1. Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?

Arwid Mednis

Prawo do prywatności w dobie transformacji ustrojowej

Sporządzając bilans prawnej ochrony prywatności w ostatnim 25-leciu w Polsce trzeba wyraźnie podkreślić: w 1989 r. nie zaczynaliśmy w tej dziedzinie od zera. Przede wszystkim był już pewien dorobek doktryny i orzecznictwa, nie był on może obszerny, ale – przynajmniej, jeśli chodzi o literaturę – był to dorobek oryginalny.

Jeszcze w latach 70. XX. w. *A. Kopff* sformułował koncepcję sfer prywatności[1]. Autor wyodrębnił trzy sfery życia prywatnego: sferę intymności, sferę prywatności, która obejmuje również sferę życia społecznego oraz sferę powszechnej dostępności. Koncepcja ta nie doczekała się jednak powszechnej recepcji w orzecznictwie. Dziś jest traktowana jako pewien etap rozważań nad koncepcją cywilnoprawnej ochrony prywatności.

Z kolei ochrona danych osobowych ma swoje źródło w idei ochrony prywatności, pojawiła się jednak dużo później. Pojęcie prawa do prywatności stworzono jeszcze pod koniec XIX w. Idea regulacji ochrony danych osobowych jest natomiast ściśle związana z rozwojem technologii. Dane o ludziach zbierano od wieków, ale to dopiero w erze komputerów zdano sobie sprawę z zagrożeń, jakie mogą wynikać z wykorzystania maszyn do przetwarzania takich danych. W latach 50. XX w. pojawiły się już pierwsze komputery polskiej

[1] *A. Kopff*, Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne), Studia Cywilistyczne, tom XX/1972.

konstrukcji, ale wówczas traktowano je jako większe i szybsze kalkulatory (stąd określenie „maszyny matematyczne", jakim wówczas się posługiwano). Lata 60. XX w. w Polsce przyniosły pierwsze próby zastosowania owych maszyn w przemyśle i administracji. W 1964 r. powołano nawet urząd Pełnomocnika Rządu ds. Elektronicznej Techniki Obliczeniowej. Na publikacje o danych osobowych trzeba było jednak trochę poczekać. Pierwsze ukazały się dopiero na przełomie lat 70. i 80. XX w.[2]. Przypomnijmy, że równolegle w Europie Zachodniej zaczęły pojawiać się już regulacje chroniące prywatność informacyjną obywateli (mowa m.in. o francuskiej ustawie z 1978 r. o informatyce i kartotekach).

Obowiązująca wówczas Konstytucja PRL z 1952 r. zapewniała w art. 87 ust. 2 nienaruszalność mieszkania i tajemnicę korespondencji[3]. Nie było w niej natomiast żadnej wzmianki o ochronie życia prywatnego ani o ochronie danych osobowych. W ustawodawstwie zwykłym kształtowała się dopiero – jak to określono w literaturze – „świadomość istnienia kwestii prywatności"[4]. Przykładem były ówczesne regulacje dotyczące statystyki państwowej czy prawa bankowego.

W 1984 r. SN zaliczył sferę życia prywatnego do dóbr osobistych, chronionych na podstawie art. 23 i 24 KC. Ochrona sfery życia prywatnego była więc domeną głównie prawa prywatnego.

W okresie transformacji ustrojowej ogromne zasługi dla ochrony prywatności i danych osobowych położył RPO, powołany ustawą z 1987 r. Z braku kompleksowej regulacji konstytucyjnej, RPO w wielu dokumentach i sprawozdaniach odwoływał się wówczas do przepisów MPPOiP, ratyfikowanego przez Polskę jeszcze w 1977 r. Akt ten w art. 17 stwierdza, że „nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię". W pierwszym okresie działalności RPO w swoich wystąpieniach do organów państwowych często powoływał się na poszczególne przepisy MPPOiP, w tym na wspomniany art. 17.

---

[2] *K. Sobczak*, Prawo a informatyka, Warszawa 1978; *A Mrózek*, Ustawowe prawo ochrony danych, Toruń 1981.

[3] Ciekawostką jest fakt, że art. 87 należy do grupy przepisów Konstytucji z 1952 r., które nie zostały formalnie uchylone, niemniej doktryna i orzecznictwo uznaje, że przestały obowiązywać wraz z wejściem w życie Konstytucji (szerzej na ten temat: *P.T. Kociubiński*, Powojenne przekształcenia własnościowe w świetle konstytucji, LEX/el. 2013, s. 80).

[4] *L. Kański*, Prawo do prywatności (miejsce w prawie polskim), Biuletyn RPO, Materiały Nr 4/1989, s. 74.

Z pierwszego podsumowania za lata 1988–1989 wynika, że RPO zajmował się następującymi sprawami z zakresu ochrony prawa do prywatności[5]:

1) naruszenie tajemnicy lekarskiej poprzez ujawnienie rodzajów chorób na zwolnieniach lekarskich dzieci (po interwencji RPO praktyk zaprzestano „dla świętego spokoju");
2) naruszenie tajemnicy korespondencji (np. przez służby celne lub wewnątrz instytucji państwowych) – korespondencja więźniów była za karę ujawniana przez więzienny radiowęzeł;
3) zbyt dużo informacji wymaganych od kandydatów do pracy w MSW (religia, krewni w krajach kapitalistycznych);
4) udzielanie przez organy państwowe (m.in. skarbowe) informacji o obywatelu, prywatnej osobie, na potrzeby prowadzonego przez tę osobę sporu;
5) przekazywanie przez milicję nieuprawnionym podmiotom danych osób zameldowanych w hotelach (przy okazji okazało się, że praktyka gromadzenia danych hotelowych wprowadzona w stanie wojennym była kontynuowana kilka lat po jego zakończeniu bez podstaw prawnych).

Charakterystyczna dla tamtych czasów była prowadzona w tamtym czasie przez RPO sprawa nauczyciela zwolnionego z pracy za to, że nie wychowywał uczniów w duchu ówczesnej Konstytucji, ponieważ w trakcie rewizji odkryto u niego nielegalne wydawnictwa. Rzuca się w oczy brak jakichkolwiek spraw związanych z informatyką.

W 1991 r. Polska przystąpiła do Rady Europy, w której przynajmniej dwie agendy zajmowały się wówczas ochroną prywatności i danych osobowych[6], a w 1993 r. ratyfikowała EKPC, przyznającą każdemu prawo do poszanowania jego życia prywatnego i rodzinnego, nienaruszalności mieszkania i tajemnicy korespondencji (art. 8).

W 1995 r. przyjęto dyrektywę 95/46. Tworzono ją w pierwszej połowie lat 90. XX w., tj. w czasach początku Internetu. Stanowiła próbę ujednolicenia warunków wykorzystania i ochrony danych osobowych, bowiem dotychczasowe ustawodawstwo poszczególnych krajów członkowskich było bardzo zróżnicowane, co znacznie utrudniało obrót gospodarczy. Z punktu widzenia praw jednostki głównymi problemami były wówczas: przetwarzanie danych osobo-

[5] *A. Mednis*, Prawo do prywatności i ochrona danych – uwagi na tle praktyki Rzecznika Praw Obywatelskich, Biuletyn RPO. Materiały 1990, Nr 6, s. 91.

[6] *Project Group on Data Protection* (CJ PD) oraz komitet konsultacyjny do Konwencji Nr 108 (*Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data* (T-PD)).

wych w elektronicznych bazach oraz powszechne wykorzystanie danych w celach marketingowych, natomiast z niebezpieczeństw płynących z umieszczania danych osobowych w sieci niewielu zdawało sobie wtedy sprawę. Szybki rozwój usług społeczeństwa informacyjnego spowodował, że już po kilku latach dyrektywa 95/46 ujawniła poważne braki. W wyr. z 6.11.2003 r. ETS wskazał, że „nie można przypisać prawodawcy wspólnotowemu zamiaru objęcia w przyszłości pojęciem przekazywania danych do państw trzecich faktu zamieszczenia przez osobę znajdującą się w sytuacji *B. Lindqvist* [autorki strony internetowej, na której zamieszczono dane osobowe – przyp. *A. M.*] danych na stronie internetowej, nawet jeżeli stały się one w ten sposób dostępne dla osób znajdujących się w państwach trzecich i posiadających środki techniczne pozwalające na dostęp do nich”[7]. Zatem to, czy mamy do czynienia z podlegającym ograniczeniom transferem danych do państw spoza UE, zależy od tego, czy strona internetowa jest umieszczona na serwerze w państwie członkowskim, czy w innym państwie. Podważa to sens ograniczeń w przekazywaniu danych do państw trzecich, skoro transferem nie jest umieszczenie danych na stronie internetowej prowadzonej na europejskim serwerze. To tylko jeden z przykładów „nieprzystawania” przepisów opracowanych w pierwszej połowie lat 90. XX w. do świata rozwijających się technologii.

W 1997 r. polski parlament uchwalił OchrDanychU, pierwszą polską kompleksową regulację chroniącą dane osobowe środkami administracyjnoprawnymi. Zainteresowanie tą ustawą było początkowo niewielkie, a głównym motywem jej przyjęcia była konieczność dostosowania naszego prawa do prawa europejskiego[8]. Ustawa ta stanowi implementację wspomnianej dyrektywy 95/46.

Polska dopiero w 2003 r. ratyfikowała Konwencję Nr 108. Pochodzący z 1981 r. akt prawny przyjęty przez Radę Europy zawierał pierwszą europejską próbę regulacji ochrony danych.

---

7 Wyrok ETS z 6.11.2003 r., C-101/01, http://curia.europa.eu/juris/liste.jsf?language=pl&jur=C,T,F&num=C-101/01&td=ALL; na ten temat również: *A. Mednis*, Dyrektywa 95/46 w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej – wybrane zagadnienia, [w:] *A. Mednis* (red.), Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym, Warszawa 2013, s. 136.

8 Na temat okoliczności powstania projektu OchrDanychU: *A. Mednis*, Jak doszło do bliższego przyjrzenia się tematowi ochrony prywatności, [w:] 15-lecie ustawy o ochronie danych osobowych, Warszawa 2013, s. 97.

Inwigilacja i zachowania internautów

Stale powiększająca się paleta usług społeczeństwa informacyjnego stanowi od dawna wielkie wyzwanie dla skuteczności regulacji dotyczących prywatności i ochrony danych osobowych. Z jednej strony, użytkownicy chętnie dzielą się informacjami na swój temat oraz na temat swoich bliskich. Modne na przełomie wieku blogi ustąpiły miejsca serwisom społecznościowym, które w ciągu kilkunastu lat stały się najpopularniejszym miejscem udostępniania informacji[9]. *Mark Zuckerberg*, twórca Facebooka, w 2010 r. stwierdził, że prywatność nie jest już postrzegana jako norma społeczna[10]. Choć niektórzy twierdzą, że korzystanie z portali społecznościowych jest nie tylko formą komunikacji, a czasem przejawem ekshibicjonizmu użytkowników, ale również chęci kreowania swojego wizerunku, to nie ulega wątpliwości, że przekazujemy za pośrednictwem portali społecznościowych wiele informacji, które trafiają nie tylko do znajomych, ale również do firm i instytucji, które wykorzystują je do różnych, często nieznanych nam celów. Właśnie kwestia wykorzystania danych pozostawionych w sieci oraz świadomości użytkowników co do konsekwencji własnych działań staje się coraz większym problemem. W 2013 r. dzięki *Edwardowi Snowdenowi* do opinii publicznej przedostały się informacje o skali inwigilacji prowadzonej przez amerykańską Narodową Agencję Bezpieczeństwa (NSA). Gromadzenie danych o obywatelach przez służby specjalne USA i innych państw nie jest niczym nowym, jednak w tym przypadku wyszła na jaw bezprecedensowa współpraca firm prywatnych z NSA. Firmy z branży internetowej, w tym Google i Facebook, podpisały w ramach programu Prism umowy z NSA, na mocy których agencja miała dostęp do danych ich użytkowników, zgromadzonych na serwerach tych firm. Jednocześnie *Snowden* ujawnił, że dane są wykorzystywane nie tylko w celu zapewnienia bezpieczeństwa i walki z terroryzmem, ale także w celach politycznych, np. analiz dotyczących zagranicznych polityków, są także udostępniane prywatnym koncernom. Warto podkreślić, że NSA gromadzi i analizuje dane nie tylko dotyczące obywateli amerykańskich, ale również obywateli innych państw, w tym Polski. Reakcja opinii publicznej na informacje *Snowdena*, a także np. na takie działania jak narzucona przez Facebooka zmiana ustawień prywatności pokazuje, że

[9] W sierpniu 2015 r. Facebook poinformował, że z serwisu korzysta 1 na 7 mieszkańców Ziemi, a liczba użytkowników logujących się do serwisu w ciągu 1 dnia przekroczyła miliard (http://www.biztok.pl/biznes/liczba-uzytkownikow-facebooka-jest-nowy-rekord_a22101).

[10] http://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

znaczna część użytkowników chce mieć wpływ na to, w jaki sposób ich dane mogą być wykorzystane.

Niezależnie od tego, jaki zakres prywatności ludzie będą chcieli zachować, określone kategorie informacji pozostaną tajemnicami. Dotyczy to np. różnego rodzaju haseł, kodów PIN i innych informacji, szczególnie takich, których ujawnienie może spowodować straty materialne. Jednostka musi przede wszystkim mieć zaufanie do bezpieczeństwa danych w sieci. Zwrócono na to uwagę w Europejskiej Agendzie Cyfrowej, gdzie za jeden z warunków rozwoju e-usług uznano bezpieczeństwo operacji w sieci i zaufanie konsumentów w tym zakresie[11]. Obawy użytkowników Internetu nadal budzą takie zjawiska, jak kradzież tożsamości oraz przypadki wycieku danych osobowych. Problemy te nie znikną, a raczej będą się powiększać.

Konsumenci mają tu jednak odpowiednie instrumenty ochrony, w postaci rozmaitych obowiązków administratorów danych osobowych i uprawnień podmiotów danych. Po wejściu w życie ogólnego rozporządzenia o ochronie danych osobowych (RODO), którego przyjęcie jest już kwestią czasu, niektóre z tych instrumentów zostaną wzmocnione (prawo usunięcia danych), zracjonalizowane (m.in. poprzez zmniejszenie liczby obowiązków, które nie mają bezpośredniego wpływu na ochronę, jak np. rejestracja danych) lub też pojawią się nowe wymogi (*privacy by design*, *privacy by default*).

Zagrożona autonomia woli

Pojawiają się jednak nowe zagrożenia dla prywatności, na które prawo może nie mieć wystarczającej odpowiedzi. Celowo odwołujemy się tu do pojęcia „prywatność", a nie tylko do ochrony danych osobowych, ponieważ podzielamy zdanie tych, którzy uważają, że zakresy prawa do prywatności i prawa do ochrony danych osobowych mają pewien wspólny zakres, ale nie do końca się pokrywają[12]. Można bowiem naruszyć prywatność jednostki nie znając jej danych osobowych. Ten aspekt chroni w pewnej części np. tajemnica telekomunikacyjna. Telefon czy SMS do abonenta w celach marketingowych stanowi naruszenie tej tajemnicy, choćby nawet abonent wywołujący nie znał tożsamości abonenta wywoływanego (art. 172 PrTelekom). Z drugiej strony, jednym z uprawnień przysługujących jednostce na gruncie prawa ochrony da-

[11] http://europa.eu/rapid/press-release_MEMO-10-200_pl.htm.

[12] Na ten temat *A. Mednis*, Prawo do prywatności a interes publiczny, Kraków 2006, s. 93.

nych jest prawo do poprawności danych, które z ochroną prywatności nie ma nic wspólnego.

Jednym z aspektów prywatności jest autonomia woli jednostki, rozumiana jako prawo do życia własnym życiem. W polskiej doktrynie takie ujmowanie prawa do prywatności jest rzadkością, prawo to bowiem często jest zawężane do ochrony tajemnicy, intymności itp.

Między innymi wspomniany już *A. Kopff* określał „*right of privacy*" jako „prawo do ochrony życia prywatnego", rozumiane jako „prawo jednostki do życia swym własnym życiem, układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[13]. Autonomia woli jako składowa prawa do prywatności częściej jednak pojawiała się w doktrynie i orzecznictwie amerykańskim[14].

Tymczasem to właśnie autonomia woli jest obszarem zagrożonym w związku z tzw. *big data*. Termin ten odnosi się do tak dużych zbiorów danych, że nie mogą być przetwarzane metodami tradycyjnymi. Oczywiście *big data* to nie tylko dane osobowe, ale nie sposób nie dostrzec oczywistych zagrożeń dla prywatności w przypadku, gdy do dużych zbiorów trafiają dane o ludziach. W dużych zbiorach dane nie tracą na wartości, wykorzystuje się je po wielokroć analizując rozmaite korelacje przy pomocy coraz bardziej skomplikowanych algorytmów. Wynikiem działania na dużych zbiorach są analizy predyktywne, czyli przewidywania określonych zdarzeń lub zachowań, tym dokładniejsze im więcej danych podlega analizie. Zasadę działania można wyjaśnić na przykładzie *Google Flu Trends*, gdzie w wyniku analizy ok. pół miliarda modeli matematycznych zidentyfikowano kilkadziesiąt rodzajów pytań do wyszukiwarki, które wskazywały na rejon, w którym pojawi się ognisko grypy. Jak piszą *V. Mayer-Schönberger* i *K. Cukier*[15], przewidywania oparte na korelacji są sercem *big data*. To zbiór danych będzie „podpowiadał" właściwe korelacje, wskazywał jakie czynniki (składowe dużego zbioru danych) występują, gdy pojawia się dane zjawisko („rezultat").

Nie sposób nie docenić pozytywnych stron takiego podejścia. Wątpliwe jest wprawdzie, czy zawsze będziemy dysponować danymi o wszystkich okolicznościach mających wpływ na dane zjawisko (to co dziś jest *big data* jutro będzie *small data*), niemniej sam fakt opierania się na tego typu analizach w od-

[13] *A. Kopff*, Koncepcja praw do intymności..., *op. cit*., s. 30.

[14] Szerzej na ten temat *A. Mednis*, Prawo do prywatności a interes publiczny..., *op. cit*., s. 57 i n.

[15] *V. Mayer-Schönberger*, *K. Cukier*, Big data. Rewolucja, która zmieni nasze myślenie, pracę i życie. Warszawa 2014, s. 80.

niesieniu do ludzkich zachowań może budzić wątpliwości co do wpływu na autonomię woli jednostki. Już dziś robi się takie analizy w sklepach internetowych: upodobania nowego użytkownika są porównywane z zachowaniami dotychczasowych użytkowników i na tej podstawie algorytm podpowiada wybór książki, płyty czy filmu. Autonomia woli nie jest zagrożona dopóki jednostka ma wybór i nie musi akceptować sugestii sprzedawcy. Gorzej, jeśli sklep na podstawie analiz np. różnicuje cenę, którą nowy użytkownik ma zapłacić i nie pozostawia mu w tej kwestii wyboru. Próbuje się już przewidywać zachowania ludzi, aby na podstawie samej analizy np. im zapobiegać. Sceny znane z filmu „Raport mniejszości" (złapanie przestępcy zanim popełni przestępstwo) być może będą kiedyś rzeczywistością, z tą różnicą, że predykcja nie będzie wynikiem przewidywania jasnowidzów, a rezultatem analizy dokonanej na dużym zbiorze zachowań podobnych osób. Innymi słowy, może dojść do ingerencji w sferę objętą wolną wolą jednostki na podstawie wskazania korelacji pomiędzy danymi dotyczącymi podobnych osób.

To również z tego powodu tak istotna jest ochrona przed profilowaniem jednostek. Prawo już od dawna pochyla się nad kwestią profilowania, ale początki regulacji tego problemu, które znajdziemy w art. 15 dyrektywy 95/46, były jedynie próbą przeciwdziałania skutkom ewentualnych błędów w danych osobowych przechowywanych w zbiorach[16]. To z tego powodu wspomniany przepis zakazuje podejmowania negatywnych decyzji dotyczących jednostek wyłącznie na podstawie automatycznego przetwarzania ich danych osobowych. Zakaz ten został powtórzony w art. 26a OchrDanychU w brzmieniu:

16 Art. 15: 1. Państwa Członkowskie przyznają każdej osobie prawo do nieobjęcia jej decyzją, która wywołuje skutki prawne, które jej dotyczą lub mają na nią istotny wpływ, oraz która oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących ją aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, zdolność kredytowa, wiarygodność, sposób zachowania itp.

2. Z zastrzeżeniem przepisów innych artykułów niniejszej dyrektywy, Państwa Członkowskie zapewniają, że każda osoba będzie mogła być wyłączona z zakresu objętego decyzją określoną w ust. 1, jeżeli decyzja taka:

a) zostanie podjęta w trakcie zawierania lub realizacji umowy, pod warunkiem że wniosek w sprawie zawarcia lub realizacji umowy, wniesiony przez osobę, której dane dotyczą, zostanie przyjęty, lub że istnieją odpowiednie sposoby zabezpieczenia jego uzasadnionych interesów, jak np. uregulowania umożliwiające mu przedstawienie swojego punktu widzenia; lub

b) zostanie dozwolona przez prawo, które określa również sposoby zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą.

„1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą, albo jeżeli zezwalają na to przepisy prawa, które przewidują również środki ochrony uzasadnionych interesów osoby, której dane dotyczą".

Zauważmy, że powyższy przepis akcentuje zakaz podejmowania „automatycznych decyzji", podczas gdy art. 15 ust. 1 dyrektywy 95/46 odwołuje się do wyniku (celu) takiej decyzji („dokonanie oceny niektórych dotyczących ją aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, zdolność kredytowa, wiarygodność, sposób zachowania itp."). Nie można tu raczej zarzucić polskiemu ustawodawcy niezgodności z dyrektywą 95/46, ponieważ przepis OchrDanychU przyznaje jednostce szerszą ochronę, z uwagi na to, że zakaz podejmowania takich decyzji jest niezależny od celu ich podjęcia. Niemniej można stwierdzić, że zakaz z art. 15 ust. 1 dyrektywy 95/46 jest *de facto* regulacją dotyczącą tworzenia profilu osoby.

Wychodząc naprzeciw wspomnianym zagrożeniom, projekt RODO zawiera definicję profilowania, przez które rozumie się jakąkolwiek formę przetwarzania danych osobowych polegającą na użyciu tych danych w celu oceny niektórych aspektów osobistych odnoszących się do osoby fizycznej, w szczególności w celu analizy lub przewidywania (ang. *predict*) aspektów dotyczących wydajności w pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, interesów, wiarygodności, zachowania, miejsca przebywania lub przemieszczania się[17]. Podmiot danych będzie miał prawo sprzeciwu wobec profilowania, ale tylko w sytuacji, gdy administrator danych będzie je przetwarzał na podstawie przesłanki realizacji zadań publicznych bądź usprawiedliwionego celu. Niezależnie od przesłanek prawo sprzeciwu będzie również przysługiwało, gdy profilowanie będzie służyło marketingowi bezpośredniemu (art. 18 ust. 1 i 2 projektu RODO). Proponuje się również powtórzenie zakazu podejmowania indywidualnych decyzji wyłącznie na podstawie automatycznego przetwarzania danych, obejmującego również profilowanie. Zakaz nie obejmowałby sytuacji, gdy owo przetwarzanie jest dokonywane w celu zawarcia i wykonywania umowy pomiędzy administratorem danych a podmiotem

[17] http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.

danych, gdy zezwala na to przepis prawa lub gdy osoba, której dane dotyczą wyraziła na to zgodę.

Te rozwiązania nie dotyczą jednak wspomnianych zagrożeń wynikających z predykcji. Jeśli bowiem osoba nie została poddana profilowaniu, ale z uwagi na podobieństwo jej cechy lub cech do profili innych osób przewiduje się jej zachowanie lub faktycznie decyduje się za nią, to niewątpliwie możemy mieć do czynienia z naruszeniem autonomii woli jednostki.

Tu zatem warto powrócić do szerokiej koncepcji prawa do prywatności, obejmującej właśnie ten aspekt. Przypomnijmy, że Konstytucja RP w art. 47 obok prawa do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia wymienia również prawo jednostki do **decydowania o swoim życiu osobistym**.

Oczywiście można się zastanawiać, czy prawodawca konstytucyjny traktuje to jako prawa odrębne czy powiązane ze sobą. Uznanie autonomii woli jednostki za element prawa do prywatności mogłoby mieć znaczenie w sferze prawa cywilnego (prywatność jako dobro osobiste). W sferze prawa administracyjnego zaś może pojawić się np. kwestia, czy predykcja będzie zawsze dotyczyć osoby zidentyfikowanej. Jeśli tak, to ewentualna decyzja podjęta wobec osoby będzie podlegała przytoczonym powyżej przepisom o ochronie danych osobowych. Jeśli jednak predykcja będzie dotyczyła osoby niezidentyfikowanej (a wydaje się to możliwe), wówczas ten aspekt nie będzie podlegał ochronie prawnoadministracyjnej.

Internet Rzeczy i anonimizacja danych

W kontekście *big data* nie sposób pominąć faktu, że źródeł danych przybywa. Po pierwsze, do sieci podłącza się coraz więcej urządzeń. Idea Internetu Rzeczy (*Internet of Things*, *IoT*), w świadomości społecznej symbolizowana przez lodówkę, która sama zamawia zakupy, to już rzeczywistość. Dziś do Internetu jest podłączonych ok. 12 mld urządzeń, Cisco szacuje, że do 2020 r. będzie ich 50 miliardów[18]. Po drugie, ludzie sami dostarczają wielu informacji i danych w sieci, używając rozmaitych aplikacji na smartfonach, smartwatchach oraz korzystając z coraz popularniejszych urządzeń typu *wearables*. Połączenie tych danych da analitykom *big data* ogromne możliwości, w tym w zakresie profilowania ludzi, a co za tym idzie, tworzenia analiz predyktywnych.

[18] http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html.

Warto w tym kontekście zwrócić uwagę na dwie kwestie prawne. Często mówi się o tym, że dane wykorzystywane w analizach są uprzednio anonimizowane. Czy jednak anonimizacja danych jest skutecznym narzędziem w batalii o zachowanie prywatności? Duża liczba informacji na temat konkretnej osoby może prowadzić do jej identyfikacji, nawet jeśli nie możemy określić imienia i nazwiska tej osoby. Identyfikacja nie polega bowiem na ustaleniu imienia i nazwiska czy adresu, tylko na możliwości wskazania tej osoby. Anonimizacja w skrócie polega na tym, że przetwarzany jest tylko taki zasób danych, który nie pozwala na wskazanie kogo dotyczą. Zazwyczaj wystarczy usunięcie właśnie imienia, nazwiska i adresu, często jednak pozostałe dane będą tak charakterystyczne, że pozwolą na identyfikację osoby, której dotyczą. Tym bardziej zatem istnieje zagrożenie, że dane zanonimizowane pochodzące z jednego źródła, połączone ze zanonimizowanymi danymi z innych źródeł, będą pozwalać na wskazanie konkretnej osoby.

Tak więc dane niepodlegające regulacjom z zakresu ochrony danych osobowych mogą w wyniku takiej operacji podlegać tym przepisom. Jednym słowem, im więcej danych tym większe prawdopodobieństwo identyfikacji jednostki. Definicja danych osobowych, jak wynika z projektu RODO, nie ulegnie zmianie, chociaż problemy z ustaleniem czy np. adres IP jest daną osobową prowokują do rozważań, czy definicja ta nie powinna zostać zmieniona w ten sposób, że danymi osobowymi byłyby wszelkie dane dotyczące osoby fizycznej, choćby nawet jej nie identyfikowały. Takie podejście utrudniłoby jednak wykorzystanie danych w analizach typu *big data*, ponieważ pomimo anonimizacji miałyby do nich zastosowanie przepisy OchrDanychU lub przyszłego RODO.

Do tego należy podnieść wątpliwości natury prawnej co do wykorzystania danych pochodzących z sektorów objętych tajemnicami? Otóż w dziedzinach tak istotnych z punktu widzenia *big data* jak bankowość, ubezpieczenia czy telekomunikacja, obowiązują tajemnice (odpowiednio: bankowa, ubezpieczeniowa i telekomunikacyjna). Specyfika tych tajemnic polega na tym, że, po pierwsze, nie dotyczą one tylko informacji o osobach fizycznych, ale również o innych podmiotach, a po drugie, ze sformułowania tych tajemnic wynika, że objęte są nimi informacje dotyczące danego klienta, nawet jeśli nie da się go zidentyfikować[19].

[19] Na ten temat *A. Mednis*, *K. Gałęzowska*, Ochrona tajemnicy bankowej w świecie „Big data", Ochrona Danych Osobowych 2015, Nr 2, s. 12.

Przykładowo, tajemnica telekomunikacyjna obejmuje:

1) dane dotyczące użytkownika;
2) treść indywidualnych komunikatów;
3) dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych, wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;
4) dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
5) dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

Katalog ten ma charakter rozłączny, a więc np. dane o lokalizacji podlegają ochronie niezależnie od możliwości identyfikacji konkretnego użytkownika.

Ułatwienie obrotu zanonimizowanymi danymi z powyższych sektorów wymagałoby zatem wyraźnego wskazania w przepisach, że tajemnicy podlegają tylko dane identyfikujące konkretnego użytkownika (klienta banku, ubezpieczającego lub ubezpieczonego).

Podsumowanie

Jeśli chodzi o ochronę prywatności i danych osobowych jesteśmy zatem w zupełnie innym miejscu niż w 1989 r. Nie startowaliśmy od zera, jednak w stosunku do państw zachodnich nie tylko mieliśmy opóźnienie technologiczne, ale brak było wówczas także świadomości wagi, jaką trzeba przywiązywać do ochrony prywatności. Być może wynikało to z przyzwyczajenia z czasów PRL, że władza wie dużo na temat obywateli. Wydaje się, że w znacznej mierze opóźnienie to nadrobiliśmy. Dziś stoimy wspólnie z innymi społeczeństwami przed zupełnie nowymi wyzwaniami, do których należy zaliczyć m.in. wspomniane analizy *big data*, profilowanie, inwigilację przez służby oraz – jak wskazał *E. Snowden* – szeroką współpracę w zakresie wymiany informacji pomiędzy służbami a biznesem. To właśnie z tego powodu być może bę-

dzie potrzebna redefinicja prawa do prywatności, poprzez położenie nacisku na aspekt autonomii woli jednostki, a także rozszerzenie pojęcia danych osobowych o takie informacje o osobach fizycznych, które ich nie identyfikują.