Maria Grzymisławska-Cybulska, Marcin Cybulski

Prawo do decydowania o zakresie i zasięgu informacji udostępnianych innym osobom na temat swojego życia w kontekście Big Data

Wprowadzenie

Rozwój technologiczny oraz będące jego naturalną konsekwencją możliwości zarządzania informacjami wydają się nieść ze sobą coraz wyraźniejsze obawy dotyczące poszanowania prawa do prywatności. Przedmiotem powszechnej troski stały się, określane mianem współczesnego wyzwania w zakresie ochrony danych osobowych, zagadnienia ze sfery zmiany sposobu zbierania rosnącej nieustannie ilości danych, dostępu do nich, ich wykorzystywania i przekazywania[1]. Jak się zauważa, w dobie postępu technologicznego i masowego korzystania z urządzeń i aplikacji mobilnych szczególnego znaczenia nabrało zagadnienie przetwarzania dużych zasobów danych (tzw. Big Data)[2]. Jednocześnie tematyka ta coraz częściej rozpatrywana jest w kontekście ochrony danych osobowych[3]. Wątpliwości rodzi także fundamentalna kwestia, jaką jest definicja terminu Big Data.

---

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku", Bruksela 2012, s. 5, www.giodo.gov.pl/plik/id_p/2619/j/pl/ (dostęp: 20 II 2014).

[2] Dzień Ochrony Danych Osobowych Rady Europy 2014, http://www.giodo.gov.pl/550/id_art/7500/j/pl/ (dostęp: 3 III 2014).

[3] W.R. Wiewiórowski, *Unia Europejska wobec ochrony danych, prywatności i bezpieczeństwa informatycznego. Aktualny stan prawny i toczące się prace legislacyjne*, referat wygłoszony podczas Konferencji „Big Data", organizator: Blue Business Media, Warszawa,

Wszystkie te obawy skłaniają do podjęcia rozważań na temat związku pomiędzy prawem do prywatności a zagadnieniem ochrony danych osobowych w kontekście przetwarzania dużych zasobów danych. W szczególności przeanalizowania wymaga, czy rozmiar przetwarzanych danych niesie jakieś swoiste ryzyko w tym zakresie.

Dlatego też w pierwszej kolejności należy rozważyć zagadnienie prawa do prywatności i gwarancji tego prawa. Następnie celowe wydaje się zdefiniowanie współczesnych zagrożeń prawa do prywatności, a ponadto dookreślenie – na potrzeby niniejszego opracowania – pojęcia Big Data i omówienie jego praktycznego znaczenia. Należy bowiem zaakcentować, że pomimo braku legalnej definicji pojęciem tym posłużyła się Rada Ministrów, podkreślając ekonomiczne i gospodarcze znaczenie przetwarzania dużych zasobów danych oraz sygnalizując obawy odnośnie do, jak się wydaje, gotowości technologicznej i przeszkód o charakterze mentalnym (w postaci niechęci do nowości), a także wątpliwości prawnych dotyczących agregacji i wykorzystania dużych zestawów danych. Stąd też zasadne wydaje się rozważenie, czy – a jeżeli tak, to jakie – swoiste zagrożenia niesie za sobą urzeczywistnienie Big Data w polskich realiach.

Przedstawione w opracowaniu wnioski uwzględniają analizę uregulowań prawnych i poglądy prezentowane w orzecznictwie Europejskiego Trybunału Praw Człowieka (ETPCz) oraz Trybunału Konstytucyjnego (TK) i polskich sądów administracyjnych. Wnioskowanie oparto również na poglądach formułowanych w polskiej doktrynie prawa. W toku badań analizie poddano opracowania literaturowe. W zakresie obejmującym próbę zdefiniowania – na potrzeby niniejszego artykułu – pojęcia Big Data były to anglojęzyczne publikacje z dziedziny ekonomii i informatyki oraz polskojęzyczne stanowiska znawców problemu.

---

11 X 2013 r., http://www.giodo.gov.pl/1520152/j/pl/ (dostęp: 10 VI 2014); W.R. Wiewiórowski, *Profilowanie osób w świecie Big Data. Możliwości techniczne v. konstytucyjne prawa i wolności*, wystąpienie podczas VI Kongresu Warsaw International Media Summit oraz towarzyszącej mu VI Konferencji „Zmiany w regulacjach i prawie Świata Telekomunikacji i Mediów", organizator: MM Conferences S.A., Warszawa, 9–10 X 2013 r., http://www.giodo.gov.pl/1520152/j/pl/ (dostęp: 10 VI 2014); W.R. Wiewiórowski, *Big data i granice personalizacji*, prezentacja podczas Dnia Ochrony Danych Osobowych w Banku BPH, organizator: Bank BPH, Warszawa, 26 IV 2013 r., www.giodo.gov.pl/503/id_art/6453/j/pl/ (dostęp: 10 VI 2014).

1. Pojęcie Big Data

Pojęcie Big Data w języku polskim utożsamiane jest z przetwarzaniem dużych zasobów danych. Takim sformułowaniem posłużono się w Załączniku do Uchwały nr 157 Rady Ministrów z dnia 25 września 2012 r. w sprawie przyjęcia Strategii Rozwoju Kraju 2020[4]. Bezspornie brak legalnej definicji pojęcia Big Data. Jak się wydaje, nie istnieje też żadna ścisła definicja tego pojęcia[5]. Istnieją jednak pewne wyznaczniki, które pozwalają przybliżyć duże zbiory danych, czyli tzw. Big Data. Znawcy problemu wśród cech charakteryzujących duże zbiory danych wymieniają duży rozmiar, wysoką zmienność i wysoką różnorodność[6] oraz istotną wartość – wskazując na „Regułę 4V" (Volume – zwiększającej się objętości danych, Variety – ich różnorodności, Velocity – zmienności i dużej szybkości pojawiania się nowych danych w czasie rzeczywistym oraz Value/Veracity – ich wiarygodności i wartości w sferze biznesowej)[7].

W literaturze przedmiotu wskazuje się, że Big Data stanowi możliwość dostępu, zbierania i przetwarzania danych zawierających szczegóły wystarczające, aby wpłynąć na procesy biznesowe silniej niż dotychczas[8]. Big Data jest również postrzegane jako związek technologii i zasobów[9], a także jako nowa generacja magazynowania danych i naturalna konsekwencja funkcjonowania czterech głównych światowych trendów, tj. faktu, iż technologia przechowywania i agregowania danych staje się coraz tańsza i wydajniejsza; Internetu rzeczy i powszechnej dostępności do mobilnych urządzeń takich jak smartfony czy tablety; cyfryzacji i popularności portali społecznościowych oraz możliwości wykorzystania tzw. chmury (*cloud computing*)[10]. Zasadne wydaje się dodanie tu jeszcze jednego globalnego trendu, a mianowicie masowej

[4] M. P. 2012, poz. 882, dalej „Uchwała".

[5] V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, New York 2013, s. 6.

[6] Ł. Bolikowski, *Granice personalizacji w świecie Big Data*, Konferencja „Prywatność w cyfrowym świecie", Warszawa, 28 I 2014 r., slajd nr 2, www.giodo.gov.pl/1520152/j/pl/ (dostęp: 10 VI 2014).

[7] D. Śpiewak, *Granice personalizacji w świecie Big Data*, Konferencja „Prywatność w cyfrowym świecie", Warszawa, 28 I 2014 r., slajd nr 2, www.giodo.gov.pl/1520152/j/pl/ (dostęp: 4 III 2014).

[8] *Big Data and Business Analytics*, ed. by J. Lebovitz, Boca Raton 2013, s. 30.

[9] B. Franks, *Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics*, New Jersey 2012, s. 24.

[10] M. Minelli, M. Chambers, A. Dhiraj, *Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses*, New Jersey 2013, s. 56.

i powszechnej archiwizacji informacji. Należy jednak zwrócić uwagę, że Big Data to nie tylko ogrom danych, liczonych obecnie w petabajtach (a więc 1024 × 1024 GB) i rosnących w postępie geometrycznym, ale również liczba dostępnych źródeł pozyskiwania tych danych i fakt, że większość z nich jest tworzona przez użytkowników. Wskazuje się bowiem, że 70% cyfrowego świata jest tworzone przez każdego z nas przy użyciu wyspecjalizowanych serwisów, np. Facebooka, Twittera czy YouTube'a[11], lub też mniej popularnych w polskich realiach: Instagramu, Google+ i Blip czy Foursquare i Flickr.

Przyjmując zatem, że Big Data to szereg pojęć i działań związanych z pozyskiwaniem, utrzymywaniem i operowaniem na danych, które definiują pojęcia omówione powyżej[12] (Volume, Variety, Velocity, Value), należy rozważyć, jaka jest rola Big Data w polskich realiach i jakie wątpliwości natury prawnej może rodzić. W tym zakresie częściowo odpowiedzi udziela uzasadnienie Uchwały.

2. Big Data w polskiej gospodarce

Jak wskazano w Uchwale, wciąż konieczne jest podnoszenie konkurencyjności polskiej gospodarki. Konkurencyjność ta powinna się opierać między innymi na wysokiej innowacyjności, wiedzy i kreatywności oraz w coraz większym stopniu na powiązaniach kooperacyjnych. Szczególną rolę w zakresie podnoszenia innowacyjności oraz konkurencyjności gospodarki Uchwała upatruje w innowacjach nietechnologicznych, które skutkować mają szybkim zdobyciem przewagi konkurencyjnej. Wśród nowych możliwości kreowania wartości gospodarczej Uchwała wymienia właśnie Big Data, zauważając jednak, że jest to nowe wyzwanie dla polskich przedsiębiorców słabo przygotowanych do tej fali zmian. Tymczasem szacuje się, że dla Polski rozwiązania Big Data to potencjał zysku na poziomie 1,9% PKB, czyli porównywalnego ze wzrostem, jaki polska gospodarka uzyskała w roku 2012[13]. Same dane również traktowane są jako cenne aktywa dla przedsiębiorców[14]. Zauważa się bowiem,

[11] T. Craig, M. Ludloff, *Privacy and Big Data*, Sebastopol 2011, s. 4.

[12] D. Śpiewak, op. cit., slajd nr 2.

[13] C. Tchorek-Helm, *Big Data i Open Data: możliwe 1,9 proc. PKB UE*, http://www.polskieradio.pl/111/1896/Artykul/1038016,Big-Data-i-Open-Data-mozliwe-19-proc-PKB-UE (dostęp: 22 II 2014).

[14] Komunikat Komisji do Parlamentu Europejskiego…, s. 5.

że *de facto* możliwe stało się wykorzystywanie przez prywatnych przedsiębiorców danych osobowych na niespotykaną dotąd skalę.

To, co staje się jednak przedmiotem szczególnej troski, to, sygnalizowana nie tylko przez Radę Ministrów, potrzeba zapewnienia stosownego poziomu bezpieczeństwa dla użytkowników zwiększonego i coraz efektywniejszego dostępu do zasobów teleinformatycznych. Budowanie zaufania do Internetu postrzegane jest bowiem jako niezwykle istotny element rozwoju gospodarczego[15]. Zauważa się, że brak tego zaufania będzie się wyrażać w powściągliwym korzystaniu z usług elektronicznych oraz z usług administracji państwowej i w konsekwencji powodować spowolnienie rozwoju gospodarczego.

W tym zakresie zwraca się szczególnie uwagę na relacje pomiędzy Big Data a ochroną danych osobowych[16]. Akcentuje się zwłaszcza konieczność przywrócenia zaufania w sferze ochrony danych osobowych. Dane te zaczynają być bowiem postrzegane jako rodzaj swoistej waluty, a co zrozumiałe, każda waluta dla zachowania swej stabilności wymaga zbudowania zaufania do niej[17].

Aby ten instrument kreowania wartości gospodarczej mógł funkcjonować prawidłowo, za konieczne uznano wprowadzenie określonych mechanizmów mających służyć realizacji gwarancji w zakresie ochrony danych osobowych. Szybki rozwój technologiczny i postępująca globalizacja postrzegane są jako impuls inicjujący działania zmierzające do przeprowadzenia reformy ram ochrony danych osobowych[18].

---

[15] Dokument Roboczy Służb Komisji z 25 I 2012 r. „Streszczenie oceny skutków towarzyszących dokumentom rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie takich danych) oraz dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych", www.giodo.gov.pl/1520142/id_art/4587/j/pl/ (dostęp: 16 II 2014).

[16] B. Marek, *Big Data i ochrona danych, prywatności: rozmowa z GIODO*, 20.01.2014 r., http://www.cyberlaw.pl/prawo/big-data-i-ochrona-danych-prywatnosci/ (dostęp: 10 II 2014).

[17] V. Reding, R. Trzaskowski, *Ochrona danych w Unii: nadszedł czas, aby podjąć decyzję*, „Dziennik Gazeta Prawna" 28 I 2014, s. B5.

[18] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie takich danych), http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF (dostęp: 14 II 2014).

Należy jednak zwrócić uwagę, że chociaż z możliwością obracania wielkoskalowymi danymi utożsamiane jest wzmożone ryzyko w sferze ochrony danych osobowych, to równocześnie podmioty zainteresowane prowadzeniem działalności gospodarczej w tej sferze podnoszą, iż wzmocnienie ochrony danych osobowych – w praktyce – stanowić może element nie do końca pożądany, bowiem stwarzający ryzyko nadmiernej uciążliwości dla przedsiębiorców obracających tymi danymi. Zauważa się przy tym, że jakkolwiek starsze pokolenia są ostrożne przy udostępnianiu swoich danych osobowych, to w przypadku młodych ludzi tylko jedna czwarta, udostępniając swoje dane osobowe, w ogóle czyta formularz zgody[19]. Stąd też celowe wydaje się określenie, na ile przetwarzanie dużych zasobów danych w swoisty, właściwy tylko sobie, sposób ingeruje w nasze prawo do prywatności. W tym celu należy dookreślić, czym jest prawo do prywatności.

3. Zagrożenia w dobie możliwości przetwarzania dużych zasobów danych

Już w pierwszych latach XXI w. wnikliwi znawcy problemu dostrzegali, że wskutek swoistej eksplozji możliwości gromadzenia i przetwarzania danych jednostka staje się nie tylko beneficjentem, ale również ofiarą nowoczesnych technik zbierania informacji[20]. W literaturze przedmiotu zwrócono jednocześnie uwagę, że prawo do prywatności jest uzależnione od osobowości jednostki oraz zmian cywilizacyjnych, które kreują zarówno zagrożenia dla prywatności, jak i nowe instrumenty ochronne[21]. Tak jak przewidywały ówczesne prognozy, obecnie zasadnicze zagrożenie związane z szybkim rozwojem technologicznym i nieograniczonym przepływem informacji upatruje się w sferze ochrony prywatności. Coraz powszechniejsza staje się świadomość, że cyberprzestrzeń kusi jedynie złudną anonimowością[22]. Jakkolwiek bowiem użycie tzw. nicka

[19] B. Rossi, *Big Data vs. Big Regulation: Will Changing the Rules Empower Consumers?*, http://www.information-age.com/industry/uk-industry/123457592/big-data-vs--big-regulation--will-changing-the-rules-empower-consumers (dostęp: 14 II 2014).

[20] M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, nr 6, s. 1.

[21] A. Sakowicz, *Prywatność jako samoistne dobro prawne (per se)*, „Państwo i Prawo" 2006, nr 1, s. 27.

[22] J. Kulesza, *Prawo do anonimowej wypowiedzi a prywatna cenzura Internetu w Polsce*, „Państwo i Prawo" 2012, nr 6, s. 1.

pozwala funkcjonować w sieci bez potrzeby ujawniania swojego imienia i nazwiska, to jednak każde działanie przeciętnie zorientowanej w cyfrowym świecie jednostki, w większości przypadków, jest możliwe do zidentyfikowania za pomocą numeru IP. Stąd też właśnie obawy dotyczące prywatności są jedną z najczęściej wskazywanych przyczyn niedokonywania przez osoby fizyczne zakupów w sieci[23].

Jak się przyjmuje, prawo do prywatności jest utożsamiane z prawem jednostki do decydowania o zakresie i zasięgu informacji udostępnianych innym osobom na temat swojego życia[24]. Niewątpliwie potencjał, jaki daje Big Data, pozbawia możliwości decydowania o zakresie i zasięgu informacji, które są udostępniane innym podmiotom. Big Data, a więc obracanie dużymi zbiorami danych, następuje *de facto* niezależnie od naszej woli. Mowa o sytuacji, gdy każdy nasz krok w cyberprzestrzeni jest śledzony. Źródłem Big Data są bowiem między innymi dane dotyczące zachowań podczas przeglądania i prowadzenia stron internetowych, tworzenia blogów, komentarzy o produktach i usługach umieszczanych na portalach społecznościowych[25]. Bardzo znamiennym przykładem wykorzystania Big Data jest przeprowadzona w Kalifornii analiza rocznych statystyk zużycia wody przez konkretne gospodarstwa domowe, na podstawie której wskazano te z nich, w których odbiega ono od normy, aby przy użyciu stosownego komunikatu wpłynąć na jego zmniejszenie[26]. Coraz więcej pozornie nieistotnych i niezwiązanych ze sobą informacji na nasz temat jest zbieranych i gromadzonych w zasobach ogólnoświatowej sieci Internet, co daje możliwość stworzenia i zaoferowania sprzedaży zainteresowanym podmiotom naszego profilu osobowego[27]. Jak wyjaśniają znawcy problemu, „tworzenie profili" oznacza automatyczne przetwarzanie danych polegające na analizie i przewidywaniu działań lub niektórych aspektów dotyczących osoby fizycznej, w szczególności na przewidywaniu i analizie m.in.

---

[23] Komunikat Komisji do Parlamentu Europejskiego…, s. 5.

[24] A. Sakowicz, *Prywatność jako samoistne dobro prawne (per se)*, za: A. Młynarska-Sobaczewska, *Wolność wirtualnej wypowiedzi*, „Państwo i Prawo" 2008, nr 2, s. 57.

[25] J. Zamora, *Big Data, czyli jak znaleźć złoto w chaosie danych*, http://www.ekonomia.rp.pl/artykul/1083096.html (dostęp: 22 II 2014).

[26] Ł. Cichy, *Życiowe zastosowanie Big Data i cloud computingu? Np. walka z suszą w Kalifornii*, http://www.computerworld.pl/news/394987/Zyciowe.zastosowanie.Big.Data.i.cloud.computingu.Np.walka.z.susza.w.Kalifornii.html (dostęp: 22 II 2014).

[27] *GIODO o Big Data: największym zagrożeniem są „małe siostry", a nie „wielcy bracia"*, http://www.polskieradio.pl/42/273/Artykul/1056917,GIODO-o-Big-data-najwiekszym-zagrozeniem-sa-male-siostry-a-nie-wielcy-bracia (dostęp: 22 II 2014).

w zakresie zdrowia osoby, jej sytuacji ekonomicznej, zachowania w pracy, preferencji lub zainteresowań osobistych[28]. Big Data daje również inne możliwości, jak informacje o położeniu użytkownika telefonu komórkowego z możliwością wskazania współrzędnych geograficznych i numeru rozmówcy[29], czy nawet rejestracji dźwięków z otoczenia przy wykorzystaniu mikrofonów telefonów komórkowych.

Tak rozumiana możliwość dostępu, zbierania i przetwarzania dużych zbiorów danych w naturalny sposób rodzi pytania o prawo do prywatności. Nie bez znaczenia w tym kontekście pozostaje to, że samo pojęcie prywatności jest trudne do zdefiniowania. Fakt ten akcentuje się zarówno w polsko-, jak i anglojęzycznych opracowaniach. W okresie braku normatywnych uregulowań w przedmiocie ochrony prywatności określenia zakresu prywatnej sfery życia dokonał Sąd Najwyższy[30], wskazując na trzy elementy: styl życia, osobiste upodobania oraz przejawy kultury obyczajowej[31]. Tymczasem każdy z tych elementów znajduje się w sferze zainteresowań podmiotów przetwarzających duże zasoby danych. To właśnie takie elementy jak nasze osobiste upodobania i prezentowany styl życia stanowią informacje, na podstawie których wyciągane są wnioski mające ogromną wartość rynkową. Oczywiście, sama tylko ta zależność nie stanowi o naruszeniu naszego prawa do prywatności. Zagadnienie staje się jednak o wiele bardziej złożone, gdy weźmie się pod uwagę, że każde działanie podejmowane w sieci jest możliwe do zidentyfikowania za pomocą numeru IP. Stąd też możliwe staje się nie tylko bieżące monitorowanie preferencji podmiotów funkcjonujących w sieci, ale również przypisanie ich z dużym prawdopodobieństwem konkretnemu spersonalizowanemu użytkownikowi – jeśli weźmiemy pod uwagę takie okoliczności, jak codzienne czy regularne logowanie się z konkretnego komputera przez osobę fizyczną, która jednocześnie swoje imię i nazwisko podaje np. na portalach społecznościowych. W ten sposób, tworząc profil osobowy obejmujący takie elementy, jak np. styl życia czy osobiste upodobania, możliwe jest ich odniesienie do

[28] W.R. Wiewiórowski, *Big Data w świecie Internetu przedmiotów*, slajd nr 15, Warszawa, 28 I 2014 r., www.giodo.gov.pl/1520204/j/pl/ (dostęp: 6 III 2014).

[29] Ł. Bolikowski, op. cit., slajd nr 3.

[30] J. Uliasz, *Prawo do prywatności osób pełniących funkcje publiczne*, „Samorząd Terytorialny" 2013, nr 3, s. 51.

[31] Wyrok Sądu Najwyższego (SN) z 8 IV 1994 r., sygn. III ARN 18/94, OSNP 1994, nr 4, poz. 55.

konkretnej, znanej z imienia i nazwiska osoby, nawet jeżeli ta osoba sama pewnych informacji nie upublicznia.

Obecnie gwarancje prawa do prywatności wywodzimy z art. 47 Konstytucji Rzeczypospolitej Polskiej[32], który stanowi, że „każdy ma prawo do ochrony prawnej życia prywatnego". Konsekwencją gwarancji wynikających z tegoż artykułu jest zawarte w art. 51 Konstytucji RP uregulowanie, w myśl którego wprawdzie można zobowiązywać jednostkę do ujawnienia informacji dotyczącej jej osoby, ale obowiązek taki może nałożyć tylko ustawa[33]. Wśród uregulowań rangi ustawowej wymienić należy natomiast Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[34] oraz Ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[35].

W doktrynie kwestią bezsporną pozostaje, że ustrojodawca, formułując treść art. 47 Konstytucji RP, posłużył się określeniami nieprecyzyjnymi. Próby dookreślenia pojęcia „życia prywatnego" podejmowano zarówno w literaturze przedmiotu, jak i w orzecznictwie Trybunału Konstytucyjnego. Konstatacja oparta na spektrum poglądów wyrażona została w ten sposób, że prywatność określana jest często mianem prawa do pozostawienia w spokoju i gwarantuje pewien stan niezależności, w którym jednostka może decydować o zakresie oraz zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu, posiadając jednocześnie prawo do zachowania w tajemnicy informacji o życiu prywatnym i ochrony danych jego dotyczących[36].

Prawo to chronione jest również na mocy art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[37]. Europejski Trybunał Praw Człowieka akcentuje, jak ważne jest, aby prawa były realne, a nie iluzoryczne. Również w odniesieniu do wspomnianej Konwencji zauważa się, że pojęcie „życia prywatnego" jest szerokim terminem niedającym się zdefiniować w sposób wyczerpujący. Jednak doprecyzowując pojęcie „życia prywatnego", ETPCz wskazuje, że oprócz imienia i nazwiska osoby jej życie prywatne i rodzinne może obejmować inne formy identyfikacji osobistej, obejmując elementy związane

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

[33] W. Skrzydło, *Komentarz do art. 51 Konstytucji Rzeczypospolitej Polskiej*, LEX nr 144797.

[34] Dz. U. 2002 Nr 101, poz. 926 ze zm.

[35] Dz. U. Nr 182, poz. 1228 ze zm.

[36] Z. Zawadzka, *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną. Problem rozstrzygania konfliktu zasad*, LEX nr 168972.

[37] Dz. U. 1993 Nr 61, poz. 284 ze zm.

z prawem osoby do jej wizerunku oraz prawo do rozwoju osobistego, a także prawo do nawiązywania i rozwijania relacji z innymi ludźmi oraz ze światem zewnętrznym[38]. ETPCz zauważa przy tym, że samo przechowywanie danych odnoszących się do życia prywatnego jednostki sprowadza się do ingerencji w rozumieniu art. 8 Europejskiej Konwencji Praw Człowieka, i podkreśla, iż fundamentalne znaczenie dla korzystania z prawa do poszanowania życia prywatnego ma ochrona danych osobowych.

Również na gruncie art. 8 Karty praw podstawowych Unii Europejskiej[39] oraz art. 16 Traktatu o funkcjonowaniu Unii Europejskiej[40] gwarantowana ochrona danych jest ściśle powiązana z ochroną życia prywatnego[41].

Już pobieżna analiza obowiązujących przepisów obrazuje doskonale fakt, że koncepcja ochrony danych jest pochodną ochrony prywatności[42]. Sama potrzeba ochrony danych osobowych ewoluuje od lat siedemdziesiątych XX w., bowiem wraz z upowszechnieniem stosowania komputerów i pojawieniem się nowych możliwości zbierania, zapisywania, przetwarzania i udostępniania danych osobowych sama informacja stopniowo zaczęła zyskiwać istotną i stale zwiększającą się wartość gospodarczą[43]. Z biegiem czasu zwrócono natomiast uwagę, że potrzeba zapewnienia odpowiednich zabezpieczeń chroniących dane osobowe rośnie, jeśli są one poddawane automatycznemu przetwarzaniu[44].

---

[38] Wyrok ETPCz z 4 XII 2008 r. w sprawie *S. Marper v. Wielka Brytania*, nr 30562/04, LEX nr 468452.

[39] Karta praw podstawowych Unii Europejskiej z dnia 12 XII 2007 r. (Dz. Urz. UE C 303 z 14 XII 2007 r., s. 1).

[40] Traktat o funkcjonowaniu Unii Europejskiej z dnia 25 III 1957 r. (Dz. Urz. UE 2012 C 326, s. 1), dalej „TFUE".

[41] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych, s. 7, www.giodo.gov.pl 1520142/id_art/4587/j/pl/ (dostęp: 21 II 2014).

[42] M. Safjan, op. cit., s. 7.

[43] J. Sobczak, *Komentarz do art. 16 Traktatu o funkcjonowaniu Unii Europejskiej*, w: *Traktat o funkcjonowaniu Unii Europejskiej*. Komentarz. T. I. Art. 1–89, pod red. D. Miąsika, N. Półtorak, A. Wróbla, LEX nr 124530.

[44] A.M. Nowicki, *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, LEX nr 159858.

4. Współczesne problemy orzecznicze

Szczególnie wartościowym źródłem informacji na temat naruszeń w sferze ochrony danych jest bez wątpienia orzecznictwo sądowe. Analiza problemów, które pojawiły się na gruncie rzeczywistych stanów faktycznych, w sposób konkretny obrazuje problemy i pozwala zdefiniować potrzeby w sferze ochrony danych. Zważywszy na przedmiot problemu, analizie poddano orzeczenia ETPCz oraz sądów administracyjnych.

ETPCz zwraca uwagę, że ryzyko wyrządzenia szkody stwarzane przez treści znajdujące się w Internecie oraz przez komunikację internetową dla wykonywania i korzystania z praw i wolności człowieka, zwłaszcza prawa do poszanowania życia prywatnego, jest szczególne, dlatego też korzystanie z materiałów publikowanych w Internecie, aby zapewnić ochronę i wspieranie praw i wolności człowieka, musi zostać dostosowane do szczególnych cech tej technologii[45]. Innym problemem stanowiącym przedmiot rozważań ETPCz było określenie charakteru rozmów telefonicznych wykonywanych z aparatu znajdującego się w miejscu pracy oraz zasad korzystania z poczty elektronicznej i Internetu w kontekście ich monitorowania przez pracodawcę[46]. W świetle poszanowania prawa do prywatności rozpatrywano zagadnienie niejawnej kontroli za pomocą urządzenia GPS oraz przetwarzania i wykorzystywania uzyskanych danych[47]. W odniesieniu do stanu faktycznego zaistniałego na gruncie sprawy *Uzun v. Niemcy* wskazano, że analogicznie jak gromadzenie i dalsze wykorzystanie próbek głosu i wizerunku, pozyskiwanie danych geolokalizacyjnych, ich systematyzowanie i dalsze wykorzystywanie w powiązaniu z konkretną osobą stanowi przetwarzanie danych osobowych, które może być bezprawne[48].

Trybunał Konstytucyjny zwraca uwagę na ten aspekt ingerencji w prawo do prywatności, który wiąże się z faktem, że wolność od ingerencji w prywatność (art. 47 Konstytucji) nie ma charakteru absolutnego, a granice jej dopuszczalnego ograniczenia może regulować tylko ustawa[49]. Uwagę zwraca jednak fakt, iż zasadnicze aspekty konstytucyjnych

[45] Wyrok ETPCz z 16 VII 2013 r. w sprawie *Węgrzynowski i Smolczewski v. Polska*, skarga nr 33846/07, LEX nr 1335404.

[46] Wyrok ETPCz z 3 IV 2007 r. w sprawie *Copland v. Wielka Brytania*, skarga nr 62617/00, LEX nr 527588.

[47] Wyrok ETPCz z 2 X 2010 r. w sprawie *Uzun v. Niemcy*, skarga nr 35623/06, LEX nr 599284.

[48] A. Lach, *Glosa do wyroku ETPC z dnia 2 września 2010 r., 35623/05*, LEX nr 132399.

[49] Wyrok TK z 29 X 2013 r., sygn. U 7/12, www.trybunal.gov.pl (dostęp: 10 VI 2014).

gwarancji prawa do prywatności były przedmiotem rozważań Trybunału w latach minionych.

Przegląd orzeczeń sądów administracyjnych pozwala na wysnucie wniosku, że w praktyce prowadzone są postępowania w przedmiocie udostępnienia informacji dotyczących autorów wpisów opublikowanych w dziennikach internetowych. Wnioskodawca domagał się od Generalnego Inspektora Ochrony Danych Osobowych (GIODO) nakazania udostępnienia informacji dotyczących osoby, która prowadziła wskazany blog i dokonała wskazanych przez wnioskodawcę wpisów, w tym zwłaszcza jej imienia i nazwiska, adresu, adresu e-mail lub innych danych pozwalających na identyfikację tej osoby, tj. adresów IP, z których zalogowano się do blogu i dokonano wskazanych wpisów. W tym przypadku sąd administracyjny, uwzględniając uzasadnienie złożonego wniosku, czyli zamiar skorzystania z drogi postępowania cywilnego, zwrócił uwagę na potrzebę wyważenia racji i interesów z jednej strony wnioskodawcy, a z drugiej strony osoby, której dane dotyczą, mającej objęty ochroną prawną interes, aby jej dane nie były przetwarzane bez jej zgody[50]. Jednocześnie Naczelny Sąd Administracyjny stanął na stanowisku, że rozróżnienia wymaga sytuacja podmiotu dążącego do ochrony dóbr osobistych przez zamiar wytoczenia powództwa cywilnego[51] oraz podmiotu, który wytoczył już powództwo[52]. W analogicznych okolicznościach, tj. żądania nakazania udostępnienia danych autorów wpisów na forum internetowym, sąd zwrócił uwagę, że nie jest możliwe przyjęcie stanowiska, które prowadziłoby do wydawania adresów IP komputerów użytkowników internetowych forów dyskusyjnych każdemu podmiotowi, który wystąpi o udostępnienie mu danych, tylko na podstawie jego zapewnienia, iż są mu one potrzebne do dochodzenia roszczeń na drodze sądowej[53].

W orzecznictwie sądowoadministracyjnym zauważa się również, że coraz więcej pytań o prawny zakres ingerencji w prywatność osób fizycznych rodzi korzystanie z monitoringu i warunki, jakie systemy monitorujące powinny spełniać, bowiem skutkiem stosowania monitoringu

[50] Wyrok Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie z 15 I 2014 r., sygn. II SA/Wa 1082/13, www.nsa.gov.pl (dostęp: 12 III 2014).

[51] Wyrok Naczelnego Sądu Administracyjnego (NSA) z 28 I 2011 r., sygn. I OSK 1214/10, www.nsa.gov.pl (dostęp: 12 III 2014).

[52] Wyrok NSA z 29 V 2012 r., sygn. II OSK 417/11, www.nsa.gov.pl (dostęp: 12 III 2014).

[53] Wyrok WSA w Warszawie z 8 III 2012 r., sygn. II SA/Wa 2821/11, www.nsa.gov.pl (dostęp: 12 III 2014).

może być utrwalanie wizerunku osób fizycznych, a następnie jego przechowywanie, opracowywanie i wykorzystywanie do różnych celów[54].

Wśród aktualnych problemów wskazać można także monitorowanie pracowników. W jednym z wyroków wojewódzki sąd administracyjny zwrócił uwagę, że oprogramowanie zbierające informacje o połączeniach pomiędzy siecią wewnętrzną pracodawcy a siecią publiczną – tj. takie, które pozwala na sprawdzenie wykazu odwiedzanych stron internetowych, czasu zainicjowanych połączeń, adresów stron lub plików, z którymi nastąpiło połączenie – musi spełniać wymogi zgodności z prawem, usprawiedliwionego celu, proporcjonalności, transparentności oraz uwzględniać przepisy o ochronie danych osobowych. Podkreślono przy tym, że wymóg transparentności oznacza, iż pracownicy powinni mieć świadomość, że są poddawani monitoringowi, a zasady monitoringu zostały im przedstawione i szczegółowo określone[55].

5. Przetwarzanie dużych zasobów danych a ochrona baz danych

W Strategii Rozwoju Kraju 2020 wyrażono przekonanie o słabym przygotowaniu polskich przedsiębiorców do korzystania z nowych możliwości kreowania wartości gospodarczej, jakie daje między innymi przetwarzanie dużych zasobów danych. Dlatego też warto przyjrzeć się, jakie aspekty natury prawnej będą zobowiązani uwzględniać przedsiębiorcy, którzy za przedmiot działalności przyjmą Big Data.

W pierwszej kolejności należy zwrócić uwagę na Ustawę z dnia 27 lipca 2001 r. o ochronie baz danych[56]. Ustawa ta definiuje pojęcie bazy danych, stanowiąc, że baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości. Jednocześnie ustawodawca ustala, że producentem bazy danych jest podmiot, który ponosi ryzyko

[54] Wyroki WSA w Warszawie: z 8 X 2013 r., sygn. II SA/Wa 977/13; z 9 IV 2013 r., sygn. II SA/Wa 211/13, www.nsa.gov.pl (dostęp: 12 III 2014).

[55] Wyrok WSA w Warszawie z 6 VI 2012 r., sygn. II SA/Wa 453/12, www.nsa.gov.pl (dostęp: 12 III 2014).

[56] Dz. U. Nr 128, poz. 1402 ze zm., dalej „ustawa o ochronie baz danych".

nakładu inwestycyjnego przy jej tworzeniu. Przepisy ustawy o ochronie baz danych stanowią też, że producentowi bazy danych przysługuje wyłączne i zbywalne prawo pobierania danych i wtórnego ich wykorzystania. Samo natomiast pojęcie „pobierania danych" w piśmiennictwie rozumiane jest między innymi jako przeglądanie zawartości baz danych, ściągnięcie bazy na twardy dysk[57].

Analiza powyżej przytoczonych przepisów prowadzi do wniosku, że ustawodawca reguluje ustawą o ochronie baz danych zagadnienia dotyczące zbiorów danych lub jakichkolwiek innych materiałów i elementów – zgromadzonych według określonej systematyki lub metody. W odniesieniu do danych ustrukturalizowanych zwraca się uwagę na specyfikę, jaką charakteryzują się rejestry państwowe. Jak zauważają znawcy problemu, zsumowanie informacji z wielu rejestrów państwowych i zastosowanie zaawansowanych mechanizmów przetwarzania pozwala na bardzo dokładne spersonalizowanie profilu dowolnego obywatela, co stanowi, w oczywisty sposób, ingerencję w jego prywatność[58]. Należy jednak zwrócić uwagę, że Big Data oznacza również obrót danymi nieustrukturalizowanymi. Analizie podlegają wszystkie informacje dotyczące określonego zagadnienia, produktu czy usługi. Można powiedzieć, że na Big Data składają się zarówno dane ustrukturalizowane – podlegające reżimowi ustawy o ochronie baz danych, upubliczniane i o dostępie ograniczonym, jak i dane o nieokreślonej strukturze, a więc wszystkie informacje, które dotycząc określonego zagadnienia (usługi, produktu), pojawiły się w zasobach ogólnoświatowej sieci Internet, m.in. na forach internetowych, w mediach społecznościowych bądź na stronach i portalach internetowych.

6. Ochrona danych a postęp technologiczny i globalizacja

Jakkolwiek coraz powszechniejsze staje się przekonanie, że ujawnianie danych stało się częścią współczesnego życia, to równocześnie – jak pokazują badania – ponad 70% Europejczyków obawia się, że ich dane mogą zostać wykorzystane niezgodnie z celem, w jakim zostały zgromadzone, a 43% użytkowników sieci Internet uważa, że żądano od nich ujawnienia bardziej osobistych informacji, niż wymagało tego

[57] P. Litwiński, *Obrót prawny bazami danych osobowych*, „Przegląd Prawa Handlowego" 2003, nr 9, s. 48.

[58] D. Śpiewak, op. cit., slajd nr 11.

korzystanie z serwisów *on-line*[59]. Poczucie braku kontroli nad danymi i jednoczesne rozdrobnienie przepisów regulujących ochronę danych w poszczególnych państwach członkowskich Unii Europejskiej skutkujące niepewnością prawną postrzega się jako swoiste bariery dla przedsiębiorców[60], a równocześnie jako impuls inicjujący zmiany w sferze ochrony danych w UE.

Podstawowym unijnym dokumentem regulującym problematykę ochrony danych osobowych jest Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[61], która weszła w życie 13 grudnia 1995 r. Przyjęto, że systemy przetwarzania danych są tworzone po to, aby służyć człowiekowi, i muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności, a szczególnie prawo do prywatności, oraz przyczyniać się do postępu gospodarczego i społecznego, rozwoju handlu i dobrobytu jednostek. Państwa członkowskie zobowiązały się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych[62].

Jakkolwiek cele obowiązującej Dyrektywy 95/46/WE – będącej głównym instrumentem prawnym w zakresie ochrony danych osobowych w Europie[63] – pozostawały aktualne, to, jak się wydaje, nie uwzględniała ona w pełni współczesnych możliwości i zagrożeń. Istniejące realia technologiczne i gospodarcze sprawiają, że omawiane przepisy nie odpowiadały w pełni istniejącym potrzebom. Taka sytuacja zrodziła potrzebę zmodernizowania przepisów. Dlatego też w 2012 r. przyjęty został pakiet zmian regulacji UE w zakresie ochrony danych, w tym wniosek dotyczący rozporządzenia zawierającego ogólne regulacje w zakresie ochrony danych oraz wniosek dotyczący dyrektywy zawierającej szczególne regulacje dotyczące ochrony danych dla sektora odpowiedzialnego za egzekwowanie prawa[64].

---

[59] Special Eurobarometer nr 359 – „Attitudes on Data Protection and Electronic Identity in the European Union", http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (dostęp: 7 III 2014).

[60] Dokument Roboczy Służb Komisji z 25 I 2012 r., op. cit.

[61] Dz. Urz. UE L 281 z 23 XI 1995 r., dalej „Dyrektywa 95/46/WE".

[62] Art. 1 ust. 1 Dyrektywy 95/46/WE.

[63] Komunikat Komisji do Parlamentu Europejskiego…, s. 5.

[64] http://www.giodo.gov.pl/1520142/id_art/4587/j/pl/ (dostęp: 10 III 2014).

Koncentrując się na potrzebach podmiotów prowadzących działalność gospodarczą, należy wskazać, że przyjęto, iż rozporządzenie ma zagwarantować przedsiębiorcom, w szczególności mikroprzedsiębiorcom oraz małym i średnim przedsiębiorcom, pewność prawną. Jednocześnie zachęca się instytucje i organy Unii, państwa członkowskie i ich organy nadzorcze, aby wzięły pod uwagę mikroprzedsiębiorców oraz małych i średnich przedsiębiorców w przypadku zastosowania rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych[65]. Wyjaśniono również, że aby stwierdzić, czy przetwarzanie można uznać za „monitorowanie zachowania", należy się upewnić, czy osoby fizyczne można wyszukać w Internecie, korzystając z technik przetwarzania danych, które polegają na przypisaniu „profilu" danej osobie fizycznej[66].

Ze szczególnym odniesieniem do wielkoskalowych zbiorów danych, akcentuje się potrzebę przeprowadzenia przez podmiot przetwarzający oceny skutków w zakresie ochrony danych przed przetwarzaniem, przy czym ocena taka powinna obejmować między innymi przewidywane środki i mechanizmy mające służyć zapewnieniu ochrony danych osobowych[67]. Obowiązek dokonania oceny skutków przewidywanych operacji w zakresie ochrony danych wiązany jest zwłaszcza z tymi operacjami przetwarzania, które stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z powodu ich charakteru, zakresu lub celów[68].

Podsumowanie

Obserwowana informatyzacja, globalizacja i postęp technologiczny powodują, że wrażenie, jakie robi na nas współczesny poziom rozwoju, przekłada się na terminologię, którą się posługujemy na określenie poszczególnych zmian. Tymczasem to, co jeszcze nie tak dawno wydawało

[65] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych…, s. 21.

[66] Ibidem, s. 23.

[67] Ibidem, s. 32.

[68] Art. 33 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie takich danych, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF (dostęp: 14 II 2014).

się utopią, powszednieje i staje się rozwiązaniem codziennego użytku. Stąd też wrażenie, jakie wywołują dzisiejsze możliwości przetwarzania dużych baz danych, czynią zapewne zasadnym określenie ich mianem „Big Data". Jest to pojęcie, którym posługują się centralne organy administracji publicznej, znawcy problemu oraz podmioty obrotu gospodarczego. Należy mieć jednak świadomość, że w ciągu kilku lat określenie to może nabrać innego znaczenia, a obecne – jak by się mogło wydawać – spektakularne możliwości w zakresie przetwarzania danych zastąpią inne, nowocześniejsze rozwiązania.

Dlatego też odwołując się do opracowań naukowych oraz prezentowanych w nich poglądów, należy brać pod uwagę nie tylko ewolucję uregulowań prawnych, ale również wpływ rozwoju technologicznego i jego stan na datę publikacji poszczególnych opracowań. Jakkolwiek bowiem pewne tezy pozostają aktualne, to część sformułowań z biegiem lat traci dotychczasowe znaczenie i nabiera zmienionego sensu. Weźmy jako przykład telefon, który – jak wielu z nas jeszcze pamięta – był urządzeniem nie tak powszechnie dostępnym, ściśle związanym z miejscem, którego warunki techniczne pozwalały na nawiązanie połączeń z innymi użytkownikami tych aparatów, którzy także przebywali w ściśle określonym miejscu, w którym połączenia należało się spodziewać. Dzisiaj telefon to praktycznie smartfon, którego użytkowanie w zasadniczy sposób odbiega od możliwości, jakie dawały telefony stacjonarne. Stąd też zupełnie inaczej należałoby interpretować pojęcie „rozwoju technicznego" i tezy formułowane w monografii z 1974 r.[69], a zupełnie inaczej to samo pojęcie i tezy formułowane w rzeczywistości 2014 r.

Powyższe ustalenia należy mieć na względzie o tyle, że podobnie, jak się wydaje, należałoby postrzegać Big Data – dziś sprowadzające się do przetwarzania dużych baz danych. Jak każde nowe rozwiązanie, tak i Big Data wiąże się z wieloma obawami i zagrożeniami. Trzeba jednak zwrócić uwagę, że obecnie Big Data nie niesie ze sobą swoistych – właściwych tylko temu rozwiązaniu – zagrożeń. Przynajmniej dzisiaj brak podstaw, by takie swoiste zagrożenia wskazać. Co jest bezsporne, to fakt, że skala zagrożeń, które co do zasady wiążą się z przetwarzaniem danych, w przypadku Big Data jest nieporównywalnie większa. Jest to zrozumiałe, zważywszy na rozmiar przetwarzanych danych. Zaakcentować jednak trzeba, że działanie instytucji operujących Big Data nie

[69] F. Budziński, *Formy i geneza postępu technicznego*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 1974, nr 3, s. 52.

jest działaniem na szkodę jednostki, ale pozwala opisywać nieoczywiste zależności między zbiorami danych na potrzeby rozwoju społecznego, biznesowego, naukowego i działań proekologicznych, z pominięciem ujęcia indywidualnego i odwołań do jednostki opisywanej z imienia i nazwiska. Stąd też trafnie Rada Ministrów upatruje w przetwarzaniu dużych baz danych szansę na wzrost rozwoju gospodarczego. Należy jednak zwrócić uwagę, że te oczekiwania będą mogły się urzeczywistnić tylko wtedy, gdy jednocześnie ustawodawca będzie monitorował na bieżąco ewolucję rozwoju technologicznego i będzie nadążał za nim, aby eliminować istniejące i zapobiegać potencjalnym zagrożeniom. Na ustawodawcy ciąży wszakże jeszcze jeden obowiązek: edukowania społeczeństwa, tak aby lęk przed nowościami – takimi jak tytułowe Big Data – czy też wykluczeniem cyfrowym nie zniechęcały przedsiębiorców do podejmowania ciekawych inicjatyw, które przecież przekładają się na rozwój społeczeństwa. Aby było to możliwe, konieczne jest z jednej strony tworzenie rozwiązań stanowiących skuteczną broń przed potencjalnymi naruszeniami naszych praw, w tym prawa do prywatności. Z drugiej jednak strony konieczne jest podejmowanie działań, które spowodują, że jednostki świadomie będą funkcjonowały w cyfrowej rzeczywistości, nie upatrując zagrożeń tam, gdzie ich nie ma, i zachowując czujność tam, gdzie jest to konieczne.

Stosowne działania w tej mierze podejmowane są na poziomie prawa unijnego. Wciąż oczekujemy na ich wdrożenie, należy jednak stwierdzić, że przyjęte już założenia powinny pozwolić na uwzględnienie tak istotnych kwestii jak utworzenie regulacji odpowiadających istniejącym potrzebom i uwzględniających w pełni współczesne możliwości i zagrożenia.

THE RIGHT TO DECIDE UPON THE SCOPE OF INFORMATION AND THE RANGE OF RECIPIENTS PERSONAL DATA AVAILABLE TO THIRD PARTIES IN THE CONTEXT OF THE BIG DATA

Summary

The technological development and naturally flowing from it possibilities of managing information generate increasing anxiety regarding the right to confidentiality of private information and its protection. In this age of considerable technological progress combined with mass access to mobile applications, big data processing has become of particular significance. A substantial economic significance of data processing was also stressed in ordinance No. 157 of the Council of Ministers held

on 25 September 2012 on the adoption of the Country's Development Strategy 2020. Acknowledging the economic importance of big data processing, the Council of Ministers seemed to recognise the potential obstacles to its advancement due to still prevailing in Poland insufficient technological development, unsatisfactory equipment and mental resistance to change and novelty, and expressed doubts concerning aggregation and use of big data sets.

Thus this paper aims to determine whether, and if, then what kind of threats may arise from the implementation of Big Data processing in Polish reality. In order to do that, the concept of Big Data needed first to be given a precise definition. Strangely enough, there is no such notion in Polish legal terminology despite the fact that the term has been used by central administrative bodies and theorists of the subject. Next the very issue of Big Data with a particular emphasis of the right to privacy and a guarantee of its protection is discussed. Since data protection derives from the protection of privacy, an attempt was also made to identify the current judicial problems related to personal data protection based on the analysis of the decisions delivered by the European Court of Human Rights, the Constitutional Court (Trybunał Konstytucyjny) and the Supreme Administrative Court (Naczelny Sąd Administracyjny) as well as regional administrative courts.

Keywords: Big Data – big data base processing – right to privacy – data protection