ANALIZA PRAWA DO PRYWATNOŚCI W KONTEKŚCIE FUNKCJONOWANIA E-USŁUG W ADMINISTRACJI PUBLICZNEJ

Małgorzata Giela

Streszczenie

Ciągły rozwój cyfrowych usług publicznych przyczynia się do zwiększonego korzystania z e-usług przez obywateli. Jest to wynikiem zarówno zmian ekonomicznych, jak i społecznych. Powstanie społeczeństwa informacyjnego i rozkwit technologii ICT determinują wprowadzanie nowych rozwiązań cyfrowych również w administracji publicznej. W konsekwencji prowadzi to do transformacji technologicznych, a co za tym idzie, wymusza zmiany prawne, które w celu zagwarantowania praw jednostki, w szczególności prawa do prywatności, muszą stale ewoluować. Funkcjonowanie e-usług rodzi wyzwania w zakresie zapewnienia ich bezpieczeństwa. W szczególności wprowadzane na rynek rozwiązania, wykorzystujące nowe technologie, chociażby blockchain, sztuczną inteligencję, czy technologie kognitywne, mogą wywierać silny wpływ na prawo do prywatności osoby fizycznej. W tym świetle kontekst znaczeniowy rozszerzyła również definicja prawa do prywatności poprzez przyjęcie, że obejmuje również tzw. prawo do spokoju cyfrowego.

Artykuł wskazuje na przepisy regulujące bezpieczeństwo e-usług oraz analizuje mechanizmy zapewniające ochronę prywatności. Odnosi się również do specyfiki technologii blockchain z punktu widzenia wykorzystania algorytmu pseudonimizacji. Z uwagi na genezę prawa do bycia zapomnianym jako instrumentu wywodzącego się z problemów w obszarze prywatności występujących w sferze Internetu, artykuł omawia jego zastosowanie na gruncie e-usług świadczonych przez administrację publiczną.

Słowa kluczowe: administracja, e-usługi, Internet, prawo do prywatności, dostępność cyfrowa

ANALYSIS OF THE RIGHT TO PRIVACY IN THE CONTEXT OF THE FUNCTIONING OF E-SERVICES IN PUBLIC ADMINISTRATION

Abstract

The continuous development of digital public services contributes to increased use of e-services by citizens. This is the result of both economic and social changes.

The emergence of the information society and the flourishing of ICT technology determine the introduction of new digital solutions also in public administration. As a consequence, this leads to technological transformations, and, consequently, necessitates legal changes, which, in order to guarantee individual rights, particularly the right to privacy, must constantly evolve. The functioning of e-services poses challenges in the area of ensuring their security. In particular, new solutions being introduced to the market that utilize cutting-edge technologies, such as blockchain, artificial intelligence, or cognitive technologies, can have a significant impact on an individual's right to privacy. In this light, the contextual meaning has also expanded the definition of the right to privacy by adopting that it also includes the so-called right to digital peace.

This paper points to regulations governing the security of e-services and analyzes mechanisms that ensure privacy protection. It also refers to the specifics of blockchain technology from the perspective of using pseudonymization algorithms. Given the origins of the right to be forgotten as an instrument stemming from problems in the area of privacy occurring in the realm of the Internet, this paper discusses its application in the context of e-services provided by public administration.

Keywords: administration, e-services, Internet, right to privacy, digital accessibility

Autor:

Małgorzata Giela
Urząd Miejski w Zabrzu
e-mail: malgorzatagiela@icloud.com

Cytowanie: Giela M. (2023). Analiza prawa do prywatności w kontekście funkcjonowania e-usług w administracji publicznej. *Etyka Biznesu i Zrównoważony Rozwój. Interdyscyplinarne studia teoretyczno-empiryczne*, 2, 15–28.

Wprowadzenie

Rozwój cyfrowy prowadzi do transformacji społecznych. Przede wszystkim wpływa on na postęp gospodarczy, ale w konsekwencji przyczynia się do zmian we wszystkich sferach życia jednostki. Zapewnia jej łatwiejszy dostęp do mediów, świadczeń opieki zdrowotnej, bankowości, komunikacji z rodziną, czy też możliwość załatwienia spraw administracyjnych. Na pierwszym planie tego zjawiska znajduje się postęp gospodarczy,

który korzysta na nowych, efektywniejszych sposobach zbierania i analizy danych, automatyzacji oraz innowacji. Rozwój przedsiębiorstw oraz występująca między nimi konkurencja, wiążą się z koniecznością przetwarzania dużej liczby danych i podejmowania szybkich decyzji, co wymusza na podmiotach gospodarczych poszukiwanie coraz bardziej zaawansowanych rozwiązań technologicznych (Ulman, Ćwiek, 2021). Technologie takie jak sztuczna inteligencja, big data czy chmura obliczeniowa stają się kluczowe w osiąganiu przewagi konkurencyjnej. Informatyzacja i automatyzacja są dziś standardem w zarządzaniu dużymi korporacjami, a także mniejszymi przedsiębiorstwami. To, co jest szczególnie ważne, to konieczność dostosowania się sfery administracji publicznej do tego dynamicznego otoczenia. W ślad za tym musi więc iść postęp w sferze administracji publicznej, a przede wszystkim świadczonych przez nią usług, dedykowanych zarówno osobom fizycznym, jak i podmiotom gospodarczym. Obywatele oczekują efektywnego i transparentnego działania organów administracji publicznej, w tym w szczególności szybkich i jasnych procedur administracyjnych. Wymaga to dokonywania także w urzędach inwestycji w nowe technologie, szkolenie kadry urzędniczej i reorganizację procesów. Trzeba mieć jednak na względzie, że postęp technologii wiąże się również z nowymi wyzwaniami i zagrożeniami, takimi jak kwestie prywatności osób czy cyberbezpieczeństwa (Kuzior i in., 2022). Jednakże tak jak mentalność człowieka, tak też przepisy prawa muszą starać się nadążyć za zmieniającymi się rozwiązaniami w sferze informatycznej, tak aby nadążały one za zmieniającą się rzeczywistością. Konsekwencje transformacji cyfrowej są widoczne zarówno w sferze gospodarczej, jak i w życiu codziennym jednostek, a także już w funkcjonowaniu administracji publicznej. Nowa perspektywa finansowania Unii Europejskiej przyczyni się do jeszcze większego rozwoju w obszarze e-usług. Tym samym, aby skutecznie korzystać z jego szans i minimalizować ewentualne ryzyka, konieczne jest ciągłe monitorowanie ram prawnych.

Wymagania przepisów prawa w obszarze wdrażania e-usług są często bardziej złożone niż w przypadku rozwiązań wprowadzanych przez przedsiębiorców. W szczególności w celu zapewnienia bezpieczeństwa ustawodawca wprowadził obowiązek utworzenia, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji. System ten jest jednym z fundamentów zapewniających ochronę wdrażanych narzędzi cyfrowych w administracji publicznej. Łączy on w sobie obowiązki nałożone na jednostki administracji publicznej, które stanowią realny mechanizm przestrzegania praw użytkowników, klientów platform, czy aplikacji oferowanych przez urzędy. Założenia systemu zarządzania bezpieczeństwem informacji są nie tylko reakcją na ewolucję zagrożeń cyfrowych, ale również mechanizmem umożliwiającym wprowadzenie innowacji w sposób kontrolowany i bezpieczny zarówno dla samej organizacji, jak i użytkowników wdrażanych rozwiązań. System zarządzania

bezpieczeństwem informacji jest więc kluczowym elementem, który integruje różne aspekty funkcjonowania administracji, od infrastruktury technicznej, środowiskowej, informatycznej, zasobów ludzkich, aż po procedury operacyjne i także normy etyczne. Celem stosowania nowych rozwiązań jest uproszczenie skomplikowanych procedur administracyjnych, otwarcie się na klienta, czy też przede wszystkim poprawa jakości świadczonych usług. Na względzie należy mieć, że w wielu przypadkach systemy budowane są w oparciu o nowoczesne technologie, w tym technologie kognitywne, sztuczną inteligencję, co może rodzić ryzyko naruszeń praw do prywatności osoby fizycznej (Wrzesiński, 2019, 127–132). Docelowo prowadzi to do automatyzacji wielu procesów. Nie można też zapomnieć o samym celu wdrażania nowych technologii w administracji, którym jest przede wszystkim uproszczenie procedur, poprawa jakości świadczonych usług i większa ich dostępność. Obywatele oczekują od administracji skuteczności i efektywności na poziomie, do jakiego przyzwyczaiły ich rozwiązania wprowadzane przez sektor prywatny, w szczególności w zakresie bankowości internetowej czy możliwości zakupów online. Przykładowo w administracji popularność zyskuje rozwiązanie w postaci chatbota czy hurtowni danych. Nowoczesna administracja musi dotrzymywać tempa rozwoju w biznesie, więc zmiany te są nie tylko oczekiwane, co wręcz stają się standardem, także w zakresie komunikacji marketingowej (Kuzior i in., 2019). Tym samym obowiązek przestrzegania praw jednostki w fazie projektowania tych usług musi być każdorazowo uwzględniany. Tylko wtedy można mówić o pełnym i odpowiedzialnym wykorzystaniu potencjału, jaki niesie ze sobą rozwój cyfrowy w administracji publicznej. Ostatecznym jednak celem jest stworzenie takich rozwiązań informatycznych, które nie tylko będą nowoczesne i efektywne, ale także bezpieczne i etycznie niebudzące wątpliwości. Tym samym każde nowe wdrożenie e-usług musi być starannie analizowane i oceniane pod kątem jego wpływu na prawa i wolności jednostki.

Pojawiające się ciągłe zmiany, wielokrotnie prowadzą do zwiększenia dotychczasowego zakresu znaczenia praw jednostki. Tak jak dawniej przyjmowało się, że prawo do prywatności obejmuje przede wszystkim prawo do nietykalności domu, mieszkania, tak obecnie obszar ten dotyczy też przestrzeni cyfrowej człowieka (Kramer, 1990, 703–704). Pojęcie to rozszerza się więc również na prywatność danych, komunikację online i wszelkie inne formy aktywności człowieka w Internecie.

Dla zrozumienia zagadnienia konieczne jest zdefiniowanie pojęcia „e-usługa". Za e-usługi uznaje się te usługi, które świadczone są drogą elektroniczną, z wykorzystaniem Internetu, i których świadczenie jest zautomatyzowane. Ponadto usługi te powinny wymagać niewielkiego udziału człowieka i muszą wykorzystywać technologię informacyjną (Szewc, 2012, 110–122). E-usługi bardzo często świadczone są więc przez platformy internetowe

czy aplikacje mobilne. Umożliwiają one użytkownikowi dostęp do różnych rodzajów usług – od bankowości, przez sklepy internetowe, aż do usług administracyjnych.

Jednym z podstawowych elementów rozwoju e-usług jest zapewnienie ich bezpieczeństwa. Może bowiem dochodzić do nadużyć w tym zakresie, np. poprzez nieodpowiednio zabezpieczone dane osobowe, które mogą zostać celem ataku cyberprzestępców. Pamiętać jednak należy, że możliwe są również bardziej niedostrzegalne na pierwszy rzut oka formy naruszenia prywatności, takie jak profilowanie użytkowników dla celów marketingowych bez ich wyraźnej zgody. Wiele aktów prawnych nakłada na administrację obowiązki w zakresie ochrony prywatności. Jako jeden z podstawowych aktów prawa obowiązujący w polskim porządku prawnym, należy wyszczególnić ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[1]. Określa ona wymagania dla systemów informatycznych używanych do realizacji zadań publicznych i działania zmierzające do informatyzacji podmiotów świadczących usługi publiczne[2].

Nie można jednak zapomnieć o etycznym aspekcie zagadnienia e-usług. Kładzenie na nie nacisku niesie za sobą również ryzyka społeczne, w szczególności takie jak wykluczenie cyfrowe osób, które z różnych powodów nie mają dostępu do komputera czy Internetu lub nie potrafią się nim posługiwać. Koniecznie więc wraz z rozwijaniem e-usług trzeba dbać o modernizacje infrastruktury technicznej oraz organizowanie programów edukacyjnych, mających na celu minimalizowanie tego rodzaju barier. Jednocześnie projektowanie nowych rozwiązań cyfrowych musi odbywać się w duchu dostępności cyfrowej. Tym samym, w dobie cyfryzacji, prawa takie jak prywatność, dostęp do informacji czy przede wszystkim równość wobec prawa nabierają nowego znaczenia, które musi wprowadzać mechanizmy ich ochrony.

Rozwój społeczeństwa informacyjnego i technologii komunikacyjno-informacyjnej w kontekście e-usług

Na kształt praw jednostki w sferze cyfrowej wywarł wpływ rozwój społeczeństwa informacyjnego i technologii komunikacyjno-informacyjnych (ICT). Ma on też bezpośredni związek z funkcjonowaniem e-usług, nie tylko w kontekście administracji publicznej, ale również w sektorze prywatnym. Jednym z najbardziej dostrzegalnych efektów dla obywatela jest zwiększenie dostępności usług. Obecnie z usług można skorzystać w dowolnym miejscu online przez 24 godziny na dobę i 7 dni w tygodniu. Dawniej te same usługi dostępne były tylko w konkretnych lokalizacjach lub w ograniczonych godzinach.

1 Dz. U. z 2023 r. poz. 57 z późn. zm., zwana dalej: ustawa o informatyzacji.

2 Art. 1 ustawy o informatyzacji.

Jednym zaś z podstawowych elementów ludzkiego życia jest proces komunikowania się. Jeszcze niedawno podstawowym sposobem komunikowania się było bezpośrednie komunikowanie się interpersonalne (Kuzior, 2011, 169–181). Internet przede wszystkim w tym zakresie dokonał fundamentalnych zmian. Chociażby w ramach wykorzystania z technologii informacyjnych rozwinęła się możliwość wizualnej interakcji pomiędzy komputerem a człowiekiem, np. poprzez korzystanie z komputera w połączeniu z kamerą czy identyfikacji dostępu za pośrednictwem rysów twarzy (Face ID) lub linii papilarnych, tzw. nietradycyjnych urządzeń wejściowych. Daje to możliwość naturalnej interakcji na płaszczyźnie człowiek–komputer w dwóch lub trzech wymiarach (Kuzior, Kochmańska, Marszałek-Kotzur, 2020, 11).

Jak zostało już wyżej wskazane, dynamiczny rozwój technik informacyjnych wiąże się z transformacją w różnych sferach życia – nie tylko w sferze ekonomicznej czy politycznej, ale przede wszystkim w sferze społecznej. W konsekwencji powoduje to powstanie nowej struktury społecznej, która opiera się na informacji i globalizacji. Funkcjonujące w niej zaś organizacje muszą przystosować się do przetwarzania ogromnych ilości danych (ang. big data) (Castells, 1996). Wpływa to też na kreatywność organizacji (Kuzior, 2013). Powstałe w ten sposób społeczeństwo informacyjne jest bardziej zaangażowane w rozwój nowych technologii, np. poprzez korzystanie z e-usług. Trzeba jednak pamiętać, że społeczeństwo to jest jednocześnie bardziej zagrożone utratą prywatności czy nieuprawnionym przetwarzaniem danych osobowych (Ciechomska, 2021, 22–25). Technologie informacyjne dają bowiem możliwość gromadzenia i analizy dużych ilości danych. Mechanizmy te z jednej strony prowadzą więc do większej personalizacji i efektywności usług, z drugiej strony mamy do czynienia z większą powszechnością udostępniania danych. Aspektem, który wyróżnia się w społeczeństwie informacyjnym, jest zastosowanie rozwiązań mobilnych. Aplikacje te umożliwiają korzystanie z e-usług w różnych sytuacjach – w podróży, w domu, w pracy. Rozwiązania te prowadzą do zmian stylu życia i powodują, że technologie te są obecne wszędzie. Wzrost ilości cyfrowych danych doprowadził do tego, że mechanizmy ich przetwarzania i przechowywania wymagają ciągłych udoskonaleń. Rozwój społeczeństwa informacyjnego i technologii ICT wpływa nie tylko na sposób, w jaki usługi są dostarczane, ich coraz większy wachlarz, ale również na wielopoziomowe integracje i przede wszystkim oczekiwania społeczne względem tych usług. W literaturze podkreśla się, że występujące zagrożenia dla ochrony danych osobowych użytkowników usług społeczeństwa informacyjnego wiążą się z zastosowaniem technik profilowania, bazujących na danych bardzo dobrej jakości oraz ilości danych udostępnianych przez samego użytkownika. Ponadto korzystanie z powyższych usług za pomocą wielu urządzeń podłączonych do Internetu pozwala na zwiększenie zasobu danych dotyczących jednej konkretnej jednostki. Dodatkowo daje to również możliwość uzupełnienia

tych danych o otrzymane dane ogólnodostępne w ramach analiz dużych zbiorów danych (Ciechomska, 2021, 19–22). Proces ten niesie więc wiele obietnic korzyści, ale jest również pełen wyzwań. Odpowiedzią na to była zmiana podejścia do ochrony danych przez organy Unii Europejskiej. Tym samym wdrożono rozwiązania wprowadzające systemowe gwarancje prawne, jak i obowiązki wdrażania adekwatnych zabezpieczeń technicznych.

Prawo do prywatności jako podstawowe prawo jednostki w zakresie korzystania przez nią z e-usług

Korzystanie z wystawianych online usług cyfrowych, zarówno na poziomie administracji centralnej, jak i lokalnej, wiąże się z koniecznością przetwarzania danych osobowych i wpisało się praktycznie w życie codzienne obywateli. Zagadnienie, jakim jest ochrona danych osobowych i prywatności, zyskała w konsekwencji na znaczeniu. Środowisko, jakim jest Internet jako przestrzeń cyfrowa, determinuje wielopłaszczyznowe przetwarzanie danych nie tylko tych, które użytkownik w pełni świadomie i bezpośrednio do niego wprowadza (np. dane identyfikacyjne czy adresowe), ale także tych, na których pozyskanie wyraża zgodę, a które to z punktu widzenia użytkownika znajdują się w tle danej czynności (np. adres IP, dane o lokalizacji, pliki cookies) (Krzysztofek, 2012, 29–34). Coraz większa popularność tych rozwiązań w pewien sposób automatycznie zwiększa skalę przetwarzania danych jednostki i tym samym środowisko to czyni podatnym na zagrożenia. W konsekwencji są to więc wyzwania dla rzeczywistej ochrony prywatności w Internecie. Zagadnieniem tym zajęły się organy Unii Europejskiej, wprowadzając do europejskiego porządku prawnego 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)[3]. Co ważne, RODO wymaga chociażby uzyskania jasnej i jednoznacznej zgody na przetwarzanie danych osobowych, a także gwarantuje prawo do bycia „zapomnianym" w sieci. Biorąc pod uwagę skalę przetwarzania oraz możliwe wytępianie negatywnych skutków dla osoby fizycznej, prawo do prywatności należy uznać za podstawowe prawo jednostki w zakresie korzystania przez nią z e-usług, w tym cyfrowych usług publicznych wprowadzanych przez organy administracji.

Szczególnie warto zwrócić uwagę na specyfikę danych określanych jako pliki cookies, tzw. ciasteczka. Jest to narzędzie, które umożliwia monitoring w zakresie aktywności, preferencji i zachowań użytkowników platform. Chociaż powinny one głównie służyć do poprawy jakości usług elektronicznych, jak na przykład zapamiętywania zawartości

3 Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm., zwany dalej: RODO.

koszyka w sklepie internetowym, to jednak w praktyce mogą zostać użyte w sposób, który narusza prywatność osoby fizycznej. Zgromadzone w ten sposób dane pozwalają także np. na personalizowanie reklam. Dzięki zmianom przepisów prawa dzieje się to na podstawie zgody użytkownika, co ma stanowić jeden z mechanizmów bezpieczeństwa jego prywatności. W kontekście tym zapewnienie ochrony danych osobowych i prywatności w związku z korzystaniem z e-usług jest wyzwaniem, które wymaga kompleksowego podejścia, tak samo od strony prawnej, jak i technologicznej. Rozwiązania prawne powinny się zaś przyczyniać również do budowania zaufania pomiędzy użytkownikami a dostawcami usług, co w dłuższej perspektywie powinno doprowadzić do uzyskania korzyści przez obie strony.

W administracji publicznej, jak również w innych dziedzinach życia bardzo często wykorzystywane są tzw. „chmury obliczeniowe", które polegają na powierzeniu przetwarzania danych podmiotom trzecim w celu realizacji przez nie usług udostępnianych użytkownikowi oprogramowania bez konieczności instalowania go w komputerze. W tym przypadku dane są więc udostępnione dodatkowo innemu podmiotowi niż temu, któremu bezpośrednio udostępnia je sam użytkownik, co stanowi również przykład zagrożenia dla prywatności podmiotu. Ich główną zaletą jest jednak przetwarzanie danych w sposób efektywny i często ekonomiczny. Często zapewnia ona też dostęp do zasobów i usług bez konieczności posiadania zaawansowanego oprogramowania czy rozwiniętej infrastruktury IT.

Z powyższego wynika, że głównym zagrożeniem dla jednostki w związku z użytkowaniem przez nią e-usług jest właśnie naruszenie prawa do prywatności.

Mając na względzie kontekst korzystania z e-usług, prawo do prywatności jest więc zagadnieniem złożonym. Warto wziąć pod uagę, że geneza tego prawa korzenie ma w podstawowych zasadach demokracji. Za to w erze cyfryzacji prawo to rozszerza się także na ochronę przed nieautoryzowanym dostępem, wykorzystaniem czy dystrybucją danych osobowych. W literaturze przyjmuje się, że głębsza dyskusja i analiza nad prawem do prywatności rozpoczęła się w 1890 r. wraz z opublikowaniem artykułu w przedmiocie prywatności, którego autorami byli Samuel D. Warren i Louis D. Brandeis (Sieńczyło-Chlabicz, 2010, 1149). Początkowo prawo do prywatności uznawano za prawo do pozostawienia w spokoju. Prywatność utożsamiano więc z prawem do całkowitej nietykalności i pozostania w samotności (Cooley, 1988, 29). W Polsce kolebkę tego prawa należy w szczególności upatrywać w ustawie z 18 lipca 1950 r. Przepisy ogólne prawa cywilnego[4]. W dosyć ogólnym przepisie dotyczącym ochrony dóbr osobistych, ustawodawca wprowadził prawo do prywatności. Obecnie zaś prawo do prywatności zostało bezpośrednio określone w Konstytucji Rzeczpospolitej Polski.

4 Dz. U. Nr 34, poz. 311.

W związku z dynamicznym rozwojem technologii i cyfryzacji prawo do prywatności ewoluowało i należy przyjąć, że zmiany te będą postępowały dalej. Obecnie interpretuje się je dodatkowo jako prawo do kontroli nad własnymi danymi, włączając w to zarówno dane identyfikacyjne, jak i metadane generowane w trakcie korzystania z różnych usług cyfrowych. W konsekwencji zmian świadomości człowieka prawo to dąży również do zagwarantowania „cyfrowego spokoju", czyli zapewnienia jednostce możliwości korzystania z usług internetowych bez nadmiernej inwazji w jej prywatność. W obliczu pojawiających się stale nowych technologii i popularności w korzystaniu z e-usług, konieczne jest zabezpieczenie prawa do prywatności w kontekście nowych form przetwarzania danych. Regulacje prawne wymagają więc stałego monitorowania i aktualizacji. Ponadto pozytywnie ocenić należy uwzględnienie w nowej perspektywie finansowania Unii Europejskiej założenia przeznaczenia środków na szkolenie zarówno społeczeństwa, jak i urzędników w zakresie e-usług i cyberbezpieczeństwa. Edukacja w tym obszarze jest bowiem kluczowa, ale jej efekty będą występować jedynie, jeżeli twórca będzie wiedział, w jaki sposób może zapewnić bezpieczeństwo praw jednostki, a użytkownik musi mieć świadomość, jakie prawa mu przysługują i jak je respektować.

W tym kontekście chociażby RODO, poprzez konstrukcje zawartych w nim przepisów, stara się dostosować wymogi dla przetwarzania danych do nowych wyzwań technologicznych. Podejmując temat prywatności w zakresie e-usług pamiętać jednak należy, że prawo do ochrony danych osobowych i prawo do prywatności to są dwa różne prawa. Wprawdzie pozostają w bardzo mocnym związku, ale są to jednak odrębne prawa (De Hert i in., 2013, 1 i n.). Tym samym celem RODO jest ochrona danych osobowych, które stanowią element prywatności osoby fizycznej.

Mechanizmy ochrony praw jednostki

Wykorzystywanie e-usług wiąże się z wyzwaniami. Najważniejszym z nich jest zapewnienie bezpieczeństwa danych osobowych i prywatności użytkownika, co na podmiot administracji publicznej nakładają również przepisy prawa. W szczególności należy pamiętać, że dane te przechowywane są na serwerach lub w chmurze, co powoduje zagrożenie nie tylko ze strony dostawcy usługi, ale również ze strony podmiotów trzecich, które mogą podejmować działania w celu przejęcia dostępu do nich w sposób nieuprawniony. W praktyce oznacza to obowiązek wdrażania zaawansowanych mechanizmów bezpieczeństwa, w szczególności takich jak szyfrowanie, uwierzytelnianie wieloskładnikowe i regularne audyty bezpieczeństwa.

Na podstawie ustawy o informatyzacji do polskiego porządku prawnego wprowadzone zostały Krajowe Ramy Interoperacyjności, czyli rozporządzenie Rady Ministrów

z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5]. Zgodnie z § 3 KRI Krajowe Ramy Interoperacyjności określają sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu oraz procedur organizacyjnych oraz sposoby postępowania podmiotu realizującego zadania publiczne w zakresie przejrzystego wyboru norm, standardów i rekomendacji w zakresie interoperacyjności semantycznej, organizacyjnej oraz technologicznej, z zapewnieniem zasady neutralności technologicznej. Tym samym obowiązki te mają za zadanie docelowo zapewnić bezpieczeństwo prywatności jednostki, także w związku z realizowanymi przez organ e-usługami.

Omawiając narzędzie służące zapewnieniu ochrony prywatności osobie fizycznej, warto zwrócić uwagę na nowe technologie, a w szczególności na jedną z nich, jaką jest blockchain. Zgodnie z art. 25 RODO pseudonimizacja jest jednym z rekomendowanych przez unijnego ustawodawcę narzędzi ochrony danych. Blockchain w swojej specyfice posługuje się właśnie danymi spseudonimizowanymi. W formule tej dochodzi do przekazywania określonych danych, które są zaszyfrowane za pomocą algorytmów i złożonych mechanizmów kryptograficznych. Jednak pamiętać należy, że ich zakres nawet w formie rozproszonej docelowo może wiązać się ze zidentyfikowaniem określonej osoby fizycznej. Jednakże mechanizm ten właśnie z uwagi na pewnego rodzaju pierwotne zapewnienie bezpieczeństwa danych powinien zacząć być szerzej wykorzystywany przez dostawców usług dla urzędów administracji publicznej. Pomimo to dokonując analizy ryzyka dla systemu z technologią blockchain trzeba mieć oczywiście na uwadze, że dane z określonego łańcucha bloków mogą mieć w swojej zawartości informacje, które doprowadzą do ustalenia tożsamości osoby, której dane dotyczą (Dymiński, Ferenc, 2020, 52–67). W konsekwencji jednak już sama charakterystyka technologii znajdzie odzwierciedlenie w wadze ryzyka. Baza tworzona w ramach technologii blockchain nie posiada centralnych komputerów, mogących samodzielnie decydować o stanie rekordów, ani scentralizowanego miejsca przechowywania danych. Zaś sam łańcuch bloków jest chroniony przed nieuprawnionymi zmianami za pomocą algorytmów kryptograficznych (Szczerbowski, 2018, 8). Oznacza to, że system taki jest zdecentralizowany i rozproszony, dzięki czemu jest bardziej odporny na cyberataki. W literaturze podkreśla się jednak, że zgodność systemu opartego na technologii „łańcucha bloków" z przypisami z zakresu ochrony danych osobowych można ocenić

5 Dz. U. z 2017 r. poz. 2247, zwane dale: KRI.

dopiero na podstawie indywidualnej, konkretnej analizy rozwiązań systemu (Finck, 2019, 1). Ogólny opis technologii blockchain odnosi się bowiem do różnych form rozproszonej bazy danych, a same stosowane w nich rozwiązania techniczne i sposoby zarządzania nimi są również różnorodne. Istota mechanizmu wpisuje się w założenia ustawodawcy, jednakże w pozostałym zakresie technologia nadal wymaga dokładnej weryfikacji.

Wyszczególniony przez ustawodawcę unijnego obowiązek przetwarzania danych osobowych w oparciu o konkretne podstawy prawne stanowi podstawowy mechanizm bezpieczeństwa jednostki. Ponadto podkreślenie roli zgody jako przesłanki do przetwarzania danych osobowych w przypadku e-usług ma kluczowe znaczenie. Art. 4 pkt 11 RODO definiuje zgodę jako dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych. Oznacza to, że ustawodawca dopuszcza wyraźne działanie potwierdzające jako wyrażenie zgody, co z jednej strony stanowi gwarancje bezpieczeństwa, a z drugiej czyni system w pewien sposób elastycznym (Kaczmarek-Templin, 2016, 104–105). Najbardziej istotny jest jednak fakt, że żadne pozyskanie danych nie może odbyć się bez przejawu woli użytkownika, czyli tzw. systemu opy-in. Motyw 32 RODO wskazuje, że wyrażenie zgody może polegać więc na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Co ważne, sposób zapytania o zgodę musi dawać możliwość wyraźnego odróżnienia jej od innych kwestii oraz zostać sporządzona w zrozumiałej i łatwo dostępnej formie, a także jasnym i prostym językiem (Lubasz, Chomiczewski, 2018).

Prawo do bycia zapomnianym

Prawo do prywatności wiąże się z prawem do bycia zapomnianym, czyli pewnego rodzaju gwarancją zapewniającą ramy prywatności. Uprawnienie do żądania usunięcia danych osobowych z przestrzeni cyfrowej daje jednostkom pewien stopień poczucia kontroli nad własną tożsamością cyfrową. Dzięki temu osoby fizyczne nie tylko mogą ograniczyć nadużycia w sferze ich danych, ale mają wpływ na to, jak są postrzegane w sieci. Istotą tego prawa jest uprawnienie do żądania usunięcia z obiegu w sieci danych osobowych umieszczonych w Internecie przez samą osobę, której dotyczą lub przez osoby trzecie. Z punktu widzenia administracji publicznej i oferowanych przez nią usług nie ma ono jednak charakteru bezwzględnego. W tym przypadku dane osobowe są podstawowym elementem,

od których zależy wykonanie określonych zadań publicznych. Pamiętać bowiem należy, że najczęściej e-usługi służą do załatwienia spraw o charakterze administracyjnym i podanie danych osobowych jest niezbędne do ich realizacji. Wykorzystanie rozwiązań cyfrowych jest więc pewnym odwzorowaniem dotychczas załatwianej sprawy w formie papierowej, która w oparciu o te same przepisy prawa wymagała podania danych osobowych. Tym samym nie ma możliwości żądania ich usunięcia, jeżeli przez okres określony przepisami prawa, organ musi je przetwarzać. Podkreślenia wymaga jednak fakt, że system powinien żądać jedynie tych danych, które są niezbędne dla danego rodzaju spraw, a dane nieobowiązkowe powinny być wyraźnie oznaczone. Tworzenie i funkcjonowanie e-usług musi więc być powiązane z analizą danych zbieranych przez dany system. Jak zostało już wcześniej wspomniane, powinno to uwzględniać zarówno dane, które użytkownik sam wprowadza w określone pola, jak i również te dotyczące informacji systemowych. Organy administracji publicznej powinny podejmować więc odpowiedzialne działania w kontekście minimalizacji danych. Instrumentem kluczowym w zapewnieniu prywatności poprzez przekazanie użytkownikowi informacji o polach obowiązkowych, jest zarówno mechanizm oznaczenia pól, jak i konieczność spełniania przewidzianego w art. 12 RODO obowiązku zapewnienia przejrzystego informowania i komunikowania, zarówno w postaci klauzul informacyjnych, jak i regulaminów czy polityk prywatności. Użytkownicy e-usług muszą więc być jasno i zrozumiale informowani o tym, jakie dane są zbierane, w jakim celu i przez jaki czas będą przechowywane.

Zarówno prawo do prywatności, jak i prawo do bycia zapomnianym zawsze są równane z innymi dobrami, jak np. bezpieczeństwo publiczne, czy wymaganiami, takimi jak inne obowiązki prawne. W praktyce wiąże się to z dokonywaniem stałej analizy i oceny przez organy administracji publicznej, w jakim zakresie i w jakim celu przetwarzają one dane osobowe, tak aby zapewnić zarówno dobra prawnie chronione, efektywność usług, jak i należytą ochronę prywatności.

Zakończenie

Nie ulega wątpliwości, że prawo do prywatności musi być uznane za fundamentalne w korzystaniu z usług elektronicznych. W erze społeczeństwa informacyjnego takie samo znaczenie mają zarówno rozwiązania techniczne, jak i regulacje prawne. Jednak zapewnienie prywatności nie będzie również możliwe bez świadomości obywateli i wiedzy kadry urzędniczej.

Analizując różne narzędzia i technologie, technologia blockchain stanowi wyjątkowo ciekawy przykład, który stanowi zarówno nowe podejście technologiczne, jak i łączy w sobie jedną

z technik gwarancji bezpieczeństwa danych. Mechanizm pseudonimizacji jest pewnego rodzaju odpowiedzią na wymagania przepisów prawa w zakresie rozwiązań technicznych. Jednakże trzeba uważać, żeby nie wpaść w pułapkę ideologicznych założeń i jednak każde rozwiązanie z technologią blockchain analizować indywidualnie pod kątem zapewnienia bezpieczeństwa danych. Istnieje bowiem ryzyko deanonimizacji, ponieważ w niektórych przypadkach może być możliwe powiązanie danych z konkretną osobą. Wiąże się to z powstaniem ryzyka naruszenia prywatności. Blockchain jest jednak technologią, która zasługuje na uwagę w kontekście ochrony danych i prywatności.

Regulacje prawne ciągle wymagają zmian, które zapewnią pewnego rodzaju elastyczność względem nowych technologii. Pozytywnie jednak należy ocenić przepisy unijne, dotyczące ochrony danych osobowych. Wprowadziły one szereg zasad i mechanizmów, mających na celu zapewnienie prywatności i bezpieczeństwa danych jednostek. Jednym z filarów tego systemu jest obowiązek przetwarzania danych na jasno określonych, w szczególności w art. 6 i 10 RODO, podstawach prawnych. Tym samym każda instytucja publiczna i prywatna, która przetwarza dane, musi kierować się przesłanką legalności.

Na zakończenie warto podkreślić rolę zgody osoby, której dane są przetwarzane. W kontekście e-usług jest to szczególnie ważne. Dochodzi tutaj bowiem do interakcji między stronami, która jest często mniej bezpośrednia niż w tradycyjnych formach wymiany dokumentów, np. poprzez złożenie pisma w formie papierowej do organu.

Bibliografia

Castells M. (1996). The Information Age: Economy, Society and Culture, t. 1, The rise of the Network Society.

Ciechomska M. (2021). E-usługi a RODO, Warszawa, s. 19–25.

Cooley T. M. (1988). A treatise on the law oj torts, Chicago: Callaghan 1888, s. 29.

De Hert P., Papakonstantinou V., Wright D., Gutwirth S. (2013). The proposed Regulation and the construction of a principles-driven system for individual data protection. Innovation, „The European Journal of Social Science Research, Technology and Privacy" 2013/1–2, s. 1 i n.

Dymiński M., Ferenc D. (2020). RODO w łańcuchu bloków, PPP 2020, nr 6, s. 52–67.

Finck M. (2019). Blockchain and General Data Protection Regulation, Bruksela, s. 1.

Kaczmarek-Templin B. (2016). Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia. W: Polska i europejskareforma ochrony danych osobowych, red. Bielak-Jomaa E., Lubasz D. Warszawa, s. 104–105.

Kramer I.P. (1990). The Birth oj Privacy Law: A Century Since Warren and Brandeis, „Cath. U. L. Rev.", vol. 39.

Krzysztofek M. (2012). „Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE, EPS 2012, nr 8, s. 29–34.

Kuzior A. (2011). Komunikacja interpersonalna w biznesie. W: Kadry i płace w przedsiębiorstwie. Red. M. Król, A. Warzecha, M. Zieliński. Gliwice. Gliwicka Wyższa Szkoła Przedsiębiorczości.

Kuzior A. (2013). The ICT as a tool for sustainable development, Contemporary developmental challenges, Kuzior A. (red), Belianum Matej Bel University Press, Banska Bystrica.

Kuzior A., Kochmańska A., Marszałek-Kotzur I. (2020). Wykorzystanie technologii informacyjno-komunikacyjnych w organizacji – korzyści i zagrożenia. Etyka Biznesu i Zrównoważony Rozwój. Interdyscyplinarne Studia Teoretyczno-empiryczne, nr 3, 2020.

Kuzior A., Sobotka B., Filipenko A., Kuzior P. (2019). Marketing communications of administrative organs of local governance and local community. Marketing and Management of Innovations, 2, 314–325.

Kuzior A., Vasylieva T., Kuzmenko O., Koibichuk V., Brożek P. (2022). Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. Journal of Open Innovation: Technology, Market, and Complexity, 8(4), 195.

Lubasz D., Chomiczewski W. (2018). Art. 6, W: RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, Warszawa.

Sieńczyło-Chlabicz J. (2010). Geneza i rozwój prawa do prywatności, O prawie i jego dziejach księgi dwie. Studia ofiarowane profesorowi Adamowi Lityńskiemu w czterdziestopięciolecie pracy naukowej i siedemdziesięciolecie urodzin. Księga II, Wydawnictwo Uniwersytetu w Białymstoku, Katowice–Białystok, s. 1149.

Szczerbowski J.J. (2018). Lex Cryptographia, Warszawa, s. 8.

Szewc T. (2012). Administracja wobec rozwoju e-usług, PPP 2012, nr 7–8.

Ulman P., Ćwiek M. (2021). Nierówności w rozwoju cyfrowym w krajach Unii Europejskie, Nierówności Społeczne a Wzrost Gospodarczy, nr 66 (2/2021), Social Inequalities and Economic Growth, no. 66 (2/2021), DOI: 10.15584/nsawg.2021.2.3.

Wrzesiński P. (2019). Bariery prawne rozwoju cyfrowych kanałów dystrybucji w działalności zakładów ubezpieczeń w Polsce, Prawo asekuracyjne 2/2019 (99).