STUDIA PRAWNICZE KUL
2 (78) 2019

https://doi.org/10.31743/sp.5848

Dorota Fleszer*, Anna Rogacka-Łukasik**

Europejskie podstawy prawne ochrony informacji

Wprowadzenie

Nie ulega wątpliwości, że w ostatnich latach następuje wzajemne przenikanie się różnych gałęzi prawa, a także zwiększona specjalizacja, co skutkuje coraz częstszym wyodrębnieniem się nowych dziedzin. Źródeł takiego stanu rzeczy upatruje się chociażby w większym wpływie prawa unijnego na krajowe porządki prawne, które to prawo bardzo często nie mieści się w utrwalonych w państwach członkowskich konstrukcjach prawnych oraz modelach postępowania[1]. Przedstawiona teza jest w pełni uzasadniona w sferze związanej z bezpieczeństwem informacji, w tym w szczególności tych mających charakter osobowy. Istotne bowiem staje się nie tyle wyspecyfikowanie pożądanych działań dających gwarancję osiągnięcia odpowiedniego poziomu ochrony przed nieuprawnioną ingerencją osób nieupoważnionych, ale raczej zapewnienie bezpieczeństwa operacji wykonywanych na informacjach, które odbywają się z wykorzystaniem systemów informatycznych. Nie budzi zatem zastrzeżeń ujmowanie problematyki prawnej ochrony informacji, w tym danych osobowych, jako dziedziny interdyscyplinarnej, która łączy prawne aspekty przetwarzania informacji z bezpieczeństwem sieci i systemów teleinformatycznych. Zgodzić się tutaj trzeba z M. Kaweckim, że przyczyną takiego

* Dr hab., Wyższa Szkoła Humanitas w Sosnowcu; e-mail: dorota.fleszer@humanitas.edu.pl, ORCID ID: https://orcid.org/0000-0001-6891-849X.

** Dr, Wyższa Szkoła Humanitas w Sosnowcu; e-mail: arogacka@tlen.pl, ORCID ID: https://orcid.org/0000-0001-6140-0591.

[1] Zob. M. Kawecki, *Prawo ochrony danych osobowych jako nowa dziedzina prawa*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 4-10.

stanu rzeczy jest także stały rozwój nowych technologii i związana z nim chęć wprowadzenia do porządku prawnego nowych, skuteczniejszych i nieznanych dotąd instrumentów prawnych[2]. Podziela to stanowisko M. Czerniawski twierdząc, że postęp technologiczny sprawił, że operacje przetwarzania danych osobowych są obecnie łatwiejsze do przeprowadzania niż kiedykolwiek wcześniej. Jednocześnie, wraz z rozwojem Internetu oraz usług świadczonych transgranicznie, coraz mniejsze znaczenie ma fizyczna lokalizacja podmiotu, który takie operacje wykonuje. Działania podejmowane z najbardziej odległych zakątków świata mogą bowiem mieć zasięg globalny i wywierać skutki dla danych podmiotów zlokalizowanych w zupełnie innym miejscu. Jednocześnie pojedyncza osoba dysponująca przenośnym komputerem może przetwarzać miliony danych[3].

Przedmiotem niniejszego opracowania będzie analiza europejskich podstaw prawnych bezpieczeństwa informacji, w tym danych osobowych. Przedstawione zostaną nie tylko mechanizmy prawne ochrony danych osobowych, ale także przetwarzania informacji w systemach informatycznych. Ustalenia w wymienionym zakresie dokonano na podstawie dorobku doktryny oraz egzegezy tekstów prawnych.

1. 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[4]

Państwa zachodniej części Europy po latach podziałów rozpoczęły budowę wspólnoty. Proces ten zainicjowano stworzeniem wspólnego rynku gospodarczego, na którym miał mieć miejsce swobodny przepływ

---

[2] Zob. tamże.

[3] Zob. M. Czerniawski, *Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016, s. 100.

[4] 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. Urz. UE L 281 z 23.11.1995, s. 31-50 z późn. zm. (dalej: dyrektywa 95/46/WE).

towarów, usług, osób i kapitału. Szybko jednak zorientowano się, że tak określony cel nie może być realizowany tylko przez wykorzystanie środków gospodarczych i ekonomicznych bez ingerencji w sferę praw i wolności osób – zwłaszcza w ich życie prywatne. Tendencja do integracji ekonomiczno-społecznej krajów Unii Europejskiej, a w konsekwencji globalizacja informacji (w tym również danych osobowych), wymiana danych pomiędzy państwami członkowskimi, duża szybkość przepływu danych i ich praktycznie powszechna dostępność, ujawniły nowe problemy w zakresie ochrony danych osobowych, co z kolei spowodowało dyskusję na temat potrzeby wprowadzenia odpowiednich uregulowań prawnych i pogodzenia prawa do prywatności ze stale rozwijającym się rynkiem wewnętrznym Unii Europejskiej[5]. Najważniejszym aktem prawnym w zakresie danych osobowych w skali międzynarodowej jest Konwencja Nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[6]. Konwencja, która jest aktem prawnomiędzynarodowym wiążącym państwa będące jej stronami, weszła w życie z dniem 1 października 1985 r., po ratyfikacji przez pięć państw (Francję, RFN, Norwegię, Hiszpanię i Szwecję). Polska ratyfikowała tę konwencję dnia 24 kwietnia 2002 r.

Tym niemniej ustawodawstwo wewnętrzne poszczególnych państw dotyczące ochrony danych osobowych, powstałe w dużej części po przyjęciu wspomnianej konwencji, okazało się bardzo zróżnicowane. Taka różnorodność utrudniła utworzenie wspólnego rynku wewnętrznego, w ramach którego miałby się odbywać swobodny przepływ towarów, osób, usług, kapitału – także danych osobowych pomiędzy państwami, przy zapewnionej ochronie prywatności[7]. W celu ujednolicenia stosowanych regulacji prawa krajowego wprowadzono dyrektywę 95/46/WE, która wyznacza zasady ochrony podstawowych praw i wolności osób fizycznych, a w szczególności określa ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych. Podstawowym jej celem było zapewnienie najwyższego możliwego poziomu ochrony danych osobowych i ułatwienie swobodnego przepływu danych na terytorium Unii

---

[5] Zob. D. Fleszer, *Zakres przetwarzania danych osobowych w działalności gospodarczej*, Warszawa 2008, s. 13.

[6] Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r., Dz. U. z 2003 r. Nr 3, poz. 25.

[7] Zob. D. Fleszer, *Zakres przetwarzania danych osobowych…*, s. 17.

Europejskiej i praktycznie w obrębie całego Europejskiego Obszaru Gospodarczego[8]. Państwa członkowskie UE były zobowiązane do wdrożenia przepisów dyrektywy w swoich systemach prawnych, otrzymały jednak pewien margines swobody w jej zastosowaniu, co może prowadzić do różnic w ustawodawstwie krajowym[9].

Reasumując, regulacje dyrektywy 95/46/WE mają za cel:

1) zabezpieczenie jednolitego minimalnego poziomu ochrony prywatności osób fizycznych w związku z przetwarzaniem danych osobowych zawartych w zbiorach danych;
2) zapewnienie możliwości swobodnego przepływu danych osobowych pomiędzy krajami członkowskimi[10].

Dyrektywa 95/46/WE precyzuje zasady przetwarzania danych osobowych, stanowiące konkretyzację prawa do poszanowania życia prywatnego, formułowanego przez wskazane tu akty prawa pierwotnego. Konkretyzacja tego prawa następuje w dyrektywie przez:

1) wprowadzenie zasad dotyczących jakości danych, do których należą określone w art. 6: zakaz poddawania danych dalszemu przetwarzaniu w sposób niezgodny z celem, dla którego zostały zebrane; zasada adekwatności danych w stosunku do celów przetwarzania; zakaz przechowywania danych w formie umożliwiającej identyfikację osób, których dotyczą, przez czas dłuższy niż niezbędny dla celów przetwarzania;
2) określenie w art. 7 kryteriów legalności przetwarzania danych;
3) wprowadzenie w art. 8 ograniczeń przetwarzania danych wrażliwych;
4) wprowadzenie w art. 10 i 11 obowiązku informacyjnego wobec osoby, której dane dotyczą;
5) przyznanie w art. 12 osobie, której dane dotyczą, prawa dostępu do nich, kontroli prawidłowości przetwarzania;
6) przyznanie w art. 14 prawa sprzeciwu wobec przetwarzania danych;
7) określenie w art. 17 wymogu stosowania środków technicznych i organizacyjnych zabezpieczających dane osobowe;

---

[8] Zob. Generalny Inspektor Ochrony Danych Osobowych, *Wybrane zagadnienia z zakresu ochrony danych osobowych. Poradnik dla przedsiębiorców*, 2010, s. 6, Instytut Spraw Publicznych, http://www.giodo.gov.pl/487/id_art/4257/j/pl [dostęp: 12.02.2020 r.].

[9] Zob. tamże.

[10] Zob. J. Barta. P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2004, s. 90.

8) określenie w art. 25 i 26 warunków przekazywania danych osobowych do krajów trzecich[11].

Dopełnieniem dyrektywy 95/46/WE, niezbędnym ze względu na specyfikę i zagrożenia dla prywatności wynikające z nieuprawnionego dostępu do danych w Internecie, są[12]:

- dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[13];
- 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)[14];
- dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE[15].

Uchwalenie tych dyrektyw wynika ze specyfiki przetwarzania danych w Internecie i towarzyszących mu zagrożeń dla prywatności. Ich zasięg oddziaływania obejmuje przetwarzanie danych niezależnie od branży lub

---

[11] M. Krzysztofek, *Ochrona danych osobowych* w *Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych, w obecnym i nadchodzącym stanie prawnym*, Warszawa 2014, s. 46-47.

[12] Zob. tamże, s. 35-36.

[13] Dyrektywa 2000/31/WE Parlamentu *Europejskiego* i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dyrektywa o handlu elektronicznym), Dz. Urz. UE L 178 z 17.07.2000, s. 1-16.

[14] 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. Urz. UE L 201 z 31.07.2002, s. 37-47.

[15] Dyrektywa 2006/24/WE Parlamentu *Europejskiego* i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych *danych* w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz. Urz. UE L 105 z 13.04.2006, s. 54-63.

sektora, w którym działa administrator danych, jeżeli stosuje określone narzędzia, kanały dystrybucji lub środki komunikacji, do których odnoszą się te dyrektywy[16].

2. 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[17]

Prawo ochrony danych osobowych jest przedmiotem szerokiej dyskusji toczącej się wśród prawodawców, przedstawicieli doktryny, przedsiębiorców i obywateli zainteresowanych ochroną swojej prywatności. W ostatnich latach osią debaty był przedstawiony przez Komisję Europejską w 2012 r. projekt ogólnego rozporządzenia o ochronie danych osobowych. Miał on na celu dostosowanie unijnych ram prawnych do nowych warunków technologicznych, wzmocnienie praw obywateli, harmonizację unijnych przepisów dotyczących ochrony danych i ułatwienie działalności przedsiębiorstw poprzez zmniejszenie kosztów działalności transgranicznej i wprowadzenie tzw. zasady *one stop shop*[18]. Przedstawiając projekt rozporządzenia, komisarz V. Reding wskazała, jakie mają być jego cele. Rozporządzenie ma zapewnić zwiększenie ochrony praw osób fizycznych przy jednoczesnym poszerzeniu możliwości biznesowych poprzez ułatwienie swobodnego przepływu danych osobowych na jednolitym rynku cyfrowym[19]. Warto zauwa-

---

[16] Zob. M. Krzysztofek, *Ochrona danych osobowych…*, s. 36.

[17] 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 (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz. Urz. UE L 119 z 4.05.2016, s. 1-88 (dalej: ogólne rozporządzenie o ochronie danych).

[18] Zob. M. Piech, *„Deregulacyjna" nowelizacja i unijna reforma zasad ochrony danych osobowych z perspektywy administratora danych osobowych*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016, s. 27.

[19] Zob. D. Lubasz, *Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016, s. 64.

żyć, że także z najnowszego orzecznictwa Trybunału Sprawiedliwości jednoznacznie wynika konieczność rozszerzenia zakresu terytorialnego stosowania unijnych przepisów o ochronie danych osobowych. Jest to właściwy kierunek działania – niezbędny, aby w dobie Internetu zapewnić efektywną ochronę tych danych[20].

W konsekwencji tej sytuacji w dniu 27 kwietnia 2016 r. Parlament Europejski i Rada (UE) przyjęły tzw. ogólne rozporządzenie o ochronie danych (RODO). Rozporządzenie to stanowi kolejny krok w kierunku zabezpieczenia prawa do ochrony danych osobowych, które w Unii Europejskiej cieszy się niezwykle istotnym statusem prawa podstawowego[21].

Rozporządzenie to zastępuje dotychczas obowiązującą dyrektywę 95/46/WE i będzie stanowić podstawowy akt prawny w zakresie ochrony danych osobowych osób fizycznych. Rozporządzenie ma zapewnić we wszystkich państwach członkowskich równy poziom ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych[22]. Zatem stanowi ono jeden z istotnych elementów na rzecz utworzenia jednolitego rynku cyfrowego w Unii Europejskiej. Jego sukces w dużej mierze zależeć będzie od organów odpowiedzialnych za jego stosowanie[23].

W ostatecznej wersji ogólnego rozporządzenia o ochronie danych podtrzymano postulat, aby ochrona danych osobowych obywateli unijnych była jednolita w ramach struktury organizacyjnej administratora i processora, niezależna od tego, czy ich siedziba, jednostki lub środki techniczne wykorzystywane do przetwarzania znajdują się na terytorium Unii oraz czy przetwarzanie danych odbywa się na tym terytorium. O właściwości unijnych zasad ochrony danych wobec przetwarzania prowadzonego poza Unią i przez podmioty spoza Unii, przesądza to, że przetwarzanie wiąże się z oferowaniem towarów lub usług podmiotom tych danych w Unii lub monitorowaniem takich podmiotów. Wobec tego, unijnym standardom ochrony danych zostanie poddane w szczególności przetwarzanie w związku z oferowaniem produktów i usług w Internecie klientom z państw UE przez

---

[20] Zob. M. Czerniawski, *Zakres terytorialny…*, s. 101.

[21] Zob. K. Rokita, *Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych*, „Europejski Przegląd Sądowy" 2016, nr 7, s. 4.

[22] Zob. J. Sobczak, *W kwestii potrzeby dostosowania przepisów prawa polskiego do treści rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych*, [w:] J. Sobczak, *Prawo a medycyna. Studia i szkice*, Poznań 2018, s. 213.

[23] Zob. tamże.

podmioty z państw trzecich, np. przez amerykański portal społecznościowy czy dostawcę „chmury”[24]. W założeniach nowa regulacja ma być technologicznie neutralna i pozostawiać administratorom danych osobowych swobodę co do wyboru metod i środków, z wykorzystaniem których będą realizować cele i zadania związane z bezpieczeństwem informacji. Zmienia się zatem optyka rozwiązań poprzez uelastycznienie podejścia i dostosowanie do różnorodnych warunków przetwarzania danych. Istotne jest, że rozporządzenie wprowadza także pewne zróżnicowanie obowiązków z zależności od wielkości podmiotu będącego administratorem danych oraz od okoliczności czy działalność administratora jest ukierunkowana na przetwarzanie danych jako cel, czy też przetwarzanie danych osobowych pełni rolę służebną, subsydiarną w jego działalności. Jest to związane z założeniem, że wolą prawodawcy jest, z jednej strony, wspieranie rozwoju małych i średnich przedsiębiorstw, a w związku z tym ograniczanie nakładanych na nich obowiązków prawnych do niezbędnego – z punktu widzenia ochrony danych osobowych – minimum, a z drugiej – odróżnienie sytuacji, gdy przetwarzanie danych jest przedmiotem działalności, od przypadków, gdy jest ono efektem lub pozostaje w związku z inną podstawową działalnością administratora[25].

Ogólne rozporządzenie o ochronie danych ma zrealizować następujące cele:

1) przejście od obecnej harmonizacji prawa w dziedzinie ochrony danych osobowych w państwach członkowskich do ujednolicenia zasad ochrony danych w ramach UE;
2) podniesienie poziomu ochrony danych osobowych obywateli UE, przez wprowadzenie uprawnień, obowiązków i rozwiązań prawnych dotychczas nieistniejących w unijnym prawie lub uzupełniających dotychczasowe regulacje i zwiększających ich skuteczność, na podstawie analizy doświadczeń wynikających z implementacji dyrektywy 95/46/WE w państwach członkowskich;
3) wprowadzenie rozwiązań prawnych, które zapewnią przepisom o ochronie danych skuteczność w obliczu nowych wyzwań wynikających z technicznych warunków przetwarzania danych

[24] Zob. M. Krzysztofek, *Ochrona danych osobowych…*, s. 71-72.

[25] Zob. D. Lubasz, *Europejska reforma ochrony danych…*, s. 64.

w Internecie, pojawienia się nowych kategorii danych osobowych oraz systematycznie rosnącej skali przetwarzania danych[26].

Podkreślić także należy, że *ratio legis* nowych ram prawnych ochrony danych, zwłaszcza ogólnego rozporządzenia, miało być uwspółcześnienie ochrony danych osobowych, podniesienie poziomu ochronnego, a także przyznanie większej kontroli osobom, których dane dotyczą, nad całością procesów przetwarzania danych. Podnoszenie standardów ochrony danych przez administratorów w naturalny sposób skorelowane jest ze zwiększaniem uprawnień podmiotów danych. Obserwujemy wyraźną tendencję do rozbudowywania obowiązków informacyjnych, nacisk na tworzenie jasnych i przejrzystych komunikatów kierowanych do osób, których dane dotyczą, a to prowadzi do zwiększania świadomości nie tylko istnienia, ale i potrzeby egzekwowania przepisów[27]. Jak bowiem wynika z pkt 6 preambuły rozporządzenia szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne, mogą w swojej działalności na niespotykaną dotąd skalę wykorzystywać dane osobowe. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych. W pkt 7 preambuły rozporządzenia podkreśla się, że przemiany te wymagają stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego ich egzekwowania, gdyż ważna jest budowa zaufania, które pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi, a osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe poczucie pewności prawa i jego stosowania w praktyce.

---

[26] Zob. M. Krzysztofek, *Ochrona danych osobowych…*, s. 64-65.

[27] E. Bielak-Jomaa, *Słowo wstępne*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016, s. 15.

3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[28]

Znakiem współczesnych czasów stało się przetwarzanie w przeróżnych systemach teleinformatycznych jak największych ilości danych o poszczególnych osobach oraz o ich działaniach. Rozwój technik informacyjnych zmienia gospodarkę światową. Wraz z nowymi usługami oraz wykorzystaniem nowych środków komunikacji do nowych sposobów realizacji różnych procesów społecznych za pomocą nowych środków komunikacji, pojawiają się coraz większe problemy z cyberbezpieczeństwem (bezpieczeństwem cyberprzestrzeni). Przyjęta definicja cyberbezpieczeństwa to przeniesienie klasycznej definicji bezpieczeństwa, które jest rozumiane jako zachowanie poufności, integralności i dostępności informacji w cyberprzestrzeni. Cyberprzestrzeń ma kluczowe znaczenie, gdyż w dobie nieustającego postępu technologicznego, stanowi ona przymiot ludzkiej aktywności, co z kolei wiąże się, w naturalny sposób, z obowiązkiem państwa wobec obywateli zapewnienia jej bezpieczeństwa. W ten sposób powstało pojęcie cyberbezpieczeństwa, które stanowi nad wyraz pojemną formułę obejmującą zwłaszcza bezpieczeństwo informacji, bezpieczeństwo operacyjne, jak również bezpieczeństwo systemów komputerowych. Cyberbezpieczeństwo definiowane jest jako:

> bezpieczeństwo państwa obejmujące zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych[29].

---

[28] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE L 194 z 19.07.2016, s. 1-30 (dalej: dyrektywa NIS).

[29] Tak cyberbezpieczeństwo definiuje *Doktryna Cyberbezpieczeństwa RP*, zob. D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, http://www.academia.edu/24309292/Cyberbezpiecze%C5%84stwo_administracji_publicznej_w_Polsce._Wybrane_zagadnienia [dostęp: 15.02.2020 r.].

Obejmuje zatem zespół działań i zasobów, które umożliwiają obywatelom, przedsiębiorstwom i państwom osiągnięcie celów informatycznych w sposób bezpieczny, jak również niezawodny, przy zachowaniu prywatności. Ponadto zakres pojęcia cyberbezpieczeństwa jest różny w zależności od adresata. Najszersza formuła dotyczy cyberbezpieczeństwa państw, które oznacza ochronę obywateli, przedsiębiorstw, infrastruktury o znaczeniu krytycznym oraz państwowych systemów komputerowych przed atakiem lub naruszeniem integralności. Z kolei w przypadku indywidualnych osób oznacza poczucie bezpieczeństwa oraz ochronę danych osobowych i prywatności. Natomiast dla przedsiębiorstw cyberbezpieczeństwo to zapewnienie dostępności funkcji biznesowych o znaczeniu krytycznym i ochrona poufnych danych dzięki zarządzaniu bezpieczeństwem operacyjnym i bezpieczeństwem informacji.

Bezpieczeństwo systemów informatycznych wymaga ochrony na różnych płaszczyznach. Wynika to między innymi z różnorodności możliwych ataków, skutkiem których może nastąpić zawirusowanie komputera, zablokowanie dostępności usług bądź zainstalowanie oprogramowania. Zabiegi zmierzające do zapewnienia jak najwyższego poziomu bezpieczeństwa w omawianym zakresie podejmowane były od dawna, a efektem jest, przyjęta 6 lipca 2016 r., dyrektywa NIS[30].

Dyrektywa NIS ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w UE, w celu poprawnego funkcjonowania rynku wewnętrznego[31]. Zatem zakres przedmiotowy dyrektywy NIS obejmuje dwa obszary. Pierwszy związany jest z powstaniem ram dla obszaru cyberbezpieczeństwa i obejmuje obowiązek opracowania i przyjęcia krajowej strategii w zakresie bezpieczeństwa systemów i sieci, a także wyznaczenie właściwego organu centralnego dla działań związanych z realizacją strategii. Natomiast drugi obszar obejmuje utworzenie hierarchicznej sieci Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (*Computer Security Incident Response Teams*, CSIRT), czyli wyspecjalizowanych zespołów odpowiedzialnych za identyfikację i reagowanie na incydenty związane z bezpieczeństwem IT. Przedstawiając powyższe w sposób bardziej szczegółowy, należy wskazać, iż cele ustanowione w dyrektywie NIS to[32]:

---

[30] Z j. ang. *Network Information Security*.

[31] Art. 1 ust. 1 dyrektywy NIS.

[32] Art. 1 ust. 2 dyrektywy NIS.

- ustanowienie procedur i obowiązku zgłaszania incydentów dotyczących cyberbezpieczeństwa dla przedsiębiorców z sektorów kluczowych;
- ustanowienie szczególnych wymogów dotyczących zapewniania bezpieczeństwa przez przedsiębiorców z sektorów kluczowych;
- przyjęcie na poziomie krajowym strategii w zakresie bezpieczeństwa sieci i systemów IT;
- utworzenie wymienionej powyżej sieci CSIRT;
- stworzenie specjalnej grupy zapewniającej strategiczną współpracę oraz wymianę informacji, w szczególności biorąc pod uwagę, że incydenty związane z cyberbezpieczeństwem często dotyczą wielu państw równocześnie;
- utworzenie Grupy Współpracy, której zadaniami będą współpraca, dyskusja, wymiana dobrych praktyk oraz zbieranie cyklicznych raportów;
- wyznaczenie również krajowego, pojedynczego punktu kontaktowego, którego zadaniem będzie uczestniczenie w Grupie Współpracy[33].

Adresatami nowej regulacji dyrektywy NIS będą dwie grupy podmiotów: dostawcy usług cyfrowych oraz operatorzy usług kluczowych.

Zgodnie z art. 4 pkt 6 dyrektywy NIS dostawcą usług cyfrowych jest każda osoba prawna, która świadczy usługę cyfrową[34], czyli taką, która jest świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług oraz która jednocześnie jest klasyfikowana jako internetowa platforma handlowa, wyszukiwarka internetowa lub usługa przetwarzania w chmurze w rozumieniu dyrektywy NIS. Jak wynika z powyższego, ustawodawca, jako kategorie usług cyfrowych, wymienia: internetową platformę handlową, wyszukiwarkę

[33] Zob. *Dyrektywa NIS – nowe wymogi dotyczące cyberbezpieczeństwa dla firm z kluczowych sektorów gospodarki*, „Alert Prawny" 2017, nr 1, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/dyrektywa-nis-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html [dostęp: 15.02.2020 r.].

[34] Z kolei w pkt 5 art. 4 dyrektywy NIS ustawodawca wskazuje, iż usługa cyfrowa oznacza usługę w rozumieniu art. 1 ust. 1 lit. b dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady (UE) z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Tekst mający znaczenie dla EOG), Dz. Urz. UE L 241 z 17.09.2015, s. 1-15.

internetową lub usługę przetwarzania w chmurze, których istotę warto chociaż pokrótce wyjaśnić. Wśród definicji ustawowych ujętych w art. 4 dyrektywy NIS, ustawodawca unijny zawarł definicję „internetowej platformy handlowej", wskazując, iż oznacza ona:

> usługę cyfrową, która umożliwia konsumentom lub przedsiębiorcom […] zawieranie online umów dotyczących sprzedaży lub usług z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który używa usług komputerowych świadczonych przez internetową platformę handlową[35].

O internetowej platformie handlowej traktuje również motyw 15 preambuły dyrektywy NIS, według którego platforma ta jest ostatecznym miejscem zawierania umowy. Ponadto internetowa platforma handlowa może świadczyć również usługi komputerowe takie jak: przetwarzanie transakcji, agregowanie danych lub profilowanie użytkowników. Za internetową platformę handlową należy uznawać również sklepy z aplikacjami będące sklepami internetowymi, które umożliwiają cyfrową dystrybucję aplikacji lub oprogramowania stron trzecich.

Z kolei „wyszukiwarka internetowa" oznacza:

> usługę cyfrową, która umożliwia użytkownikom wyszukiwanie – co do zasady – wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, wyrażenia lub innej wartości wejściowej[36].

W dalszej części powyższej definicji wyszukiwarki internetowej wskazano, iż wyszukiwarka internetowa w generowanym wyniku wyszukiwania przedstawia odnośniki, pod którymi można znaleźć informacje związane z zadanym zapytaniem[37]. Dodatkowo motyw 16 preambuły dyrektywy NIS wskazuje, iż usługa wyszukiwarki internetowej umożliwia przeszukania wszystkich stron internetowych w zakresie zadanego pytania, które może dotyczyć jakiegokolwiek zagadnienia. Powyższy motyw wskazuje równocześnie, że wyszukiwanie może być zawężone do stron internetowych prowadzonych w określonym języku. Jednak, za usługę cyfrową w formie wyszukiwarki internetowej nie może być uznana funkcja

---

[35] Art. 4 pkt 17 dyrektywy NIS.

[36] Art. 4 pkt 18 dyrektywy NIS.

[37] Tamże.

wyszukiwania, która dotyczy wyszukiwania treści wyłącznie w zakresie jednej konkretnej strony internetowej (tzw. wyszukiwarki wewnętrzne). Z zakresu pojęcia „wyszukiwarki internetowej" wyłączono również świadczenie „usług online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego, aby tam dokonał zakupu produktu"[38]. Ostatnią kategorią usługi cyfrowej jest wspomniana usługa „przetwarzania w chmurze", która oznacza: „usługę cyfrową umożliwiającą dostęp do skalowalnego[39] i elastycznego zbioru[40] zasobów obliczeniowych[41] do wspólnego wykorzystywania[42]"[43]. Ponadto, w regulacji art. 16 dyrektywy NIS, ustawodawca unijny w sposób szczegółowy formułuje katalog obowiązków dostawców usług cyfrowych. Jako pierwszy wymienia obowiązek określania oraz podejmowania odpowiednich i proporcjonalnych środków technicznych oraz organizacyjnych w celu zarządzania ryzykami. Dodatkowo, środki te mają odpowiadać aktualnemu stanowi wiedzy oraz muszą zapewniać poziom bezpieczeństwa odpowiedni do istniejącego ryzyka, a także uwzględniać następujące elementy: a) bezpieczeństwo systemów i obiektów; b) postępowanie w przypadku incydentu; c) zarządzanie ciągłością działania; d) monitorowanie, audyt i testowanie; e) zgodność z normami międzynarodowymi[44]. Drugi obowiązek dotyczy podejmowania środków zapobiegających i minimalizujących wpływ incydentów, które mają na celu zapewnienie

[38] Motyw 16 zdanie 4 dyrektywy NIS.

[39] Pojęcie „skalowalne" odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi, niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania, zob. motyw 17 preambuły dyrektywy NIS.

[40] Pojęcia „elastyczny zbiór" używa się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie do zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia, zob. motyw 17 preambuły dyrektywy NIS.

[41] Pojęcie „zasoby obliczeniowe" obejmuje zasoby takie, jak: sieci, serwery lub inną infrastrukturę, pamięć, aplikacje i usługi, zob. motyw 17 preambuły dyrektywy NIS.

[42] Pojęcia „wspólne wykorzystywanie" używa się do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, jednak przetwarzanie odbywa się oddzielnie dla każdego z użytkowników, choć usługa ta jest świadczona z tego samego sprzętu elektronicznego, zob. motyw 17 preambuły dyrektywy NIS.

[43] Art. 4 pkt 19 dyrektywy NIS.

[44] Art. 16 pkt 1 dyrektywy NIS.

ciągłości usług[45]. Kolejnym obowiązkiem nałożonym na dostawcę usług cyfrowych jest zgłaszanie, bez zbędnej zwłoki, właściwemu organowi lub CSIRT wszelkich incydentów mających istotny wpływ na świadczenie usług internetowej platformy handlowej, wyszukiwarki internetowej oraz usługi przetwarzania w chmurze. Dokonywane przez dostawców zgłoszenia muszą zawierać informacje umożliwiające określenie istotności wpływu transgranicznego[46]. Wśród obowiązków dostawcy usług cyfrowych należy również wymienić obowiązek zgłoszenia operatorowi usług kluczowych – który jest zależny od tego dostawcy w zakresie usługi, która ma istotne znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej – wszelkiego istotnego wpływu na ciągłość usług kluczowych związanego z incydentem, który dotyczy tego dostawcy usług cyfrowych[47]. Należy mieć również na uwadze, iż jeden z rozdziałów dyrektywy NIS[48] odnoszący się do dostawców usług cyfrowych, nie ma zastosowania do mikro oraz małych przedsiębiorców[49].

Drugą grupą podmiotów, wymienioną powyżej, do których adresowana jest dyrektywa NIS, są operatorzy usług kluczowych. Operator usług kluczowych oznacza podmiot publiczny lub prywatny, należący do jednego z sektorów, takich jak: energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa[50]. Zgodnie z art. 5 ust. 2 dyrektywy NIS kryteria identyfikacji operatorów usług kluczowych są następujące:

– podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. Państwa członkowskie są zobowiązane do przygotowania we własnym zakresie list operatorów kluczowych z powyższych sektorów, biorąc pod uwagę szereg czynników takich jak: znaczenie danego przedsiębiorcy dla działalności sektora czy świadczenia kluczowych usług, jego udział w rynku, powiązanie z innymi sektorami kluczowymi lub zależność świadczenia danej usługi od systemów informatycznych[51];

---

[45] Art. 16 pkt 2 dyrektywy NIS.
[46] Art. 16 pkt 3 dyrektywy NIS.
[47] Art. 16 pkt 5 dyrektywy NIS.
[48] Rozdział V dyrektywy NIS.
[49] Art. 16 pkt 11 dyrektywy NIS.
[50] Art. 4 pkt 4 dyrektywy NIS w związku z załącznikiem nr 2 do dyrektywy.
[51] Zob. *Dyrektywa NIS – nowe wymogi…*

– świadczenie tej usługi zależy od sieci i systemów informatycznych;
– incydent miałby istotny skutek zakłócający dla świadczenia tej usługi.

Należy dodać, iż w związku z koniecznością zmiany przepisów krajowych w zakresie omawianej dyrektywy NIS, polska Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii rozpatrzyła informacje Ministra Cyfryzacji o *Strategii Cyberbezpieczeństwa RP na lata 2017-2022* oraz o pracach nad rządowym projektem ustawy o krajowym systemie cyberbezpieczeństwa[52].

Celem strategii jest określenie ramowych działań, których zadaniem będzie uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Wśród celów szczegółowych wskazano w strategii, iż „kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni”[53].

Z kolei efektem prac nad rządowym projektem ustawy, która dotyczyłaby systemu cyberbezpieczeństwa w kraju była uchwalona na posiedzeniu nr 66 dnia 5 lipca 2018 r. ustawa o krajowym systemie cyberbezpieczeństwa[54]. Ustanowiony przedmiotową ustawą krajowy system cyberbezpieczeństwa ma na celu „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów”[55].

---

[52] *Informacja o posiedzeniu Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii*, 20.10.2016, http://www.sejm.gov.pl/Sejm8.nsf/komunikat.xsp?documentId=A21D37927AB687FCC125805200499367 [dostęp: 15.02.2020 r.].

[53] Zob. *Strategia Cyberbezpieczeństwa RP na lata 2017-2022. Poszanowanie praw i wolności w cyberprzestrzeni. Kompleksowe podejście do bezpieczeństwa. Cyberbezpieczeństwo istotnym elementem polityki państwowej*, s. 4, https://www.gov.pl/attachment/00aa12ca-ec73-4982-9632-002707dffb81; dostęp: 15.02.2020 r. (dalej: strategia).

[54] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. z 2018 r. poz. 1560 z późn. zm. (dalej: u.k.s.c.).

[55] Art. 3 u.k.s.c.

Podsumowanie

Powszechne stosowanie systemów informatycznych i przetwarzanie w nim informacji, w tym danych osobowych, wymagają na nowo przyjrzenia się prawnym aspektom bezpieczeństwa informacji.

Należy zwrócić uwagę na niedoskonałość przepisów ustawy o ochronie danych osobowych. O ile jeszcze w latach 90. ubiegłego wieku różnice w brzmieniu ustawy oraz dyrektywy 95/46/WE w odniesieniu do zakresu terytorialnego miały ograniczone konsekwencje dla sytuacji prawnej podmiotów danych, to wraz z rozwojem Internetu i technologii przetwarzania danych oraz postępującą globalizacją kwestia ta staje się coraz bardziej paląca[56].

Dlatego też nie jest możliwe budowanie unijnego systemu bezpieczeństwa informacji z pominięciem cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, informacja, dane osobowe, system informatyczny, Internet

Bibliografia

Źródła prawa

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. Urz. UE L 281 z 23.11.1995, s. 31-50; Dz. Urz. UE polskie wyd. spec.: rozdz. 13, t. 15, s. 355-374.

Rozporządzenie (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. dostosowujące do decyzji Rady 1999/468/WE przepisy odnoszące się do komitetów, które wspomagają Komisję w wykonywaniu jej uprawnień wykonawczych ustanowionych w instrumentach podlegających procedurze określonej w art. 251 Traktatu WE, Dz. Urz. UE L 284 z 31.10.2003, s. 1-53.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku

[56] M. Czerniawski, *Zakres terytorialny…*, s. 101.

z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz. Urz. UE L 119 z 4.05.2016, s. 1-88.

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego („Dyrektywa o handlu elektronicznym"), Dz. Urz. UE L 178 z 17.07.2000, s. 1-16; Dz. Urz. UE polskie wyd. spec.: rozdz. 13, t. 25, s. 399-414.

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. Urz. UE L 201 z 31.07.2002, s. 37-47; Dz. Urz. UE polskie wyd. spec.: rozdz. 13, t. 29, s. 514-524.

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz. Urz. UE L 105 z 13.04.2006, s. 54-63.

Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady (UE) z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Tekst mający znaczenie dla EOG), Dz. Urz. UE L 241 z 17.09.2015, s. 1-15.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE L 194 z 19.07.2016, s. 1-30.

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. Urz. UE L 119 z 4.05.2016, s. 1-88.

Literatura

Barta J., P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2004.

Bielak-Jomaa E., *Słowo wstępne*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Czerniawski M., *Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Dyrektywa NIS – nowe wymogi dotyczące cyberbezpieczeństwa dla firm z kluczowych sektorów gospodarki, „Alert Prawny" 2017, nr 1, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/dyrektywa-nis-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html [dostęp: 15.02.2020 r.].

Fleszer D., *Zakres przetwarzania danych osobowych w działalności gospodarczej*, Warszawa 2008.

Generalny Inspektor Ochrony Danych Osobowych, *Wybrane zagadnienia z zakresu ochrony danych osobowych. Poradnik dla przedsiębiorców*, 2010, Instytut Spraw Publicznych, http://www.giodo.gov.pl/487/id_art/4257/j/p [dostęp: 12.02.2010 r.].

Gibson W., *Neuromancer*, New York 1984.

Informacja o posiedzeniu Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, 20.10.2016, http://www.sejm.gov.pl/Sejm8.nsf/komunikat.xsp?documentId=A21D37927AB687FCC125805200499367 [dostęp: 15.02.2020 r.].

Kawecki M., *Prawo ochrony danych osobowych jako nowa dziedzina prawa*, „Europejski Przegląd Sądowy" 2017, nr 5.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych, w obecnym i nadchodzącym stanie prawnym*, Warszawa 2014.

Lisiak-Felicka D., M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, http://www.academia.edu/24309292/Cyberbezpiecze%C5%84stwo_administracji_publicznej_w_Polsce._Wybrane_zagadnienia [dostęp: 15.02.2020 r.].

Lubasz D., *Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Piech M., *„Deregulacyjna" nowelizacja i unijna reforma zasad ochrony danych osobowych z perspektywy administratora danych osobowych*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Rojszczak M., *Coraz mniej czasu na wdrożenie dyrektywy o cyberbezpieczeństwie*, „Biznes Alert" z dnia 27 marca 2017 r., BiznesAlert.pl, http://biznesalert.pl/rojszczak-coraz-mniej-czasu-na-wdrozenie-dyrektywy-o-cyberbezpieczenstwie/ [dostęp: 15.02.2020 r.].

Rokita K., *Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych*, „Europejski Przegląd Sądowy" 2016, nr 7.

Sobczak J., *W kwestii potrzeby dostosowania przepisów prawa polskiego do treści rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych*, [w:] J. Sobczak, *Prawo a medycyna. Studia i szkice*, Poznań 2018.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

EUROPEAN LEGAL BASIS FOR INFORMATION PROTECTION

Summary

The issue of information and ensuring its legal security, in particular to the extent of its processing in IT systems, becomes an important issue not only for the national legislator. Taking into consideration the existence of cross-border information flow – which is necessary for the creation of a common market – there are new threats, such as the need to ensure the protection of individuals' privacy. Legal solutions at the EU level, that address those threats, aim if not to eliminate, at least to minimise them by creating a common legal framework for information security and protection of personal data. The purpose of this publication is to analyse the European regulations that provide the basis for ensuring the safe information processing in information systems.

Key words: cyber security, information, personal information, IT system, Internet

ЕВРОПЕЙСКИЕ ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Резюме

Вопрос информации и обеспечения ее правовой безопасности, особенно в отношении обработки в информационных системах, становится важной проблемой не только для национального законодателя. Учитывая наличие трансграничного потока информации, что, в конце концов, необходимо с точки зрения создания общего рынка, появляются новые угрозы, например, связанные с необходимостью обеспечения защиты приватности лиц. Правовые решения на уровне ЕС должны если не устранить эти угрозы, то свести к минимуму путем создания общей правовой базы для информационной безопасности и защиты персональных данных. Целью данной публикации является анализ европейских правовых норм, лежащих в основе обеспечения безопасной обработки информации в информационных системах.

Ключевые слова: кибербезопасность, информация, персональные данные, IT-система, интернет