Justyna Zygmunt

Program Safe Harbour – pomost między europejskim a amerykańskim systemem ochrony danych osobowych

Wstęp

Niemalże każda czynność sprawia, że ludzie zostawiają po sobie ślady. Dzieje się tak, gdy robią zakupy w sklepie, znajdują się w miejscach objętych monitoringiem czy rejestrują na wizytę u lekarza. W każdej z wymienionych sytuacji utrwalają się informacje na ich temat. Gdyby właściciel sklepu pamiętał o tym, że jeden klient codziennie rano kupuje jagodziankę, mógłby po pewnym czasie dostosować swoją ofertę do jego oczekiwań i w ten sposób stać się bardziej konkurencyjnym. Jednakże, mając tysiące klientów, nie jest w stanie zebrać i przetworzyć danych na temat wszystkich kupujących – w efekcie upodobania jednostki gubią się wśród innych i nikt nie skorzysta na dokonanej wymianie informacji.

Choć automatyczne przetwarzanie danych było możliwe już dziesiątki lat temu, to dopiero Internet wyniósł je na nowy poziom, umożliwiając szybkie kojarzenie ze sobą informacji znajdujących się w rozmaitych, rozproszonych, rozbudowanych i przewidzianych dla realizacji odmiennych celów zbiorach oraz ich błyskawiczne rozpowszechnianie w zmodyfikowanej formie. Zebrane w ten sposób informacje mogą zdradzać nie tylko preferencje konsumenckie, ale także sytuację życiową i cechy osobowości. Zagrożenia i korzyści płynące z rozwoju techniki w miarę upływu czasu coraz lepiej zauważali także ustawodawcy, bo choć wyspecjalizowane ustawy pojawiły się już dziesiątki lat temu – ogłoszenie pierwszej miało miejsce w 1970 roku w Hesji – dopiero popularyzacja Internetu, w wyniku której informacja zaczęła mieć stale zwiększającą się wartość ekonomiczną[1], naświetliła palącą potrzebę kompletnej regulacji dotyczącej danych osobowych. Obecnie takie cyfrowe ślady mają skrajne konsekwencje w odniesieniu do różnych podmiotów: z jednej strony mogą nieść za sobą znaczną wartość ekonomiczną (na

1 *Cf.* J. Barta, R. Markiewicz, P. Fajgielski, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 27.

przykład poprzez wspomaganie udoskonalania strategii marketingowej czy ocenę ryzyka transakcji z danym podmiotem), a z drugiej, mają potencjał, by spowodować wielkie szkody dla podmiotu, którego dane dotyczą[2]. To zróżnicowanie interesów uwidacznia się w dwóch podejściach do problematyki ochrony danych osobowych: europejskim – przyznającym prym ochronie obywatela – oraz amerykańskim – uznającym za priorytet swobodę działalności gospodarczej.

Właściciel sklepu będzie wiedział, że jego klient jada bułki z jagodami i przygotuje dla niego specjalną ofertę, by utrzymać zainteresowanie bądź, zauważając preferencje konsumenta, zaproponuje mu nowe produkty. Być może poinformuje o tych preferencjach także sąsiedni sklep, który wprowadzi do swojej oferty specjalny proszek do prania ubrań zabrudzonych jagodami. Właściciel odniesie korzyść w postaci utrzymania bądź rozrostu rynku zbytu oraz nawiąże nowe kontakty handlowe, a konsument otrzyma korzystniejsze oferty. Pozostaje jednak pytanie, czy producent mógł zebrać dane klienta bez jego zgody, czy są to dane „osobowe", komu można je udostępnić i czy konsument może się tym działaniom sprzeciwić. O ile w kontekście przykładu z jagodziankami pytanie to mogłoby zostać uznane za trywialne, to gdyby zastąpić je produktami medycznymi, a właściciel sklepu informowałby inne przedsiębiorstwa – na przykład firmy ubezpieczeniowe – o stanie zdrowia klienta bądź przesyłał dane do kraju, w którym nie istnieją normy chroniące dane osobowe, punkt widzenia niewątpliwie uległby znacznej zmianie[3]. Celem ochrony danych osobowych jest zatem „zagwarantowanie możliwości podejmowania decyzji w sferze informacji przez jednostkę, której te informacje dotyczą, a zarazem zapewnienie realizacji prawnie chronionego prawa jednostki do prywatności i intymności"[4].

Artykuł ma na celu, poza nakreśleniem ogólnej charakterystyki europejskiego i amerykańskiego systemu ochrony danych osobowych, przedstawić problemy i stanowiska w przedmiocie warunków transferu danych osobowych z obszaru wysokiej ochrony na teren ochrony szczątkowej, czyli z Unii Europejskiej do USA, przy czym szczególna uwaga zostanie poświęcona Programowi Safe Harbour[5].

Podstawowe pojęcia

Ochrona danych osobowych zarówno na świecie, jak i w Polsce jest refleksem podstawowych praw i wolności obywatelskich zawartych w aktach najwyższego rzędu[6]. W Polsce

2 *Cf.* A. Savin, *EU Internet Law*, Cheltenham 2013, s. 191.
3 M. Chrabonszczewski, *Prywatność. Teoria i Praktyka,* Warszawa 2012.
4 P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013, s. 3.
5 Dalej: „S. H." lub „Program". Zarówno pisownia „Harbor" jak i „Harbour" jest poprawna.
6 H. P. Gotting, C. Schertz, W. Seitz *et. al.*, *Handbuch des Personlichkeitsrechts, Monarium* 2009, S. 102 i n.

są to konstytucyjnie chronione prawo do prywatności ujęte w art. 49 oraz prawo do autonomii informacyjnej z art. 51. Transpozycja postanowień konstytucyjnych jest widoczna w ustawowym zwrocie: „każdy ma prawo do ochrony dotyczących go danych", który stanowi połączenie założeń kryjących się za prawem do prywatności oraz autonomią informacyjną.

Określenie „ochrona danych osobowych" używane zarówno przez polską Ustawę o Ochronie Danych Osobowych z dnia 29 sierpnia 1997 r.[7], jak i światową doktrynę, stanowi pewien skrót myślowy[8]. Nie tyle bowiem jest celem ochrona danych samych w sobie, ile osób, których te dane dotyczą. Widać to wyraźnie na przykładzie Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku (Dz. Urz. UE. L Nr 281, str. 31; dalej jako „Dyrektywa" lub „Dyrektywa 95/46/WE"), której tytuł brzmi: „W sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych". Ta konstatacja, choć na pozór oczywista, jest kluczowa, bowiem językowe ujęcie aktu prawnego niejednokrotnie przesądza o jego autorytecie i sposobach wykładni: o ile z potrzebą „ochrony danych osobowych" jako takich można polemizować z uwagi na dodatkowe koszty, które taka ochrona generuje, to już hasło ochrony obywatela, realizowanej poprzez ochronę jego danych, wydaje się być mniej dyskusyjne.

Dane osobowe są elementem życia prywatnego – informacjami o tożsamości, działaniach i przekonaniach. Przełożeniem tej reguły na język prawny na gruncie prawa polskiego jest definicja legalna zawarta w art. 6 ust. 1 Ustawy: za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej bądź możliwej do zidentyfikowania osoby fizycznej, przy czym za osobę możliwą do identyfikowania uważa się osobę, której tożsamość można określić bezpośrednio lub pośrednio przez powołanie się na numer identyfikacyjny lub jeden albo kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, kulturowe, ekonomiczne lub społeczne. Dodatkowo nie uważa się za informację umożliwiającą określenie tożsamości takiej informacji w sytuacji, gdy określenie wymagałoby nadmiernych kosztów, działań lub czasu. Dane osobowe są zatem rozumiane bardzo szeroko; reasumując, są nimi takie informacje, które można powiązać z konkretną osobą, jeśli wiadomo, kogo one dotyczą, albo pozwalają bez podejmowania nadmiernych wysiłków taką osobę ustalić.

Wyróżnia się także specjalną grupę danych, tak zwane dane sensytywne (wrażliwe), do których art. 27 Ustawy – za Dyrektywą – zalicza dane ujawniające pochodzenie rasowe lub etniczne, poglądy religijne, polityczne, przynależność wyznaniową, stan zdrowia, kod genetyczny, nałogi czy życie seksualne. W stosunku do takich wprowadzane są dalsze obostrzenia. Kategoria danych sensytywnych jako danych wymagających szczególnej

7 Dz. U. 1997 nr 133 poz. 883; dalej jako „Ustawa".

8 P. Fajgielski, *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno - prawne* , Lublin 2008, s. 34.

ochrony wyszczególniona jest także w innych systemach prawnych, w tym w amerykańskim. Systemy różnią się jednak katalogiem informacji uznawanych za wrażliwe oraz dodatkowymi restrykcjami.

Przetwarzanie (*processing*) danych osobowych to jakiekolwiek operacje wykonywane na danych takie jak zbieranie, utrwalanie czy udostępnianie. Odbiega to od potocznego rozumienia słowa „przetwarzanie" jako procesu dokonywania pewnych zmian.

Ochrona danych osobowych w Unii Europejskiej

Choć zagadnienie ochrony danych osobowych jest nie tylko współczesne, ale też coraz szerzej dyskutowane, dla jego pełnego zrozumienia, w szczególności zrozumienia zasygnalizowanych różnic w europejskich i amerykańskich uregulowaniach, warto sięgnąć do historii. W Europie, w której od wieków panowały różne formy dyktatury – od monarchii absolutnej po nazizm i komunizm – ochrona danych osobowych została, dla nadania jej szczególnego statusu i zapewnienia ścisłego przestrzegania, zakwalifikowana do katalogu podstawowych praw i wolności człowieka. Szczególnie ważnym okresem dla uświadomienia społeczności europejskiej wagi ochrony danych był okres II wojny światowej oraz lata powojenne. Przykładowo: niemiecki urząd bezpieczeństwa zatrudniał 500000 tajnych współpracowników, przy czym zadaniem 10000 z nich było dokonywanie transkrypcji rozmów telefonicznych obywateli. Do podobnych sytuacji nie dochodziło w Stanach Zjednoczonych. W USA od początku podejście do ochrony danych osobowych kształtowane jest głównie uwarunkowaniami wolnorynkowymi. Przełomowe wydarzenia działały tam raczej na rzecz złagodzenia niż zaostrzenia ochrony danych; na przykład po ataku terrorystycznym, jaki miał miejsce 11 września 2001 roku wszedł w życie US Patriot Act znacznie zmniejszający restrykcje dotyczące gromadzenia i przetwarzania danych przez upoważnione do tego organy.

Podstawowymi celami europejskiej regulacji były i są nadal ujednolicenie minimalnego poziomu ochrony oraz znalezienie równowagi pomiędzy zapewnieniem swobodnego przepływu danych między krajami członkowskimi – co pozostaje niezbędne dla gwarantowanego wspólnotowo przepływu towarów, usług i osób – a wysokim poziomem ochrony życia prywatnego. Z tego powodu gromadzenie i wykorzystywanie danych osobowych podlega ścisłym ograniczeniom, a państwa UE wezwano do powołania niezależnych krajowych organów odpowiedzialnych za ochronę tych danych[9]. W Polsce jest to Generalny Inspektor Danych Osobowych[10].

9 A. Savin, *op. cit.*, s. 196.
10 Dalej: „GIODO".

Założenia Dyrektywy 95/46/WE

Owocem europejskiej myśli prawniczej dotyczącej potrzeby ochrony danych osobowych jest Dyrektywa 95/46/WE wprowadzająca katalog minimalnych uprawnień i restrykcji, których naruszenie może być powodem zarządzenia przez sąd wypłaty odszkodowania. Jej podstawowe założenia można ująć w poniższych pięciu punktach.

Po pierwsze, w sytuacji, w której na zbieranie i przetwarzanie danych wymagana jest zgoda, osoba przed jej wyrażeniem ma obowiązkowo zostać poinformowana o administratorze zbioru, o celu, dla którego dane są zbierane oraz o możliwości wglądu do nich i korekty. Dyrektywa zakazuje zasadniczo przetwarzania danych w innym celu niż ten, dla którego zostały zebrane i innym niż ten, na który osoba uprawniona wyraziła zgodę. Przetwarzanie danych bez obligatoryjnej zgody jest możliwe tylko w wyjątkowych przypadkach. Po drugie, istnieją specjalne postanowienia dotyczące danych sensytywnych, w przypadku przetwarzania których konieczna jest wyraźna zgoda[11]. Po trzecie, osoba, której dane zostały zebrane, może domagać się ich sprostowania bądź usunięcia, jeśli zawierają fałszywe informacje lub zostały zebrane z naruszeniem dyrektywy. Po czwarte, każda osoba ma prawo do uzyskania informacji o tym, czy dane o niej znajdują się w zbiorze, a jeśli tak, to w jakim celu. Po piąte, zainteresowany może wnieść sprzeciw wobec przetwarzania dotyczących go danych wyłącznie w celach marketingu bezpośredniego oraz w sytuacji, gdy choć zebrane one zostały w warunkach dozwolonych przez prawo (na przykład w wypadku, gdy było to niezbędne dla korzystania z nich na rzecz dobra publicznego), to indywidualna sytuacja sprawia, że działanie takie nie powinno być legitymizowane.

Kształt polskiej regulacji dotyczącej ochrony danych osobowych jest wynikiem implementacji Dyrektywy. Porównanie tych dwóch aktów prawnych pozwala dostrzec pewne różnice[12], jednakże polska Ustawa jest z nią w znacznej części zharmonizowana, zwłaszcza po trzech obszernych nowelizacjach z 2001, 2004 i 2012 roku, dlatego w dalszej części opracowania nie zostaną omówione osobno regulacje polskie i unijne, a jedynie te drugie. Warto podkreślić, iż stopień harmonizacji prawa w innych państwach UE jest równie wysoki, co w Polsce. Nad tym procesem czuwa powołana specjalnie w tym celu mocą art. 29 Dyrektywy Grupa Robocza do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych[13], która ma zapewniać wzajemne zbliżanie się ustawodawstw krajowych, w szczególności przez wydawanie stosownych rekomendacji. Obecne ujednolicanie prawa na terenie UE nasuwa wniosek, iż dostrzeżono stale rosnący międzynarodowy przepływ danych i postawiono na spójną, kompletną, ogólnoeuropejską

11 W tym aspekcie polska Ustawa jest bardziej restrykcyjna od unijnej Dyrektywy, gdyż dla udzielenia zgody wymaga jest forma pisemna.

12 J. Barta, R. Markiewicz, P. Fajgielski, O*chrona danych osobowych. Komentarz*, Kraków 2007 s. s. 126.

13 Dalej: „Grupa Robocza art. 29" lub „Grupa Robocza".

regulację[14]. Już samo przejście od formy dyrektywy do bezpośrednio obowiązującego rozporządzenia jest jasnym sygnałem, że postawiła sobie zadanie ścisłego i bezkompromisowego uregulowania przedmiotowej materii.

Przekazywanie danych osobowych do krajów trzecich

Zasady ogólne

Postępująca globalizacja wpływa na wzrost transgranicznej wymiany informacji i sprawiła, iż unijna Dyrektywa nie mogła obejść się bez zasad regulujących transfer danych osobowych do państw trzecich, której poświęcony jest IV rozdział Dyrektywy. Jednakże przed omówieniem szczegółów regulacji należy sprecyzować, czym jest sam transfer danych. W zakresie tego pojęcia mieszczą się: udostępnianie danych administratorowi z państwa trzeciego, czyli spoza Unii Europejskiej, przekazanie ich do przetwarzania w państwie trzecim oraz transfer danych w ramach struktury organizacyjnej jednego administratora danych (na przykład do oddziału spółki znajdującego się w państwie trzecim)[15].

Artykuł 25. Dyrektywy wprowadza kluczową zasadę głoszącą, że transfer danych osobowych dopuszczalny jest wyłącznie do państwa, które zapewnia odpowiedni poziom ochrony (*adequate level o protection*). Dyrektywa nie przesądza o procedurze weryfikowania istnienia odpowiedniego poziomu ochrony, pozostawiając w tym zakresie swobodę krajom członkowskim[16]. Kraj członkowski może przykładowo wprowadzić obowiązki po stronie administratorów bądź zdecydować się na system udzielania uprzednich lub następczych zezwoleń. Dyrektywa nie zawiera wyczerpującego katalogu cech prawodawstwa zapewniającego odpowiednią ochronę, a jedynie wskazuje w art. 25 ust. 2 pewne czynniki, w świetle których należy dokonywać jego oceny: szczególną uwagę należy zwracać na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, normy prawne (materialne, procesowe i egzekucyjne), obowiązujące w kraju trzecim oraz środki mające zapewnić bezpieczeństwo przetwarzania danych w tym kraju. Pewne wytyczne w tym zakresie wydała także Grupa Robocza art. 29. w dokumencie WP 12 z dnia 24 lipca 1998 roku, w którym zdefiniowała podstawowe zasady, jakie powinno przestrzegać państwo trzecie[17]:

14 Więcej na ten temat w końcowej części artykułu.

15 X. Konarski, G. Sibiga, *Zasady przekazywania danych osobowych do państwa trzeciego w prawie polskim i UE*, [w:] *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, ss. 89–90.

16 H. H. Wohlgemuth, J. Gerloff, *Datenschutzrecht. Eine Einfuhrung mit praktischen Falen*, Darmstadt 2005, s. 16.

17 *ABC zasad przekazywania danych osobowych do państw trzecich*, Wydawnictwo sejmowe 2007.

- zasada celowości: przetwarzanie danych powinno mieć określony cel; dalsze ich wykorzystywanie możliwe jest jedynie wtedy, gdy zgodne jest z pierwotnym celem przekazywania danych;
- zasada jakości danych oraz ich adekwatności: dane powinny być dokładne i aktualne oraz adekwatne do celu ich przekazywania;
- zapewnienie obowiązku informacyjnego: osoba, której dane dotyczą, powinna być poinformowana o celu przetwarzania tych danych oraz o administratorze danych w państwie trzecim;
- zabezpieczenie danych: powinny być zastosowane odpowiednie do istniejącego ryzyka środki techniczne i organizacyjne w celu zabezpieczenia danych osobowych;
- prawo dostępu do danych, poprawiania oraz sprzeciwu: osoba, której dane dotyczą, powinna mieć dostęp do informacji o przetwarzanych o niej danych, prawo do ich poprawiania, a w określonych sytuacjach także prawo sprzeciwu wobec ich przetwarzania;
- ograniczenie dalszego przekazywania danych: przekazywanie danych przez operatora w państwie trzecim kolejnemu podmiotowi dopuszczalne jest, co do zasady, jedynie wtedy, gdy podmiot otrzymujący dane jest również związany zasadami gwarantującymi odpowiednią ochronę danych osobowych.

Decyzja Komisji Europejskiej w przedmiocie poziomu ochrony

Zgodnie z art. 25 ust. 6 Dyrektywy, na podstawie oceny prawa wewnętrznego lub zobowiązań międzynarodowych danego kraju Komisja Europejska[18] może stwierdzić, że dane państwo zapewnia poziom ochrony wymagany w Dyrektywie. W wyniku wydania takiej decyzji dopuszczalny jest transfer danych osobowych do tego kraju już bez konieczności zapewniania dodatkowej kontroli, w tym badania, czy poziom ochrony jest odpowiedni, bądź wydawania dodatkowych aktów czy zawierania umów. Komisja uznała, iż taki poziom ochrony zapewniają Szwajcaria, Kanada oraz Wyspa Man. Z uwagi na różnice pomiędzy prawodawstwem Unii Europejskiej oraz Stanów Zjednoczonych, USA nie może być uznane za takie państwo.

Wyjątki od zakazu przekazywania danych osobowych do krajów niezapewniających należytego poziomu ochrony

Dyrektywa wprowadziła szereg wyjątków od zasady, iż dane osobowe mogą być przekazywane wyłącznie do kraju zapewniającego należytą ochronę. Dzieje się tak po pierwsze w sytuacji wykonywania obowiązku nałożonego na administratora danych przepisami prawa lub ratyfikowaną umową międzynarodową. Po drugie wówczas, gdy osoba,

18 W procesie oceny istotną rolę doradczą pełni Grupa Robocza art. 29.

której dane dotyczą, wyrazi zgodę na taki transfer. Zgodę należy rozumieć tak samo jak w przypadku wyrażania „zgody na przetwarzanie danych", gdyż transfer jest jedną z form przetwarzania[19], czyli jako oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana na podstawie oświadczenia woli o innej treści. Po trzecie wówczas, gdy przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, a po czwarte niezbędne do wykonania umowy w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem. Dodatkowo wprowadzono wyjątki zakładające przekazanie danych ze względu na dobro publiczne, ochronę żywotnych interesów podmiotu danych oraz danych ogólnodostępnych. *Ratio legis* tego ostatniego wyjątku leży w założeniu, iż dane takie i tak są dostępne dla nieograniczonego kręgu podmiotów i nie chodzi tylko o formalną jawność (na przykład rejestry publiczne), ale ich faktyczną dostępność (na przykład umieszczenie na stronie internetowej), przy czym należy pamiętać, że przekazanie będzie możliwe wówczas, gdy upublicznienie zostało dokonane zgodnie z przepisami prawa[20].

Ochrona danych osobowych w USA

Stany Zjednoczone mają zupełnie odmienne od europejskiego podejście do ochrony danych osobowych, gdyż nie mają jednego, federalnego, pełnego i wszechstronnego uregulowania dotyczącego ich zbierania i przetwarzania. Zamiast tego regulacja dokonywana jest sektorowo, wieloma różnymi aktami prawnymi, w tym regulaminami oraz przez tak zwaną samoregulację (*self-regulation)*. Wielość aktów prawnych sprawia, że normy w nich zawarte niejednokrotnie są ze sobą sprzeczne[21]. Na poziomie stanowym w większości przypadków wdrożono pewne regulacje dotyczące ochrony danych osobowych, są one jednak bardzo zróżnicowane i nie stanowią szczelnego systemu ochrony tak, jak to ma miejsce w UE. Ponadto w USA nie wymaga się ani kreowania niezależnych organów zajmujących się ochroną danych osobowych, ani rejestrowania baz danych, w których dane są przetwarzane, ani zgody podmiotu na przetwarzanie jego danych.

Przykładem ilustrującym różnice europejskich i amerykańskich regulacji oraz uświadamiającym potrzebę znalezienia konsensusu stała się sytuacja wynikła z amerykańskich regulacji wprowadzonych po ataku terrorystycznym na World Trade Center. USA zobowiązały wówczas linie lotnicze do podawania dokładnych informacji (między innymi

19 Tak: X. Konarski, G. Sibiga, *Zasady przekazywania danych osobowych do państwa trzeciego w prawie polskim i UE,* [w:] *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, s. 98.

20 *Ibidem*, s. 101.

21 I. Jolly z Loeb & Loeb LLP w artykule *Data protection in United States: overview* napisanym dla Practical Law. A. Thomson Reuters Legal http://uk.practicallaw.com/6–502–0467.

imienia, daty urodzenia, numeru karty kredytowej, narodowości) o pasażerach, którzy dokonali rezerwacji i odprawy. Wśród wymaganych informacji znalazły się także takie, które mogłyby być uznane za wrażliwie w rozumieniu Dyrektywy 95/46/WE. Linie niedostosowujące się do obowiązków musiałyby liczyć się z karami finansowymi. Z uwagi na oczywistą sprzeczność powyższego zarządzenia z przepisami dotyczącymi danych osobowych w UE w maju 2004 roku zawarto specjalną umowę zezwalającą na przesyłanie wymaganych przez USA danych[22].

Najważniejsze amerykańskie akty prawne z dziedziny ochrony danych osobowych to:

- *The Federal Trade Commission Act* (FTCA): krajowa ustawa chroniącą prawa konsumenta i zwalczającą nieuczciwe praktyki rynkowe. W praktyce ma zastosowanie do ochrony danych osobowych online i offline. i często jest podstawą roszczeń. Spod zakresu FTCA wyłączone są instytucje finansowe, transportowe i telekomunikacyjne,
- *The Financial Services Modernization Act*: reguluje gromadzenie, przetwarzanie i ujawnianie informacji finansowych. Ma zastosowanie w wypadku banków, firm ubezpieczeniowych i odszkodowawczych oraz innych instytucji świadczących usługi finansowe,
- *The Health Insurance Portability and Accountability Act*[23]: dotyczy danych medycznych,
- *The Controlling the Assault of Non-Solicited Pornography and Marketing Act*[24] i the *Telephone Consumer Protection Act*: regulują gromadzenie i wykorzystywanie adresów e-mail, numerów telefonów i adresów zamieszkania.

Każda z tych regulacji zawiera własne wyłączenia, własne wymagania dotyczące zgody na przetwarzanie danych i warunków tego przetwarzania, własne odrębności dotyczące danych sensytywnych, obowiązków informacyjnych i egzekucji roszczeń.

Regulacja amerykańska ma coraz liczniejszych przeciwników[25] oraz wpływowych zwolenników. Rząd, zdaniem przedstawicieli biznesu, powinien powstrzymać się od regulowania tej sfery, bo brak obostrzeń napędza innowacyjność w Internecie[26]. Z zasygnalizowaniem takiego stanowiska można spotkać się także w polskiej doktrynie[27]. Przeciwnicy wprowadzania restrykcji, poza powoływaniem się na korzyści płynące z innowacyjności, zwracają także uwagę na to, że Amerykanie sami nie dbają o swoje dane, gdyż umieszczają ich codziennie na portalach społecznościowych setki gigabajtów, więc wprowadzanie obostrzeń będzie działaniem na wyrost. Jest to jednak, jak się wydaje,

22 A. Savin, *op. cit.*, s. 205.

23 W skrócie: HIPAA.

24 W skrócie: CAN-SPAM Act.

25 W tym charakterze na łamach Wall Street Journal wypowiadał się Thomas H. Davenport, pracownik naukowy Harvard Business School http://online.wsj.com/article/SB10001424127887324338604578328393797127094.html (wejście 10 października 2013 r. o 9:49).

26 H. P. Gotting, C. Schertz, W. Seitz, *op. cit.*, Monarium 2009, s. 1175.

27 J. Barta, R. Markiewicz, P. Fajgielski *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 28.

jedynie pusty slogan, gdyż świadomość potrzeby ochrony prywatności, choć niższa niż u Europejczyków, stale wzrasta, o czym świadczą wyniki raportu PEW Institute[28], według którego aż 86% Amerykanów przedsięwzięło kroki w celu usunięcia bądź ukrycia śladów, jakie pozostawili w sieci, a przeważająca większość użytkowników chciałaby pozostać w sieci anonimowa. Co więcej, aż 66% użytkowników uważa obecną regulację za niewystarczającą w zakresie ochrony prywatności online, przy czym tylko 24% uważa ją za wystarczająco dobrą. Wyrazem tych statystyk jest coraz głośniej wyrażana krytyka liberalnego podejścia uznająca samoregulację za porażkę amerykańskiego systemu.

Prekursorem ochrony danych osobowych w USA jest Kalifornia[29]. RTamtejsze regulacje niejednokrotnie są przełomowe i dają impuls dla wprowadzenia regulacji krajowych. Przykładowo: w 2002 roku Kalifornia wprowadziła system informowania o naruszeniach ochrony danych i od tego czasu analogiczna regulacja pojawiła się w każdym stanie. Jednym z najważniejszych dokonań Kalifornii było wydanie w 2004 roku *Online Privacy Protection Act* („OPPA"), który wymaga od operatorów stron internetowych umieszczania w widocznym miejscu informacji o stosowanej przez nich polityce prywatności. Najnowszym osiągnięciem kalifornijskiej legislacji w tym zakresie jest projektowany *Right to Know Act* z 2013 roku, który ma umożliwić konsumentom między innymi wgląd i otrzymanie kopii pełnego katalogu danych, które zostały o nich zebrane przez dane firmy oraz uzyskanie informacji o tym, komu zostały ujawnione. Decyzja o jego wejściu w życie zostanie podjęta w 2014 roku.

Obecnie polityka USA w zakresie ochrony danych osobowych ulega ewolucji w kierunku zaostrzenia rygorów co do ich przetwarzania. Potwierdzeniem dla tej tezy jest raport *Consumer data privacy in a networked world*: *A framework for protecting privacy and promoting innovation in the global digital economy*[30] wydany w lutym 2012 roku przez rząd USA. Dokument otwierają słowa Baracka Obamy: „Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones", co świadczy o wzroście zainteresowania ukształtowaniem na nowo dotychczasowej regulacji. Choć dokument nie ma mocy wiążącej, przemawia za nim siła autorytetu, przez co uważa się go za wskazujący nowy kierunek i standardy w zakresie ochrony danych osobowych w USA. Możemy w nim znaleźć zalecenia adresowane między innymi do amerykańskich firm, by te umożliwiały konsumentom kontrolę sposobu zbierania oraz wykorzystywania dotyczących ich danych.

---

28 http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

29 Prawo Kalifornii jest pierwszym, które wprowadziło „prawo do bycia zapomnianym" (*right to be forgotten*). Szczegółowe informacje można znaleźć na stronie internetowej *California Legislative Information:*
http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

30 Dostępny pod adresem: http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf .

Safe Harbour

By nie dopuścić do osłabienia ochrony, w Unii Europejskiej co do zasady zabrania się transferu danych do krajów niezapewniających adekwatnego poziomu ochrony. Za takie państwo uznawane są Stany Zjednoczone. Jednocześnie po stronie europejskich firm istnieje duże zapotrzebowanie na amerykańskie oprogramowanie i serwery służące przetwarzaniu danych. Dochodzi zatem do zderzenia interesów i dwóch skrajnie różnych spojrzeń na problematykę ochrony danych osobowych. W rezultacie, by nie wstrzymywać wymiany gospodarczej, konieczne było wprowadzenie w tym zakresie kompromisowej regulacji. Tę rolę miał spełniać Program Safe Harbour, którego celem było danie europejskim firmom gwarancji, że podlegające transferowi dane osobowe będą miały zapewniony w USA podobny do europejskiego poziom ochrony. Opracowany został przez Departament Handlu Stanów Zjednoczonych w porozumieniu z Komisją Europejską (decyzja Komisji 520/2000/WE z 26 lipca 2000 roku) i umożliwia amerykańskim podmiotom gospodarczym sprostanie wymaganiom Dyrektywy. Uzyskanie certyfikatu w ramach Programu S. H. przez uczestniczące w nim podmioty świadczy o tym, że gwarantują one odpowiedni poziom ochrony danych osobowych, o którym mowa w Dyrektywie 95/46/WE. Okazało się jednak, iż Program nie spełnia przewidzianej dla niego roli. Przyczyny takiego stanu rzeczy zostaną szczegółowo omówione.

S. H. jest systemem opartym na dobrowolnym zobowiązaniu się przez amerykańskie firmy przetwarzające dane osobowe pochodzące z UE do przestrzegania podstawowych zasad ochrony danych osobowych obowiązujących w Unii. Program S.H. przewiduje bardzo łagodne warunki przystąpienia i pozostawia szerokie pole do interpretacji hasłowo sformułowanych wymogów członkostwa w Programie. Do wymogów tych należą:

- obowiązek informacyjny: osoby, których dane dotyczą, muszą zostać poinformowane o tym, że ich dane zostały zebrane oraz o sposobie ich wykorzystania;
- dalsze przekazanie danych: osoby, których dane dotyczą, mogą nie wyrazić zgody na dalsze przekazanie danych;
- transfer: transfer danych może nastąpić wyłącznie do podmiotu, który spełnia wymogi należytej ochrony;
- bezpieczeństwo: należy podjąć rozsądne środki w celu zapobieżenia utracie danych;
- celowość: zebrane dane muszą być istotne dla celu, w którym zostały zebrane;
- dostęp: osoby, których dane dotyczą, muszą mieć dostęp do zebranych o nich danych oraz mieć możliwość skorygowania błędów;
- egzekucja: należy zapewnić efektywne środki egzekwowania powyższych reguł.

Zobowiązanie do przestrzegania zasad Programu odbywa się poprzez oficjalne powiadomienie Departamentu Handlu USA (*self certification letter*) i powinno być corocznie odnawiane. Lista organizacji jest sporządzana przez Departament Handlu.

Procedura polegająca na samocertyfikacji opiera się na złudnym założeniu, iż firmy będą się same kontrolować, dobrowolnie wprowadzać kosztowne obostrzenia oraz same sobie odbierać status certyfikowanych. Podejście takie wydaje się nieprawidłowe także z tego powodu, że w Stanach Zjednoczonych brakuje wielowiekowej kultury prawnej w zakresie zbierania i przetwarzania danych, więc narzucone przez S. H. działania nie są dla amerykańskich firm naturalne. W USA brakuje także efektywnych mechanizmów egzekwowania postanowień wynikających z S. H. – problemy rozwiązywane są przez indywidualne, ustalane przez każdą z firm w miarę potrzeby systemy rozwiązywania problemów.

Analizując prawo USA, w 2010 roku grupa niemieckich rzeczników ochrony danych osobowych, tak zwana „Düsseldorf Group", w swojej decyzji[31] dotyczącej legalności transferów danych z Niemiec do USA w ogóle zakwestionowała, w zakresie niektórych grup danych możliwości egzekwowania zasad Programu S. H. przez organy amerykańskie. Wynikało to z faktu, iż naruszenie S. H. traktowane jest jako działanie naruszające zasady uczciwych praktyk rynkowych w rozumieniu Federal Trade Commission Act i z tego powodu egzekwowane właśnie przed tym organem. Jednakże FTC ma jurysdykcję wyłącznie nad osobami fizycznymi i przedsiębiorstwami, ale już nie nad bankami i innymi instytucjami finansowymi, więc w tym zakresie egzekwowanie spełnienia warunków S. H jest po prostu niemożliwe. „Düsseldorf Group" we wspomnianej wcześniej decyzji postawiła także inne tezy. Uznała między innymi, iż do czasu, aż nie zostanie wprowadzony urzędowy system weryfikacji spełnienia wymogów S. H., obowiązek zbadania spełnienia warunków oraz ważności certyfikatu ciąży na stronie europejskiej. Grupa rekomendowała także wprowadzenie, na wypadek istnienia wątpliwości co do wiarygodności amerykańskiego kontrahenta, odpowiednich klauzul umownych mających zniwelować negatywne skutki niedotrzymania warunków. Zalecenie takiego zapobiegawczego działania można odczytać także z rekomendacji Grupy Roboczej art. 29: *Companies cannot rely on cloud providers' „self-certification" that they comply with Safe Harbor standards*[32]. Powyższe stanowisko grupy niemieckich rzeczników przesuwa ciężar udowodnienia spełnienia standardów z amerykańskich, certyfikowanych Programem S. H. firm na firmy europejskie, co stawia pod znakiem zapytania celowość istnienia certyfikatu.

Przestrzeganie zasad S. H.

Raporty Komisji Wspólnot Europejskich

W 2002 roku, w dwa lata po wprowadzeniu Programu, Komisja Wspólnot Europejskich wydała, w odezwie na apel Parlamentu Europejskiego, pierwszy raport dotyczący

31 Decyzja dostępna pod adresem: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile.

32 H. H. Wohlgemuth, J. Gerloff, *op. cit.*, s. 17.

funkcjonowania Programu S. H. Przyznano w nim, że w porównaniu do stanu sprzed wprowadzenia S. H., kontakty gospodarcze między UE a USA są znacznie ułatwione, a sam Program zmniejszył niepewność prawa i obawy przed zawieraniem kontraktów. Stwierdzono, że wszystkie elementy Programu S. H. wdrożono, ale wciąż duża liczba certyfikowanych organizacji nie dotrzymuje oczekiwanego poziomu transparentności prowadzonej przez siebie polityki prywatności. Komisja podkreśliła, iż transparentność w systemach samocertyfikowania jest kwestią bardzo istotną, więc działanie organizacji wymaga znacznej poprawy. Komisja nalegała na restrykcyjne przestrzeganie S. H. i zachęcała do uczestnictwa w nim. Przyznała także, że ilość firm, które przystąpiły do Programu jest niższa niż spodziewana, jednak podkreśliła, iż pozostałe amerykańskie firmy mogą zapewniać odpowiedni poziom ochrony poprzez klauzule umowne.

W roku 2004 Komisja Wspólnot Europejskich wydała kolejny raport. Najważniejsze z poczynionych spostrzeżeń dotyczyło tego, iż nie wszystkie organizacje, które określają się jako certyfikowane, faktycznie nimi są. Ponadto nie wszystkie firmy zamieszczają na swoich stronach informacje o polityce prywatności. Stwierdzono, że należy wprowadzić mechanizmy weryfikujące spełnienie warunków przed umieszczeniem danej organizacji na liście S. H., co było jasnym sygnałem, iż ówczesny system samocertyfikacji się nie sprawdził.

Raporty Galexii

Galexia, niezależna i renomowana australijska firma konsultingowa specjalizująca się w zagadnieniach prywatności i handlu elektronicznego także przygotowała, bardziej wyczerpujące niż te pochodzące od Komisji, raporty ewaluujące Program S. H.

Pierwszy z nich – *The Safe Harbor – Fact or Fiction* autorstwa Chrisa Conolliego, dyrektora Galexii – został opublikowany w 2008 roku[33]. We wstępie raport ocenił wszystkie 1597 umieszczonych na liście firm pod kątem podstawowych kryteriów, które należy spełnić, jeśli chce się uzyskać certyfikat. Następnie skupił się wyłącznie na jednej z przesłanek warunkujących członkostwo w Programie, mianowicie możliwości egzekwowania praw i zapewnienie systemu rozwiązywania sporów.

Z raportu wynika, że wiele aspektów S. H. nie funkcjonuje poprawnie. Tylko 1109 z 1597 organizacji umieszczonych na liście było w chwili dokonywania badań członkami Programu S. H. Wiele firm znajdujących się na liście przestało w ogóle prowadzić działalność bądź nie odnowiło swojego certyfikatu. Firmy często bądź nie opublikowały informacji o swojej polityce prywatności, bądź nawet nie wspomniały o uczestniczeniu w Programie. Tylko 348 firm spełniło szczegółowo badaną w raporcie przesłankę możliwości egzekucji i wprowadzenia metod rozwiązywania sporów. Do zbadania pozostało

33 Raport jest dostępny pod adresem: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.

jeszcze 6 innych przesłanek, co pozwala wnosić, iż procent firm, które spełniłyby wszystkie wymogi byłby skrajnie niski.

Z raportu wynika zalecenie dla UE, by ta renegocjowała ze Stanami Zjednoczonymi całość Programu. Natomiast dla USA sformułowano zalecenie zweryfikowania poziomu ochrony danych osobowych we wszystkich umieszczonych na liście firmach. Conolly polecił także, podobnie jak Düsseldorf Group i Grupa Robocza art. 29, by europejscy kontrahenci przeprowadzili własne badania dotyczące poziomu ochrony danych osobowych przestrzeganej przez drugą stronę kontraktu, nie pokładając całego zaufania w S. H.

Conolly powtórzył swoje stanowisko w październiku 2013roku[34], oświadczając Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego, iż „many claims of Safe Harbour membership are false", a następnie doprecyzował, iż fałszywe jest jedno na siedem zgłoszeń[35]. Liczba fałszywych zgłoszeń wzrosła względem badań przeprowadzonych w 2008 roku i we wrześniu wyniosła 427. Część z firm, które nie były faktycznymi uczestnikami Programu, umieściła logo certyfikatu na swoich stronach internetowych. Wciąż około 30% firm nie zapewnia metod rozwiązywania sporów, które są jednym z siedmiu warunków uczestniczenia w Programie. Wciąż, jak zaznaczono wcześniej, z uwagi na brak jurysdykcji FTC dane finansowe i telekomunikacyjne pozostają wyłączone z Programu S. H. Conolly powtórzył także zalecenie kierowane w stronę europejskich firm, by te nie opierały się wyłącznie na S. H., a sprawdzały poziom ochrony danych osobowych amerykańskich kontrahentów na własną rękę.

Po pojawieniu się tej opinii Komisja Europejska przyznała, iż Program S. H. może mieć luki legislacyjne („it is possible the agreement contains loopholes"), a wcześniej, w lipcu 2013roku, europejska komisarz do spraw sprawiedliwości Viviane Reding przyznała, iż Program S. H. przestał spełniać swoją funkcję gwaranta: „The Safe Harbour agreement may not be so safe after all".

Transfer danych osobowych w rozporządzeniu o ochronie danych osobowych

Uregulowaniu transferu danych do państw trzecich będzie miało okazję przysłużyć się nowe europejskie rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych[36]. Odejście od formy dyrektywy na rzecz rozporządzenia ujednolici w zupełności uregulowanie tej materii w Unii Europejskiej. Projekt Rozporządzenia został oficjalnie opublikowany przez Komisję Europejską w dniu 25 stycznia 2012 roku[37]; procedura uchwalania następuje

34 Stanowisko dostępne pod adresem: http://www.galexia.com/public/about/news/about_news-id225.html.

35 O tym N. Nielsen dla EU Observer http://euobserver.com/justice/121695.

36 Dalej jako: „Rozporządzenie".

37 Brussels, 25.1.2012, COM(2012) 11 final C7–0025/12.

w tak zwanym trilogu, czyli ustalaniu ostatecznej wersji projektu między PE, Komisją Europejską i Radą Europejską. Ostatnie spotkanie szefów rządów i państw Unii Europejskiej z 24 i 25 października 2013 roku dało wyraźny sygnał, iż państwa UE uważają za konieczne jak najszybsze zakończenie prac.

Ostateczne brzmienie Rozporządzenia nie zostało jeszcze ustalone, ale z propozycji Komisji oraz poprawek Prezydencji Litewskiej i Komisji LIBE wynika, iż regulacja dotycząca transferu danych do państw trzecich ma podlegać szerszym restrykcjom. Zgodnie z rozporządzeniem przekazanie danych osobowych będzie możliwe bądź dzięki wydaniu decyzji Komisji stwierdzającej odpowiedni poziom ochrony, bądź poprzez gwarancje udzielone przez podmiot, któremu dane mają zostać przekazane, bądź w sytuacjach wyjątkowych.

Podsumowanie

Program Safe Harbour zawiódł oczekiwania; okazało się, iż system samocertyfikacji nie jest wystarczający dla tak istotnego dla Europejczyków zagadnienia, jakim jest ochrona danych osobowych. Z czasem europejskie przedsiębiorstwa, kierując się także zaleceniami Grupy Roboczej art. 29 oraz niezależnych ośrodków badawczych, przestały polegać na Safe Harbour i zaczęły wprowadzać do umów odrębne postanowienia dotyczące ochrony danych osobowych oraz odpowiedzialności za ich nieprzestrzeganie. Tym samym Program S. H. stracił rację bytu, gdyż przestał być postrzegany jak gwarant ochrony; ciężar weryfikacji bezpieczeństwa znów spoczął na barkach europejskich przedsiębiorstw.

Szansą na poprawienie skuteczności S. H. byłoby wprowadzenie organów nadzoru, które na bieżąco kontrolowałyby przedsiębiorstwa pod kątem spełniania przesłanek wymaganych do uczestniczenia w Programie.

Przyszłość Programu stoi pod znakiem zapytania z uwagi na projektowane Rozporządzenie, gdyż na chwilę obecną jego ostateczny kształt nie jest jeszcze znany i nie da się z pewnością stwierdzić, czy procedura samocertyikacji będzie uznana za zapewniającą należyty poziom ochrony.

SUMMARY

The Safe Harbour Program – a bridge between the European and American systems of personal data protection

The article is devoted to a comparison of the American and European systems of data protection and the transfer of personal data from the European Union to the United States of America. The author outlines the problems and then analyzes the regulations in order to identify differences between the two systems. Then, based on the previous considerations, she assesses the effectiveness of the Safe Harbour Program, which was set up to serve as a tool to facilitate the transfer of personal data. The article ends by providing information about the directions of policy changes and work on the new EU Regulation on the protection of personal data.

Keywords: Safe Harbour Program, system of personal data protection, legal systems comparison