosa do wyroku TS z dnia 8 kwietnia 2014 r., C-293/12 i C-594/12 oraz do wyroku TK z dnia 30 lipca 2014 r., K 23/11*, „Europejski Przegląd Sądowy" 2016, nr 1, s. 31–36.

Kudła J., *Dostęp służb do danych telekomunikacyjnych. Omówienie wyroku TS z dnia 2 marca 2021 r., C-746/18 (Prokuratuur)*, Lex/el. 2021.

Lubasz D., *Art. 1*, w: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, pod red. E. Bielak-Jomaa, D. Lubasza, Warszawa 2018, s. 105–118.

Madejski M., *Cambridge Analytica – czym jest firma, która pokazała Trumpowi i komuś z Polski twojego Facebooka*, Bezprawnik, 21 III 2018, https://bezprawnik.pl/cambridge-analytica/ (dostęp: 6 V 2023).

Mielnik Z., *Prawo do prywatności (zagadnienia wybrane)*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 58(2), s. 29–41.

Marr B., *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, Forbes, 21 V 2018, https://tinyurl.com/bdccef2h (dostęp: 4 V 2023).

Największe zagrożenia bezpieczeństwa związane z chmurą, TyrantsThem, 2019, https://tyrantsthem.com/pl/artykuly/zagrozenia-bezpieczenstwa-chmura/ (dostęp: 6 V 2023).

Newman L.H., *Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency*, Wired, 28 II 2018, https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/ (dostęp: 6 V 2023).

New report: Time spent online falls to pre-pandemic levels, while social media use increases, Meltwater, 26 I 2023, https://tinyurl.com/bd7ch9yx (dostęp: 4 V 2023).

Olejnik Ł., *RODO, zgoda i przetwarzanie danych – analiza*, Prywatnik.pl, 8 I 2018, https://prywatnik.pl/2018/01/08/analiza-rodo-zgoda-przetwarzanie-danych/ (dostęp: 6 V 2023).

Podkowik J., *Niezależna kontrola udostępniania danych telekomunikacyjnych*, „Przegląd Legislacyjny" 2015, nr 2(92), s. 23–40.

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

Sakowicz A., *Prywatność jako samoistne dobro (per se)*, „Państwo i Prawo" 2006, nr 1, s. 16–29.

Sarnecki P., *Art. 47*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. L. Garlickiego, M. Zubika, t. 2, wyd. 2, Warszawa 2016, s. 248.

Sarnecki P., *Art. 51*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. L. Garlickiego, M. Zubika, t. 1, wyd. 2, Warszawa 2016, s. 267–272.

Warren S.D., Brandeis L.D., *The Right to Privacy*, „Harvard Law Review" 1890, nr 4(5), s. 193–220.