MARTA BŁOTNY
Wydział Prawa i Administracji,
Uniwersytet im. Adama Mickiewicza w Poznaniu

Prawo do ochrony danych osobowych w Konstytucji RP na tle prawa Unii Europejskiej oraz orzeczenia Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-362/114 *Schrems* v. *Data Protection Commissioner*

Wprowadzenie

20-lecie Konstytucj RP to okazja do dokonania weryfikacji i zdystansowanego spojrzenia na zawarte w niej regulacje, tworzone w specyficznych okolicznościach i funkcjonujące przez ostatnie dwadzieścia lat w dynamicznie zmieniającej się rzeczywistości. Dwie minione dekady pozwoliły na wypełnienie wielu przepisów dodatkową treścią wyrosłą z praktyki orzeczniczej oraz refleksji doktryny. Znamiennym wydarzeniem było również wejście Polski do Unii Europejskiej w 2004 r., które nadało nowy kontekst interpretacyjny wielu przepisom zawartym w Konstytucji.

Jednym z zagadnień, które zmienia się wyjątkowo dynamicznie ze względu na wyzwania współczesnego świata jest prawo do ochrony danych osobowych wyrażone w art. 51 Konstytucji RP. Co więcej, jest ono również przedmiotem regulacji prawa Unii Europejskiej. Wraz z wejściem w życie Traktatu z Lizbony w 2009 r. prawnie wiążąca stała się Karta Praw Podstawowych[1], a tym samym zawarte w jej art.

[1] Dz. Urz. UE C 326 z 26.10.2012, s. 391.

7 i 8 prawo do ochrony danych osobowych zyskało status samodzielnego prawa podstawowego[2]. Stąd też prawo do ochrony danych osobowych odczytywać należy również przez pryzmat regulacji unijnych, pamiętając o szczególnej uwadze, jaką zagadnienie to darzy się w Unii Europejskiej.

Konstytucyjne prawo do ochrony danych osobowych jest jednym z tych, które ze względu na rozwój technologii stają się coraz ważniejsze we współczesnym świecie i dostosowywać się muszą do wyzwań zmieniającej się rzeczywistości, zyskując coraz to nowe aspekty. Dlatego też zasadne wydaje się, omawiając prawo do ochrony danych osobowych wyrastające zarówno z przepisów polskich, jak i unijnych, odwołać się do orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej ze szczególnym uwzględnieniem sprawy Maximiliana Schremsa[3], która w symboliczny sposób unaocznia znaczenie prawa wspólnotowego i jego znaczącego wpływu na polskie regulacje w tym zakresie.

Polska w Unii Europejskiej

Zagadnienie ochrony danych osobowych jest jednym z tych, które w Unii Europejskiej otacza się szczególnym zainteresowaniem, a stworzony w ramach Wspólnoty standard ochrony jest jednym z najlepiej chroniących interesy jednostki. Kiedy ponad dwadzieścia lat temu powstała

[2] Boillat P., Kjaerum M., *Handbook on European data protection law*, Luxemburg 2014, str. 3.
[3] C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner* (EU:C:2015:650).

Konstytucja RP członkowstwo w Unii Europejskiej i integracja z państwami Zachodu były jednymi z priorytetów i celem, do którego dążyły władze państwa, a przystąpienie Polski do Unii Europejskiej stało się jednym z wyzwań ustrojowych, któremu nowa Konstytucja musiała sprostać i nadać mu formę norm prawnych. Było to konieczne przede wszystkim dla zapewnienia efektywności prawu unijnemu, w którego system Polska miała zostać włączona. Ostatecznie uczyniono to w formie art. 90 Konstytucji, który zezwolił na przekazanie kompetencji organów władzy państwowej w niektórych sprawach organizacji międzynarodowej lub organowi międzynarodowemu. W doktrynie aprobuje się tego rodzaju rozwiązanie legislacyjne, podkreślając, że słusznie zastosowano konstrukcję ogólną, stawiając jednocześnie warunek, że daną organizację „musi łączyć z Polską wspólny system wartości uniwersalnych”[4], co miało zapewnić, by Polska wstępowała do organizacji międzynarodowych łączących państwa demokratyczne i przestrzegające praw człowieka, a katalog praw i wolności wyrażonych w Konstytucji spełniać musiał standardy europejskie.

Prawo do prywatności a ochrona danych osobowych

Prawo do ochrony danych osobowych uznaje się za jeden z aspektów szeroko rozumianego prawa do prywatności,

[4] Wójtowicz K., *Konstytucja RP z 1997 r. a członkowstwo Polski w Unii Europejskiej* [w:] *Prawo Unii Europejskiej. Zagadnienia systemowe. Prawo materialne i polityki*, red. Barcz J., Warszawa 2006, str. 462.

a to w Konstytucji RP uregulowano poprzez zespół przepisów zawartych w rozdziale drugim, a więc jako jedną z wolności i praw osobistych. Regulacją kluczową, bo dotykającą również pozostałych emanacji tego prawa, pozostaje art. 47, na mocy którego każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Pozostałe normy dotyczące prywatności zawarto m.in. w art. 39 (zakaz eksperymentów naukowych bez zgody osoby zainteresowanej), art. 41 (gwarancja nietykalności i wolności osobistej), art. 45 ust. 2 (wyłączenie jawności rozprawy), art. 51 (ochrona danych osobowych), art. 52 (swoboda poruszania się), art. 53 (wolność sumienia i religii).

Doktryna wyraża jednak wątpliwość, czy normy dotyczące prywatności kreują trudno definiowalne konstytucyjne „prawo do prywatności", z którego wyrastać miałby szereg dalszych norm, czy raczej źródła tych gwarancji szukać należy w wyrażonej art. 47 autonomii jednostki[5], określonej jako „prawo do decydowania o swoim życiu osobistym". Zasada autonomii jednostki wyrasta z kolei wprost z zasady godności człowieka, stanowiącej, obok zasad wolności i równości, jedną z węzłowych idei, z których wyrasta cały system praw i wolności proklamowanych w polskiej Konstytucji.

Prawo do ochrony danych osobowych wyrasta natomiast bezpośrednio z art. 51, stanowiącego uszczegółowienie pojemnej normy art. 47. Stąd też, biorąc pod uwagę, iż norma art. 51 dotyczy relacji wertykalnej i przyznaje

[5] Konstytucja RP. Tom I. Komentarz do art. 1-86, red. Bosek L., Safjan M.Warszawa 2016, wyd. 1, komentarz do art. 47.

jednostce prawo do ochrony swoich danych przed ingerencją ze strony władzy publicznej, prawa do ochrony przed działaniami podmiotów prywatnych upatrywać należy w uniwersalnej normie ustanowionej w art. 47[6].

Warto zauważyć, co podkreśla się w doktrynie, że samo pojęcie „prawa do ochrony danych osobowych" „(…) nie należy do konstytucyjnej siatki pojęciowej" [7], jest natomiast uzasadnione z punktu widzenia terminologii używanej w prawie międzynarodowym, a w szczególności w prawie Unii Europejskiej.

Art. 51 stanowi konkretyzację prawa do prywatności w aspekcie proceduralnym[8] i jest zdecydowanie bardziej precyzyjny od art. 47, który określa raczej standard stanowiący podstawę dla dalszej ochrony danych[9]. Głosi on, iż nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby (ust. 1), władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (ust. 2), każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa (ust. 3), każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą (ust. 4), zasady i tryb

[6] Ibidem.
[7] Sakowska-Baryła M. *Konstytucjonalizacja prawa do ochrony danych osobowych w Polsce* [w:] Przegląda Prawa Konstytucyjnego 2016/4, str. 128.
[8] Wyrok TK z 19 maja 1998 r., sygn. U 5/97.
[9] Konstytucja RP. Tom I. Komentarz do art. 1-86, red. Bosek L., Safjan M.Warszawa 2016, wyd. 1, komentarz do art. 51.

gromadzenia oraz udostępniania informacji określa ustawa (ust. 5).

W przypadku gwarancji wyrażonej w ust. 1 oraz 3, 4 zakres podmiotowy obejmuje wszystkie jednostki, natomiast w ust. 2 ograniczony jest on do obywateli polskich. Zobowiązanymi do przestrzegania wyrażonego w art. 51 zakazu są władze publiczne; w przypadku podmiotów prywatnych, należy, jak już wspominano, odnosić się do gwarancji z art. 47. Istotą art. 51 jest, jak i w odniesieniu do art. 47, autonomia jednostki względem wszelkiej informacji „bez względu na jej zawartość treściową”[10]

Ustawa o ochronie danych osobowych

Art. 51 ust. 5 zakłada, że zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa; przepis ten stanowi uzupełnienie ust. 4, który przewiduje, iż władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Norma ust. 5 art. 51 jest w oczywisty sposób zbieżna unormowaniami art. 31 ust. 3 Konstytucji RP wyrażającego zasadę proporcjonalności ograniczeń wolności i praw, które mogą być ustanawiane tylko w akcie normatywny o randze ustawowej. W tym wypadku jest nim ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Dz.U. 1997 nr 133 poz. 883), która spełnia jednak zdecydowanie większą rolę niż tylko regulującą sposoby pozyskiwania, gromadzenia i udostępniania informacji o obywatelach przez władze państwowe. Nakaz

[10] Ibidem.

dalszego uregulowania materii ochrony danych osobowych zawarty w omawianej normie „obejmuje kompleksowe unormowanie problematyki ochrony danych osobowych, w tym również w relacjach horyzontalnych”[11], a więc szerzej niż tylko w relacji jednostka-państwo. Tak więc ustawa ta, zgodnie zresztą z intencją twórców[12], uregulowała kompleksowo materię ochrony danych osobowych, nie ograniczając jej tylko do ingerencji ze strony władz publicznych.

Powstawała ona jako nowy akt normatywny regulujący nieregulowaną dotąd materię w oparciu o rozwiązania przyjęte w dyrektywie 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 z 23.11.1995,), stanowiącej wciąż jeszcze główny akt prawny Unii Europejskiej dotyczący ochrony danych osobowych. Polska już w Układzie Europejskim ustanawiającym stowarzyszenie między Rzecząpospolitą Polską z jednej strony a Wspólnotami Europejskimi i ich Państwami Członkowskimi z drugiej strony, sporządzonego w Brukseli dnia 16 grudnia 1991 r. (Dz. U. z 1994 r. Nr 11, poz. 38, zał.) zobowiązała się do zbliżania istniejącego i przyszłego ustawodawstwa Polski do ustawodawstwa istniejącego we Wspólnocie, choć przyjęte w ustawie rozwiązania wymagały jeszcze dostosowania do prawa unijnego po wejściu Polski do Unii Europejskiej w 2004 r.

[11] Ibidem.

[12] Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz, wyd. VI*, Warszawa 2015.

Sprawa Maximilliana Schremsa

Polskie przepisy prawne nie funkcjonują więc w próżni, a bardzo istotny kontekst interpretacyjny stanowi dla nich orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej. Wchodząc do Unii Europejskiej Polska wkroczyła w system rozwiązań prawnych rozciągający się na wszystkie państwa członkowskie oraz z bogatym orzecznictwem i charakterystyczną rolą Trybunału Sprawiedliwości, a także, co sprawa Schremsa dobitnie pokazała, z pięciuset milionami obywateli, którym specyficzne procedury pozwalają na podejmowanie samodzielnych działań o charakterze obywatelskim, szczególnie w sytuacji, gdy działania podejmowane przez instytucje unijne są nieskuteczne[13]. Prześledzenie ścieżki jaką sprawa ta przeszła przez kolejne instytucje, najpierw krajowe, później wspólnotowe, pozwala unaocznić znaczenie jego działań, których ostateczne skutki odczuwalne są na terenie całej Unii Europejskiej i wpłynęły na weryfikację dotychczasowych regulacji w zakresie danych osobowych.

Austriak Maximillian Schrems w 2013 roku złożył skargę do irlandzkiego komisarza ds. ochrony danych osobowych, na działania zarejestrowanej w Irlandii spółki Facebook Ireland Ltd. Skarga, dotycząca transferowania do Stanów Zjednoczonych danych osobowych europejskich użytkowników serwisu, gdzie niemal nieograniczony dostęp miały do nich amerykańskie służby, uruchomiła proces, który

[13]Azoulai L., van der Sluis M., *Institutionalizing personal data protection in times of global institutional distrust: Schrems* [w:] Common Market Law Review nr 53, 2016, str. 1344.

zaowocował w 2015 r. orzeczeniem TSUE. Jest ona rezultatem działań samego Schremsa oraz Edward Snowdena, który w 2013 r. ujawnił skalę działań oraz nadużyć ze strony amerykańskich służb, które miały praktycznie nieograniczony dostęp do danych gromadzonych przez amerykańskie przedsiębiorstwa na swoich serwerach.

Sprawa Schremsa nie jest jedyną, która w ostatnich latach dotknęła materii ochrony danych osobowych, wpływając bezpośrednio na wspólnotowy, jak i polski system prawny[14], jednak jawi się szczególnie wyraźnie, przede wszystkim ze względu na ogromną skalę oddziaływania orzeczenia, które miało bezpośrednie przełożenie na codzienną sytuację tak ogromnej liczby obywateli Unii Europejskiej. W samej Polsce, według statystyk Facebooka, korzysta z niego codziennie ponad piętnaście milionów użytkowników, co stanowi około dwóch trzecich wszystkich użytkowników Internetu w Polsce. W Unii Europejskiej natomiast prawie ćwierć miliarda ludzi. W 2013 r. M. Schrems złożył skargę do irlandzkiego komisarza ds. ochrony danych osobowych, w której zażądał, aby organ ten, w wykonaniu swoich kompetencji, zakazał spółce Facebook Ireland przekazywania jego danych osobowych do Stanów Zjednoczonych. Podniósł on w skardze, że prawo i praktyka obowiązujące we

[14] Warto wyróżnić najbardziej istotne sprawy rozpatrywane przez Trybunał: C-131/12*Google Spain SL, Google Inc.* przeciwko *Agencia Espanola de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* (Dz.Urz. UE L Nr 212, s. 4–5), wyrok w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland Ltd* przeciwko *Minister for Communications i in., oraz Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl i in.* (Dz.Urz. UE L Nr 175, s. 6–7).

wskazanym państwie nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na jego terytorium przed działaniami nadzorczymi prowadzonymi w nim przez władze publiczne. Schrems odniósł się w tym względzie do informacji ujawnionych przez Snowdena na temat działalności amerykańskich służb wywiadowczych, a w szczególności służb National Security Agency. Stany Zjednoczone, szczególnie po 11 września, wzmocniły inwigilację i zezwoliły służbom bezpieczeństwa na szerszy dostęp do prywatnych danych.

Sprawa została odrzucona przez irlandzkiego komisarza, który uznał, że jest w tej sytuacji związany decyzjami Komisji Europejskiej, która w decyzji 2000/520, kreującej system Safe Harbour – system tzw. bezpiecznej przystani - stwierdziła, że Stany Zjednoczone zapewniały odpowiedni stopień ochrony. Decyzja ta stanowiła podstawę dla transferowania danych przez Atlantyk. Przystąpienie do programu było dla amerykańskich przedsiębiorstw dobrowolne i polegało na przedstawieniu przez organizację wydanego przez siebie certyfikatu w amerykańskim Departamencie Handlu zaświadczającego, że organizacja będzie przestrzegać zasad zgodnie z instrukcjami określonymi w decyzji. W praktyce nie dawało to unijnym instytucjom żadnej kontroli nad prawidłowym wykonywaniem postanowień.

Od negatywnej decyzji komisarza Schrems odwołał się do irlandzkiego Sądu Najwyższego, który na sposób przekazywania i przetwarzania danych do państw trzecich spojrzał abstrahując w pewnym sensie od prawa wspólnotowego, lecz podkreślając potencjalne naruszenia irlandzkiej konstytucji. Irlandzki SN stwierdził, że prawo

irlandzkie zakazuje przekazywania danych osobowych poza terytorium krajowe, z wyjątkiem przypadków, w których dane państwo trzecie zapewnia odpowiedni stopień ochrony życia prywatnego oraz praw i wolności podstawowych, o czym nie może być mowy w przypadku Stanów Zjednoczonych. Masowy dostęp do danych osobowych jest w oczywisty sposób sprzeczny z podstawowymi wartościami chronionymi przez irlandzką konstytucję. Zdaniem High Court gdyby sprawa w postępowaniu głównym miała zostać rozstrzygnięta wyłącznie na podstawie prawa irlandzkiego, należałoby stwierdzić, że komisarz miał obowiązek przeprowadzenia dochodzenia w przedmiocie okoliczności faktycznych przedstawionych przez M. Schremsa w jego skardze, którą niesłusznie oddalił.

W tych okolicznościach High Court postanowił zawiesić postępowanie i przedłożyć Trybunałowi pytanie prejudycjalne, sprowadzające się do tego, czy niezależny urzędnik, któremu powierzono funkcje administracyjne i wykonawcze w odniesieniu do ochrony danych, jest bezwzględnie związany postanowieniami Komisji wyrażonymi w decyzji dotyczącej systemu Safe Harbour, że Stany Zjednoczone zapewniają adekwatny stopień ochrony danych osobowych. Pytanie prejudycjalne w sprawie Schremsa w istocie dotyczyło więc przede wszystkim kompetencji organów państw członkowskich do rozpatrywania skarg i stopnia ich związania decyzjami Komisji.

Trybunał w swojej argumentacji skupił się więc przede wszystkim na kompetencjach organów państw członkowskich, dla których podstawę prawną ich działania stanowi wspominana już dyrektywa 95/46/WE. Ostatecznie uznał, że decyzja Komisji nie stoi na przeszkodzie temu, by

dany organ państwa członkowskiego rozpatrzył daną skargę samodzielnie, bez względu na istniejącą już w tej sprawie decyzję Komisji Europejskiej. Dodatkowo uznał również, że decyzja w sprawie Safe Harbour jest nieważna, co miało doniosłe znaczenie, ponieważ natychmiast pozbawiło podstawy prawnej dla transferu danych przez przedsiębiorstwa, które przystąpiły do tego programu – nie tylko Facebooka, ale również Google czy Microsoft.

Trybunał podkreślił tutaj specyficzny, zdecentralizowany charakter systemu ochrony danych, w którym istnieją dwie niezależne od siebie instytucje – z jednej strony Komisja, z drugiej natomiast organy państw członkowskich, które działają odrębnie po to, aby zapewnić wyższy poziom ochrony danych, co jednocześnie sprzyja podejmowaniu oddolnych działań skierowanych o charakterze obywatelskim skierowanych do odpowiednich urzędów w państwach członkowskich. Urzędnicy ci zrzeszeni są w tzw. Grupie Roboczej Art. 29, do której należy między innymi polski Generalny Inspektor Ochrony Danych Osobowych.

W sprawie Schremsa specyficzna jest niespotykana wcześniej konfiguracja, w której jednostka występuje nie przeciwko władzom publicznym albo prywatnym przedsiębiorstwom, ale przeciwko, jednym i drugim jednocześnie[15], a Trybunał Sprawiedliwości w swoim orzeczeniu opowiedział się po pierwsze po stronie jednostki oraz wyraził swoją preferencję dla zdecentralizowanego systemu ochrony z silną pozycją krajowych organów.

[15] Ibidem, str. 1356.

Polski obywatel jako podmiot Konstytucji RP oraz Karty Praw Podstawowych Unii Europejskiej

W argumentacji Trybunału ogromne znaczenie miały art. 7 i 8 Karty Praw Podstawowych, które głoszą, że każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się, a także do ochrony danych osobowych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

Regulacje UE o charakterze konstytucyjnym w zakresie prawa do prywatności zbieżne są więc z regulacjami Konstytucji RP zawartymi w art. 47 oraz 51. Karta Praw Podstawowych zyskała charakter prawnie wiążący, jak już wspominano wyżej, wraz z wejściem w życie Traktatu z Lizbony 1 grudnia 2009 r. i zyskała status prawa pierwotnego UE. Wówczas Unia Europejska przystąpiła również do europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, co ma niebagatelne znaczenie w przypadku omawianych tu art. 7 i 8 Karty. Karta Praw Podstawowych w art. 7 i 8 formułuje prawo do prywatności podobnie jak czyni to Konstytucja. W tak zdefiniowanym systemie gwarancji praw i wolności polski obywatel występuje w dwojakiej roli - z jednej strony jako obywatel Rzeczypospolitej Polskiej, podmiot praw i wolności zawartych w Rozdziale II Konstytucji RP, z drugiej natomiast

jako obywatel Unii Europejskiej, będący podmiotem gwarancji zawartych w Karcie Praw Podstawowych. Co więcej, prawa odnoszące się do prywatności zagwarantowane w Karcie Praw Podstawowych odpowiadają prawom zagwarantowanym w EKPC. Instytucje Unii Europejskiej oraz państwa członkowskie są zobowiązane do zagwarantowania stosowania tych praw również w odniesieniu do wdrażania praw unijnego[16].

Zakończenie

Prawo do ochrony danych osobowych stanowi więc materię, która wraz z rozwojem technologicznym wymaga nieustannego modyfikowania i dookreślania, tak by nie dopuścić do jej dezaktualizacji, biorąc pod uwagę fakt, jak istotne ma ona znaczenie dla codziennego funkcjonowania współczesnych ludzi. Jako zagadnienie niewystępujące uprzednio w polskich konstytucjach przez ostatnie dwie dekady zostało uzupełnione o orzecznictwo oraz regulacje aktów normatywnych niższego rzędu, a także, co wydaje się być najistotniejsze – o przepisy wyrastające z systemu prawa Unii Europejskiej, dzięki czemu zyskało zupełnie nowy kształt w polskim systemie prawnym.

[16] Boillat P., Kjaerum M., Handbook on European data protection law, Luxemburg 2014, str. 21.