MAGDALENA SITEK
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi
ms@wsge.edu.pl

PRAWO DO PRYWATNOŚCI W DOBIE PERMANENTNEJ INWIGILACJI WSPIERANEJ TECHNIKAMI ELEKTRONICZNYMI

THE RIGHT TO PRIVACY IN THE ERA OF PERMANENT SURVEILLANCE SUPPORTED BY THE ELECTRONIC TECHNIQUES

ABSTRACT

The right to privacy is one of the fundamental human rights and it is an expression of the need to protect the individual's dignity. Rapid technological progress, particularly in the area of information, opens the way to a fairly deep penetration into the human's privacy. Additionally, there is a process of globalization, which initiated the era of post-modernity. This era is characterized by changes in axiology, polycentricism and the loss of faith in the progress with the simultaneous acceleration of innovation. It is necessary to redefine the concepts of privacy and to build a system, based on good law, to protect the human right to privacy.

Keywords: *privacy, the Constitution of the Republic of Poland, European law, globalization, media, consumer*

STRESZCZENIE

Prawo do prywatności jest jednym z podstawowych praw człowieka i wyrazem potrzeby ochrony godności jednostki. Szybki postęp technologiczny i techniczny, w szczególności w obszarze informatyki, otwiera drogę do dość głębokiej penetracji prywatności człowieka. Do tego dochodzi jeszcze globalizacja, która zapoczątkowała epokę ponowoczesności. Epoka ta charakteryzuje się zmianami w aksjologii, policentrycznością, utratą wiary w postęp z jednoczesnym przyspieszeniem innowacyjności. Konieczne jest ponowne zdefiniowanie pojęcia prywatności oraz zbudowanie systemu jej ochrony na bazie dobrego prawa.

Słowa kluczowe: *prywatność, Konstytucja RP, prawo europejskie, globalizacja, media, konsument*

WPROWADZENIE

Prawo do prywatności należy do podstawowych praw człowieka, a jednocześnie jest fundamentalną jego potrzebą, zwłaszcza w kulturze Zachodu. Prawo to jest wyrazem wolności człowieka do decydowania o zakresie dostępu do informacji o nim samym. M. Pryciak zauważa, że sfera prywatności jest dość szeroka i obejmuje dane dotyczące samej osoby jako takiej, a także przestrzeni, w której się porusza i żyje, jak chociażby pomieszczeń, w których żyje (zob. M. Pryciak, s. 212). Autor ten wykazał, że namiastek tego prawa należy szukać już w przekazie biblijnym. Koncepcyjnie prawo to jednak było rozwijane dopiero pod koniec XIX wieku (zob. M. Pryciak, s. 213), między innymi dzięki takim badaczom, jak V. Brandeis i E. Warren (zob. S.D. Warren, L. Brandeis, 1890, s. 193–220).

Według M. Safjana prywatność jest sferą wolności człowieka, która podlega jego wyłącznej kontroli (zob. M. Safjan, 2006, s. 211 i nast.; L. Leszczyński, B. Liżewski, 2008, s. 88). Prywatność jest dobrem i prawem osobistym przynależnym każdemu człowiekowi, niezależnie od jego stanu fizycznego, psychicznego, stadium rozwoju, a także płci, wyznania bądź rasy. Podlega też ochronie prawnej. Prawo do prywatności jest sferą zamkniętą przed dociekliwością innych. Może jednak doznawać pewnych ograniczeń na podstawie szczególnych przepisów prawa, zwłaszcza dotyczących bezpieczeństwa publicznego, jak np. przeciwdziałanie wszelkim formom terroryzmu. Do tego konieczne jest niejednokrotne ingerowanie w sferę prywatności przez ustawowo uprawnione do tego służby specjalne.

Prawo do prywatności rozumiane jako sfera prywatności jest jednocześnie potrzebą każdego człowieka. Potrzeba ta jednak może być różnie rozumiana w różnych kręgach kulturowych bądź nawet grupach społecznych tej samej kultury. Inna jest granica tej sfery w przypadku naturystów, a inna w przypadku przeciwników publicznego obnażania swojej cielesności, chociaż przedstawiciele obu grup przynależą do tej samej rodziny kulturowej. Dlatego to człowiek ma wyłączne uprawnienie do decydowania o tym, jakie informacje dotyczące jego mogą być publicznie ujawnione, a które podlegają wyłączeniu i są zachowywane tylko do wiadomości samego zainteresowanego lub osób, którym te informacje ujawnił. Tak rozumiane prawo do prywatności pozwala na obronę człowieka przed nieuprawnionymi nadużyciami, np. ośmieszaniem go albo redukcjonizmem, np. sprowadzenie go do poziomu tylko konsumenta lub narzędzia do promocji samochodu – ten ostatni przypadek może dotyczyć w szczególności kobiety (zob. M. Sitek, 2016, s. 181).

Przedmiotem niniejszego opracowania jest analiza i ukazanie wpływu rozwoju współczesnych technik informatycznych na prawa człowieka, zwłaszcza w obszarze prawa do prywatności. Rozwój nowych technologii powoduje zagrożenie dla takich danych, jak: kontakty, tożsamość osoby, tożsamość telefonu, w tym jego numer, lokalizacja, historia przeglądania, e-maile, SMS-y, dane biometryczne (odciski palców, twarz), informacje pozwalające na uwierzytelnienie w usługach społecznościowych lub karta kredytowa i dane dotyczące płatności.

Już na samym początku można postawić hipotezę badawczą, że współczesne narzędzia informatyczne, takie jak portale społecznościowe, bazy danych, programy do współdzielenia dokumentów, budowane są z wykorzystaniem elementów psychologii człowieka, jego potrzeb, zwłaszcza zaspokojenia wiadomości o życiu innych, a także potrzeby dzielenia się z innymi swoimi sekretami, sukcesami, porażkami bądź uczuciami. Ta potrzeba rośnie proporcjonalnie do narastania zjawiska samotności w społeczeństwie masowym, wielokulturowym. Ludzie szukają przyjaźni coraz częściej właśnie w Internecie, nie zaś w świecie realnym (zob. J. Zawisza, s. 403–415). Praca ma być odpowiedzią na podstawowe obecnie pytanie, a mianowicie: na ile rozwój technik informatycznych ogranicza tradycyjnie rozumiane prawo prywatności? Drugim pytaniem jest: czy można mówić dzisiaj o prywatności w świetle postępu technologicznego umożliwiającego właściwie bezgraniczną ingerencję w sferę prywatności człowieka?

TECHNOLOGIA ELEKTRONICZNA ZAGROŻENIEM DLA PRAWA DO PRYWATNOŚCI?

W kulturze Zachodu prawo do prywatności jest jednym z tych praw człowieka, które obok prawa do życia są najczęściej naruszane nie tylko przez media, ale również przez organy państwowe, instytucje biznesowe bądź też przez portale społecznościowe.

Media

Tempo współczesnego postępu technologicznego najlepiej uwidacznia się w obszarze mediów. Polega on na odchodzeniu od mediów tradycyjnych, czyli gazety, a nawet telewizji. Ich miejsce zajmuje Internet i urządzenia mobilne, zwłaszcza telefon. Zmienia się też filozofia komunikowania i formy zagrożeń. Dodaną wartością tych przemian jest łatwość komunikowania

się, wymiany informacji, większa aktywizacja społeczeństwa, podniesienie poziomu kultury ogólnej i zaspokojenie w większym stopniu niż dotychczas potrzeby informacji.

Różne formy funkcjonowania mediów można sprowadzić do tych, które zalicza się do mediów tradycyjnych i tych, które zalicza się do mediów interaktywnych. Co do zasady, oba rodzaje mediów spełniają te same funkcje, tj. przekazywanie różnorakich informacji. Zasadnicza jednak różnica między nimi koncentruje się na roli czytelnika. W mediach tradycyjnych jest on biernym odbiorcą informacji wytwarzanych przez określone centra opiniotwórcze, nierzadko skoncentrowane w ręku kilku potentatów prasowych. Z klei w mediach interaktywnych odbiorca staje się jednocześnie odbiorcą i aktorem, który nie tylko czyta, ogląda, ale i tworzy. Do tego służą możliwości komentowania artykułów zamieszczanych w mediach elektronicznych, tworzenie blogów bądź też własnych storn internetowych (zob. Ł. Kołodziejczyk, 2014).

W konsekwencji codziennie dostarczane są informacje ze świata polityki, gospodarki, sportu, kultury, nauki, ale też ważne miejsce zajmują informacje dotyczące życia prywatnego gwiazd filmowych, polityków lub innych osób publicznych. Społeczna potrzeba sensacji popycha dziennikarzy do łamania coraz to nowych granic tabu, dostarczając szczegółów pochodzących ze sfery prywatności albo nawet sfery intymnej, o istnieniu których przeciętny człowiek nie ma pojęcia (zob. M. Puwalski, 2003, s. 11). Jedną z najbardziej negatywnych grup dziennikarzy są wszechobecni paparazzi, dla których nie ma żadnych granic moralnych ani etycznych.

Media interaktywne stworzyły nieograniczone możliwości nie tylko odbioru, ale i produkcji oraz dystrybucji, a także rozpowszechniania informacji pozytywnych i negatywnych. Przykładem może być rozpowszechnianie treści pornograficznych, ale też np. rasistowskich. W mediach tradycyjnych odbiorca był biernym uczestnikiem rynku pornograficznego. Obecnie jest nie tylko odbiorcą, ale też może sam dostarczać materiału, chociażby w postaci zdjęć zrobionych samemu sobie i umieszczonych w sieci, a które następnie są powielane najczęściej już bez jego zgody czy wiedzy (zob. D. Boyd, 2007). Media interaktywne pozwalają również na szerzenie agresji lub też wyrządzanie szkody na poszczególnych dobrach osobistych człowieka, o których jest mowa w art. 23 kc (zob. J. Pyżalski, 2012, s. 92). W szczególności zagrożone bądź naruszane jest dobro, jakim jest atak na dobre imię innych

osób poprzez zniesławienie, czyli ujawnianie prawdziwych i nieprawdziwych informacji o charakterze intymnym albo prywatnym. Raz ujawnione w ten sposób zniesławiające informacje i zamieszczone w tzw. chmurze, są nie do usunięcia. Wprawdzie wprowadzone zostało prawo do zapomnienia, czyli możliwość usunięcia z sieci danych wrażliwych, w praktyce jednak jest to prawie niemożliwe. Wpisy te są chronione domniemaniem, że posiadają one znaczenie dla społeczeństwa.

Można powiedzieć, że chociaż rozwój interaktywnych mediów ma niewątpliwie pozytywny wkład w rozwój naszej cywilizacji, to jednak należy brać pod uwagę również i zagrożenia dla właśnie prywatności jednostki.

Służby specjalne

We wzroście poziomu działań ograniczających sferę prywatności mają swój udział również organy państwa, a zwłaszcza jego służby korzystające z coraz to nowszych urządzeń inwigilujących. Do tego wykorzystywane są urządzenia tak mobilne (telefony mobilne, chipy w telefonach, gniazdkach do prądu, żyrandolach itp.), jak i stałe (np. kamery). Z jednej strony społeczeństwo masowe wymusza, a nawet żąda i akceptuje zwiększenie poziomu kontroli w celu zapewnienia bezpieczeństwa w wymiarze jednostkowym i wspólnotowym. Z drugiej jednak strony narasta coraz większy społeczny niepokój wobec permanentnej inwigilacji prowadzonej prawie że już na wzór orwellowskiego Wielkiego Brata z książki pt. „Rok 1984".

W państwie prawa służby zobowiązane są do podejmowania działań na podstawie prawa i w zakresie swoich kompetencji określonych ustawami. Tak to ustawodawca zapisał w art. 5 ust. 1 pkt 3 ustawy z 9 czerwca 2006 roku o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz.U. 2016 poz. 1318). Działania wszystkich służb winny przestrzegać postanowień ustawy z 5 sierpnia 2010 roku o ochronie informacji niejawnej (t.j. Dz.U. 2016 poz. 1167).

Nie zawsze jednak działania służb bezpieczeństwa są uzasadnione, a nawet często motywowane są imperatywami o charakterze politycznym w celu np. dyskredytacji oponenta bądź oponentów politycznych. Gromadzone dane przez funkcjonariuszy mogą być potem wykorzystywane do szantażowania albo politycznej eliminacji danej osoby. Służby dzięki takim informacjom mogą mieć realny wpływ na wydarzenia polityczne. Przykładem wybory w USA, kiedy to FBI stopniowo ujawniała maile pochodzące

z komputera Hillary Clinton. W efekcie przegrała ona wybory. Do dzisiaj nie zostały wyjaśnione motywy, ani tym bardziej to, kim byli prawdziwi protektorzy nagrań członków rządu PO-PSL, jakie miały miejsce w 2013 roku w restauracji „Sawa i Przyjaciele". Doszło wówczas do ujawnienia szeregu informacji należących do sfery prywatności, nawet osób publicznych. Widocznym efektem tych działań były przegrane w 2015 roku wybory przez ówczesne elity rządzące.

Specyfika służb oraz możliwości techniczne sprawiają, że istniejące normatywne ograniczenia, chociażby w znowelizowanej w 2016 roku ustawie w sprawie zasad inwigilacji, nie ograniczają wykraczania służb poza te granice. Każdy motyw – prawdziwy bądź nieprawdziwy – jest dobry dla działań ludzi zatrudnionych we wszelkiego rodzaju agencjach. We wspomnianej noweli kontrola operacyjna nie może trwać dłużej niż 18 miesięcy. Może za to polegać na podsłuchu, poglądzie osób w pomieszczeniach, środkach transportu, kontroli korespondencji, w tym elektronicznej, kontroli przesyłek, kontroli informatycznych nośników danych systemów informatycznych i teleinformatycznych. Służby mogą inwigilować za pomocą nadajnika GPS i z wykorzystaniem dronów. Obowiązek przechowywania bilingów został utrzymany na wcześniejszym poziomie, tj. 12 miesięcy. Nad tymi działaniami pozostaje właściwie tylko kontrola sądowa.

Biznes

Trzecią grupą podmiotów gromadzących dane o jednostce i jej funkcjonowaniu w społeczeństwie są instytucje biznesowe, jak banki, sieci sklepów, pizzerii, dealerzy samochodów, sklepy internetowe itp. Dane dotyczące prywatności gromadzone są za pomocą kart płatniczych, kart lojalnościowych, poprzez używanie wielu aplikacji na telefon oraz komputer. Nieuczciwe aplikacje są w stanie przesłać na zdalny serwis informacje z książki adresowej, informacje na temat sieci albo samego urządzenia, ustalić lokalizację urządzenia, a tym samym i jego posiadacza. Ponadto ściągnięte aplikacje mogą uzyskiwać dostęp do wielu funkcjonalności urządzenia. W konsekwencji ze zdalnego komputera mogą być wysłane na rachunek posiadacza urządzenia SMS-y albo maile. Można w ten sposób przejmować zdjęcia. Media co jakiś czas donoszą, że zostały skradzione intymne zdjęcia z komputera znanych aktorek. Nie zawsze twórcy aplikacji informują użytkowników o rodzaju i celu gromadzenia informacji. Większość z uzyskanych w ten sposób da-

nych przekazywana jest osobom trzecim dla przeprowadzenia analizy. To wszystko jest robione w celu pozyskania, a następnie zbudowania obrazu potrzeb potencjalnego klienta (zob. L. Pułka, 2010).

Przykładem działań powyżej opisanych może być informacja, jaka ukazała się na portalu auto-swiat.pl. Znamienny jest już sam tytuł artykułu, a mianowicie „Uważaj: Twoje auto to szpieg"[1]. Autor artykułu opisał sposób gromadzenia informacji producenta samochodów o ich użytkownikach. Zamontowane urządzenia w najnowszych typach samochodów zbierają takie dane, jak: położenie, przebieg kilometrów, zużycie paliwa, stan paliwa w zbiorniku oraz błędy odnotowane przez układy diagnostyczne. Ponadto monitorowany jest styl jazdy, brak zamknięcia drzwi w czasie parkowania, a także przekroczenie dozwolonej liczby obrotów silnika, czyli bardzo szybka jazda samochodem. Takie systemy do monitorowania pracy samochodu, ale też i użytkownika montują już w najnowszych modelach BMW i Volvo. Systemy te pozwalają na wyciągnięcie korzyści dla obu stron, tj. użytkownika i producenta. Zebrane dane pozwalają bowiem na usprawnienie funkcjonowania samochodów i poszczególnych jego elementów, usprawnienie ruchu na drodze, zwiększają bezpieczeństwo użytkowania. Z drugiej jednak strony gromadzone dane są poddawane analizie, najczęściej w firmach zewnętrznych dla producentów. Działania te są podejmowane w celu zbudowania sylwetki użytkownika dla potrzeb marketingu bądź też dla innych celów. W tym kontekście konieczne jest zastanowienie się nad bezpieczeństwem danych gromadzonych przez producenta samochodów. Co robi z danymi firma analityczna? Na ile te dane są tam bezpieczne, a nie są np. przedmiotem handlu? Dalej, na ile te dane są wrażliwe i pozwalają na identyfikację użytkownika? Jaka jest podstawa prawna dla takiego działania? Na te pytania bez drobiazgowej analizy sposobów gromadzenia oraz wykorzystywanych urządzeń do gromadzenia odpowiedź jest prawie niemożliwa.

Portale społecznościowe

Odrębną grupą narzędzi wykorzystywanych do gromadzenia danych należących do sfery prywatności są portale społecznościowe, np. Facebook, Instagram, Nasza Klasa, które zostały stworzone w oparciu o jedną

[1] http://www.auto-swiat.pl/eksploatacja/uwazaj-twoje-auto-to-szpieg-wyjasniamy-po-co-producentom-dane-o-autach-i-kierowcach/4e0b6d [data dostępu: 29.11.2016].

z największych słabości człowieka, a mianowicie potrzebę chwalenia się zdjęciami, podróżą lub innymi zdarzeniami z życia osobistego. Tak informatycznie i psychologicznie skonstruowane narzędzia wywołują brak autokontroli u wielu użytkowników tych portali. Oni sami dokonują samoobnażania się, zdradzając miejsca pobytu, zamieszczając zdjęcia z wakacji, nierzadko intymne. Do tej samej kategorii narzędzi należy zaliczyć iCloud lub iCloud Drive. W obu przypadkach jest to tzw. chmura, w której można przechować zdjęcia, dokumenty, apki, notatki, kontakty, a także dokumenty prywatne, naukowe albo służbowe.

Jednym z przykładów portali społecznościowych są portale randkowe oraz matrymonialne. Chociaż inne mają one cele niż FB oraz Instagram, to jednak ich funkcjonowanie opiera się na podobnych zasadach. Na portalach randkowych oraz społecznościowych spotykają się osoby, które chcą realizować swoje potrzeby o charakterze matrymonialnym bądź tylko towarzyskim, o charakterze krótkotrwałym. Portale tego rodzaju stosują różne techniki gromadzenia informacji o różnym charakterze. Bez wątpienia chodzi jednak nierzadko o dane wrażliwe, zaliczane do dóbr osobistych wchodzących w skład sfery prywatności. Są to takie dane, jak światopogląd, stosunek do religii, orientacja i preferencje seksualne. Dane te są gromadzone w celu lepszego doboru partnerów.

Jednak z funkcjonowaniem tych portali wiąże się wiele wątpliwości i pytań natury technicznej i prawnej. Przede wszystkim rodzi się pytanie o to, czy klienci są poprawnie informowani o tym, co dzieje się z ich danymi, nierzadko wyjątkowo drażliwymi. Jaka jest gwarancja, że osoba przeglądająca opis w celu poszukiwania partnera zachowa w tajemnicy uzyskane dane wrażliwe? Kto ponosi odpowiedzialność prawną za ujawnienie tych danych w sieci lub w środowisku rodzinnym, zawodowym bądź małych społeczności? Problem nie jest łatwy ani z punktu widzenia technicznego, ani prawnego, a to z tego względu, że już ponad 3 mln Polaków odwiedza takie portale[2]. W USA jedno na sześć zawartych małżeństw ma swoje początki w korzystaniu z portali matrymonialnych.

Korzystanie z portali matrymonialnych albo randkowych rodzi też problemy natury prawnej i finansowej, jak np. odpłatność za korzystanie

[2] *Oto najpopularniejsze serwisy randkowe w Europie*, http://interaktywnie.com/biznes/artykuly/portale/oto-najpopularniejsze-serwisy-randkowe-w-europie-250222 [data dostępu: 29.11.2016].

z nich. Co do zasady nieodpłatne korzystanie z tych portali jest czasowe, zwykle do 6 miesięcy. Użytkownicy najczęściej nie czytają treści umowy, w której nierzadko zapisane jest, że przed upływem okresu darmowego korzystania z portalu należy umowę wypowiedzieć. Zaniedbanie tego obowiązku skutkuje naliczaniem opłat. Do tego w przypadku sporu najczęściej stosuje się prawo niemieckie i sądy niemieckie, chociaż portale są pisane w języku angielskim albo polskim. Takie rozwiązanie powoduje, że dochodzenie roszczeń jest bardzo utrudnione. Portale te często nie mają jasno zbudowanych polityk prywatności. Te mechanizmy stosowane są również w innych rodzajach portali.

Badania naukowe

Kolejnym obszarem możliwego naruszenia prawa do prywatności jest przechowywanie próbek i profili DNA. W jednym z wyroków Europejskiego Trybunału Praw Człowieka odnotowano, że odciski palców, próbki i profile DNA zawierają wiele wrażliwych i osobistych informacji o osobie, wliczając w to dane o stanie zdrowia. Istnienie niepowtarzalnego kodu genetycznego umożliwia identyfikację osoby, a także jej bliskich. Tym samym gromadzenie tych danych może być naruszeniem art. 8 i 14 Europejskiej Konwencji Praw Człowieka, co zostało zarzucone rządowi Wielkiej Brytanii. W wyroku ETPCz z 4 grudnia 2008 roku 3056/04 (S. i Marper przeciwko Wielkiej Brytanii) stwierdzono, że tylko termin „prywatność" i „życie prywatne" jest szerokim terminem, niemającym wyczerpującej definicji i kryje się pod nim psychiczna i fizyczna integralność osoby. Trybunał orzekł, że samo gromadzenie tych danych nie narusza postanowień ETPC, dopiero charakter i ilość informacji zawartych w próbkach oraz ich przechowywanie bez wyraźnego powodu musi zostać uznane za naruszające prawo do poszanowania prywatności osób, których sprawa dotyczy.

Ponadto Trybunał zauważył, że nie można tak samo traktować przechowywania próbek biologicznych i profili DNA, jak i przechowywania odcisków palców, a to ze względu na ilość danych zgromadzonych w materiale DNA. Nie oznacza to, że przechowywanie odcisków palców bez zgody osób zainteresowanych jest bez znaczenia.

Innym przykładem może być wprowadzenie e-mediacji nowelizacją kpc, jaka weszła w życie z dniem 8 września 2016 roku. Mediacja rodzinna dotyczy zawsze danych wrażliwych o różnym charakterze. Dotyczy

więc wspólnej historii życia dwóch osób, ale też zdarzeń jednej lub drugiej strony uczestniczącej w mediacji. W zamyśle ustawodawcy było ułatwienie prowadzenia mediacji pomiędzy osobami zamieszkującymi w znacznej od siebie odległości, oszczędzenie środków na przejazd i po prostu uniknięcie kolejnego konfliktu między stronami przy okazji fizycznego spotkania. Komunikacja między stronami i mediatorem odbywa się za pomocą komunikatorów Gadu-Gadu, Facebooka i innych. Wątpliwości jednak, jakie tu są wskazywane przez doktrynę dotyczą bezpieczeństwa transmisji przekazu podczas mediacji. W przypadku komunikatorów pisemnych: w jaki sposób tekst zapisany jest chroniony? Najczęściej mediator korzysta z komunikatorów powszechnie dostępnych i łatwych do przechwycenia przez osoby niepożądane (zob. A. Arkuszewska, M. Bosak, 2008, s. 166; M. Bobrowicz, 2008, s. 27–28).

OCHRONA PRAWNA PRZED NARUSZENIEM PRYWATNOŚCI

Zdobyte w ten sposób informacje o jednostce, grupie społecznej, np. klasie, a także o grupie zawodowej, sąsiedzkiej itp. są nie tylko gromadzone, ale przede wszystkim przetwarzane. Pomimo zapewnień o uczciwości czy istnienia kodeksów etyki informatyka, w wielu przypadkach dane te są przetwarzane nielegalnie. Istniej rynek danych zgromadzonych w ten sposób o jednostce czy jakiejś grupie społecznej. Takie działania nie tylko mogą budzić moralny sprzeciw, etyczną odrazę, ale mogą być również najnormalniej w świecie bezprawne. Jakie zatem jest lub powinno być remedium na tego rodzaju przypadki? W jaki sposób chronić prywatność zwłaszcza jednostki? Niewątpliwie takim narzędziem do ograniczenia, a przynajmniej rzetelnej kontroli nad gromadzonymi bazami danych jest dobre ustawodawstwo. Czyli nadążające za zmianami nie tylko mentalnościowymi, które są coraz szybsze, ale również, a może przede wszystkim, za rewolucją technologiczną.

Najszersze spektrum narzędzi prawnych służących do ochrony prywatności stworzyła Unia Europejska. Wystarczy tylko wyliczyć akty normatywne wydane głównie dla ochrony danych osobowych, a w konsekwencji i dóbr osobistych. Do najważniejszych z nich należy zaliczyć:

- dyrektywę 2002/58/WE z dnia 12 lipca 2002 roku w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.Urz. WE L 201 z 31.07.2002),

- dyrektywę 2002/21/WE z dnia 7 marca 2002 roku w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/20/WE z dnia 7 marca 2002 roku w sprawie zezwoleń na udostępnienie sieci i usługi łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/19/WE z dnia 7 marca 2002 roku w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz ich łączenia (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/22/WE z dnia 7 marca 2002 roku w sprawie usługi powszechnej i praw użytkowników odnoszących się do sieci i usług łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/58/WE z dnia 12 lipca 2002 roku w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.Urz. WE L 201 z 31.07.2002),
- dyrektywę 2002/77/WE z dnia 16 września 2002 roku w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej (Dz.Urz. WE L 249 z 17.09.2002),
- dyrektywę 2014/53/UE z dnia 16 kwietnia 2014 roku w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylającej dyrektywę 1999/5/UE (Dz.Urz. UE L 153 z 22.05.2014, str. 62);
- dyrektywę 89/336/EWG z dnia 3 maja 1989 roku o zbliżeniu praw państw członkowskich dotyczących kompatybilności elektromagnetycznej (Dz.Urz. L 139 z 23.05.89).

Analiza powyższych przepisów prawa pozwala na stwierdzenie, że współczesne społeczeństwo informacyjne, w szczególności poszanowanie życia prywatnego i ochrona danych osobowych – są ważnym obszarem działania Unii Europejskiej. Między innymi poprzez Europejską Agendę Cyfrową, Komisja Europejska podkreśliła kluczową rolę ICT, w szczególności Internetu, który stanowi „ważny środek działalności gospodarczej i społecznej: służy on pracy, zabawie, komunikacji oraz pozwala na swobodne wyrażanie poglądów[3].

[3] Unijny plan bezpieczeństwa cybernetycznego na rzecz ochrony otwartego Internetu oraz wolności i możliwości w Internecie, http://europa.eu/rapid/press-release_IP-13-94_pl.htm [data dostępu: 2.12.2016].

Podkreśla się potrzebę wzmocnienia zaufania i bezpieczeństwa w sieci oraz zagwarantowanie dostępu do różnych informacji, źródeł i poglądów. Można to osiągnąć poprzez zajęcie się problematyką praw podstawowych w cyberprzestrzeni, w szczególności poprzez wzmocnienie polityki na rzecz ochrony i poprawy wolności i pluralizmu mediów, wspierania umiejętności korzystania z mediów, wspierania ochrony prywatności i danych osobowych oraz zwalczania cyberprzestępczości (zob. A. Mednis, 2006). Na poziomie UE podjęto konkretne inicjatywy, takie jak dyrektywa w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, strategia UE w zakresie cyberprzestępczości, uruchomienie w ramach Europolu Europejskiego Centrum ds. Walki z Cyberprzestępczością, dyrektywa w sprawie zapobiegania handlowi ludźmi oraz nowe ramy prawne UE dotyczące ochrony danych. Prawa podstawowe w Internecie są także ważnym elementem zarządzania Internetem[4].

W prawie polskim podstawę ochrony prawa do prywatności stanowi art. 47 ust. 2 Konstytucji RP gwarantujący ochronę prawa każdego człowieka do poszanowania życia rodzinnego, czci, dobrego imienia oraz decydowania o swoim życiu. Ponadto w art. 49 Konstytucji RP ustrojodawca gwarantuje swobodę i tajemnicę komunikowania się, w art. 50 nienaruszalność mieszkania, a w art. 50 ust. 1 gwarantowana jest ochrona informacji dotyczących danej osoby.

Prawo do prywatności wymaga również ochrony informacji o aktywności człowieka na rynku konsumenckim. Karty kredytowe, przedpłatnicze (pre-paid), debetowe, bankomatowe bądź karty lojalnościowe pozwalają nie tylko na identyfikację konsumenta, ale przede wszystkim na odtworzenie jego osobowości. Uzyskane w ten sposób dane mogą być następnie wykorzystywane do marketingu, a także dla dokonywania czynów przestępczych. Wytworzony na podstawie karty płatniczej profil konsumenta może posłużyć do sprofilowania przesyłanej mu oferty. W konsekwencji konsument może być nękany ofertami poprzez maile, telefony albo oferty przesyłane pocztą. Stąd w art. 76 Konstytucji RP zapisano zobowiązanie władz publicznych do stworzenia systemu normatywnego i instytucjonal-

[4] Decyzja Rady ustanawiająca wieloletnie ramy prac dla Agencji Praw Podstawowych Unii Europejskiej na lata 2018–2022. COM(2016) 442 final.

nego w celu ochrony konsumentów oraz użytkowników i najemców przed naruszeniem ich prywatności i nieuczciwymi praktykami rynkowymi, w tym poprzez handel danymi w celu oferowania produktów lub usług w porze obiadowej. Wypełnienie tego konstytucyjnego zadania ustawodawca spełnił poprzez wprowadzenie art. 22.1 do Kodeksu cywilnego, w którym zdefiniowano pojęcie konsumenta, oraz poprzez art. 66.1 kc, w którym ustawodawca wprowadził regulacje dotyczące wymogów, jakie musi spełniać oferta elektroniczna.

Prawo do prywatności jest kwalifikowane jako dobro osobiste chronione na podstawie art. 23 Kodeksu cywilnego. Nie jest ono *expressis verbis* wymienione w tekście przepisu, jednak *opinio communis* oraz orzecznictwo wyraźnie wskazują na interpretację rozszerzającą art. 23 kc. Ochrona prawa do prywatności może być realizowana nie tylko na drodze cywilnej (art. 23 kc), ale również i karnej (art. 212–217 kk). Podstawowym jednak aktem prawnym służącym do ochrony prywatności jest ustawa z 29 sierpnia 1997 roku o ochronie danych osobowych. Według art. 1 ust. 1 tejże ustawy ochronie podlegają wszelkie dane osobowe, które mogłyby doprowadzić do zidentyfikowania lub nawet stworzenia możliwości zidentyfikowania osoby fizycznej.

W art. 1 ust. 1 pkt 7 ustawy z dnia 16 lipca 2005 roku prawo telekomunikacyjne (t.j. Dz.U. z 2016 r. poz. 1489; dalej: PrTel) ustawodawca postanowił, że tym aktem prawnym określa m.in. warunki ochrony użytkowników usług, w szczególności w zakresie prawa do prywatności i poufności. Ochrona ta jest realizowana głównie przepisami działu VII, ale nie tylko. W art. 56 PrTel ustawodawca określił formę i treść umowy telekomunikacyjnej z odbiorcą końcowym. Zgodnie z art. 56 ust. 3 pkt 19 PrTel w takiej umowie należy określić „sposób przekazywania abonentowi informacji o zagrożeniach związanych ze świadczoną usługą, w tym o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych". Według S. Piątka w przepisie tym ustawodawca zobowiązał dostawcę usługi do przekazywania informacji abonentowi o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych. Obowiązek przygotowania strategii bezpieczeństwa nałożył na prezesa UKE (zob. S. Piątek, 2013, Legalis). Filozofia ochrony prywatności w PrTel opiera się na zapewnieniu bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów w związku ze świadczonymi usługami integralności.

PODSUMOWANIE

Prawo do prywatności, dość dobrze dookreślone w XX wieku, ulega daleko idącym zmianom. Powodowane są one szybkim postępem technologicznym i technicznym, w szczególności w obszarze informatyki. Do tego dochodzi jeszcze globalizacja, która zapoczątkowała epokę ponowoczesności. Epoka ta charakteryzuje się zmianami w aksjologii, policentrycznością, utratą wiary w postęp z jednoczesnym przyspieszeniem innowacyjności.

Najważniejszą jednak cechą obecnej epoki jest postęp techniczny. Pozwala on na niezwykle głębokie wchodzenie w życie człowieka, a właściwie na jego permanentne „podglądanie" i „podsłuchiwanie". Możliwości technologiczne pozwalają na gromadzenie ogromnej ilości danych przez służby, organy administracji państwowej i samorządowej oraz przez prywatne firmy. To sprawia, że sfera prywatności, a nawet intymności podlega ciągłemu kurczeniu się. Konieczne zatem jest ponowne zdefiniowanie pojęcia prywatności oraz budowanie jej ochrony na dobrym prawie. Chodzi tutaj nie tylko o dobre prawo od strony legislacyjnej, ale takie, które dostosowane będzie do potrzeb nowych technologii i człowieka posługującego się najnowszymi wynalazkami technologicznymi. Tym bardziej że użytkownik nie zawsze jest świadomy możliwości urządzeń, którymi się posługuje, i sam udostępnia liczne informacje o sobie, najczęściej nieświadomie. Ponadto prawna ochrona prywatności aby była skuteczna – winna mieć charakter międzynarodowy.

Bibliografia

Arkuszewska A., Bosak M. (2008). *Mediacja jako metoda rozwiązywania indywidualnych i zbiorowych sporów z zakresu prawa pracy*, [w:] J. Olszewski (red.), *Sądy polubowne i mediacja*. Warszawa.

Bobrowicz M. (2008). *Mediacja. Jestem za*. Warszawa.

Boyd D. (2007). *Why youth (heart) social network sites: The role of networked publics in teenage social life*, [w:] D. Buckingham (ed.). *Mc Arthur Foundation on Digital Learning – youth, identity, and digital media volume*. Cambridge.

Decyzja Rady ustanawiająca wieloletnie ramy prac dla Agencji Praw Podstawowych Unii Europejskiej na lata 2018–2022. COM(2016) 442 final.

Kołodziejczyk Ł. (2014). *Prywatność w Internecie*. Warszawa.

Leszczyński L., Liżewski B. (2008). *Ochrona praw człowieka w Europie – szkic zagadnień podstawowych*. Lublin.

Mednis A. (2006). *Prawo do prywatności a interes publiczny*. Warszawa.

Piątek S. (2013). *Prawo telekomunikacyjne. Komentarz*. Warszawa.

Pryciak M. (2010). *Prawo do prywatności*. „Studia Erasmiana Wratislaviensia", nr 4.

Pułka L. (2010). *Utracona prywatność: u progu XX-wiecznej ekspansji mediów: studia antropologiczne*. Wrocław.

Puwalski M. (2003). *Prawo do prywatności osób publicznych*. Toruń.

Pyżalski J. (2012). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*. Kraków.

Safjan M. (2006). *Prawo do ochrony życia prywatnego*, [w:] *Szkoła Praw Człowieka, Helsińska Fundacja Praw Człowieka*. Warszawa, s. 211 i nast.

Sitek M. (2016). *Prawa (potrzeby) człowieka w ponowoczesności*. Warszawa.

Warren S.D., Brandeis L. (December 1890). *The Right to Privacy*. Harvard Law Review, vol. IV.

Zawisza J., *Cyberprzestrzeń jako zagrożenie bezpieczeństwa państwa*, JoMS 4/27/2015.

Źródła internetowe

http://www.auto-swiat.pl/eksploatacja/uwazaj-twoje-auto-to-szpieg-wyjasniamy-po-co-producentom-dane-o-autach-i-kierowcach/4e0b6d [data dostępu: 29 11 2016].

Oto najpopularniejsze serwisy randkowe w Europie, http://interaktywnie.com/biznes/artykuly/portale/oto-najpopularniejsze-serwisy-randkowe-w-europie-250222 [data dostępu: 29.11.2016].

Unijny plan bezpieczeństwa cybernetycznego na rzecz ochrony otwartego Internetu oraz wolności i możliwości w Internecie, http://europa.eu/rapid/press-release_IP-13-94_pl.htm [data dostępu: 2.12.2016].

Źródła prawa

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 23 sierpnia 2016 roku w sprawie ogłoszenia jednolitego tekstu ustawy – Prawo telekomunikacyjne (Dz.U. 2016 poz. 1489).

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 28 lipca 2016 roku w sprawie ogłoszenia jednolitego tekstu ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. 2016 poz. 1318).

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 6 lipca 2016 roku w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie informacji niejawnych (Dz.U. 2016 poz. 1167).