Małgorzata Olszewska*

Prawne zasady dotyczące plików cookies a ochrona danych osobowych użytkownika Internetu

Spis treści

Streszczenie

Celem opracowania jest wskazanie wzajemnej relacji uregulowań prawnych zawartych w przepisach o ochronie danych osobowych oraz prawie telekomunikacyjnym w odniesieniu do podstaw legalnego wykorzystywania oprogramowania instalowanego na urządzeniach użytkowników (nazywanego „ciasteczkami" lub „cookies"). Przedmiotem artykułu jest wskazanie regulacji prawnych w tym obszarze w kontekście reformy ram prawnych Unii Europejskiej dotyczących ochrony danych osobowych, ze szczególnym zwróceniem uwagi na sposób wykonania obowiązków informacyjnych oraz pozyskania zgód przez obowiązanych do tego dostawców usług.

Słowa kluczowe: dane osobowe; cookies; Internet; dostęp; informacja.

JEL: K23

I. Wprowadzenie

Bezdyskusyjnym faktem jest, że rozwój łączności elektronicznej, w szczególności sieci Internet, daje co prawda wszystkim użytkownikom nowe możliwości, jeśli chodzi o dostęp zarówno do wiedzy, jak i do różnego rodzaju usług, ale stwarza także wiele zagrożeń. Z tych też powodów jednym z podstawowych celów prawodawstwa Unii Europejskiej stało się zapewnienie odpowiedniego poziomu bezpieczeństwa w sieci użytkownikowi usług telekomunikacyjnych oraz usług świadczonych drogą elektroniczną. Cel ten nie tak łatwo osiągnąć choćby z tego powodu, że wraz z rozwojem baz danych i możliwości elektronicznego przetwarzania informacji ustała naturalna ochrona w postaci technicznych granic możliwości kojarzenia różnych danych dotyczących poszczególnych osób (Lewiński, 2008, s. 9).

* Doktorantka Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego; e-mail: m.olszewska@mmiproconnect.pl

Zapewnienie bezpieczeństwa danych osobowych w Internecie dotyczy także urządzeń, z których użytkownik korzysta na co dzień. Na gruncie prawa krajowego problematyki tej dotyczą przepisy ustawy – Prawo telekomunikacyjne[1] (dalej: pt), która reguluje zagadnienie związane z dostępem do informacji znajdujących się w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego (dalej: urządzenie użytkownika). Kwestia ta niewątpliwie wiąże się również z zagadnieniem podstaw prawnych przetwarzania danych osobowych, uregulowanym w ustawie o ochronie danych osobowych[2], w której pojęcie przetwarzania (danych osobowych w rozumieniu ustawy) rozumiane jest w sposób szerszy niż w dokumentach prawnomiędzynarodowych i w języku potocznym (Szpor, 1999, s. 2).

W literaturze wiele miejsca poświęca się zagadnieniom ochrony danych osobowych w środkach komunikacji elektronicznej, które rodzą szereg problemów zarówno teoretycznych, jak i praktycznych (Adamski, 2007, s. 1). Zagadnienie to należy rozpatrywać bez wątpienia w aspekcie prawa do prywatności oraz ochrony tzw. prywatności informacyjnej, na którą składa się uprawnienie jednostki do kontrolowania treści i obiegu informacji, które tej jednostki dotyczą (Mednis, 2002, s. 61). Za punkt wyjścia można przyjąć pogląd Trybunału Konstytucyjnego, zgodnie z którym ochrona życia prywatnego, gwarantowana konstytucyjnie w art. 47 Konstytucji RP, obejmuje także autonomię informacyjną rozumianą jako prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeżeli znajdują się w posiadaniu innej osoby[3]. Co więcej, jak podkreśla się w literaturze prezentującej poglądy nauki prawa, cała koncepcja nowoczesnego podejścia do sfery autonomii informacyjnej przyjmuje za punkt wyjścia ochronę wszelkich danych osobowych i kryterium zgody jako podstawową przesłankę legalności ich ujawniania (Safjan, 2002, s. 223). Wskazuje się także, że prawo do posiadania wszystkich informacji dotyczących osoby – składających się na jej tożsamość informacyjną – może przysługiwać wyłącznie temu, którego one bezpośrednio dotyczą (Piotrowski, 2016, s. 17). Postrzeganie skutecznej ochrony danych osobowych użytkownika Internetu nabiera zatem wymiaru dalece wykraczającego poza klasyczny zakres danych, ewoluując w kierunku ochrony tożsamości osoby, której te dane dotyczą w powiązaniu z ochroną prywatności informacyjnej. Dotyczy to także kwestii dostępu do informacji znajdujących się w urządzeniu użytkownika poprzez instalowanie w nich plików cookies. Osoby fizyczne korzystające z usług internetowych można łatwo identyfikować na podstawie identyfikatorów plików cookies. Mogą one zostawiać ślady, które, w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskanymi przez serwery, mogą być wykorzystywane do tworzenia profili poszczególnych osób i ich identyfikacji. Jednakże wskazane wyżej numery identyfikacyjne, dane dotyczące lokalizacji, identyfikatory internetowe lub inne szczególne czynniki jako takie niekonieczne muszą być uważane za dane osobowe w każdych okolicznościach. Zagadnienie to nie jest w sposób precyzyjny i jednoznaczny uregulowane w przepisach prawa ani unijnego, ani polskiego.

Jak wskazuje doktryna, cechę prywatności nabywają dzisiaj, zwłaszcza w obliczu możliwości, jakie przyniosła ze sobą nowoczesna technika informatyczna, właściwie wszelkie już dane (informacje) dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby, dane „z różnych

[1] Ustawa z 16.07.2004 r. - Prawo telekomunikacyjne (Dz.U. 2016, poz. 1489 z późn. zm.).

[2] Ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. 2016, poz. 922).

[3] Wyr. TK z 19.2.2002 r., U 3/01, OTK-A 2002, Nr 1, poz. 3.

dziedzin życia", o ile istnieje możliwość powiązania ich z oznaczoną osobą (Barta 2015, s. 143). Warto w tym miejscu wspomnieć o orzeczeniu Sądu Najwyższego, w którym sąd ten wskazał, że prawnej ochronie podlega nazwa czy pseudonim internetowy (nick) użytkownika, którym posługuje się on biorąc udział choćby w aukcjach internetowych[4]. SN podkreślił, że nazwa indywidualizuje osobę, która korzysta z serwisu aukcyjnego, składa ofertę, jest stroną konkretnej umowy sprzedaży, wystawia lub otrzymuje komentarz określonej treści, prowadzi korespondencję z innymi użytkownikami. Niekiedy już samo wzięcie udziału w aukcji przez użytkownika posługującego się konkretną nazwą może stanowić źródło informacji dla pozostałych uczestników, którzy wiedzą, że dany użytkownik zwykle bierze udział w aukcjach danego typu, licytuje tylko do pewnej kwoty, tylko w określone dni, w określony sposób, nie konkuruje z użytkownikami posługującymi się określonymi nazwami, że użytkownik ten jest rzetelny, sprawnie i bezzwłocznie przeprowadza transakcje itp. Z pewnością można powiedzieć, że nazwa użytkownika identyfikuje konkretną osobę fizyczną. W stanowisku tym sąd zauważył zatem problem dotyczący klasyfikacji danych osobowych, a także okoliczność, iż tworzą one niezamknięty zbiór.

Powyższe tezy należy odnieść również do sytuacji, w której następuje ingerencja w urządzenie użytkownika, aczkolwiek nie w sposób bezwzględny, ponieważ prawodawcy zarówno unijny, jak i krajowy zdecydowali o pewnych, prawnie dopuszczalnych przypadkach takiej ingerencji.

Za punkt wyjścia do dalszych rozważań należy przyjąć pogląd, zgodnie z którym rozwój technologii i aplikacji związanych z Internetem szczególnie osłabiają ochronę prywatności, a co za tym idzie ochronę naszych danych osobowych, przede wszystkim z uwagi na zjawiska, za którymi nie nadąża prawo (Konarski 2002, s. 118). Taka właśnie sytuacja wystąpiła w związku z próbą prawnego uregulowania problemu ingerencji w urządzenia użytkowników poprzez instalowanie na nich plików cookies. Regulacja taka została podjęta przez ustawodawcę unijnego, a następnie krajowego. Uregulowania te uwzględniają fakt, iż „przeciętny" użytkownik nie zdaje sobie sprawy z ilości danych pozostawianych przez siebie podczas każdej sesji w Internecie, których zresztą nie sposób definitywnie skasować (Brzozowska, 2012, s. 39).

Na przestrzeni ostatnich lat nastąpiła istotna zmiana w podejściu prawodawcy do dopuszczalności dostępu do informacji już przechowywanej w urządzeniu użytkownika. Obecnie czynności te uzależnione są włącznie od zgody użytkownika. Aczkolwiek szersza ocena tych regulacji jest uzasadniona choćby z tego powodu, że analizy dotyczące zachowań użytkowników urządzeń na podstawie uzyskanych danych o nich, czy informacji wygenerowanych za pośrednictwem ich urządzeń, mogą być użyteczne dla wielu firm i podmiotów, które prowadzą działalność gospodarczą w Internecie. Użytkownicy urządzeń nie mają często świadomości, że takie dane są pozyskiwane wyłącznie wskutek samej ich aktywności w Internecie, takich jak choćby zakupy, bez konieczności bardziej konkretnych działań związanych wprost z udostępnianiem danych.

Innym źródłem zagrożeń, jak już wcześniej wspomniano, jest to, iż dostęp do informacji znajdujących się na urządzeniu użytkownika może prowadzić do jego profilowania czy wręcz śledzenia jego aktywności w Internecie. W tym miejscu warto wskazać, że pierwsze działania zmierzające do wzmocnienia ochrony konsumentów w Internecie podjęła Rada Europy już w 2010 r., kiedy Komitet Ministrów Rady Europy przyjął rekomendację w sprawie ochrony osób w związku

[4] Wyr. SN z dnia 11 marca 2008 r. sygn. akt II CSK 539/07.

z automatycznym przetwarzaniem danych podczas tworzenia profili[5]. Już wówczas, ponad 7 lat temu, w przedmiotowej rekomendacji zwrócono m.in. uwagę na nieprzejrzystość czy nawet „niewidzialność" profili, co powoduje, że kategoryzowanie użytkowników odbywa się bez ich wiedzy i oznacza poważne zagrożenia dla praw konsumentów i wolności obywateli.

W tej sytuacji powstaje zasadnicze pytanie, czy dla ochrony konsumenta wystarczające jest wyrażenie przez niego zgody na przetwarzanie jego danych i wgląd do nich. Zwłaszcza dotyczy to sytuacji, gdy rozwiązania technologiczne umożliwiają dostawcy usług umieszczanie w urządzeniu, bez wiedzy ich użytkownika, różnego rodzaju oprogramowania. Umożliwia ono nie tylko dostęp do informacji zgromadzonej w tym urządzeniu, ale może prowadzić właśnie do śledzenia aktywności użytkownika.

Jest to istotne także z tego względu, że omawiane zagadnienie nie ogranicza się tylko do prawa krajowego, a ma naturę globalną i wykracza poza ramy prawnego porządku państwowego. Sprawa uzyskiwania dostępu do informacji zgromadzonych w urządzeniach użytkowników ma zdecydowanie charakter transgraniczny. Dlatego musi być rozpatrywana nie tylko na gruncie prawa danego państwa odnoszącego się do problematyki ochrony danych osobowych użytkownika, lecz także przepisów, które w sposób zharmonizowany winny obowiązywać w całej Unii Europejskiej. Aktualnymi stają się zatem następujące pytania:

1) jak w perspektywie prawa europejskiego wygląda standard legalności uzyskiwania dostępu do informacji zgromadzonych w urządzeniu użytkownika z punktu widzenia ochrony danych osobowych i ochrony wspomnianej prywatności informacyjnej użytkownika Internetu;
2) jakie są niezbędne warunki legalnego stosowania oprogramowania w urządzeniach użytkowników gwarantujących pełną ochronę ich danych osobowych i czy ochrona dotyczy urządzenia, czy osoby użytkownika;
3) jaka jest efektywność istniejących rozwiązań prawnych ze względu na ich cel?

II. Ochrona urządzenia końcowego użytkownika oraz informacji w nim przechowywanej w prawie UE

Punktem wyjścia rozważań na temat interesującego nas zagadnienia na poziomie unijnym była teza, że oprogramowania służącego do przechowywania informacji lub umożliwiającego dostęp do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym nie można zlikwidować. Dlatego Komisja Europejska za główny cel postawiła sobie uświadomienie użytkowników, by wiedzieli o istnieniu tego oprogramowania i mogli świadomie sami zdecydować czy dopuścić aktywne działanie takiego oprogramowania na swoich urządzeniach. W trakcie reformy pakietu przepisów telekomunikacyjnych w 2009 r.[6] doszło do zmiany art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej[7] (dalej: dyrektywa 2002/58/WE), który dotyczy przechowywania informacji i uzyskiwania dostępu do informacji już przechowanych w urządzeniu użytkownika. Podniesiono wówczas obawy, że niektóre obecne praktyki w zakresie stosowania cookies, w powiązaniu

[5] Rekomendacja CM/Rec. (2010) 13.

[6] Na mocy Dyrektywy Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz. Urz. L 337, s. 11, 18.12.2009).

[7] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. U. L 201, s. 37, 31.7.2002).

z reklamami internetowymi, nie zapewniają dostatecznej ochrony praw użytkowników, w szczególności w odniesieniu do przejrzystości i możliwości wyboru. Głównym celem art. 5 ust. 3 dyrektywy 2002/58/WE w zmienionym brzmieniu jest zatem zapewnienie ochrony urządzeń użytkowników i wszelkich informacji przechowywanych na tych urządzeniach traktowanych jako część prywatnej sfery użytkowników. Jak wyjaśniono w motywie 24 dyrektywy 2002/58/WE, sfera ta podlega ochronie na mocy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (art. 7 i 8 Konwencji – prawo do poszanowania życia prywatnego i rodzinnego oraz prawo do ochrony danych osobowych). W tym samym motywie wskazano także, że programy określane mianem *spyware*, błędy sieciowe, ukryte identyfikatory i inne podobne narzędzia mogą się znaleźć w urządzeniu użytkownika bez jego wiedzy w celu uzyskania dostępu do informacji, przechowania ukrytych informacji lub śledzenia czynności użytkownika i mogą w poważny sposób naruszyć jego prywatność. Z tych powodów uznano, że stosowanie takich narzędzi powinno być dozwolone wyłącznie w uzasadnionych przypadkach, po powiadomieniu zainteresowanych użytkowników.

Dla większej skuteczności tej ochrony wskazano, że postanowienia artykułu 5 ust. 3 dyrektywy 2002/58/WE stosuje się niezależnie od tego, czy przechowywanie lub dostęp do informacji zgromadzonej w urządzeniu użytkownika stanowi przetwarzanie danych osobowych w rozumieniu dyrektywy 95/46/WE[8] (dalej: dyrektywa 95/46/WE). Wychodząc z tak szerokiego zakresu tego przepisu, należy zatem uznać, że art. 5 dyrektywy 2002/58/WE stosuje się do ciasteczek HTTP, ciasteczek Flash i innego podobnego oprogramowania, które mogą spełniać funkcje opisane w przepisie (tj. przechowywania informacji lub odczytania jej w urządzeniach użytkowników). Ochrona użytkownika, na podstawie tego przepisu, rozciąga się zatem, jak już wskazano powyżej, na programy szpiegujące i inne złośliwe oprogramowanie, na błędy sieciowe, ukryte identyfikatory czy wirusy. Ma ona również zastosowanie bez względu na metodę dostawy oprogramowania i jego instalacji w sprzęcie użytkownika: nie tylko poprzez dystrybuowanie plików do pobrania z Internetu, lecz także za pośrednictwem zewnętrznych nośników danych, takich jak płyty CD, CD-ROM-y, klucze USB, zewnętrzne dyski twarde itp. W dyrektywie podkreślono jednak uprawnione wykorzystanie cookies do analizy stron i witryn www, efektywności reklam i identyfikacji użytkowników korzystających z usług (Piątek, 2013, s. 1011).

Artykuł 3 dyrektywy 2002/58/WE przewiduje, że dyrektywę stosuje się do przetwarzania danych osobowych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie. Zgodnie z art. 1 przepisy dyrektywy 2002/58/WE dookreślają i uzupełniają dyrektywę 95/46/WE, dlatego zasadne wydaje się w tym miejscu odwołanie się do jej art. 4. Artykuł 4 ust. 1 lit. c dyrektywy 95/46/WE przewiduje w szczególności, że środki krajowe wykonujące dyrektywę stosuje się wtedy, gdy administrator danych nie prowadzi działalności gospodarczej na terytorium UE, a do celów przetwarzania danych osobowych wykorzystuje środki zautomatyzowane, jak i inne znajdujące się na terytorium tego państwa, chyba że taki sprzęt jest używany jedynie do celów tranzytu przez terytorium UE. Na podstawie tego przepisu, przykładowo komputer osobisty użytkownika, powinien być postrzegany jako urządzenie podlegające ochronie, gdy pliki cookies mogą być wprowadzane i kontrolowane przez firmę, która nie posiada siedziby na terenie Unii Europejskiej.

[8] 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 (Dz. U. L 281, s.355, 23.11.1995).

Ustawodawca europejski w dyrektywie 2002/58/WE starał się także wymusić większą inicjatywę ze strony państw czy podmiotów rynkowych, jeśli chodzi o zapewnienie lepszej ochrony danych osobowych użytkownika Internetu. Jak wynika z motywu 61 dyrektywy 2002/58/WE zarówno państwa członkowskie, jak i Komisja Europejska mają obowiązek zachęcać podmioty gospodarcze do opracowania kodeksów postępowania dotyczących m.in. plików cookies, tak aby były stosowane zgodnie z ich celem. Środkiem do tego celu może być samoregulacja. Zgodnie z artykułem 27 dyrektywy 2002/58/WE, podmioty te mogą przedstawić kodeksy postępowania krajowym organom ochrony danych osobowych. Taka inicjatywa została jednak podjęta wyłącznie w Wielkiej Brytanii w celu ułatwienia dostawcom usług wypełniania obowiązku prawnego, w szczególności informacyjnego, dotyczącego użytkowników Internetu. W Polsce brakuje takich inicjatyw.

Jak już wspomniano wyżej, kwestia stosowania oprogramowania służącego do przechowywania informacji lub umożliwiającego dostęp do informacji już przechowywanej w urządzeniu użytkownika stała się przedmiotem uregulowania na poziomie europejskim w 2009 r. Ustawodawca europejski rozróżnił sytuacje, w których stosowanie takiego oprogramowania jest legalne oraz określił warunki jego stosowania, ale bez wątpienia był to jeden z przypadków tzw. regulacji ex post dotyczącej zmian, jakie nastąpiły w związku z rozwojem Internetu na całym świecie.

Na tle uregulowań prawnych związanych z problematyką plików cookies szczególnie istotne jest postrzeganie wzajemnej relacji regulacji dotyczących cookies i przepisów w zakresie ochrony danych osobowych, albowiem, jak już wykazano powyżej, regulacje te są względem siebie komplementarne. Dodatkowo w styczniu 2012 r. Komisja Europejska postanowiła dokonać kompleksowej reformy przepisów dotyczących ochrony danych w UE. Efektem tych prac jest ogólne rozporządzenie o ochronie danych[9], które uchyli dyrektywę 95/46/WE. Zgodnie z komunikatem Komisji Europejskiej celem nowych przepisów ma być przywrócenie obywatelom kontroli nad swoimi danymi osobowymi oraz uproszczenie otoczenia regulacyjnego dla przedsiębiorstw[10]. Jako nadrzędny cel tej reformy wskazano, że nowe przepisy mają jednak przede wszystkim lepiej chronić dane w Internecie. Brak zaufania sprawia, że konsumenci nie są przekonani czy dokonywać zakupów online i czy korzystać z nowych usług oferowanych w sieci Internet.

W art. 1 ogólnego rozporządzenia o ochronie danych osobowych zdefiniowano pojęcie „danych osobowych" jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Chodzi tu o osobę, którą można zidentyfikować, bezpośrednio lub pośrednio, za pomocą wszelkich środków, które z rozsądnym prawdopodobieństwem mogą być użyte przez administratora lub inną osobę fizyczną bądź prawną, szczególnie przez odniesienie do numeru identyfikacyjnego, danych dotyczących lokalizacji, identyfikatora online lub też przynajmniej jednego czynnika charakterystycznego dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby. Z brzmienia tego przepisu można więc wyprowadzić wniosek, że unijne regulacje w zakresie ochrony danych osobowych znajdują zastosowanie do sytuacji, w której za pośrednictwem plików cookies, znajdujących się w urządzeniu użytkownika, są zbierane dane użytkownika o powyższym charakterze. Jeśli te pliki znajdą się na dysku komputera, strony zapamiętują, kto je odwiedza. W ten sposób sklepy

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. L 119/1, s.1, 4.05.2016).

[10] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Ochrona prywatności w połączony świecie – europejskie ramy ochrony danych osobowych w XXI w. (COM/2012/9).

internetowe pozdrawiają swoich klientów z imienia i nazwiska oraz wiedzą, jakie oferty interesowały ich podczas ostatnich odwiedzin. Pełne profile użytkowników stają się atrakcyjną biznesowo informacją, pozwalają bowiem w stosunku do tych użytkowników na spersonalizowaną reklamę[11] i z taką rzeczywistością w sieci mamy dziś do czynienia.

Ze względu na zawarte w dyrektywie 2002/58/WE odwołanie do dyrektywy 95/46/WE, która zostanie uchylona po wejściu w życie rozporządzenia, koniecznym staje się również dokonanie rewizji tej dyrektywy. W dniu 10 stycznia 2017 r. Komisja Europejska przedstawiła projekt nowych przepisów mających na celu zmiany w dyrektywie 2002/58/WE, które mają skuteczniej zapewniać prywatność w łączności elektronicznej i jednocześnie zaktualizować obowiązujące regulacje[12]. Jak wskazuje komunikat Komisji Europejskiej z 10 stycznia 2017 r.[13], działania te mają dostosować przepisy w sprawie łączności elektronicznej do nowych unijnych standardów zawartych w ogólnym rozporządzeniu o ochronie danych osobowych. Dotyczy to również przepisów dotyczących plików cookies. Komisja przedstawiła w swoim komunikacie stanowisko, że przepisy dotyczące cookies, które dotychczas prowadziły do wysyłania użytkownikom zbyt dużej liczby próśb o zaakceptowanie tego rodzaju plików, zostaną uproszczone. Dzięki nowym przepisom użytkownicy będą mogli skuteczniej kontrolować swoje urządzenia, ponieważ za pomocą ustawień przeglądarki będą oni mieli możliwość łatwego zaakceptowania lub odrzucenia trwałych cookies i innych identyfikatorów, jeżeli zaistnieje zagrożenie dla prywatności. Zgodnie z tą propozycją pliki cookies, które nie stanowią zagrożenia dla prywatności i mają ułatwiać użytkownikowi korzystanie ze strony – na przykład takie, które zapamiętują zawartość koszyka – nie będą już wymagały zgody użytkownika. Jego zgoda nie będzie też potrzebna w przypadku cookies, które służą do liczenia wejść użytkowników na daną stronę internetową.

Mimo to, propozycja Komisji Europejskiej już spotkała się z wieloma uwagami krytycznymi[14], w szczególności organizacji reprezentujących przedsiębiorców, w których zarzuca się, że nowa propozycja stanowi *de facto* nie złagodzenie a zaostrzenie rygorów w zakresie przetwarzania danych osobowych o użytkownikach Internetu. Europejska koalicja organizacji zajmujących się prawami cyfrowymi przedstawiła jednak stanowisko, że nowy akt prawny powinien przede wszystkim uwzględniać wymogi silnej ochrony prawa do prywatności[15]. Wydaje się więc, że znalezienie konsensusu w tej sprawie nie będzie zadaniem łatwym.

Warto też w tym miejscu wspomnieć o orzeczeniu Europejskiego Trybunału Sprawiedliwości. Jak podkreślił w swoim orzeczeniu ETS, prawo do ochrony danych osobowych nie jest prawem absolutnym i powinno być analizowane w kontekście funkcji, jaką pełni w społeczeństwie[16]. Tezę tę z pewnością można odnieść do regulacji prawnych dotyczących plików cookies, które pozwalają – pod pewnymi prawnie określonymi warunkami – na zwolnienie niektórych rodzajów plików cookies z wymogu uzyskania świadomej zgody użytkownika urządzenia. W przeciwnym razie korzystanie z wielu usług w Internecie byłoby utrudnione czy wręcz niemożliwe.

[11] Komputer Świat „Szpiegujące pliki cookies", wrzesień 2009, pobrano z: http://www.komputerswiat.pl/jak-to-dziala/2009/09/szpiegujace-pliki-cookies.aspx.

[12] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/10.

[13] Komunikat Komisji Europejskiej z dnia 10 stycznia 2017 r. Pobrano z: http://europa.eu/rapid/press-release_IP-17-16_pl.htm.

[14] Pobrano z: https://www.iabeurope.eu/wp-content/uploads/2016/11/FAO-Vice-President-Ansip-Commissioner-Oettinger-Joint-letter-from-European-publishers-in-the-light-of-the-ePrivacy-Directive-revision-23-11-16.pdf.

[15] https://panoptykon.org/wiadomosc/dyrektywa-e-prywatnosc-do-rewizji

[16] Wyr. TS UE z dnia 9.11.2010 w sprawach C-92/09 i 93/09 „*Schecke*".

III. Obowiązujące warunki legalnego stosowania oprogramowania na urządzeniach użytkownika w prawie polskim

W prawie polskim po raz pierwszy materia ta znalazła wprost swoje uregulowanie w art. 173 pt zawartym w dziale VII „Tajemnica telekomunikacyjna i ochrona danych użytkowników końcowych". Ochroną są objęte wszelkie urządzenia przeznaczone do zapewnienia telekomunikacji, tj. aparaty telekomunikacyjne, smartfony, modemy, dekodery telewizyjne (Piątek, 2013, s. 1012). Przepis art. 173 pt nie określa katalogu informacji, do których mają zastosowanie warunki określone w tym przepisie i z których mogą korzystać przez pliki cookies podmioty świadczące usługi telekomunikacyjne czy usługi zapewniane drogą elektroniczną. Może to dotyczyć – jak wskazał ustawodawca – dwóch rodzajów czynności: przechowywania informacji w urządzeniu użytkownika lub uzyskiwania do nich dostępu. Zgodnie z ust. 1 tego artykułu, przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego jest dozwolone pod warunkiem, że:

1) abonent lub użytkownik końcowy zostanie uprzednio bezpośrednio poinformowany w sposób jednoznaczny, łatwy i zrozumiały o:
   a) celu przechowywania i uzyskiwania dostępu do tej informacji;
   b) możliwości określenia przez niego warunków przechowywania lub uzyskiwania dostępu do tej informacji za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi;
2) abonent lub użytkownik końcowy, po otrzymaniu wskazanych powyżej informacji wyrazi na to zgodę;
3) przechowywana informacja lub uzyskiwanie do niej dostępu nie powoduje zmian konfiguracyjnych w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego i oprogramowaniu zainstalowanym w tym urządzeniu.

Powyższy przepis nakazuje zatem wszystkim podmiotom, które mają możliwość przechowywania i uzyskiwania dostępu do informacji przechowywanych w urządzeniach użytkowników przedstawienie stosownych informacji i uzyskanie ich zgody na instalowanie cookies. Efekty tej regulacji są zauważalne dla każdego użytkownika sieci Internet. Właściwie przy każdym odwiedzeniu strony www otrzymujemy komunikat, że strona ta wykorzystuje pliki cookies. Jest to bezpośredni skutek regulacji wprowadzonej w art. 173 pt. Na marginesie warto zaznaczyć, że prawo telekomunikacyjne nie odsyła wprost do ustawy o świadczeniu usług drogą elektroniczną, ale bez wątpienia adresatami norm są także usługodawcy w rozumieniu tej ustawy. Zgodnie z jej przepisami, świadczeniem usługi drogą elektroniczną jest wysyłanie i odbieranie danych za pomocą systemów teleinformatycznych na indywidualne żądanie usługobiorcy, bez jednoczesnej obecności stron, przy czym dane te są transmitowane za pośrednictwem sieci publicznych w rozumieniu pt. Możemy w tym względzie mówić zatem o wzajemnym oddziaływaniu norm prawnych i o istnieniu związku funkcjonalnego pomiędzy normami prawnymi zawartymi w prawie telekomunikacyjnym oraz ustawie o świadczeniu usług elektronicznych.

Przepis art. 173 ust. 3 pt w ślad za przepisem dyrektywy 2002/58/WE legalizuje też pod pewnymi warunkami używanie cookies w celu umożliwienia stworzenia witryn www, które pamiętają imiona użytkowników i wykorzystują je do generowania odpowiednio spersonalizowanych treści.

Są one używane do przechowywania tzw. krótkich informacji, umożliwiających rozróżnianie użytkowników (klientów) odwiedzających daną stronę WWW czy też zawierających takie informacje, jak login, preferencje użytkownika, zawartość koszyka zakupów czy dane rejestracyjne użytkownika programu. Dane te mogą następnie posłużyć do tworzenia statystyk odwiedzin witryny WWW, personalizacji stron oraz systemów e-commerce. Zgodnie z omawianym przepisem spełnienie obowiązku informacyjnego i uzyskania zgody nie będzie zatem wymagane, gdy uzyskanie dostępu jest konieczne do:

1) wykonania transmisji komunikatu za pośrednictwem publicznej sieci telekomunikacyjnej lub
2) dostarczania usługi świadczonej drogą elektroniczną, żądanej przez abonenta lub użytkownika końcowego.

Podejście takie wydaje się być spójne w świetle poglądów wyrażanych w doktrynie, a odnoszących się do ochrony danych osobowych. W istocie bowiem autonomia informacyjna podlega jednak pewnym ograniczeniom, ponieważ niezależnie od zgody osoby, której informacje dotyczą, dane mogą być przetwarzane zgodnie z warunkami określonymi w art. 23 ustawy o ochronie danych osobowych. Przepis ten obejmuje warunki odnoszące się zarówno do potrzeb mieszczących się w kategorii interesu publicznego (zrealizowanie uprawnienia lub obowiązku wynikającego z przepisów prawa, zadań realizowanych dla dobra publicznego), jak i prywatnego, dotyczącego danej osoby (Federczyk, 2013, s. 118).

Pierwszy przypadek wyłączający obowiązek pozyskania zgody to sytuacja, w której cookies jest niezbędne w celu transmisji komunikatu, czyli sytuacja, w której usługodawca musi wiedzieć, jakie parametry przekazać przedsiębiorcy telekomunikacyjnemu w celu właściwego pokierowania przez tego ostatniego transmisji komunikatu nadanego przez użytkownika. Chodzi tu np. o wskazanie „mapy" punktów końcowych w sieci, według której komunikat ma być transmitowany (czyli kierowany jest z punktu A do punktu B, za pośrednictwem punktu C, ale z pominięciem punktu D, E etc.). Chodzi o nadanie pakietom transmitowanych danych odpowiedniej kolejności lub priorytetu, czy także o możliwość identyfikowania błędów lub przypadków utraty danych.

Drugi przypadek wyłączający zgodę w praktycznym ujęciu to np. umożliwienie komentowania artykułów prasowych zamieszczonych na stronie lub umożliwienie „włożenia" do koszyka zakupów w sklepie internetowym.

Z art. 173 pt wynika, że użytkownik powinien być poinformowany nie tylko o celach związanych z przechowywaniem cookies, lecz także o prawie sprzeciwu. Ustawodawca szczególny nacisk położył na właściwe poinformowanie użytkownika, albowiem, jak już było wspomniane, w cyfrowej rzeczywistości pliki cookies są nieusuwalne. Należy zgodzić się z poglądem, zgodnie z którym informacja jest przenaszalnym dobrem niematerialnym zmniejszającym niepewność (Szpor, 2011, s. 97). Z tego właśnie powodu dobrze poinformowany konsument jest najlepszym gwarantem przyznanej mu przez przepisy prawa ochrony. Państwo natomiast powinno stworzyć przyjazny system prawny i instytucjonalny, gwarantujący konsumentowi jak najszersze prawo do jej uzyskania (Pachuca-Smulska, 2013, s. 1).

W trakcie prac nad wdrożeniem zmian dyrektywy 2002/58/WE w odniesieniu do cookies pojawiło się szereg wątpliwości, co do tego jakie pliki podlegają legalizacji, gdyż pt nie wskazuje tego w sposób bardzo precyzyjny. Chodzi tu o wskazanie enumeratywnie, jakie pliki cookies mogą zostać wyłączone spod wymogu pozyskania świadomej zgody, a tym samym konstytuują

zakres prawa do informacji użytkownika urządzenia. W tym zakresie przepisy prawa polskiego nie dają też precyzyjnej odpowiedzi. Pomocne jest tu stanowisko, które w dniu 7 czerwca 2012 r. przedstawiła Grupa Robocza do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych, ustanowiona na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (dalej: Grupa Robocza). Grupa Robocza przyjęła opinię[17], w której uznała, że zgody nie wymagają, pod określonymi warunkami, o ile nie są wykorzystywane do dodatkowych celów:

1) pliki cookies z danymi wprowadzanymi przez użytkownika (identyfikator sesji) na czas trwania sesji lub trwałe pliki cookies ograniczone w niektórych przypadkach do kilku godzin;
2) uwierzytelniające pliki cookies wykorzystywane do usług wymagających uwierzytelniania na czas trwania sesji;
3) pliki cookies zorientowane na bezpieczeństwo użytkownika wykorzystywane do wykrywania nadużyć dotyczących uwierzytelniania na dłuższy, lecz ograniczony czas;
4) sesyjne pliki cookies odtwarzaczy multimedialnych, takie jak pliki odtwarzacza „flash", na czas trwania sesji;
5) sesyjne pliki cookies do równoważenia obciążenia, na czas trwania sesji;
6) trwałe pliki cookies do personalizacji interfejsu użytkownika na czas trwania sesji (lub nieco dłużej);
7) pliki cookies osób trzecich dla wtyczek portali społecznościowych pozwalających na wymianę treści dla zalogowanych członków sieci społecznej.

Grupa Robocza zwróciła także uwagę na jeszcze inny ważny element, a mianowicie, że pliki cookies wyłączone spod wymogu pozyskania zgody powinny mieć żywotność pozostającą w bezpośrednim związku z celem, jakiemu służą i muszą wygasać z chwilą, gdy przestają być potrzebne, przy uwzględnieniu rozsądnych oczekiwań przeciętnego użytkownika. Ustawodawcy, zarówno europejski, jak i krajowy, nie dookreślili aż tak szczegółowo tych kwestii, co nadal budzi szereg uwag i kontrowersji przy stosowaniu przepisów, ale też prowadzi do pytania czy cel, który przyświecał ustawodawcy został w pełni osiągnięty. Czy można na tej postawie uznać, że każdy użytkownik Internetu jest w pełni poinformowany, co tak naprawdę dzieje się na jego urządzeniu i potrafi skutecznie się temu sprzeciwić? Co wreszcie z sytuacją, gdy użytkownik ma do czynienia z technologią często określaną jako tzw. ever-cookies (zawsze istniejące pliki cookie) lub tzw. zombie-cookies (zawsze istniejące pliki cookie) Umożliwiają one plikom cookies trwałe pozostanie w urządzeniu użytkownika, mimo należytych starań w celu ich usunięcia. Jak wreszcie skutecznie dochodzić swoich praw w sytuacji, w której w sposób bezprawny, przy użyciu takich plików, profil użytkownika Internetu został wykorzystany albo naruszone zostały dane osobowe użytkownika.

W tym zakresie pt również nie daje jednoznacznej odpowiedzi. W katalogu penalizowanych sytuacji w art. 209 ust. 1 – przewidziana jest wyłącznie kara pieniężna, w pkt 25 – z powodu nieuzyskania zgody abonenta lub użytkownika końcowego, a w pkt 27 – w przypadku niezgodnego z art. 173 pt przechowywania informacji w urządzeniach użytkowników lub korzystania z takich informacji.

[17] Opinia Grupy Roboczej art. 29 Nr 4/2012 w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody WP 194.

Warto także nadmienić, iż mimo tak zdefiniowanych obowiązków ustawowych, obserwowanym zjawiskiem jest to, że na stronach internetowych często mylona jest polityka prywatności z informacjami o cookies, co w praktyce uniemożliwia właściwe wypełnienie w szczególności obowiązku informacyjnego względem użytkownika, a w szczególności poinformowanie użytkownika o celach stosowania plików cookies. Jest to dość powszechne zjawisko i z tego powodu trudno uznać, iż obowiązek ustawowy względem użytkownika urządzenia – przed wyrażeniem zgody – został w pełni wypełniony. Prawo telekomunikacyjne nie przewiduje w tym względzie jednak dalszych konsekwencji prawnych.

IV. Zgoda użytkownika na cookies

Art. 5 ust. 3 dyrektywy 2002/58/WE stanowi, że przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowanych w urządzeniu użytkownika jest dozwolone tylko pod warunkiem, że wyraził on na to zgodę; po otrzymaniu jasnych i pełnych informacji, między innymi o celach przetwarzania. Ustawodawca unijny podkreślił, że przy uzyskiwaniu dostępu do informacji przechowywanej w urządzeniu użytkownika mają zastosowanie reguły odnoszące się do ochrony danych osobowych. Co więcej, art. 2 dyrektywy 2002/58/WE stanowi, że definicje zawarte w dyrektywie 95/46/WE stosuje się do dyrektywy 2002/58/WE. Zgoda udzielona w trybie opisanym w art. 5 ust. 3 2002/58/WE, ma takie samo znaczenie jak zgoda podmiotu danych określona w dyrektywie 95/46/WE. Motyw 17 dyrektywy 2002/58/WE dodatkowo wyjaśnia, że zgoda może być udzielona w jakikolwiek sposób umożliwiający swobodne i świadome wyrażenie woli użytkownika, w tym przez zaznaczenie okna wyboru podczas przeglądania witryny internetowej.

Jak podkreśla się w doktrynie prawa, zgoda nie może być wyrażona *per facta concludentia*, w sposób „milczący" lub inne pasywne działanie (Barta, 2004, s. 416). Ponadto zgoda nie może być wyprowadzana z faktu korzystania z usługi (Piątek, 2013, s. 1019). Jak jednak wyjaśnia w motywie 25 dyrektywy 2002/58/WE ustawodawca europejski, nie jest konieczne uzyskanie zgody co do każdej operacji dotyczącej dostępu do lub przechowywania informacji na urządzeniu użytkownika. Informacja i prawo do odmowy mogą być oferowane jednorazowo dla różnego rodzaju narzędzi instalowanych w urządzeniu użytkownika w czasie tego samego połączenia oraz mogą obejmować wszelkie dalsze korzystanie z tych narzędzi w trakcie kolejnych połączeń. W polskim prawie telekomunikacyjnym kwestia ta nie została jednak wprost uregulowana.

Ponadto zgoda powinna być swobodna, tzn. użytkownik może również cofnąć tę zgodę w każdym czasie.

Motyw 17 dyrektywy 2002/58/WE stanowi, że zgoda może zostać udzielona przez zaznaczenie okna wyboru podczas przeglądania witryny internetowej. W taki sam sposób kwestia ta została uregulowana w polskim prawie, gdzie zgodnie z art. 173 ust. 2 pt abonent lub użytkownik końcowy może wyrazić zgodę, za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi.

Podsumowując, przepisy prawne wprost nakazują by zgoda miała charakter wyraźny, a nie dorozumiany czy *per facta concludentia*, a jej wszystkie aspekty muszą być jasne w momencie jej wyrażania. Jak już wspomniano, przepisy ustawy pt przewidują w art. 209 ust. 1 pkt 25 sankcję w postaci kary pieniężnej za brak realizacji obowiązku uzyskania zgody abonenta lub użytkownika końcowego.

V. Uwagi końcowe

Regulacje dotyczące przetwarzania danych osobowych sięgają lat osiemdziesiątych, począwszy od 1981 r., kiedy to przyjęto pierwszą konwencję Rady Europy w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych. Od tego czasu mamy do czynienia z rewolucją technologiczną, która stawia prawodawcę przed coraz to nowszymi wyzwaniami, w tym dotyczącymi problemów, jakie wiążą się z dostępem do urządzeń, za pomocą których korzystamy z Internetu. Zwiększa się objętość informacji lokowanych w urządzeniach użytkowników, zmieniają mechanizmy jej wykorzystywania i obsługiwane funkcje. Jednocześnie nowsze technologie działają w sposób mniej jawny dla użytkownika w porównaniu z klasycznymi cookies (Piątek, 2015, s. 51). Wymusza to odmienny sposób podejścia do kwestii regulacji. Ewoluuje ona w kierunku zapewnienia użytkownikom większej kontroli nad urządzeniami, z których korzystają, a także większego nacisku na precyzyjne obowiązki informacyjne ze strony dostawców usług oraz uzyskanie wyraźniej i świadomej zgody użytkownika. Nowe ogólne rozporządzenie o ochronie danych osobowych ma odpowiedzieć na problemy związane ze znacznym zwiększeniem transgranicznego przepływu danych czy zbierania tych danych. Powinno umożliwić horyzontalne spojrzenie na ochronę danych osobowych także w odniesieniu do cookies. Szczególny nacisk w tej regulacji położono na zapewnienie osobom fizycznym kontroli nad własnymi danymi osobowymi. Wprost wskazano, że ochrona danych osobowych powinna mieć także zastosowanie do przetwarzania danych osobowych w sposób zautomatyzowany. Mając dostęp do informacji w urządzeniu telekomunikacyjnym użytkownika można bowiem wyciągnąć konkretne wnioski na temat jego zachowań.

Jak podkreśla się w doktrynie, z praktycznego punktu widzenia, największy wpływ ogólnego rozporządzenia o ochronie danych osobowych na regulacje prawne społeczeństwa informacyjnego może być widoczny właśnie w aspekcie nowych zasad zbierania zgód, w tym zgody na przetwarzanie danych osobowych (Litwiński, 2016, s. 16). Dotyczyć to będzie także sytuacji przechowywania informacji lub uzyskiwania dostępu do informacji już przechowanych w urządzeniu użytkownika. Zmianę w tym zakresie może przynieść propozycja Komisji Europejskiej dotycząca rewizji przepisów dyrektywy 2002/58/WE (zwanej dyrektywą e-privacy), nad którą trwają aktualnie prace legislacyjne. Ma ona na celu uproszczenie przepisów w zakresie cookies, przy założeniu, iż w szerszym niż obecnie zakresie zgoda na zainstalowanie cookies będzie mogła być wyrażona poprzez ustawienia przeglądarki internetowej. W tym zakresie konieczna będzie analiza proponowanych zmian w odniesieniu do zharmonizowanych w UE nowych reguł dotyczących ochrony danych osobowych pod kątem zgodności i spójności tych regulacji.

Bibliografia

Barta, P. i Litwiński. P. (2015). *Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Brzozowska, M. (2012). *Ochrona danych osobowych w sieci*. Wrocław: PRESSCOM.

Federczyk, W. (2013). Badania podstaw aksjologicznych prawa procesowego w zakresie jawności i jej ograniczeń. W: Z. Cieślak, G. Szpor (red.), *Jawność i jej ograniczenia*. T. II. *Podstawy aksjologiczne* (wyd. 1.). Warszawa: Wydawnictwo C.H. Beck.

Adamski, D. (2007). O ochronie danych w telekomunikacji. W: J. Gołaczyński (red.), *Prawo Mediów Elektronicznych,* 6/2007 – dodatek do Monitora Prawniczego Nr 4.

Kmieciak, Z. (2013). Podstawy teoretyczne badania skuteczności regulacji prawnej jawności i jej ograniczeń. W: G. Szpor (red.), *Jawność i jej ograniczenia*, t. III, *Skuteczność regulacji*. Warszawa: Wydawnictwo C.H. Beck.

Konarski, X. (2002). *Internet i prawo w praktyce*, Warszawa: Wydawnictwo Stowarzyszenie Marketingu Bezpośredniego.

Lewiński, A. (2008). Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. 10-lecie polskiej Ustawy o ochronie danych osobowych. W: G. Goździkiewicz, M. Szabłowska (red.), *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, Toruń: TNOIK.

Litwiński, P. (2016). Nowe rozporządzenie ogólne w sprawie ochrony danych osobowych i jego wpływ na społeczeństwo informacyjne. Wybrane zagadnienia. W: K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne. Współczesne problemy prawne*. Warszawa: Wydawnictwo C.H. Beck.

Mednis, A. (2002). Ochrona danych osobowych i ochrona prywatności w świetle dyrektywy UE z dnia 12 lipca 2002 roku o prywatności w komunikacji elektronicznej. *Prawo i Ekonomia w Telekomunikacji*, 4.

Pachuca-Smulska, B. (2013). Prawo do informacji i edukacji podstawą ochrony interesów konsumenta. W: M. Królikowska-Olczak, B. Pachuca-Smulska (red.), *Ochrona konsumenta w prawie polskim i Unii Europejskiej*. Warszawa: Wydawnictwo C.H. Beck.

Piątek, S. (2013). *Prawo telekomunikacyjne. Komentarz*, Warszawa: Wydawnictwo C.H. Beck.

Piotrowski, R. (2016). Prawo do prywatności i ochrony danych osobowych jako wartości konstytucyjne. W: A. Mednis (red.), *Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość*. Warszawa: Wydawnictwo C.H. Beck.

Safjan, M. (2002). Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych. *Kwartalnik Prawa Prywatnego*, 1.

Szpor, G. (1991). Publicznoprawna ochrona danych osobowych. *Przegląd Ustawodawstwa Gospodarczego*, 12.

Szpor, G. (2011). W: I. Lipowicz, Z. Niewiadomski, K. Strzyczkowski, G. Szpor, *Prawo administracyjne*. Warszawa: LexisNexis.