Wyciek danych z systemu teleinformatycznego na przykładzie działalności wybranych organów administracji publicznej

Agata Jałowiecka[1]

Tematem opracowania są zagadnienia związane z aspektami wycieku danych z systemów teleinformatycznych wybranych organów administracji publicznej. Autorka porusza tematykę wycieku danych z systemu teleinformatycznego, częstotliwość takich incydentów, okoliczności kontaktu elektronicznego podmiotu z jednostkami samorządu terytorialnego oraz obustronnego przesyłania danych i dokumentów, w tym poprzez system ePUAP. Przedstawia także konsekwencje, sposoby postępowania w sytuacji wycieku danych oraz dobre praktyki, które należy stosować, aby do takiego zdarzenia nie doszło.

Uwagi wstępne

W XXI w. technologie informacyjne wspomagają pracę ludzkości na całym świecie praktycznie w każdej dziedzinie życia. Powiązane jest to z silnym rozwojem społeczeństwa informacyjnego oraz technologii informacyjno-komunikacyjnych, których rozkwit nieustannie postępuje. Wspomniane rozwiązania techniczne są stosowane również w polskim systemie prawnym, co wymusza wprowadzanie nowych sposobów zarządzania zasobami informacyjnymi pozostającymi w dyspozycji podmiotów publicznych[2]. Wprowadzanie takich rozwiązań staje się metodą zwiększania efektywności przetwarzania danych[3], co z kolei jest silnie związane z zasadą szybkości, efektywności i prostoty postępowania[4]. Jest to także ważny element zarządzania publicznego. Prawo administracyjne m.in. reguluje kwestie związane z wykorzystywaniem technologii w działalności administracji publicznej[5], w tym (jak zostało określone w art. 2a § 1 KPA) wykonywanie obowiązku, o którym mowa w art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[6], w postępowaniach wymienionych w art. 1 i 2 KPA. W ostatnim dziesięcioleciu wprowadzono również wiele rozwiązań z zakresu e-governmentu, elektronicznej komunikacji z administracją publiczną oraz elektronicznego postępowania administracyjnego[7] umożliwiających m.in. załatwianie spraw przez Internet oraz elektroniczne przesyłanie dokumentów do urzędów. Wszystkie te rozwiązania mają na celu usprawnienie działania administracji publicznej i ułatwienie obywatelom kontaktu z urzędami. Czasem dochodzi jednak do niedociągnięć ludzkich, wad systemów teleinformatycznych oraz ataków hakerskich, które mogą powodować wycieki danych poufnych przechowywanych oraz zaszyfrowanych przez takie systemy[8]. W takim wypadku należałoby zbadać, czym jest wyciek danych z systemu teleinformatycznego oraz na przykładzie funkcjonowania jednostek administracji publicznej i korzystania przez nie z systemów teleinformatycznych przedstawić, jakie są skutki takiego zdarzenia oraz konsekwencje nieprawidłowości w funkcjonowaniu tych systemów, jak unikać takich zdarzeń, a także wskazać przykładowe sposoby postępowania w wyniku wycieku danych.

Wybrane zagadnienia związane z wyciekiem danych z systemu teleinformatycznego

Wyciek danych z systemu teleinformatycznego administracji publicznej to sytuacja, w której dane zgromadzone w systemie informatycznym są przypadkowo lub celowo udostępnione osobom nieupoważnionym. Może to obejmować dane osobowe, finansowe lub inne poufne informacje, które zostały przechowywane np. przez urząd, jednostkę administracji publicznej lub system teleinformatyczny. Wyciek danych może być spowodowany różnymi przyczynami, takimi

[1] Autorska jest studentką V roku prawa na Uniwersytecie Wrocławskim, przewodniczącą koła naukowego SKN Blok Prawa Komputerowego LegalNet.

[2] *S. Kotecka-Kral*, Informatyzacja usług publicznych – Założenia Konstrukcyjne, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, Prawo nowych technologii, Warszawa 2021, s. 13–15.

[3] *Ł. Dubiński*, RODO a postępowanie administracyjne (zagadnienia wybrane), [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński* (red.), Ochrona danych osobowych w postępowaniach sądowych i przed organami administracji publicznej (Polska), Warszawa 2019, s. 163–177.

[4] *J. Zimmermann*, Prawo administracyjne (Polska), Warszawa 2022, s. 164–166.

[5] *A. Łożykowski*, *J. Sarnowski* (red.), GovTech, czyli nowe technologie w sektorze publicznym, Warszawa 2019, s. 13–19.

[6] Dz.Urz. UE. L Nr 119, s. 1; dalej jako: RODO.

[7] *K. Chałubińska-Jentkiewicz*, *M. Karpiu*k, Podstawowe zasady regulacyjne w systemie infrastruktury informacyjnej państwa [w:] *K. Chałubińska-Jentkiewicz*, *M. Karpiuk*, Prawo nowych technologii. Wybrane zagadnienia, Warszawa 2015, s. 52–56.

[8] *J. Wasilewski*, Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne, pod kierunkiem *E.M. Guzik-Makaruk*, Białystok 2017, s. 60–72.

jak błędy ludzkie (np. nieautoryzowane przenoszenie danych za pomocą pendrive'a skutkujące wyciekiem danych[9]), błędy techniczne (systemu) lub działania hakerów (np. cyberataki). Takie zdarzenie może prowadzić do poważnych konsekwencji, m.in. takich jak szkody finansowe, utrata danych poufnych, co może wiązać się z utratą dobrego imienia, czy naruszenie prywatności osób, których dane wyciekły. W związku z tym ważne jest, aby administracja publiczna dbała o bezpieczeństwo danych i stosowała odpowiednie środki ostrożności, takie jak szyfrowanie danych czy stosowanie zabezpieczeń przed atakami hakerskimi. Związane jest to stricte z określoną w art. 8 KPA zasadą zaufania do władzy publicznej. Przepis ten wskazuje, że organy administracji publicznej prowadzą postępowanie w sposób budzący zaufanie jego uczestników do władzy publicznej, kierując się zasadami proporcjonalności, bezstronności i równego traktowania. Wyciek danych z systemu teleinformatycznego administracji publicznej może mieć negatywny wpływ na zaufanie obywateli do władzy publicznej oraz systemów, z których korzysta. To z kolei może prowadzić do konfliktów i niezadowolenia społecznego. Innym istotnym zagadnieniem jest atak hakerski[10]. Może to obejmować takie działania, jak włamanie się do systemu, nielegalne kopiowanie danych czy zmiana lub usunięcie danych. Atak hakerski może być motywowany np. chęcią uzyskania wiedzy lub dostępu do poufnych informacji, chęcią zaszkodzenia lub szantażu. Ważnym aspektem jest również zdefiniowanie incydentu. Przez incydent na gruncie art. 2 pkt 5 ustawy z 10.5.2018 r. o ochronie danych osobowych[11] rozumie się zdarzenie, które poprzez naruszenie przepisów o ochronie danych osobowych może mieć na celu niekorzystny wpływ na cyberbezpieczeństwo. Za to według art. 2 ustawy z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa[12] przez incydent w podmiocie publicznym rozumie się incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Zgodnie z art. 22 KrajSysCybU podmiot publiczny, realizujący zadanie publiczne zależne od systemu informacyjnego, zapewnia zarządzanie incydentem w podmiocie publicznym, zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia oraz zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV. Ponadto przekazując niezbędne dane, w tym dane osobowe, zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej, o której mowa w art. 21 KrajSysCybU, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

Częstotliwość wycieków danych z systemów teleinformatycznych

Coraz częściej korzystamy z rozwiązań technologicznych do załatwiania własnych spraw, w związku z czym w celu zbadania dokładnej skali wykorzystywania takich zastosowań przez społeczeństwo w 2021 r. Główny Urząd Statystyczny przeprowadził badanie dotyczące wykorzystywania Internetu i urządzeń do korzystania z usług administracji oraz sektora publicznego. Według danych uzyskanych w wyniku tego badania odsetek osób w wieku 16–74 lata korzystających z usług administracji publicznej przez Internet w ciągu ostatnich 12 miesięcy wyniósł 47,5%, co wskazuje na to, że prawie połowa społeczeństwa korzystała z takich rozwiązań[13]. Ilość ta jest niezwykle istotna, ponieważ ważnym aspektem związanym z korzystaniem z elektronicznych systemów administracyjnych jest fakt przesyłania danych poufnych m.in. do jednostek administracyjnych, co przez swoją skalę oraz możliwości, które przynosi, staje się dużą korzyścią, ale jednocześnie także coraz większym zagrożeniem. Przekazując takie informacje, użytkownik ma na celu przesłanie ich administratorowi albo odpowiednim pracownikom reprezentującym jednostkę[14], często może nawet nie biorąc pod uwagę zagrożeń, jakie związane są z elektronicznym przesyłem tych danych. Na całym świecie zdarzają się sytuacje, w wyniku których dane ulegają wyciekowi i może z nich skorzystać osoba trzecia, która nie powinna ich otrzymać. Jest to niezwykle ważny aspekt, ponieważ wiąże się on z możliwością wykorzystania cudzych danych osobowych. Ze względu na szybki rozwój technologii informacyjnych tworzenie się coraz nowocześniejszych programów, nienadążanie prac legislacyjnych związanych z bezpieczeństwem danych oraz szkoleń pracowników administracji[15], a także tworzeniem wytycznych związanych z cyberbezpieczeństwem, przesył danych może być związany z ewentualnym zagrożeniem wypłynięcia. Skalę problemu

[9] *R. Krupa-Dąbrowska*, Wyciek danych osobowych w urzędzie miasta, skopiowano dane na pendrive, Prawo.pl [(dostęp 12.12.2022 r.).

[10] Atak hakerski jest to działanie mające na celu w sposób zamierzony lub przypadkowy zniszczyć lub uszkodzić system informatyczny lub wykraść dane zgromadzone w nim – zob. *W.Z. Dziomdziora*, Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik, Warszawa 2021, s. 22–23.

[11] T.j. Dz.U. z 2019 r. poz. 1781 ze zm.; dalej jako: OchrDanychU.

[12] T.j. Dz.U. z 2022 r. poz. 1863 ze zm.; dalej jako: KrajSysCybU.

[13] *M. Wegner*, Społeczeństwo informacyjne w Polsce w 2021 r., Główny Urząd Statystyczny, 24.11.2021 r., s. 1.

[14] *Ł. Dubiński*, RODO a postępowanie…, s. 3.

[15] *A. Harężа*, The Role of Administrative Law in Times of Technological, [w:] *J. Gołaczyński*, *W. Kilian*, *T. Scheffler* (red.), Legal Innovation in Polish Law, Warszawa 2019, s. 107–118.

wycieku danych może zobrazować fakt, że według szacunków CERT Polska, „do 2020 r. wyciekły informacje dotyczące co najmniej 10 milionów kont polskich użytkowników internetu”[16]. Biorąc pod uwagę faktyczne zdarzenia związane z tymi zabiegami w administracji, sektorze publicznym czy chociażby organach administracji o znaczeniu funkcjonalnym takich jak uniwersytety, w ostatnich latach zdarzyło się wiele takich incydentów. Między innymi należałoby wspomnieć o wycieku danych z Urzędu Miejskiego w Otwocku[17] czy Urzędu Gminy w Nowinach[17], a także utracie danych przez instytucje oświatowe, takie jak Politechnika Warszawska[19] oraz Uniwersytet Warszawski[20].

Wybrane dobre praktyki związane z bezpieczeństwem danych

Udostępnianie wszelkiego rodzaju dokumentów oraz danych w postaci elektronicznej poprzez systemy teleinformatyczne wymaga zagwarantowania bardzo wysokich standardów, do których należy zaliczyć konieczność zapewnienia bezpieczeństwa teleinformatycznego, w tym odpowiednich sposobów oraz metod uwierzytelniania, identyfikacji, interoperacyjności, a także właściwego przetwarzania danych na podstawie ustaw[21]. Ogólne zasady bezpieczeństwa danych w systemie ePUAP i elektronicznych kontaktach z urzędami zostały określone w ustawie o ochronie danych osobowych. Między innymi do takich praktyk należy zachowywanie ostrożności podczas korzystania z elektronicznych usług urzędów. Nie powinno się udostępniać haseł, loginów ani innych poufnych informacji osobom trzecim. Należy korzystać z bezpiecznych połączeń internetowych, takich jak sieć Wi-Fi zabezpieczona hasłem lub połączenie przez VPN[22]. Następnie należy wspomnieć o używaniu silnych haseł i zmienianiu ich regularnie. Trzeba korzystać z aktualnego oprogramowania antywirusowego. Za każdym razem również należy upewniać się, że wykorzystuje się zaufane i oficjalne strony internetowe urzędów i serwisy, a także poprawność ich adresów URL. Ponadto trzeba unikać korzystania z podejrzanych stron internetowych lub linków zawartych w e-mailach, które mogą zawierać złośliwe oprogramowanie. Prośby o podanie haseł, loginów czy innych poufnych informacji poprzez e-mail lub wiadomości SMS nie są praktyką urzędów. W przypadku otrzymania polecenia wydania takich danych nie należy ich udostępniać i powinno się skontaktować z urzędem w sposób bezpieczny, np. przez oficjalną stronę internetową lub osobiście w siedzibie urzędu. Zgodnie z art. 190a § 2 KK osoba podszywająca się pod inną osobę, która wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej, podlega pozbawieniu wolności do lat 3. Ponadto według ustawy o ochronie danych osobowych, kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Ponadto według *S. Koteckiej*[23] w przypadku udzielania informacji sądowej, ale również urzędowej za pomocą poczty elektronicznej albo systemu ePUAP należy również dokonywać przeglądu stron internetowych sądu pod kątem aktualności danych dotyczących adresów poczty elektronicznej. Należy monitorować pracę urzędników sądowych oraz to, czy udzielają informacji na zapytania poprzez skrzynkę lub system ePUAP. Co więcej, należy sprawdzać, czy sądy oraz urzędy posiadają elektroniczne skrzynki na ePUAP oraz czy informacja jest uwidoczniona w BIP sądów. Powinno się również wdrażać systemy centralnej poczty elektronicznej, które powstały w wyniku projektu „Poprawa zdolności administracyjnych sądów powszechnych, w tym systemów informatycznych”. Jeżeli jest to wymagane, należy wydawać stosowne zarządzenie o wspomnianej treści.

Elektroniczny przesył danych

Postanowienia RODO skupione są na ochronie danych osobowych, a także regulacjach dotyczących ich swobodnego przepływu. Według *Ł. Dubińskiego*, który analizował tą tematykę, „określenie szczegółowych zasad prowadzenia postępowań administracyjnych w sprawach dotyczących ochrony danych osobowych zostało pozostawione prawodawcom krajowym”[24]. Elektroniczny przesył danych do urzędów jest regulowany przez polskie prawo administracyjne, a konkretnie przez ustawę z 18.7.2002 r. o świadczeniu usług drogą elektroniczną[25], która określa zasady korzystania z usług świadczonych przez administrację publiczną drogą elektro-

[16] Krajobraz bezpieczeństwa polskiego internetu. Raport roczny z działalności CERT Polska 2020, NASK – Państwowy Instytut Badawczy, Polska 2020, s. 140.

[17] *M. Wojtczuk*, Gigantyczny wyciek danych w Otwocku. Hakerzy wykradli PESEL-e i numery dowodów wszystkich mieszkańców, Wyborcza.pl (dostęp 10.12.2022 r.).

[18] Urząd Gminy Nowiny, Zawiadomienie Administratora Danych Osobowych o naruszeniu ochrony danych osobowych z 11.12.2021 r., s. 1–2.

[19] *A. Sanocki*, Nieuprawniony dostęp do danych z Politechniki Warszawskiej, Urząd Ochrony Danych Osobowych 2020 r., www.uodo.gov.pl/pl/138/1518 (dostęp 7.12.2022 r.).

[20] *P. Strzelecki*, Komunikat w sprawie incydentu naruszenia danych osobowych w portalu mim, Uniwersytet Warszawski, www.mimuw.edu.pl/incydent-naruszenia-danych-osobowych-w-portalu-mim (dostęp 7.12.2022 r.).

[21] *A. Zalesińska*, Dobre praktyki w zakresie udostępniania dokumentów w postaci elektronicznej w sądach powszechnych w kontekście ochrony danych osobowych, [w:] *J. Gołaczyński* (red.), Wybrane dobre praktyki w zakresie usług elektronicznych (Polska), Warszawa 2016, s. 359–372.

[22] *P. Ferguson*, *G. Huston*, What is a VPN?, 1998, s. 1–22, www.potaroo.net/papers/1998-3-vpn/vpn.pdf (dostęp 12.12.2022 r.).

[23] *S. Kotecka*, Kodeks dobrych praktyk w zakresie zarządzania informacją sądową i jej udostępniania, [w:] *J. Gołaczyński* (red.), Wybrane dobre praktyki w zakresie usług elektronicznych (Polska), Warszawa 2016, s. 461–468.

[24] *Ł. Dubiński*, RODO a postępowanie…, s. 3.

[25] T.j. Dz.U. z 2020 r., poz. 344 ze zm.; dalej jako: świadczeniu usług drogą elektroniczną.

niczną. Ustawa ta umożliwia m.in. elektroniczne załatwianie spraw, składanie wniosków, a także przesyłanie dokumentów do jednostek administracyjnych za pośrednictwem Internetu. Dokumenty przesyłane elektronicznie muszą spełnić wiele wymagań, zostały one wymienione w rozporządzeniu Prezesa Rady Ministrów z 14.9.2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[26] – m.in. należy do nich składanie dokumentu w formacie elektronicznym[27], np. takim jak PDF, DOC lub DOCX, opatrzenie dokumentu bezpiecznym podpisem elektronicznym weryfikowalnym za pomocą ważnego kwalifikowanego certyfikatu. Jak zostało określone w uchylonej już ustawie z 18.9.2001 r. o podpisie elektronicznym[28], podpis elektroniczny jest elektronicznym poświadczeniem potwierdzającym tożsamość osoby, która go posiada, oraz jej uprawnienia do podpisywania dokumentów elektronicznych w sposób wiarygodny i niepodważalny. Artykuł 131 ustawy z 5.9.2016 r. o usługach zaufania oraz identyfikacji elektronicznej[29] mówi za to, że bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z 18.9.2001 r. o podpisie elektronicznym jest kwalifikowanym podpisem elektronicznym w rozumieniu niniejszej ustawy, więc zapis ten jest dalej aktualny. Według art. 4 ust. 6 tej ustawy minister właściwy do spraw informatyzacji, po rozpatrzeniu wniosku, o którym mowa w ust. 1, wydaje decyzję o wpisie dostawcy usług zaufania i świadczonych przez niego usług zaufania do rejestru, jeżeli spełniają wymagania określone w przepisach o usługach zaufania, kwalifikowanej usługi zaufania do rejestru, w przypadku gdy usługa spełnia wymagania określone w przepisach o usługach zaufania. Podmiot świadczący usługi certyfikacyjne wydaje certyfikat na podstawie umowy. Artykuł 10 ust. 1 wspomnianej ustawy mówi za to, że Narodowe Centrum Certyfikacji tworzy i wydaje kwalifikowanym dostawcom usług zaufania certyfikaty służące do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, o których mowa w załączniku I lit. g, załączniku III lit. g i załączniku IV lit. h do rozporządzenia 910/2014, oraz certyfikatów służących do weryfikacji innych usług zaufania świadczonych przez kwalifikowanych dostawców, zwanych dalej „certyfikatami dostawcy usług zaufania". Wspomniany certyfikat jest niezbędny do składania podpisanego elektronicznie dokumentu do jednostek administracyjnych w celu poświadczenia dokumentu oraz identyfikacji osoby, która go składa. Ponadto dokument musi zostać dostarczony do urzędu za pomocą bezpiecznego kanału komunikacji, takiego jak np. ePUAP lub Platforma Usług Elektronicznych (PUE) czy inne systemy stosowane przez organy o znaczeniu ustrojowym oraz funkcjonalnym. Warto jednak pamiętać, że niektóre jednostki mogą mieć dodatkowe wymagania dotyczące składania dokumentów elektronicznych oraz przesyłu danych, więc należy za każdym razem sprawdzić regulaminy oraz inne wewnętrzne zakładowe źródła przed przesyłaniem wymaganych dokumentów oraz danych i zapoznać się z wytycznymi dotyczącymi danej sprawy. W przypadku przesyłu danych należy spełnić również przesłanki poprawności oraz kompletności danych, zgodności z obowiązującymi przepisami, przejrzystości, wymaganej formy, aktualności oraz biorąc pod uwagę aspekt bezpieczeństwa, niektóre dane muszą również zostać zabezpieczone przed nieuprawnionym dostępem np. przez szyfrowanie lub inne metody ochrony danych[30]. Oprócz wspomnianych działań należy również umożliwić ich weryfikację, tzn. jednostka administracyjna powinna mieć możliwość sprawdzenia ich poprawności oraz autentyczności.

Przetwarzanie danych przez wybrane jednostki administracji publicznej i systemy teleinformatyczne

W doktrynie przyjął się pogląd, że administratorem danych, który je przetwarza zgodnie z definicją zawartą w art. 4 pkt 7 RODO, „administrator" jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Zgodnie z tą definicją pojęcie administratora ma szeroki zakres znaczeniowy, gdyż może nim być w zasadzie każdy podmiot, jeśli ustala cele i sposoby przetwarzania danych osobowych. Biorąc ten fakt pod uwagę, należy stwierdzić, że w zależności od rodzaju danych osobowych, które są przetwarzane, czy kompetencji podmiotu przetwarzającego administratorem może być inny podmiot. Ponadto według RODO podmioty przetwarzające dane osobowe muszą mieć uzasadniony i konkretny cel przetwarzania danych oraz muszą one przetwarzać dane zgodnie z prawem i w sposób zgodny z celami, dla których zostały one zebrane. Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy przede wszystkim dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych. Ocena ta powinna być dokonywana w odniesieniu do konkretnego procesu przetwarzania. W związku z czym można byłoby wspomnieć o art. 18 ust. 1 ustawy z 8.3.1990 r. o samorządzie gminnym[31],

[26] Dz.U. poz. 1625.
[27] *A. Słysz*, Metody doręczania dokumentów elektronicznych, Powiatowa Stacja Sanitarno-Epidemiologiczna w Pile, www.gov.pl/web/psse-pila/metody-doreczania-dokumentow-elektronicznych (dostęp 20.12.2022 r.).
[28] Dz.U. Nr 130, poz. 1450 ze zm.
[29] T.j. Dz.U. z 2021 r. poz. 1797 ze zm.
[30] *A. Pyka*, Przetwarzanie Danych Osobowych do Celów Badań Naukowych. Aspekty Prawne, Studia Prawa Publicznego 2019, Nr 4 (28), Warszawa 2019, s. 98–104.
[31] T.j. Dz.U. z 2023 r. poz. 40 ze zm.; dalej jako: SamGminU.

w którym zawarte są przykłady zadań jednostki samorządu terytorialnego (w tym przypadku rady gminy), gdzie mogą być wykorzystywane dane poufne obarczone ryzykiem. Stanowi on m.in., że do właściwości rady gminy należą wszystkie sprawy pozostające w zakresie działania gminy, czyli między innymi uchwalanie studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy oraz miejscowych planów zagospodarowania przestrzennego, uchwalanie programów gospodarczych, przyjmowanie programów rozwoju w trybie określonym w przepisach o zasadach prowadzenia polityki rozwoju, ustalanie zakresu działania jednostek pomocniczych, zasad przekazywania im składników mienia do korzystania oraz zasad przekazywania środków budżetowych na realizację zadań przez te jednostki, o ile ustawy nie stanowią inaczej. Za to innym przykładem są określone w art. 30 SamGminU kompetencje wójta gminy, czyli m.in. przygotowywanie projektów uchwał rady gminy, opracowywanie programów rozwoju w trybie określonym w przepisach o zasadach prowadzenia polityki rozwoju, gospodarowanie mieniem komunalnym, wykonywanie budżetu, zatrudnianie i zwalnianie kierowników gminnych jednostek organizacyjnych. Podsumowując, jeżeli przepisy prawa wskazują, że określone zadania należą do właściwości gminy i dla ich wykonania niezbędne jest przetwarzanie określonych danych, to co do zasady administratorem jest wójt, burmistrz lub prezydent miasta. Przetwarzanie danych przez jednostki samorządu administracyjnego może być przeprowadzane również w ramach funkcjonowania ePUAP. Jest to system informatyczny, który umożliwia składanie dokumentów elektronicznych do urzędów za pośrednictwem Internetu[32]. Elektroniczna Platforma Usług Administracji Publicznej jest częścią PUE, która została wprowadzona w celu usprawnienia działania administracji publicznej i umożliwienia obywatelom kontaktów z urzędami drogą elektroniczną. Dzięki ePUAP możliwe jest m.in. załatwienie spraw, wnioskowanie o różnego rodzaju dokumenty czy też przesyłanie dokumentów do urzędów. System ePUAP jest dostępny na stronie internetowej www.epuap.gov.pl. Nie jest to jednak jedyna forma elektronicznego przesyłu danych do urzędu. Przykładowo istnieje możliwość, że dany urząd wymaga dodatkowego załącznika, określonej formy podpisania dokumentu lub też wysyłania dokumentów w inny sposób, np. przez specjalną aplikację dostępną na stronie internetowej danego urzędu. Stąd w każdym przypadku należy upewnić się, że dokument zostanie dostarczony do urzędu w sposób prawidłowy i zgodny z wymaganiami. W przypadku odpowiedzialności za wyciek danych bezpośrednio z ePUAP, w tym zakresie obowiązują przepisy zawarte w ustawie o ochronie danych osobowych. Zgodnie z tym aktem prawnym odpowiedzialność za wyciek danych z ePUAP ponosi administrator danych, czyli podmiot, który przetwarza dane osobowe. W przypadku ePUAP – zgodnie z ustawą z 17.2.2005 r. o informatyzacji podmiotów realizujących zadania publiczne[33] – administratorem danych jest Minister Cyfryzacji, odpowiedzialny za bezpieczeństwo przetwarzanych danych oraz za zapewnienie odpowiednich środków technicznych i organizacyjnych, które mają chronić te dane przed nieuprawnionym dostępem. Jeśli doszło do wycieku danych z ePUAP i naruszenia przepisów o ochronie danych osobowych, to minister właściwy do spraw informatyzacji, jako administrator danych użytkowników ePUAP oraz konta Mój Gov, ponosi odpowiedzialność za ten wyciek oraz odpowiada za zapewnienie funkcjonowania ePUAP i m.in. może zostać zobowiązany do usunięcia skutków naruszenia. Osoba, której dane dotyczą, może również dochodzić swoich praw na drodze sądowej, np. poprzez wniesienie pozwu o ochronę dóbr osobistych. W takim przypadku osoba poszkodowana ma również prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia tej osoby. Bazując na treści art. 60 OchrDanychU, postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych jest prowadzone przez Prezesa Urzędu (zgodnie z art. 7 OchrDanychU „Prezesem Urzędu" jest Prezes Urzędu Ochrony Danych Osobowych, o którym mowa w rozdziałach 4–7 i 11 ustawy). Ponadto według art. 34 OchrDanychU, Prezes Urzędu jest organem nadzorczym w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW[34]. Dodatkowo, według art. 5 ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[35] zadaniami Prezesa UODO jest m.in. monitorowanie i egzekwowanie stosowania przepisów niniejszej ustawy oraz wydanych na jej podstawie aktów wykonawczych, a także upowszechnianie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych w celu, o którym mowa w art. 1 pkt 1 tejże ustawy.

[32] *D. Fleszer*, Funkcjonowanie elektronicznej administracji na przykładzie ePUAP, Roczniki Administracji i Prawa 12, Wyższa Szkoła Humanitas 2012, s. 119–138.
[33] T.j. Dz.U. z 2023 r. poz. 57 ze zm.
[34] Dz.Urz. UE L Nr 119, s. 89.
[35] Dz.U. poz. 125 ze zm.

Bezpieczeństwo informacji poufnych przesyłanych elektronicznie do jednostek samorządu terytorialnego oraz elektronicznych systemów administracyjnych

Polskie prawo administracyjne reguluje kwestie dotyczące cyberbezpieczeństwa w kilku aktach prawnych, w tym m.in. w ustawie o świadczeniu usług drogą elektroniczną. Ustawa ta wprowadza m.in. w rozdziale 2 obowiązek zapewnienia bezpieczeństwa danych przetwarzanych drogą elektroniczną oraz umożliwia stosowanie środków zabezpieczających w celu ochrony przed nieuprawnionym dostępem do danych, które mogą zniwelować ryzyko wycieku danych. Jest to m.in. określone w art. 3b ŚwUsłDrogElekU ograniczenie swobody świadczenia usług drogą elektroniczną na zasadach określonych przez przepisy odrębne, jeżeli jest to niezbędne ze względu na ochronę zdrowia, obronność, bezpieczeństwo państwa lub bezpieczeństwo publiczne. Ponadto zawiera przepisy dotyczące zarządzania bezpieczeństwem informacji w administracji publicznej, których tematyka została również poruszona w rozporządzeniu Rady Ministrów z 12.4.2012 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[36]. Zawiera ono m.in. wymagania dotyczące tworzenia i wdrażania systemów zarządzania bezpieczeństwem informacji oraz zasady odpowiedzialności za naruszenie bezpieczeństwa informacji. Poruszono w nim m.in. takie wymagania jak to, że według § 20 podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Ważnym aspektem tego paragrafu jest również to, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie takich działań, jak m.in. zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy czy zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

Konsekwencje nieprawidłowości w funkcjonowaniu systemów informatycznych oraz konieczne działania

Wyciek danych z systemu informatycznego jednostki samorządowej może mieć poważne konsekwencje zarówno dla jednostki samorządowej, jak i dla osób, których dane uległy wyciekowi[37]. W przypadku jednostki samorządowej takie wydarzenie może prowadzić do strat finansowych związanych z usuwaniem skutków wycieku i zapobieganiem podobnym sytuacjom w przyszłości oraz utraty zaufania ze strony społeczności. Może on też skutkować odpowiedzialnością prawną, m.in. jeśli wyciek danych był spowodowany brakiem odpowiednich środków bezpieczeństwa lub nieodpowiednim zabezpieczeniem systemu. Dla osób, których dane uległy wypłynięciu, wyciek może prowadzić do utraty prywatności, a także do ryzyka kradzieży tożsamości lub innych oszustw. Może też prowadzić do szkód finansowych, np. jeśli dane zostały wykorzystane do nieuprawnionych transakcji. W celu zminimalizowania ryzyka wycieku danych oraz skutków takiego wycieku jednostki samorządowe powinny stosować odpowiednie środki bezpieczeństwa. Ważne jest też, aby jednostki samorządu informowały odpowiednio szybko o wycieku danych i podjęły odpowiednie działania, aby zapobiec dalszemu rozprzestrzenianiu się wycieku oraz zminimalizować jego skutki. Jeśli chodzi o orzeczenia i decyzje związane z tą problematyką, to należałoby wspomnieć o Decyzji Prezesa UODO z 18.10.2019 r. stwierdzającej naruszenie m.in. zasady przetwarzania zgodnie z prawem i zasady poufności oraz nakazującej dostosowanie operacji przetwarzania do przepisów o ochronie danych osobowych[38]. Prezes UODO określił w niej, że niezależnie od tego, czy Burmistrz lub inny administrator poinformował Prezesa Urzędu o skierowaniu wniosku z wątpliwościami do Ministra Cyfryzacji o interpretację przepisów ustawy z 6.9.2001 r. o dostępie do informacji publicznej[39] oraz wniósł o zawieszenie postępowania do czasu otrzymania ww. interpretacji. Minister Cyfryzacji, jako podmiot odpowiedzialny za stworzenie głównej strony Biuletynu Informacji Publicznej, nie jest podmiotem właściwym do interpretacji przepisów ustawy o dostępie do informacji publicznej, a wydawane przez niego wytyczne nie są prawnie wiążące. To w tym przypadku burmistrz jest administratorem, a zatem to na nim spoczywa obowiązek zapewnienia, aby przetwarzanie danych zamieszczonych w BIP

[36] Dz.U. poz. 526.
[37] *P. Jatkiewicz*, Ochrona danych osobowych, Polskie Towarzystwo Informatyczne, Warszawa 2015, s. 7–9.
[38] Decyzja PUODO z 18.10.2019 r., ZSPU.421.3.2019, Legalis.
[39] Dz.U. z 2022 r. poz. 902.

było zgodne z przepisami ogólnego rozporządzenia o ochronie danych, tym samym zgodne z zasadą ograniczenia przechowywania, określoną w art. 5 ust. lit. e RODO. Burmistrz powinien opracować i wdrożyć procedury, z których będą wynikały terminy usuwania z BIP informacji zawierających dane osobowe oraz zasady dokonywania przeglądów zawartości BIP w celu weryfikacji, czy określone w ten sposób terminy usuwania danych osobowych są przestrzegane (art. 24 RODO). W przypadku tej decyzji kara pieniężna dla administratora wyniosła 40 000 zł i spełnia w ustalonych okolicznościach niniejszej sprawy funkcje, o których mowa w art. 83 ust. 1 RODO. Kwota ta jest w tym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca, co było celem tej decyzji, ze względu na proporcjonalność do stwierdzonego naruszenia, wagę naruszenia, kategorie danych osobowych, których dotyczyło naruszenie, brak realizacji obowiązków administratora wynikających z ogólnego rozporządzenia o ochronie danych i czas trwania naruszenia. W przypadku orzeczeń ciekawym przykładem jest wyrok WSA w Warszawie z 7.8.2020 r.[40], w którym UODO powziął informację o nieprawidłowościach w procesie przetwarzania danych osobowych uczniów pewnej szkoły podstawowej, polegających na gromadzeniu odcisków palców dzieci korzystających z usług stołówki szkolnej. Wojewódzki Sąd Administracyjny zasądził od Prezesa UODO na rzecz skarżącej szkoły kwotę 400 zł tytułem zwrotu kosztów postępowania sądowego. Jednak wcześniej przetwarzanie przez skarżącą szkołę danych biometrycznych uczniów zostało uznane sporną decyzją Prezesa UODO za niezgodne z zasadą minimalizacji, o której mowa w art. 5 ust. 1 lit. c RODO. Zastosował on uprawnienia wynikające z przepisów art. 58 ust. 2 lit. f i lit. g RODO, nakazując skarżącej szkole usunięcie danych osobowych w zakresie przetworzonych do postaci cyfrowej informacji o charakterystycznych punktach linii papilarnych palców dzieci korzystających z usług stołówki szkolnej, a także w sposób nieuprawniony nakazując stronie skarżącej zaprzestanie zbierania wspomnianych danych biometrycznych uczniów. W tym przypadku również w sposób nieuzasadniony zastosował wobec skarżącej szkoły uprawnienie wynikające z przepisów art. 58 ust. 2 lit. i w zw.z art. 83 RODO, nakładając na stronę skarżącą karę pieniężną w wysokości 20 000 zł, co było nieprawidłowe pod kątem prawnym, ale jest ciekawym przykładem nałożenia kary na jednostkę systemu szkolnictwa. Oprócz wspomnianych konsekwencji prawnych skutkiem nieprawidłowości oraz wycieków danych jest również utrata zaufania społeczeństwa do organów administracji. Zdarzają się, sytuacje gdy podmiot przetwarzający dane osobowe uzyskuje informację o ich wycieku, jednak nie zawiadamia o tym organów ścigania ani osób, których dane wyciekły. Takie zaniechanie związane jest z obawą przed negatywnymi skutkami zawiadomienia dla swojej działalności. Postępując w ten sposób, można doprowadzić do kradzieży czyjegoś wizerunku i nieautoryzowanego wykorzystywania go na niekorzyść poszkodowanego, który jest nieświadomy zdarzenia. Tymczasem działania podjęte w porę, czyli zwiększona ostrożność użytkowników, ściganie czy stosowanie wskazówek dotyczących działań zapobiegających wyciekom i atakom hakerskim mogłoby pozytywnie wpłynąć, ograniczyć lub nawet zapobiec negatywnym skutkom takiego wycieku[41]. Wspomniane działania związane są z obowiązkiem notyfikacyjnym, który został określony w art. 174a–174d ustawy z 16.7.2004 r. – Prawo telekomunikacyjne[42]. Obowiązek ten nakazuje dostawcy publicznie dostępnych usług telekomunikacyjnych zawiadomienie GIODO o naruszeniu danych osobowych niezwłocznie, nie później jednak niż w terminie trzech dni od stwierdzenia naruszenia. Według art. 174a ust. 2 PrTel przez naruszenie danych osobowych rozumie się przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych. Obowiązek notyfikacji pojawił się również w art. 34 RODO. Ten przepis stanowi, że jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki powiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie powinno zostać sformułowane w jasny i prosty sposób oraz przedstawiać charakter naruszenia ochrony danych osobowych. Powinno również zawierać informacje i środki, takie jak wskazanie imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji. Ważnym elementem jest również opis możliwych konsekwencji naruszenia ochrony danych osobowych, ale również opis środków proponowanych i zastosowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki użyte w celu zminimalizowania ewentualnych negatywnych skutków[43]. Jeżeli wspomniany incydent wiąże się z wysokim ryzykiem naruszenia praw i wolności osób objętych naruszeniem, to zawiadomienie nie będzie konieczne jedynie w szczególnych, wyjątkowych sytuacjach, wskazanych w art. 34 ust. 3 RODO, czyli gdy administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak

[40] II SA/Wa 809/20, Legalis.

[41] *A. Lach*, Obowiązek notyfikacyjny, Karnoprawna reakcja na zjawisko kradzieży tożsamości, Warszawa 2015, www.sip.lex.pl/#/monograph/369361923 dostęp 20.12.2022 r.).

[42] T.j. Dz.U. z 2022 r. poz. 1648 ze zm.; dalej jako: PrTel.

[43] *A. Baranowska-Górecka*, Obowiązki prawne po ataku hakerskim, Pismo Samorządu Terytorialnego Wspólnota z 17.5.2021 r.

szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych, administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. Ponadto koniecznością będzie odnotowanie incydentu w wewnętrznym rejestrze naruszeń. Obowiązek taki wynika z art. 33 ust. 5 RODO. Stanowi on, że administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze, a dokumentacja musi pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania art. 33 RODO. Uwzględnione powinny zostać nie tylko naruszenia zgłoszone do Prezesa UODO, ale również wszystkie naruszenia z oceną ryzyka.

Naruszenie prawa i możliwe działania osoby poszkodowanej

W przypadku przetwarzania danych osobowych z naruszeniem przepisów o ochronie danych osobowych (np. w wyniku wycieku danych z ePUAP), to według art. 77 ust. 1 RODO, osoba której dane dotyczą, ma prawo do wniesienia skargi do Prezesa UODO. Skarga ta powinna zawierać informacje dotyczące naruszenia przepisów o ochronie danych osobowych oraz wskazywać na szkodę, jaką osoba ta poniosła w wyniku tego naruszenia. Prezes UODO w takim wypadku rozpatruje skargę i wydaje decyzję w sprawie, w której może zobowiązać administratora danych do usunięcia naruszenia oraz zastosowania odpowiednich środków zaradczych. W przypadku naruszenia przepisów o ochronie danych osobowych PUODO może również nałożyć na administratora danych karę finansową. Osoba, której dane dotyczą, może również dochodzić swoich praw na drodze sądowej, np. poprzez wniesienie pozwu o ochronę dóbr osobistych. Ochrona dóbr osobistych obejmuje m.in. prawo do ochrony danych osobowych, czyli prawo do decydowania o tym, czy i w jaki sposób dane osobowe są przetwarzane oraz prawo do wyrażenia zgody na ich przetwarzanie. Jeśli sąd uzna, że doszło do naruszenia prawa osoby, której dane dotyczą, do ochrony dóbr osobistych, to może nakazać administratorowi danych usunięcie skutków naruszenia oraz zasądzić na rzecz osoby poszkodowanej odpowiednią sumę pieniężną tytułem odszkodowania lub zadośćuczynienia. Jeśli chodzi o sumę pieniężną, jaka może zostać zasądzona na rzecz osoby poszkodowanej w wyniku naruszenia prawa do ochrony danych osobowych, to w tym zakresie nie ma konkretnych wytycznych. W każdym konkretnym przypadku sąd będzie oceniał indywidualnie, jaka kwota jest odpowiednia w danej sytuacji. Przykładowo w wyroku WSA w Warszawie z 7.8.2020 r. nałożono karę w wysokości 40 000 zł. Innym przykładem jest decyzja Prezesa UODO z 23.3.2022 r.[44] dotycząca pełnomocnika inicjatorów referendum gminnego w sprawie odwołania rady gminy przed upływem kadencji, za naruszenie polegające na braku współpracy z Prezesem UODO w ramach wykonywania przez niego jego zadań oraz na niezapewnieniu dostępu do danych osobowych i innych informacji niezbędnych Prezesowi UODO do realizacji jego zadań, stwierdzająca naruszenie przez pełnomocnika inicjatorów referendum gminnego przepisów art. 31 i art. 58 ust. 1 lit. e RODO, która nałożyła karę pieniężną w wysokości 2285 zł. Ciekawym przykładem, pokazującym wysokość kar pieniężnych, jest również decyzja Prezesa UODO z 24.8.2020 r.[45], która zapadła w związku z naruszeniem przez Głównego Geodetę Kraju art. 5 ust. 1 lit. a RODO i art. 6 ust. 1 RODO. W swoich decyzjach sąd oraz Prezes UODO biorą pod uwagę m.in. rodzaj i stopień naruszenia przepisów o ochronie danych osobowych, skalę szkody, jaką poniosła osoba poszkodowana, oraz inne okoliczności sprawy. Dlatego trudno precyzyjnie określić, jaka kwota będzie odpowiednia w konkretnym przypadku.

Podsumowanie

Prawo nowych technologii jest nową, dynamicznie rozwijającą się gałęzią prawa. Tworzy ona nie tylko nieznaną dotąd terminologię i reguły prawne, ale również wpływa bezpośrednio na sposób kształtowania regulacji prawnych we wszystkich obszarach polskiego prawa. Ze względu na nieustanny rozwój nowych technologii oraz systemów teleinformatycznych konieczne są rozwiązania prawne, które będą regulować ramy i zasady ich wykorzystywania nie tylko w sektorze publicznym, ale również prywatnym. Tworzenie różnorakich systemów teleinformatycznych oraz sposobów komunikowania się pomiędzy stronami za pomocą Internetu jest dużym ułatwieniem w funkcjonowaniu polskiej administracji publicznej, ale jednocześnie obarczone jest ono niebezpieczeństwem związanym z wypłynięciem danych poufnych oraz zagrożeniem cyberatakami. W niniejszej pracy poruszono tematykę utraty danych osobowych, ich konsekwencji oraz działań, które należy podjąć w wypadku takie zdarzenia. Przedstawiono również propozycje postępowań, które może zastosować osoba poszkodowana, oraz rzeczywiste wydarzenia, które zaszły w ostatnich latach. Ze względu na zwiększanie się ilości cyberataków oraz

[44] Decyzja PUODO z 23.3.2022 r., DKE.561.18.2021, LEX 3446491.
[45] Decyzja PUODO z 24.8.2020 r., DKN.5112.13.2020, LEX 3285237.

ciągły rozwój technologii i systemów teleinformatycznych, a także dzisiejsze problemy społeczeństwa informacyjnego konieczne jest nowe spojrzenie na zarządzanie zasobami informacyjnymi pozostającymi w dyspozycji podmiotów publicznych oraz postawienie większego nacisku na bezpieczeństwo przetwarzania danych.

Słowa kluczowe: wyciek danych, prawo administracyjne, prawo nowych technologii, system teleinformatyczny, administracja publiczna, ePUAP.

Data leakage from the ICT system on the example of activities of selected public administration bodies

The subject of the study are issues related to the aspects of data leakage from the ICT systems of selected public administration bodies. The author brings up the subject of data leakage from the ICT system, the frequency of such incidents, the circumstances of electronic contact of an entity with local government branches and the bilateral transfer of data and documents, including via the ePUAP system. She also presents the consequences, ways of proceeding in the event of data leakage and good practices that should be followed to prevent such an event.

Keywords: data leakage, administrative law, new technology law, ICT system, public administration, ePUAP.