PME
1/2023

Adres redakcji:
Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: pme@beck.pl

C.H.BECK

Wydawca:
Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600
www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Contents

C.H.BECK

Szanowni Państwo,

Zapraszam Państwa do lektury pierwszego numeru kwartalnika naukowego Prawo Mediów Elektronicznych z 2023 r. Tym razem publikujemy artykuł dotyczący wycieku danych z systemu teleinformatycznego na przykładzie działalności wybranych organów administracji publicznej – autorstwa *Agaty Jałowieckiej* oraz artykuł na temat zmian prawnopodatkowych w branży e-commerce, wraz z uwzględnieniem celów i dalszych perspektyw rozwoju regulacji – autorstwa *Klaudii Bajduk*. Kolejny artykuł odnosi się do sztucznej inteligencji, a w szczególności zawiera analizę *AI Act* na podstawie jej ugruntowania w przestrzeni komercyjnego użycia (autor *Kamil Palacz*). Dalej można się zapoznać z problematyką obowiązku tzw. strażników dostępu w świetle Aktu o rynkach cyfrowych z perspektywy ochrony danych osobowych (autor r.pr. *Krzysztof Wyderka*). Publikacja ta dotyczy problemu kontrolowania ważnych ekosystemów w gospodarce cyfrowej przez kilka dużych platform, które są określane mianem strażników dostępu (*gatekeepers*) oraz działań podjętych przez UE mających na celu ustanawianie nowych ram prawnych tworzących bezpieczniejszą przestrzeń cyfrową oraz sprawiedliwe warunki działania w celu wspierania innowacji, wzrostu gospodarczego i konkurencyjności. Numer zamyka glosa aprobująca do wyroku WSA z 30.11.2021 r. (I SA/Łd 699/21). Przedmiotem tego opracowania jest interpretacja Dyrektora Krajowej Informacji Skarbowej z 27.7.2021 r. Organ podatkowy dokonał wykładni art. 22 ust. 14 ustawy z 26.7.1991 r. o podatku dochodowym od osób fizycznych, zgodnie z którym uznał, że zakup energii elektrycznej niezbędnej do pracy koparki kryptowalut oraz zakup sprzętu komputerowego do budowy koparki kryptowalut nie powinny być kwalifikowane jako koszty uzyskania przychodów z tytułu odpłatnego zbycia waluty wirtualnej (autor *Gracjan Ciupa*).

Zapraszam do lektury
prof. dr hab. *Jacek Gołaczyński*
Redaktor naczelny

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.

Zmiany prawnopodatkowe w branży e-commerce – cele i perspektywy rozwoju regulacji

Klaudia Bajdiuk[1]

W opracowaniu podjęta została problematyka cybernetycznych zmian prawnopodatkowych w branży e-commerce, wraz z uwzględnieniem celów i dalszych perspektyw rozwoju regulacji. Poruszono tematykę dynamicznej ewolucji gałęzi handlu oraz konsekwencji za tym idących. Autorka szczegółowo omawia cztery przełomowe regulacje, które stanowią fundament do zmian prawnych w zakresie uszczelniania systemu podatkowego w ramach obecnej ery cyfrowej, uwzględniając także skutki zaimplementowania tych aktów prawnych do krajowego ustawodawstwa.

Uwagi wstępne

E-commerce, czyli handel elektroniczny, to gałąź gospodarki, która rozwija się w niezwykle szybkim tempie. Dynamiczny rozwój tej branży jest efektem nieustannej ewolucji elektronizacji wszelakich procesów, zarówno społecznych, dotyczących grup ludzi oraz jednostek, jak i gospodarczych. Istota korzystania z możliwości handlu internetowego wiąże się z potrzebami rynku, wygodą konsumentów oraz powszechnym dostępem do technologii teleinformatycznych, narzucając nowy model ekonomiczny i organizacyjny[2]. Popyt na zawieranie transakcji internetowych przejawia tendencję wzrostową – w 2020 r. 73% internautów dokonywało zakupów w e-sklepach, w 2021 r. zaś aż 78% użytkowników[3]. Liczne źródła wskazują również, że w 2023 r. do 22% światowego handlu odbywać się będzie za pomocą Internetu[4].

Autonomicznie, rozwój ten wywołuje skutki w sferze prawnej i tworzy wyzwania w formie prób uregulowania tych zmian przez ustawodawców na szczeblu krajowym i międzynarodowym. Działania podjęte przez normodawców w zakresie utworzenia ram prawnych dla tej gałęzi rozpoczęte zostały już na przełomie XX i XXI w. Wyłonił się wówczas pogląd, iż płaszczyzna Internetu stanowi odrębną rzeczywistość, której to należałoby nadać niezależny status prawny[5]. Za stosowne również należy uznać stanowisko reprezentowane przez Światową Organizację Własności Intelektualnej, zgodnie z którym konieczne jest przystosowanie regulacji prawnych do zmieniających się warunków gospodarczych[6].

Okazało się to jednak procesem trwającym do dziś, nie jest możliwe bowiem jednorazowe uregulowanie wszystkich aspektów technologicznych ze względu na nieustanne, pojawiające się nowe możliwości. Dlatego też na tym tle warto podkreślić problematykę przepisów podatkowych, ponieważ w ciągu ostatnich paru lat odnotować należy szeroką działalność organów unijnych i chęć dostosowywania aktów prawnych przez państwa europejskie w celu osiągnięcia ujednoliconego, konkurencyjnego rynku globalnego. Jest to również inicjatywa kreowania mechanizmów i schematów podatkowych, które uszczelnią system podatkowy, uniemożliwiając podatnikom podejmowanie prób unikania i uchylania się od opodatkowania. Kluczowym momentem, niejako wymuszającym dostosowanie przepisów podatkowych, była pandemia COVID-19, która nieodwracalnie zmieniła nawyki przedsiębiorców i konsumentów na całym świecie, uwydatniając tym samym luki prawne we wcześniej obowiązujących ustawach. W niniejszym artykule zostaną przedstawione zatem cztery, ocenione przez autorkę jako najistotniejsze, zmiany podatkowe obecnej dekady, tj. Dyrektywa DAC7, Pakiet VAT e-commerce, VAT w erze cyfrowej oraz raportowanie dotyczące dostawców usług płatniczych, wraz z przedstawieniem celów i perspektyw rozwoju tych regulacji w przyszłości oraz ze szczególnym uwzględnieniem pierwszych dwóch regulacji. Przyjęte w artykule metody badawcze obejmują analizę aktów prawnych, studium literatury, w tym opracowania rządowe oraz unijne i wnioskowanie logiczne.

Dyrektywa DAC7

Najważniejszą tegoroczną regulacją, która zmieniać będzie diametralnie rynek e-commerce, jest dyrektywa Rady UE 2021/514 z 22.3.2021 r. zmieniająca dyrektywę 2011/16/UE w sprawie współpracy administracyjnej w dziedzinie opo-

[1] Autorka jest studentką V roku Prawa na Uniwersytecie Wrocławskim oraz II roku Finansów i Rachunkowości na Uniwersytecie Ekonomicznym we Wrocławiu. Wiceprzewodnicząca koła naukowego BPK LegalNet oraz członkini koła naukowego Fiscus.

[2] *I. Kin-Dittmann*, Handel elektroniczny w Polsce, [w:] Dynamika działalności gospodarczej w warunkach globalizacji, Ekonomia 15, No 3018, Acta Universitatis Wratislaviensis, Uniwersytet Wrocławski, Wrocław 2007, s. 173.

[3] E-commerce w Polsce 2021, Gemius dla eCommerce Polska, Warszawa 2020, https://www.gemius.pl/wszystkie-artykuly-aktualnosci/raport-e--commerce-w-polsce-2021.html (dostęp 20.12.2022 r.).

[4] Opinia Polski dotycząca możliwego wpływu projektu dyrektywy COM (2020) 314 – DAC7 na Jednolity Rynek Cyfrowy, Ministerstwo Finansów, Warszawa 2020, s. 2, https://www.gov.pl/web/finanse/opinia-polski-ws--dac7 (dostęp 20.12.2022 r.).

[5] *M. Stec* (red.), Prawo umów handlowych, System Prawa Handlowego, t. 5c, wyd. 1, Warszawa 2020, s. 1069.

[6] *Ibidem*, s. 1070.

datkowania[7]. Skierowana jest ona do operatorów platform cyfrowych, których to definicja oraz dokładne, ujednolicone obowiązki zostaną opisane poniżej. Są to przepisy zmieniające brzmienie i zakres poprzedniej dyrektywy Rady UE 2011/16/UE z 15.2.2011 r. w sprawie współpracy administracyjnej w dziedzinie opodatkowania i uchylająca dyrektywę 77/799/EWG[8], której ocenę zakończono w 2019 r. Wpłynęło to na znaczne usprawnienia w elektronizacji procesów podatkowych oraz automatycznej wymiany informacji, jednakże wskazano na konieczność dalszej poprawy tych przepisów[9].

Warto na wstępie zauważyć, że niniejszy akt prawny realizować będzie przede wszystkim funkcję przejrzystości podatkowej w całej UE, za pomocą wykorzystywania narzędzi raportujących i sprawozdawczych[10]. Co za tym idzie, wpłynie to pozytywnie na uszczelnienie systemu podatkowego, zmniejszy statystyki prób unikania lub uchylania się od opodatkowania, zarówno w zakresie podatków dochodowych, jak i podatku VAT i ułatwi globalny przepływ informacji między organami podatkowymi[11]. W państwach członkowskich Unii odpowiednie organy często występują do operatorów platform cyfrowych o udzielenie im informacji oraz przekazanie danych dotyczących konkretnych transakcji i sprzedawców, zatem również wpłynie to na zmniejszenie kosztów takich działań i przyspieszenie czynności wyjaśniających czy też procesowych, co zmniejszy obciążenia administracyjne[12].

Polska również przyczyniła się do powstania niniejszej dyrektywy oraz jej postulatów, angażując się w prace jej kreowania, co zakończyło się kompromisowym rozwiązaniem w formie obecnej regulacji unijnej[13]. Należy podkreślić zatem, że brzmienie polskiej ustawy odpowiada regulacjom wyszczególnionym w dyrektywie, co potwierdzają udostępnione założenia kierowane do posiadaczy platform cyfrowych, jak również zaprezentowany projekt ustawy[14]. Polska oraz inne kraje członkowskie otrzymały wyznaczony czas na implementację tych przepisów do 31.12.2022 r., a pierwsze raportowanie odbyć się ma do 31.1.2024 r., lecz wskazuje się na opóźnienia w tym zakresie oraz na potencjalne komplikacje w przeprowadzeniu pierwszego raportowania, ponieważ do 31.12.2022 r. nie pojawił się oficjalny tekst polskiej ustawy, mimo zakładanej konieczności wcześniejszego przygotowania rozwiązań legislacyjnych i przystosowania środowiska e-commerce do omawianych zmian[15]. W lipcu 2022 r. przeprowadzono prekonsultacje społeczne oraz zapowiedziano, że cały proces legislacyjny zostanie zakończony do grudnia 2022 r., w październiku zaś, w wykazie prac projektowych, pojawiła się informacja o trwających pracach nad tą ustawą[16]. Dopiero 8.2.2023 r. na stronie Rządowego Centrum Legislacji został opublikowany projekt ustawy implementujący założenia dyrektywy do polskiego systemu prawnego[17].

Na postawie opinii Polski w zakresie wprowadzenia tych przepisów można dostrzec sceptycyzm i dystans organów rządowych do przedstawionych postulatów, związany z ich potencjalnymi konsekwencjami, co mogło wpłynąć na wstrzymanie się z ich ogłoszeniem. Wskazano w opinii m.in. na naruszenie prywatności mniejszych przedsiębiorców, wysokie obciążenia finansowe dla istniejących biznesów, zmniejszenie konkurencyjności rynkowej, ryzyko pojawienia się luk prawnych, wywołanie niepewności podatników poprzez zwiększenie nierówności w sprzedaży online i offline oraz spowolnienie transformacji cyfrowej Unii Europejskiej[18]. W realizacji określonych celów konieczne jest zatem podejście proporcjonalne, przy poborze minimalnej ilości danych od platform cyfrowych oraz bez zakłócenia działania rynku e-commerce, co otworzy możliwości osiągania dochodów poprzez Internet.

Zgodnie z informacjami, przedstawionymi w polskiej ustawie implementującej, fundamentem oraz istotą zmian jest realizacja systemu wymiany danych oraz współpracy administracyjnej poprzez oparcie się na trzech podstawowych założeniach:

1) nałożenie na operatorów platform cyfrowych obowiązku sprawozdawczego dotyczącego sprzedawców działających za pośrednictwem tych platform;
2) zbudowanie mechanizmu wymiany informacji o sprzedawcach pomiędzy państwami członkowskimi;

[7] Dz.Urz. UE L Nr 104, s. 1; dalej jako: dyrektywa DAC7.

[8] Dz.Urz. UE L Nr 64, s. 1.

[9] Projekt ustawy o podatkowych obowiązkach sprawozdawczych operatorów platform cyfrowych nr UC136, Wykaz prac legislacyjnych i programowych Rady Ministrów, Kancelaria Prezesa Rady Ministrów, https://www.gov.pl/web/premier/projekt-ustawy-o-podatkowych-obowiazkach-sprawozdawczych-operatorow-platform-cyfrowych (dostęp 22.12.2022 r.).

[10] Pkt 1 dyrektywy DAC7.

[11] Informacja dla Sejmu i Senatu RP o udziale Rzeczypospolitej Polskiej w pracach Unii Europejskiej w okresie styczeń – czerwiec 2021 r., Kancelaria Prezesa Rady Ministrów, Druk Nr 461, Warszawa 2021, s. 18.

[12] Pkt 7 dyrektywy DAC7.

[13] Informacja dla Sejmu i Senatu RP o udziale Rzeczypospolitej Polskiej w pracach Unii Europejskiej w okresie styczeń – czerwiec 2021 r., Kancelaria Prezesa Rady Ministrów, Druk Nr 461, Warszawa 2021, s. 18.

[14] Założenia kierowane do posiadaczy platform cyfrowych – Prekonsultacje społeczne, Ministerstwo Finansów, Warszawa 2022, https://www.gov.pl/web/finanse/prekonsultacje-zalozen-kierowanych-do-posiadaczy-platform-cyfrowych-rozpoczete (dostęp 22.12.2022 r.).

[15] *M. Szulc*, *A. Pokojska*, Dyrektywa DAC-7: Obowiązki internetowych platform z legislacyjnym falstartem, Gazeta Prawna, Podatki i Księgowość, Warszawa 2022, https://podatki.gazetaprawna.pl/artykuly/8613820,dyrektywa-dac-7-platformy-internetowe-obowiazki.html (dostęp 22.12.2022 r.).

[16] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne dla branży e-commerce: Pakiet VAT e-commerce, DAC-7, Dyrektywa Omnibus, Deloitte Polska, Warszawa 2022, s. 13, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Prezentacje-webinary/Webinar_Deloitte_DAC7_e-commerce_3_11_2022.pdf (dostęp 22.12.2022 r.).

[17] Rządowe Centrum Legislacji, https://legislacja.rcl.gov.pl/projekt/12369201/katalog/12949551#12949551 (dostęp 4.5.2023 r.).

[18] Opinia Polski dotycząca możliwego wpływu projektu dyrektywy COM (2020) 314 – DAC7 na Jednolity Rynek Cyfrowy, Ministerstwo Finansów, Warszawa 2020, s. 1–4, https://www.gov.pl/web/finanse/opinia-polski-ws-dac7 (dostęp 22.12.2022 r.).

3) poprawa obecnych mechanizmów współpracy między administracjami, np. poprzez wprowadzenie możliwości przeprowadzania wspólnych kontroli[19].

W celu zrozumienia szczegółowych założeń dyrektywy należy najpierw wyjść od definicji określonych w niej platform cyfrowych oraz operatorów tych platform. Na wstępie termin „platform cyfrowych", w rozumieniu dyrektywy, posiada, określoną w regulacji, własną definicję legalną. Platforma bowiem „oznacza każde oprogramowanie, w tym stronę internetową lub jej część, oraz wszelkie aplikacje, w tym aplikacje mobilne, które są dostępne dla użytkowników i które umożliwiają sprzedawcom łączność z innymi użytkownikami w celu wykonywania stosownej czynności, bezpośrednio lub pośrednio, na rzecz takich użytkowników"[20]. Jest to szeroka definicja, dlatego unijny ustawodawca zdecydował się na jej zawężenie poprzez określenie przesłanek negatywnych, co takiej platformy nie obejmuje. Nie dotyczyć to będzie oprogramowania, które umożliwia wyłącznie wykonanie jednej z następujących działań: przetwarzanie płatności w odniesieniu do stosownej czynności, wystawianie przez użytkowników ofert lub reklamowanie przez nich stosownej czynności, przekierowywanie lub przenoszenie użytkowników na platformę[21].

Jeżeli zaś chodzi o operatorów tych platform, są to podmioty zobowiązane do raportowania, które to ułatwiają sprzedawcom dokonanie specyficznie określonych czynności na platformach lokalnych, czyli wszystkich działających na terenie Unii Europejskiej oraz co do sprzedawców będących rezydentami podatkowymi jednego z państw unijnych. Treść dyrektywy wskazuje, że operatorzy platform to jednostki udostępniające sprzedawcom całą platformę lub jej część[22]. Warto tutaj wyszczególnić pojęcie „wyłączonego operatora platformy", czyli takiego, który wykazuje co roku właściwemu organowi, że jego model biznesowy jest taki, że nie obejmuje on sprzedawców podlegających raportowaniu[23].

Należy też podkreślić, że obowiązki podlegające raportowaniu dotyczą konkretnej grupy sprzedawców. Dyrektywa określa sprzedawcę jako „użytkownika platformy będącego albo osobę fizyczną, albo podmiot, który to użytkownik w każdym momencie okresu sprawozdawczego jest zarejestrowany na platformie i wykonuje stosowną czynność". Stosowne czynności sprzedawców, objęte raportowaniem, dotyczą 4 kategorii szczególnych działań, do których normodawca zaliczył usługi świadczone osobiście, sprzedaż towarów, najem środków transportu oraz najem nieruchomości lub miejsc parkingowych[24]. Adekwatnie do terminu „wyłączonego operatora platformy" został wyszczególniony również katalog sprzedawców wyłączonych, do których zalicza się:

– sprzedawców, którzy dokonali mniej niż 30 transakcji sprzedaży towarów za pośrednictwem platformy i których wynagrodzenie nie przekroczyło 2000 euro w danym okresie sprawozdawczym;
– podmioty rządowe;
– podmioty notowane na giełdzie;
– sprzedawców w sektorze wynajmu nieruchomości, jeżeli dokonali ponad 2000 transakcji najmu nieruchomości w danym okresie sprawozdawczym[25].

Podstawowym celem raportowania jest identyfikacja sprzedawców, wraz z przestrzeganiem procedur należytej staranności. Operatorzy platform są zobowiązani do podjęcia kroków w celu zebrania, weryfikacji oraz przekazania danych o sprzedawcach, którzy podejmują czynności na ich platformach, a przekazanie takie dotyczyć będzie zarówno organu podatkowego (w Polsce przyjęto, że będzie to Szef KAS), jak i samej raportowanej jednostki[26]. Zarówno w tekście dyrektywy, jak i w założeniach polskiej ustawy, przedstawione zostały wytyczne, jakie informacje dokładnie będą zbierane, w rozróżnieniu, czy raportowanie dotyczy osoby fizycznej, czy podmiotu gospodarczego. Należy mieć na uwadze, że operator platformy jest administratorem w rozumieniu przepisów rozporządzenia Parlamentu Europejskiego i Rady UE Nr 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[27], zatem musi on dopełniać obowiązki w zakresie ochrony danych. Raportujący operator jest też zobowiązany do prowadzenia i przechowywania dokumentacji, która potwierdzi, że przy wszelkich podjętych krokach spełnione zostały procedury należytej staranności, przez okres od 5 do 10 lat (w Polsce planowane jest przyjęcie najniższego wymiaru, czyli 5 lat)[28]. Postulaty zakładają tak-

[19] Projekt ustawy o podatkowych obowiązkach sprawozdawczych operatorów platform cyfrowych nr UC136, Wykaz prac legislacyjnych i programowych Rady Ministrów, Kancelaria Prezesa Rady Ministrów, https://www.gov.pl/web/premier/projekt-ustawy-o-podatkowych-obowiazkach-sprawozdawczych-operatorow-platform-cyfrowych (dostęp 22.12.2022 r.).

[20] Załącznik Nr V Sekcja I lit. A ust. 1 dyrektywy DAC7.

[21] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 16.

[22] Załącznik Nr V Sekcja I lit. A ust. 2 dyrektywy DAC7.

[23] Założenia kierowane do posiadaczy platform cyfrowych – Prekonsultacje społeczne, Ministerstwo Finansów, Warszawa 2022, s. 5, https://www.gov.pl/web/finanse/prekonsultacje-zalozen-kierowanych-do-posiadaczy-platform-cyfrowych-rozpoczete (dostęp 22.12.2022 r.).

[24] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 16.

[25] *M. Lachowicz*, *J. Węgrzyn*, Obowiązki sprawozdawcze operatorów platform cyfrowych w Unii Europejskiej – Prekonsultacje założeń, Ministerstwo Finansów, Warszawa 2022, s. 8, https://www.gov.pl/web/kas/obowiazki-sprawozdawcze-operatorow-platform-cyfrowych-w-unii-europejskiej (dostęp 23.12.2022 r.).

[26] *Ibidem*, s. 9.

[27] Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej 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 (Dz.Urz. UE L Nr 119, s. 1).

[28] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 17.

że wymóg dokonania rejestracji przez operatora platformy w jednym z państw członkowskich, co wiąże się z konsekwencją przydzielenia platformie jej indywidualnego numeru[29].

W dyrektywie DAC7 zostały uwzględnione sankcje karne za nieprzestrzeganie obowiązku raportowania oraz wytycznych przez operatorów platform. Zgodnie z postulatem unijnym „Wybór sankcji pozostaje wprawdzie w gestii państw członkowskich, lecz przewidziane sankcje powinny być skuteczne, proporcjonalne i odstraszające"[30]. Polskie przepisy zakładać będą wysokość kary pieniężnej między 100 000 a 5 000 000 zł oraz, jako drugą sankcję, wykreślenie operatora platformy z rejestru jako podatnika VAT, zatem będą to poważne konsekwencje[31].

Dyrektywa DAC7 stanowi nowy MDR, czyli kolejne raportowanie schematów podatkowych. Analizując poprzednie regulacje w tym zakresie, można stwierdzić, iż w najbliższych latach przepisy te zatem ulegać będą kolejnym modyfikacjom i rozszerzeniom, by dopasowywać je do intensywnych zmian w zakresie elektronizacji procesów podatkowych oraz rozwijającej się branży e-commerce.

Pakiet VAT e-commerce

Kolejną istotną regulacją, która obowiązuje od 2021 r. zarówno na szczeblu unijnym, w formie wydanej dyrektywy Rady UE 2017/2455 z 5.12.2017 r. zmieniającej dyrektywę 2006/112/WE i dyrektywę 2009/132/WE w odniesieniu do niektórych obowiązków wynikających z podatku od wartości dodanej w przypadku świadczenia usług i sprzedaży towarów na odległość[32], jak i w polskim systemie prawnym, jest pakiet VAT e-commerce. Podstawowym celem wydanej nowelizacji jest eliminacja luk prawnych, które stanowiły dotychczas bariery rozwojowe przedsiębiorstw z zakresu B2C, czyli między przedsiębiorcami a konsumentami, ze szczególnym uwzględnieniem tych działających za pośrednictwem Internetu i specjalizujących się w e-handlu dóbr konsumenckich[33]. Potrzeba wynikała również z konieczności uszczelnienia importu małych przesyłek, zmniejszenia obciążeń i kosztów związanych z obowiązkami zapłaty VAT oraz zwiększenia efektywności poboru podatku. Zmiany te są jednymi z pierwszych prób realnego ujednolicenia systemów podatkowych państw UE w zakresie cybernetycznego rynku. Fundamentalnym działaniem w tym zakresie było wpierw ustanowienie, iż usługi telekomunikacyjne, nadawcze oraz elektroniczne[34] opodatkowane będą w docelowym państwie przeznaczenia.

Z dniem 1.7.2021 r., za pomocą ustawy nowelizującej[35], uchylone zostały pojęcia sprzedaży wysyłkowej z terytorium kraju oraz sprzedaży wysyłkowej na terytorium kraju, jak też i regulacje odnoszące się do tej sprzedaży, a w to miejsce wprowadzono definicję wewnątrzwspólnotowej sprzedaży towarów na odległość w zakresie państw unijnych[36] oraz tym samym odpowiednie zmiany w przepisach związane z tym rodzajem sprzedaży[37]. Związane to było z realizacją tzw. reguły terytorialności[38], zgodnie z którą VAT powinien być ponoszony w kraju ostatecznej konsumpcji świadczenia.

Wprowadzono także, na poziomie Unii Europejskiej, rozszerzony system MOSS, tj. nową procedurę szczególną VAT-OSS (unijna oraz nieunijna) dla usług oraz towarów[39]. Jest to mechanizm, który upraszcza rozliczanie podatku VAT należnego za usługi TNE w różnych krajach UE, w jednym wybranym kraju, co służy lepszej organizacji podatkowej i standaryzuje ten proces. Dokonuje się tego za pomocą elektronicznej deklaracji w kraju siedziby w terminie do końca miesiąca następującego po każdym kolejnym kwartale rozliczeniowym. Nowa procedura jest poszerzona o WSTO i niektóre usługi B2C, dzięki czemu przy takiej sprzedaży podatnicy nie są zobowiązani do rejestracji z tytułu podatku VAT w każdym kraju nabywcy, nawet jeżeli przekroczyli oni limit sprzedaży zagranicznej[40]. Zgłoszenie takie ma charakter fakultatywny, jednakże przy wyborze takiego sposobu rozliczeń stosowana jest zasada „wszystko albo nic", wobec czego podatnik musi płacić podatek w ramach VAT-OSS albo dla wszystkich transakcji, albo dla żadnej z nich[41]. Limit wysokości obrotów został ujednolicony zaś do kwoty 10 tysięcy euro[42].

Problematyczną kwestią było również nabywanie towarów przez obywateli państwa Wspólnot od sprzedawców spoza tego terytorium, ze względu na pobór podatku VAT, zatem, w zakresie dostaw towarowych spoza Unii Europejskiej,

[29] *Ibidem*, s. 18.
[30] Pkt 21 dyrektywy DAC7.
[31] Założenia kierowane do posiadaczy platform cyfrowych – Prekonsultacje społeczne, Ministerstwo Finansów, Warszawa 2022, s. 19, https://www.gov.pl/web/finanse/prekonsultacje-zalozen-kierowanych-do-posiadaczy-platform-cyfrowych-rozpoczete (dostęp 23.12.2022 r.).
[32] Dz.Urz. UE L Nr 348, s. 7.
[33] *M. Suwalska*, Wpływ implementacji rozwiązań unijnego pakietu VAT na sektor e-commerce, [w:] *M. Biernacki*, *R. Kowalak* (red.), Rachunkowość, Debiuty Studenckie, Uniwersytet Ekonomiczny we Wrocławiu, Wrocław 2021, s. 61.
[34] Dalej jako: TNE.
[35] Ustawa z 20.5.2021 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw (Dz.U. poz. 1163).
[36] Dalej jako: WSTO.
[37] Objaśnienia podatkowe z 1.9.2021 r. w zakresie tzw. pakietu VAT e-commerce wprowadzonego ustawą z 20.5.2021 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw (Dz.U. poz. 1163).
[38] Art. 5 ust. 1 ustawy o VAT, [za:] wyrokiem WSA w Warszawie z 7.7.2017 r., III SA/Wa 2047/16, Legalis.
[39] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 17.
[40] *T. Michalik*, Pakiet VAT e-commerce – Zmiany w 2021 roku, MDDP, Warszawa 2021, s. 8, https://www.mddp.pl/wp-content/uploads/2021/08/Pakiet-VAT-e-commerce_Zmiany-w-2021-roku.pdf (dostęp 4.1.2023 r.).
[41] *Ibidem*.
[42] Dyrektywa Rady (UE) 2019/1995 z 21.11.2019 r. zmieniająca dyrektywę 2006/112/WE w odniesieniu do przepisów dotyczących sprzedaży towarów na odległość oraz niektórych krajowych dostaw towarów, Dz.Urz. UE L Nr 244, s. 3.

podjęto unifikujące działania[43]. Warto podkreślić, że rosnąca skala handlu elektronicznego wpłynęła na wzrost wolumenu przesyłek deklarowanych jako nisko cenne, generując istotne straty budżetowe z tytułu unikania płacenia należności, co istotnie skutkowało naruszaniem zasad wolnego, unijnego rynku[44]. Została zatem wprowadzona nowa kategoria transakcji, którą określono jako sprzedaż na odległość towarów importowanych (SOTI) oraz ustanowiono nową procedurę rozliczania tych towarów[45]. Zniesiono zwolnienie z VAT importowego przesyłek do kwoty 22 euro, wprowadzając nowy limit wartości rzeczywistej przesyłki do kwoty 150 euro, lecz nie oznacza on wyłącznie zwolnienia, lecz również uproszczenia w poborze oraz rozliczaniu VAT od tych przesyłek, w ramach specjalnego systemu IOSS (procedura importu), który działa analogicznie do mechanizmu VAT-OSS[46].

Regulacje te, poza określeniem miejsca opodatkowania transakcji, wprowadzają również domniemanie związane z identyfikacją podmiotu odpowiedzialnego za jej rozliczenie[47]. Zasadą jest to, że ciężar podatku spoczywa na oferującym towary sprzedawcy, jednakże w określonych sytuacjach przejdzie on na pośredników partycypujących w łańcuchu dostaw. W szczególnym przypadku sprzedaży towarów importowanych o wartości nieprzekraczającej kwoty 150 euro rozliczenia dokonuje podmiot określany w przepisach jako „interfejs elektroniczny", ponieważ zostanie wprowadzona fikcja dla celów VAT, zgodnie z którą pełniąca funkcję łącznika platforma staje się automatycznie stroną transakcji[48]. Wątpliwości może budzić pojęcie interfejsu elektronicznego, ale przyjęto tutaj szeroką interpretację, że jest to „każdy rodzaj systemu kontaktującego się z konsumentem"[49]. Wcześniejsza, bezpośrednia transakcja, ulegnie zatem podziałowi na wstępną dostawę pomiędzy dostawcą a interfejsem elektronicznym, odbywającą się na zasadach B2B[50]. Platformy zostały, w konkretnych przypadkach, włączone do łańcucha dostaw, przy przyjęciu koncepcji, jakoby one same nabywały i dostarczały dane towary.

Możliwa jest wstępna ocena zmian, które nastąpiły po zaimplementowaniu przepisów dyrektywy w systemach prawnych państw unijnych. Przez pierwsze pół roku obowiązywania, w okresie od lipca do grudnia 2021 r., kwota VAT pobrana w systemie VAT-OSS wyniosła ok. 6,8 mld euro, a za pośrednictwem VAT-IOSS prawie 2 mld euro[51]. Jeżeli chodzi o Polskę, w ramach procedury IOSS wpływy wynosiły w tym samym okresie ok. 92,34 mln zł, a w pierwszym kwartale 2022 r. – 75 mln zł[52]. Na poziomie UE zmiany te zostały sklasyfikowane jako pozytywne biznesowo, ponieważ jest to procedura upraszczająca, a atrakcyjność tego systemu jest potwierdzona przez liczbę rejestracji, w szczególności do VAT-OSS, który jest bardziej pożądany przez podmioty, mimo początkowej konieczności poniesienia kosztów zmiany schematów wewnętrznych firm. Podatnicy przedstawili swoje obawy związane z systemem IOSS, ze względu na potencjalne wyłudzenia numeru IOSS, ryzyko podwójnego opodatkowania oraz brak powiązań celnych i podatkowych[53].

Zostały także zidentyfikowane trudności związane z procedurą zaimplementowanych przepisów na szczeblu krajowym. Zanotowano takie problemy, jak: niejasności co do oceny wartości rzeczywistej przesyłki przez organy celne, co wiąże się z możliwościami popełniania oszustw, rozbieżności przy prawidłowej klasyfikacji taryfowej i prawidłowe zgłaszanie towarów objętych zakazami lub ograniczeniami, brak wymaganych danych do zastosowania odpowiedniego rodzaju zgłoszenia celnego[54]. Jednakże, zgodnie z opinią, stwierdzono, że:

„Krajowa Administracja Skarbowa przygotowała i wdrożyła dla podatników system umożliwiający rozliczenie podatku VAT w ramach procedury szczególnej IOSS. Procesy związane z rejestracją do procedury, obsługą deklaracji VAT oraz dokonywaniem płatności należnego podatku VAT są prawidłowo realizowane przez jednostkę KAS wskazaną w ustawie. Ponadto, po stronie jednostki KAS, która właściwa jest do poboru dla Polski należnego podatku VAT z tytułu procedury IOSS, nie odnotowano problemów z realizacją zadań określonych w ustawie"[55].

W związku ze wskazanymi problemami należy zauważyć, że regulacja ta nie wyczerpała tematu dostosowywania przepisów do dynamicznych zmian cybernetycznych, szczególnie w zakresie podatku VAT. Konieczne jest uwzględnienie w tym zakresie nowszych regulacji rozszerzających pierwotne założenia pakietu e-commerce, które obecnie ulegają dynamicznemu rozwojowi, m.in. pakiet SLIM VAT 3. Przepisy te zakładają w szczególności: podwyższenie limitu sprzeda-

[43] VAT and electronic commerce: The new rules as a means for simplification, combatting fraud and creating a more level playing field? – *M. Papis-Almansa*, ERA Forum, 20(2) DOI: 10.1007/s12027-019-00575-9, Berlin 2019, s. 202.

[44] *M. Suwalska*, Wpływ implementacji…, s. 63.

[45] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 30.

[46] *M. Suwalska*, Wpływ implementacji..., s. 63.

[47] *Ibidem*, s. 64.

[48] Rozporządzenie wykonawcze Rady (UE) 2019/2026 z 21.11.2019 r. zmieniające rozporządzenie wykonawcze (UE) Nr 282/2011 w odniesieniu do dostaw towarów lub świadczenia usług ułatwianych poprzez użycie interfejsów elektronicznych oraz w odniesieniu do procedur szczególnych dla podatników, którzy świadczą usługi na rzecz osób niebędących podatnikami, prowadzą sprzedaż towarów na odległość i dokonują niektórych krajowych dostaw towarów, Dz.Urz. UE L Nr 313, s. 14.

[49] *M. Suwalska*, Wpływ implementacji..., s. 65.

[50] *Ibidem*, s. 64.

[51] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 31.

[52] *E. Witek*, Zapytanie nr 5136 w sprawie pakietu VAT e-Commerce, Marszalek Sejmu Rzeczpospolitej Polskiej, Kancelaria Ministra Finansów, Warszawa 2022, s. 1.

[53] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 35.

[54] *Ibidem*.

[55] *E. Witek*, Zapytanie Nr 5136 w sprawie pakietu VAT e-Commerce, Marszalek Sejmu Rzeczpospolitej Polskiej, Kancelaria Ministra Finansów, Warszawa 2022, s. 1.

ży małego podatnika do 2 mln euro, rezygnacja z wymogu posiadania faktury dot. wewnątrzwspólnotowego nabycia towarów (WNT) przy odliczaniu podatku naliczonego z tego tytułu, doprecyzowanie zasad stosowania kursu przeliczeniowego dla faktur korygujących oraz wprowadzenie uproszczeń w zakresie raportowania rozliczeń przy fakturowaniu[56]. Analogicznie, w następnych latach nieuniknione jest również wprowadzenie kolejnych przełomowych aktów prawnych na gruncie unijnym, a jedna z nich zostanie opisana poniżej.

VAT w erze cyfrowej (*VAT in the Digital Age*)

Kolejną rewolucyjną regulacją w zakresie podatku VAT jest pakiet VAT w erze cyfrowej. W dniu 8.12.2022 r. Komisja Europejska zaproponowała szereg środków mających na celu zmodernizowanie przepisów i sprawienie, by unijny system podatku od wartości dodanej działał lepiej dla przedsiębiorców oraz by był bardziej odporny na nadużycia poprzez przyjęcie i promowanie cyfryzacji czy procesów elektronicznych[57]. Warto zaznaczyć, że luka VAT za 2020 r. w całej UE jest szacowana na 93 mld euro, a wpływy z tego podatku stanowią około 7% krajowego PKB, dlatego zapobieganie zjawisku uchylania się od opodatkowania jest jednym z priorytetowych działań unijnych, przede wszystkim w cybernetycznym zakresie[58]. Zmiany te są na tyle szerokie, że ich implementacja odbywać się będzie sukcesywnie w latach 2024–2028, ponieważ okazuje się, że obecne przepisy podatkowe nie są wciąż dostosowane do możliwości prowadzenia działalności gospodarczej w erze cyfrowej, zatem służyć to ma również sferze biznesowej, przynosząc przedsiębiorstwom wymierne korzyści oraz kształtując konkurencyjny rynek, co potwierdzają opinie wielu interesariuszy[59]. Przedstawiono potrzeby dotyczące nowych schematów raportowania VAT, zmiany w gospodarce platformowej, pozytywnie odebrano także pomysł rozszerzenia mechanizmu VAT OSS/IOSS, co wiąże się z wprowadzonym pakietem VAT e-commerce, oraz wyrażono chęć posiadania narzędzi do e-fakturowania[60]. Ostatnia zmiana będzie tworzyć wyzwania w polskim ustawodawstwie, ponieważ konieczne będzie ujednolicenie tych wymogów z rodzimymi uregulowaniami w tym zakresie, ze względu na wprowadzenie obowiązku fakturowania elektronicznego, tzw. systemu KSeF od 2024 r.[61].

Zauważono, iż rozbieżność między 30-letnimi przepisami VAT a obecną cyfrową rzeczywistością stwarza dwuaspektowy problem:

1) nieoptymalny pobór i kontrola podatku VAT – unijne ramy prawne dotyczące VAT nie są w pełni dostosowane do nowej rzeczywistości cyfrowej i są podatne na oszustwa;
2) nadmierne obciążenia i koszty przestrzegania przepisów – gospodarka cyfrowa i nowe modele biznesowe stwarzają nowe wyzwania i koszty dla administracji podatkowych i przedsiębiorstw[62].

W ramach udoskonalonego podejścia oczekuje się od 135 mld euro do 177 mld euro dodatkowych dochodów z VAT (tj. 0,1% PKB średniorocznie w latach 2024–2032), co wiąże się jednak z kosztami wdrożenia w wysokości od 2,2 mld euro do 3,4 mld euro[63].

Pierwszym obszarem innowacji jest rozszerzenie obowiązującego już systemu rozliczania VAT i jego dalsze upraszczanie w ramach koncepcji pojedynczej rejestracji VAT[64]. Na potrzeby stosowania unijnej procedury OSS proponowane jest rozszerzenie pojęcia państwa członkowskiego konsumpcji, tak aby po zmianach obejmowało swoim zakresem inne dostawy towarów B2C:

– dostawy towarów wraz z instalacją lub montażem;
– dostawy towarów na pokładzie statków, samolotów lub pociągów;
– dostawy gazu, energii elektrycznej, ogrzewania i chłodzenia;
– dostawy krajowe[65].

Zgodnie z planowanymi nowelizacjami także dostawy towarów używanych, dzieł sztuki, przedmiotów kolekcjonerskich i antyków będą opodatkowane w miejscu przeznaczenia, co pozwoli stosować do nich system uproszczeń OSS. Planowane jest także wprowadzenie obowiązkowego stosowania systemu IOSS, przynajmniej przez platformy cyfrowe i niewykluczone na tym polu jest też rozszerzenie odpowiedzialności tych platform za dostawy towarów[66]. Istotne będzie także doprecyzowanie zasad stosowania uproszczenia dla transakcji B2C w obszarze usług telekomunikacyjnych,

[56] Projekt ustawy z 14.4.2023 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw. Druk nr 3025, Wykaz prac legislacyjnych i programowych Rady Ministrów, Kancelaria Prezesa Rady Ministrów, sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=3025 (dostęp 7.5.2023 r.).

[57] Dokument roboczy służb komisji – Streszczenie sprawozdania z oceny skutków, SWD/2022/394, Komisja Europejska, Bruksela 2022.

[58] VAT gap in the EU – Raport za 2022 r., CASE – Center for Social and Economic Research (Project Leader), Economisti Associati (Consortium Leader), Komisja Europejska, Bruksela 2022, s. 15.

[59] Zaproszenie do zgłaszania uwag dotyczących oceny skutków, Podatek VAT w Erze Cyfrowej, Ares (2022)933162, Komisja Europejska, Bruksela 2022, s. 1.

[60] *Ibidem*.

[61] *J. Fornalik*, Pakiet unijnych zmian VAT in the Digital Age cz. 1, MDDP, Warszawa 2022, https://www.mddp.pl/pakiet-unijnych-zmian-vat-in-the-digital-age-cz-1/ (dostęp 5.1.2023 r.).

[62] Dokument roboczy służb komisji – Streszczenie sprawozdania z oceny skutków, SWD/2022/394, Komisja Europejska, Bruksela 2022.

[63] *Ibidem*.

[64] Single VAT Registration, tj. SVT.

[65] Proposal for a COUNCIL DIRECTIVE amending Directive 2006/112/EC as regards VAT rules for the digital age, COM/2022/701, Komisja Europejska, Bruksela 2022.

[66] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 35.

nadawczych i elektronicznych oraz wewnątrzwspólnotowej sprzedaży towarów na odległość, czyli WSTO, realizowanych poniżej progu 10 000 euro, oraz planowane wprowadzenie od stycznia 2025 r. obowiązkowego odwrotnego obciążenia (*reverse charge*) dla rozliczania transakcji realizowanych przez sprzedawcę nieposiadającego rejestracji VAT w danym państwie członkowskim[67].

Następnym aspektem jest cyfryzacja sprawozdawczości VAT i konieczność dostosowania jej do wyzwań ery rozwoju Internetu[68]. Jest to szczególnie związane ze wspomnianym wcześniej wprowadzeniem faktury elektronicznej jako standardu, bez wymogu uzyskiwania zgody nabywcy na otrzymywanie e-faktur, jak również skutkować będzie zaimplementowaniem faktury ustrukturyzowanej jako standardu faktury elektronicznej[69]. Będą one pojawiać się w systemie w czasie rzeczywistym, tak samo jak informacje o transakcjach wewnątrzwspólnotowych, co zastąpi obecne miesięczne informacje podsumowujące VAT-UE i będzie pomocne w zwalczaniu oszustw typu „znikający przedsiębiorca"[70]. Ponadto warto zwrócić uwagę, że opublikowane propozycje zmian w przepisach unijnych zabraniają wprowadzenia krajowych systemów e-fakturowania w formule walidacji prawidłowości e-faktur, a takie założenia przyjęto w polskim rozwiązaniu, zatem może to spowodować dalszą rozbieżność prawa unijnego oraz krajowego i konieczność ponownej zmiany polskich przepisów.

Ostatni katalog zmian dotyczy samych platform elektronicznych, z czym są związane dodatkowe obowiązki takich platform (*platform economy*). Należy zauważyć, iż rozwój technologii umożliwił otwarcie nowych obszarów e-biznesu, gdzie w ocenie organów unijnych konieczne jest uszczelnienie poboru podatku od towarów i usług. W konsekwencji planowane jest nałożenie na nie dodatkowych obowiązków w obszarze VAT obejmujących m.in. rozszerzenie zakresu fikcji prawnej, czyli domniemania, w której platformy pełnią rolę tzw. uznanego dostawcy, zobowiązanego do rozliczenia VAT, w zakresie ułatwianych przez daną platformę transakcji dotyczących niektórych obszarów[71]. Będą to strefy usług krótkoterminowego zakwaterowania oraz usług transportu pasażerskiego, wszystkich transakcji towarowych w UE ułatwianych przez platformę, bez względu na pochodzenie faktycznego sprzedawcy i status nabywcy (B2C i B2B) i przemieszczeń towarów faktycznego sprzedawcy między krajami UE na potrzeby działalności prowadzonej na platformie, np. w modelach fulfilement center wspieranych przez platformę[72].

W potencjalnych skutkach podkreślono, iż oczekuje się wysokich kosztów związanych z wprowadzeniem nowych obowiązków sprawozdawczych, co będzie wymagało nowych inwestycji IT na najwyższym poziomie i może wiązać się z dłuższym okresem realizacji pakietu[73]. W zależności od poziomu centralizacji infrastruktury IT, którą trzeba będzie zbudować, realizacja może potrwać aż do 2030 r., lecz może stanowić to przełom w walce z nadużyciami podatkowymi, zapewniając większą możliwość weryfikacji i ściągalności podatku VAT[74]. Wywoła to również istotne oszczędności i uproszczenia dla przedsiębiorstw w zakresie kosztów rejestracyjnych czy administracyjnych, ze względu na wprowadzenie jednokrotnej rejestracji dla celów VAT dla transakcji B2C[75]. Pomoże to także zredukować bariery handlowe na terenie UE.

Mimo założeń zbliżonych do opisywanej powyżej regulacji pakietu VAT e-commerce VAT w erze cyfrowej będzie prawdopodobnie jedną z najszerzej dotychczas utworzonych regulacji w cybernetycznym ujęciu prawa podatkowego. Wszelkie skutki tego procesu najsilniej odczują firmy korzystające z platform cyfrowych oraz podmioty zajmujące się szeroko pojętym handlem międzynarodowym[76].

Warto pamiętać, że pakiet zmian to dopiero projekt, który będzie musiał przejść przez odpowiednią procedurę legislacyjną, czyli zostać przyjęty przez Radę Unii Europejskiej oraz Parlament Europejski, lecz prawdopodobieństwo przyjęcia rozwiązań idących w tym kierunku należy ocenić jako dosyć wysokie ze względu na statystyki w zakresie luk i strat w podatku VAT i potrzeby budżetowe państw unijnych[77].

Nowe raportowanie dotyczące dostawców usług płatniczych

Ostatnia regulacja, która jest bezpośrednio związana z branżą e-commerce, dotyczy dostawców usług płatni-

[67] Proposal for a COUNCIL DIRECTIVE amending Directive 2006/112/EC as regards VAT rules for the digital age, COM/2022/701, Komisja Europejska, Bruksela 2022.

[68] Digital Reporting Requirements, tj. DRR.

[69] VAT in the Digital Age Final Report, Volume 1, DIGITAL REPORTING REQUIREMENTS, Economisti Associati, Oxford Research, CASE, Wavestone, Hédeos, Mazars, Desmeytere Services and Università di Urbino, Komisja Europejska, Bruksela 2022, s. 12, https://taxation-customs.ec.europa.eu/system/files/2022-12/VAT%20in%20the%20Digital%20Age_Final%20Report%20Volume%201.pdf (dostęp 5.1.2023 r.).

[70] *J. Fornalik*, Pakiet unijnych zmian… (dostęp 5.1.2023 r.).

[71] *Ibidem*.

[72] VAT in the Digital Age Final Report, Volume 1 SINGLE PLACE OF VAT REGISTRATION AND IMPORT ONE STOP SHOP, Economisti Associati, Oxford Research, CASE, Wavestone, Hédeos, Mazars, Desmeytere Services and Università di Urbino, Komisja Europejska, Bruksela 2022 r., s. 40, https://taxation-customs.ec.europa.eu/system/files/2022-12/VAT%20in%20the%20Digital%20Age_Final%20Report%20Volume%201.pdf (dostęp 5.1.2023 r.).

[73] Zaproszenie do zgłaszania uwag dotyczących oceny skutków, Podatek VAT w Erze Cyfrowej, Ares (2022)933162, Komisja Europejska, Bruksela 2022, s. 3.

[74] *Ibidem*.

[75] *M. Goździewska,* Dyrektywa „VAT in the Digital Age", KR Group, Warszawa 2022, https://www.krgroup.pl/dyrektywa-vat-in-the-digital-age/ (dostęp 6.1.2023 r.).

[76] VAT w epoce cyfrowej – istotne zmiany zaproponowane przez Komisję Europejską, *K. Wróblewska,* EY Polska, Warszawa 2022, https://www.ey.com/pl_pl/tax/vat-dyrektywa-digital-age (dostęp 6.1.2023 r.).

[77] *Ibidem*.

czych[78]. Podstawami prawnymi tych zmian jest dyrektywa Rady (UE) 2020/284 z 18.2.2020 r. zmieniająca dyrektywę 2006/112/WE w odniesieniu do wprowadzenia pewnych wymogów dla dostawców usług płatniczych[79], jak również rozporządzenie Rady (UE) 2020/283 z 18.2.2020 r. zmieniające rozporządzenie (UE) Nr 904/2010 w odniesieniu do środków służących wzmocnieniu współpracy administracyjnej w celu zwalczania oszustw w dziedzinie VAT[80].

Od 1.1.2024 r. wchodzi w życie nowy obowiązek raportowania wybranych transakcji transgranicznych właśnie przez te podmioty. Regulacja ta ma na celu możliwość monitorowania przez odpowiednie organy transakcji, które zostały dokonane poprzez elektroniczne systemy płatności, i będzie wiązała się z oceną ich prawidłowości oraz ewentualną reakcją na dokonywane czynności, jak również zostanie ona wprowadzona w celu kontroli dostaw towarów i świadczenia usług, które uznaje się za mające miejsce w państwie członkowskim[81].

W kwestii obecnego stanu legislacyjnego w Polsce Ministerstwo Finansów opublikowało projekt ustawy zmieniającej[82], a 24.10.2022 r. Komitet do Spraw Europejskich przyjął projekt oraz zarekomendował jego rozpatrzenie Stałemu Komitetowi Rady Ministrów, po przedłożeniu przez Ministra Finansów[83]. Dyrektywa ta ma zostać zaimplementowana do polskiego systemu prawnego do 31.12.2023 r., a analizując poziom zaawansowania prac, jest bardzo prawdopodobne, że jeszcze w tym roku przepisy dyrektywy zostaną wprowadzone w Polsce.

Dostawcy usług płatniczych będą mieli obowiązek raportowania transakcji wówczas, gdy łączna liczba płatności otrzymanych przez danego odbiorcę przekroczy minimum 25 płatności na kwartał oraz będzie miała charakter transgraniczny[84]. Raportowanie odbywać się będzie w formie elektronicznej, za pomocą ustrukturyzowanego pliku XML, a dane gromadzone będą na poziomie krajowym i również co kwartał przekazywane do Centralnego Elektronicznego Systemu Informacji o Płatnościach (CESOP)[85]. System ten będzie prowadzony na poziomie unijnym. Analizy prowadzone w programie będą rozszerzone również o dodatkowe narzędzia, które posłużą skuteczniejszemu zwalczaniu oszustw związanych z VAT w branży e-commerce[86].

W zakresie obowiązku podmiotów będzie prowadzenie szczegółowej ewidencji odbiorców płatności i płatności w odniesieniu do usług płatniczych, które świadczą. Podmiotami zobowiązanymi będą dostawcy usług płatniczych zlokalizowani na terenie państw unijnych. Artykuł 243a dyrektywy Rady UE[87] ogranicza jednak zakres obowiązku sprawozdawczego do następujących czterech kategorii dostawców usług płatniczych:

- instytucje kredytowe, które obejmują głównie banki mające siedzibę w Europie oraz europejskie oddziały instytucji kredytowych mające siedzibę poza UE;
- pieniądz elektroniczny, który może obejmować szeroki zakres instytucji świadczących usługi płatności elektronicznych, takich jak dostawcy portfela elektronicznego lub dostawcy elektronicznych kuponów/kart;
- instytucja płatnicza, która może obejmować szeroki zakres usług płatniczych, w tym wydawanie kart kredytowych/debetowych, pozyskiwanie transakcji płatniczych, przetwarzanie płatności, inicjowanie płatności itp.;
- poczta w GIRO (produkt pozabankowy oferowany przez firmy pożyczkowe), która świadczy usługi płatnicze[88].

W aspekcie raportowania dostawców usług płatniczych istotne jest określenie danych, które będą jemu podlegały. Należą do nich informacje umożliwiające identyfikację odbiorcy płatności, szczegółowe informacje dotyczące płatności transgranicznych i informacje dotyczące zwrotów płatności zidentyfikowanych jako odnoszące się do płatności transgranicznych[89]. Ewidencje zaś będą zachowane w formie elektronicznej przez okres trzech lat kalendarzowych od końca roku kalendarzowego, w którym nastąpiła płatność.

System ten ocenić należy jako suplementarny do regulacji, które zostały omówione w poprzednich akapitach. Dzięki znajdującym się w bazie ewidencjom z danymi organy będą mogły realizować funkcję nadzorującą nad wszelkimi transakcjami transgranicznymi, które obarczone są najwyższym ryzykiem nadużyć podatkowych.

Uwagi końcowe

Podsumowując działania władz unijnych oraz krajowych, należy stwierdzić, że zmiany obecnej dekady w zakresie nowych aktów prawnych w branży e-commerce mają dynamiczny charakter, co wynikać mogło z nagłego rozwoju wielu nowych technologii oraz możliwości używania coraz now-

[78] Payment Service Providers, dalej: PSP.
[79] Dz.Urz. UE L Nr 62, s. 7.
[80] Dz.Urz. UE L Nr 62, s. 1.
[81] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 25.
[82] Projekt ustawy o zmianie ustawy o podatku od towarów i usług oraz ustawy o Krajowej Administracji Skarbowej (Nr UC128 w wykazie prac legislacyjnych i programowych Rady Ministrów).
[83] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 25.
[84] Dostawcy usług płatniczych, Ministerstwo Finansów, Krajowa Administracja Skarbowa, Warszawa 2022, https://www.gov.pl/web/kas/dostawcy-uslug-platniczych (dostęp 6.1.2023 r.).
[85] *Ibidem*.
[86] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 28.
[87] Dyrektywa 2006/112/WE Rady z 28.11.2006 r. w sprawie wspólnego systemu podatku od wartości dodanej.
[88] Dostawcy usług płatniczych, Ministerstwo Finansów, Krajowa Administracja Skarbowa, Warszawa 2022, https://www.gov.pl/web/kas/dostawcy-uslug-platniczych (dostęp 6.1.2023 r.).
[89] *M. Wachowiec*, *A. Dwornik*, *W. Janik*, Zmiany podatkowo-prawne..., s. 27.

szych, cybernetycznych narzędzi, w celu uchylania się oraz unikania opodatkowania. Głównym czynnikiem motywującym organy do podjęcia szerszej legislacji mogła okazać się pandemia COVID-19, która gwałtownie wpłynęła na rozwój handlu elektronicznego i związane z nim liczne nadużycia podatkowe. Są to zatem zmiany niewątpliwie pożądane, ponieważ umożliwią one tworzenie konkurencyjnego rynku dla przedsiębiorców, w którym każdy podmiot ma równe szanse na rozwój. Wpłynie to również pozytywnie na budżet państw unijnych, ponieważ dojdzie do szerszego uszczelnienia podatkowego. Należy również zauważyć, że kontrola podatkowa w formie systemów elektronicznych jest znacznie bardziej skuteczna, ujednolicona oraz przejrzysta, a odpowiednie monitorowanie danych następuje za pomocą skutecznych programów. Najwięcej nowych uregulowań jest związanych z podatkiem od towarów i usług ze względu na dostrzeżony problem ogromnych luk i strat z powodu niezapłaconych należności z tytułu VAT należnego, dlatego rozwiązania prawne tego problemu są bardzo istotne.

Ustawodawstwo obecnej dekady ma przed sobą liczne wyzwania, ponieważ konieczne jest dostosowanie brzmienia wielu przepisów do obecnych standardów technologicznych. Zgodnie z zasadą „prawo nie nadąża za rzeczywistością", lecz ważna jest próba dopasowania choć części z nich do realiów nowej, cyfrowej ery. W artykule przedstawione zostały cztery najbardziej przełomowe akty prawne, które w najbliższych latach zaważyć mogą o dalszym kształtowaniu się przepisów podatkowych oraz o ich niezaprzeczalnym rozwoju. Po dokonaniu analizy założeń i celów wszystkich z nich należy stwierdzić, że uregulowania te są fundamentem do kreowania kolejnych przepisów, szczególnie na szczeblu unijnym, w zakresie harmonizacji systemów prawnych, handlu transgranicznego oraz udogodnień systemowych, aby ułatwić podatnikom rozliczanie podatkowe. Należy dostrzec zatem ogromny potencjał w sferze elektronicznej, ponieważ właśnie w cybernetycznym środowisku może rozwijać się podłoże do wszelkich przyszłych rozwiązań prawnych i wpłynąć na branżę e-commerce jako przeważającą na rynku globalnym.

Słowa kluczowe: e-commerce, era cyfrowa, prawo podatkowe, dyrektywa, platforma cyfrowa, podatek VAT, elektronizacja, ustawodawstwo, uszczelnienie systemu podatkowego.

Legal and tax changes in the e-commerce industry – objectives and prospects for regulation development

The paper discusses the issues of cybernetic legal and tax changes in the e-commerce industry, including the objectives and further prospects for the development of regulations. The author brings up the subject of dynamic evolution of the trade industry and its consequences. She discusses in detail the four groundbreaking regulations that are the foundation for legal changes in regard to the sealing of the tax system in the current digital era, also considering the effects of implementing these legal acts into national legislation.

Keywords: e-commerce, digital era, tax law, directive, digital platform, VAT, digitization, legislation, sealing the tax system.

Jak inteligentne jest prawo regulujące sztuczną inteligencję? Próba analizy AI Act na podstawie jej ugruntowania w przestrzeni komercyjnego użycia

Kamil Palacz[1]

Celem niniejszego opracowania jest przybliżenie regulacji prawnych zagadnienia sztucznej inteligencji (*artificial intelligence*), przykładów jej zastosowania oraz ryzyka, jakie ze sobą niesie. W niniejszym artykule poruszono także temat AI Act, przeanalizowano kwestię sztucznej inteligencji w ujęciu prawa kontynentalnego oraz common law, a także podjęto próbę odpowiedzi na pytanie, czy legislacja AI na naszym aktualnym poziomie wiedzy jest legislacją trafną.

Uwagi wstępne

Sztuczna inteligencja jest technologią inspirującą ludzi, od kiedy ten koncept po raz pierwszy pojawił się w przemówieniu *J. McCarthy'ego* na konferencji w Dartmouth Collage w 1956 r.[2]. Po prawie 70 latach, gdy sztuczna inteligencja jest nam bliższa niż była kiedykolwiek, nie milkną echa konieczności prawnego uregulowania tej kwestii.

To, w jaki sposób patrzymy na sztuczną inteligencję, jest różny. Kiedyś popularne było spojrzenie na nią jak na inną istotę żywą. Zagubioną w świecie stworzonym przez ludzi dokładnie tak jak w filmie *AI: Artificial Inteligence*. Jednak obecnie patrzymy na nią jak na potencjalne zagrożenie mogące zagrozić cywilizacji – w taki sam sposób, który w książce „Superinteligence: Paths, Dangers, Strategies"[3] przedstawia *N. Bostrom* lub który popularyzuje seria filmów o terminatorze.

Na początku warto przytoczyć definicje AI. Czym więc jest ten koncept, który tak interesuje ludzi? Otóż jak wynika z definicji przytoczonej na stronie Parlamentu Europejskiego: „sztuczna inteligencja (SI) to zdolność maszyn do wykazywania ludzkich umiejętności, takich jak rozumowanie, uczenie się, planowanie i kreatywność. Sztuczna inteligencja umożliwia systemom technicznym postrzeganie ich otoczenia, radzenie sobie z tym, co postrzegają i rozwiązywanie problemów, działając w kierunku osiągnięcia określonego celu. Komputer odbiera dane (już przygotowane lub zebrane za pomocą jego czujników, np. kamery), przetwarza je i reaguje. Systemy SI są w stanie do pewnego stopnia dostosować swoje zachowanie, analizując skutki wcześniejszych działań i działając autonomicznie"[4].

Temat wart jest poruszenia nie tylko ze względu na jego szybki rozwój, ale także fakt, iż w przeciwieństwie do masowej opinii nie jest to już technologia przyszłości, a coś, co zaczyna w coraz większej mierze dotyczyć każdego z nas. By się o tym przekonać, wystarczy odebrać telefon, wiele firm nie może bowiem sobie pozwolić (lub nie chce) na dział Call Center. W efekcie wykorzystują dzisiaj boty, które doradzają klientom i prezentują im najnowsze promocje. Szczątkową wersję tegoż możemy zobaczyć już na wielu portalach. Konsultant, którym w rzeczywistości jest *chatbot*, nie jest wart więcej niż koszty jego kupna i administracji, a jest w stanie odsiać większość prozaicznych i prostych do rozwiązania problemów dnia codziennego. Oczywiście taki *chatbot* musi mieć wbudowaną możliwość kontaktu z prawdziwym człowiekiem, który będzie w stanie rozwiązać bardziej skomplikowane sprawy. Jest to już wielki skok technologiczny w porównaniu do czasu sprzed dekady, kiedy możliwość rozmawiania przez telefon z konsultantem nieposiadającym fizycznego ciała, a jedynie zaprogramowany ciąg wypowiedzi, byłaby fikcją, którą można było zobaczyć jedynie w filmach.

Zagrożenia użytku AI a AI Act

W takich czasach legislacja taka jak AI Act zdaje się odpowiednio ugruntowana w potrzebach nowoczesnego społeczeństwa. Zwłaszcza (o czym będzie mowa w dalszej części artykułu), że AI oprócz wspaniałych możliwości niesie równie wspaniałe zagrożenia. Zagrożenia, które już dzisiaj, mimo raczkującej wciąż technologii wspomaganej sztuczną inteligencją, sprawiły realne problemy realnym ludziom.

Jak zaznacza ekspert w dziedzinie AI – *G. Mauro* w swoim filmie „EU ARTIFICIAL INTELIGENCE ACT: Why we need it, how it works, what it means"[5] w USA działał program, który jedynie na podstawie danych pacjenta oszacowywał prawdo-

[1] Autor jest studentem czwartego roku kierunku Prawo na Uniwersytecie Wrocławskim oraz aktywnym członkiem studenckiego Koła Naukowego Blok Prawa Komputerowego LegalNet. Piastuje także stanowisko młodszego specjalisty ds. prawnych w kancelarii prawnej HYPERION Gałek i Gałan.

[2] Redakcja portalu Ai.nl, Timeline of AI: a brief history of artificial intelligence it's highlights, https://www.ai.nl/artificial-intelligence/timeline-of-ai-a-brief-history-of-artificial-intelligence-its-highlights (dostęp 14.1.2023 r.).

[3] *N. Bostrom*, Superinteligence: Paths, Dangers, Strategies, Oksford 2014, s. 114–115.

[4] Parlament Europejski, Sztuczna inteligencja: co to jest i jakie ma zastosowania?, https://www.europarl.europa.eu/news/pl/headlines/society/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania (dostęp 14.1.2023 r.).

[5] *G. Mauro*, EU ARTIFICIAL INTELLIGENCE ACT: Why we need it, how it works, what it means, https://www.youtube.com/watch?v=l0h5gjturV4 (dostęp 14.1.2023 r.).

podobieństwo, że dana osoba będzie potrzebować większej liczby badań. Algorytm stojący za tym programem różnicował ludzi. Osoby czarnoskóre oraz Azjaci byli przez ów algorytm dyskryminowane, gdyż ten znacznie rzadziej wskazywał u nich na konieczność przeprowadzenia dodatkowych badań, co wielokrotnie skończyło się śmiercią pacjentów.

W tym samym filmie *G. Mauro* mówi o algorytmie wprowadzonym przez firmę Amazon, który miał różnicować CV kandydatów ubiegających się o pracę. Ten algorytm również różnicował ludzi pod względem ich płci, dyskryminując kobiety. Bierze się to ze zjawiska nazwanego: „skrzywieniem algorytmicznym".

Skrzywienie algorytmiczne i ryzyko, jakie wprowadza

Zjawisko to zostało opisane przez *A. Obem* w wywiadzie udzielonym dla portalu Papaya.rocks: „do wytrenowania sieci neuronowej, czyli złożonego, uczącego się modelu statystycznego, potrzebna jest odpowiednio duża liczba przykładów, o dużej różnorodności, które pozwolą wykryć najdrobniejsze zależności. Zbyt mały, nie dość różnorodny i nieaktualizowany zbiór danych prowadzi do tego, że system popełnia błędy, tworząc skrzywienie. Badacze z Uniwersytetu w Waszyngtonie celowo »skrzywili« algorytm, którego zadaniem było klasyfikowanie zwierząt na zdjęciach – wilków i psów rasy husky. Dane treningowe obejmowały 20 zdjęć wilków – wszystkie w tle miały śnieg. Co się wydarzyło? Wytrenowany na takich danych algorytm zwierzęta występujące na tle śniegu oznaczał zawsze jako wilki – zwracając uwagę tylko na tło, a nie na cechy charakterystyczne zwierzęcia"[6].

Wobec czego oczywistym krokiem wydaje się konieczność wprowadzenia regulacji, która zapewniłaby poprawną administrację nad tymi algorytmami. Wszystko po to, by sytuacja nie powtórzyła się, zwłaszcza w momencie, w którym sztuczna inteligencja na stałe zawita do naszych domów. Również do gałęzi życia, w których mogłaby – nieodpowiednio administrowana – spowodować więcej zniszczeń.

Przykłady wykorzystania AI na świecie

Pod koniec 2022 r. agencja Reuters[7] podała, że w Pekinie ma wystartować start-upowa sieć „robo taksówek". Krytycy tego pomysłu postulują o niebezpieczeństwach, jakie niesie za sobą wprowadzenie takiej technologii do użytku publicznego. Stoi za tym BAIDU, chińskie przedsiębiorstwo, które zapowiada, że zwiększy liczbę swoich autonomicznych taksówek do 200 w ciągu trwającego roku.

W tym samym artykule podano, że większość producentów samochodowych wycofała się z tego pomysłu, jednak BAIDU już prowadzi działania na skalę większą niż tylko Chiny. Do miejsc, gdzie owe autonomiczne samochody trafią, zaliczają się Arizona oraz California. Jednak gdy myślimy o autonomicznych samochodach, firmą, która najbardziej wysuwa się na pierwszy plan, jest Tesla.

Swego czasu przedsiębiorstwo założone przez *E. Muska* było najlepszym kandydatem do zaimplementowania tej technologii do naszego świata. Dziś po śledztwie, które przeprowadził amerykański rząd, Tesla utrzymuje, że ich autonomiczne pojazdy wymagają człowieka gotowego na szybką reakcję, w razie gdyby samochód nie reagował samoczynnie na zjawisko występujące na drodze. Tym mocniej w pamięć zapada zdarzenie, które wydarzyło się w trakcie jazdy takiego samochodu Tesli. Ten, by ominąć liść, wykonał manewr, który kosztował życie nieuważnego przechodnia.

W Europie również możemy pochwalić się pewnym postępem w tej dziedzinie. W trakcie konferencji „Cyberspace", która odbyła się na Uniwersytecie Masaryka w Brnie w 2022 r., podczas paralelnego panelu „The world of AI sandboxes, and their use in practice"[8], zastępca dyrektora ds. mobilności autonomicznej oraz badań, rozwoju i innowacji przy Ministerstwie Transportu Republiki Czeskiej – *T. Čížková* wypowiadała się o trudnościach, z jakimi aktualnie mierzą się Czechy w dostosowywaniu infrastruktury drogowej do użytku przez samochody autonomiczne.

Z kolei, jak podaje gazeta *New York Post*, chińscy naukowcy zdołali zaprogramować algorytm, który po wystawieniu na dane ponad 17 000 spraw, „jest w stanie do pewnego stopnia zastąpić prokuratora w procesie podejmowania decyzji"[9] – mówi prof. *S. Yong*, który sprawował pieczę nad tymi badaniami. Wskazuje na jego niebywałą skuteczność sięgającą aż 97%.

W przypadku analizowania AI łatwo o wniosek, że niebezpiecznie zbliżamy się do dystopii. Jednak pamiętajmy, że są to dopiero pierwsze kroki technologii, której wkład w świat zależeć będzie od naszego podejścia do niej. Oczywiste jest, że braki w stworzonym algorytmie sztucznej inteligencji mogą zabić przechodniów lub doprowadzić do skazania niewinnego człowieka. To słusznie budzi w nas niepokój, jednak ta sama technologia używana jest również do rzeczy, które ułatwiają nam życie codzienne, jak chociażby komunikator Alexa lub Siri.

---

[6] *J. Czechowicz*, Sztuczna inteligencja, ale prawdziwa dyskryminacja. Jakie są potencjalne zagrożenia wynikające z AI?, https://papaya.rocks/pl/trendbook/sztuczna-inteligencja-ale-prawdziwa-dyskryminacja-jakie-sa-p (dostęp 14.1.2023 r.).

[7] *K. Krolicki*, Baidu, Pony.ai start driverless robotaxi tests in Beijing, https://www.reuters.com/technology/baidu-gets-license-driverless-robotaxi-tests-beijing-2022-12-30/ (dostęp 14.1.2023 r.).

[8] Uniwersytet Masaryka, 21. Międzynarodowa konferencja Cyberspace 2022, www.cyberspace.muni.cz/programme (dostęp z 14.1.2023 r.).

[9] *H. Sparks*, China's AI attorney prosecutes crimes 'with 97% accuracy', https://nypost.com/2021/12/27/chinas-ai-attorney-prosecutes-crimes-with-97-accuracy/ (dostęp 14.1.2023 r.).

W tej sytuacji warto przypomnieć sobie popularną analogię z nożem. On sam w sobie nie jest zły, używamy go w końcu każdego dnia i choć skaleczenia są jak najbardziej bolesne, wynikają z naszego własnego roztargnienia lub braku umiejętności, nie z jego natury. Nie zmienia to jednak faktu, że to samo narzędzie, w nieodpowiednich rękach może przyczynić się do tragedii.

AI Act, czyli prawo oparte na ryzyku

W wyżej opisanej rzeczywistości UE zdecydowała się wprowadzić legislację, która miałaby zahamować niektóre niepożądane użycia AI.

AI Act jest aktem, który za swój rdzeń ma wartości, którym hołduje UE i na podstawie wyliczonego prawdopodobieństwa wystąpienia ryzyka pogwałcenia tychże zasad, klasyfikuje pewne gałęzie komercyjnego użycia, które powinny być obwarowane szczególnymi przepisami. Ryzyko podzielono na cztery kategorie.

Nieakceptowalne użycie stanowi pierwszą kategorię, którą wyszczególnia AI Act. Zawiera się w niej użycie AI do m.in. manipulowania ludźmi. Nietrudno sobie wyobrazić, jakie możliwości posiadałoby mikrotargetowanie reklam czy komunikatów przy użyciu analizującej każde kliknięcie sztucznej inteligencji. Zwłaszcza że już teraz pojawiają się badania nad tym, jakie komunikaty działają na poszczególne jednostki najbardziej. Liczni eksperci cytowani na łamach bussinesinsider.com, potwierdzają, że właśnie takie działania i badania przyczyniły się do wygranej *Trumpa* w wyborach prezydenckich w 2016 r.[10].

Kolejnym nieakceptowalnym użyciem technologii AI jest rozpoznawanie twarzy przy użyciu kamer monitoringu miejskiego w czasie rzeczywistym. Jednak tu istnieje wyjątek. Wciąż legalne będzie wykorzystywanie tego sposobu do odnajdywania zagubionych dzieci oraz identyfikowania terrorystów w przestrzeni publicznej.

Użycie o wysokim ryzyku – w tej kategorii mieści się używanie sztucznej inteligencji do oceniania i różnicowania ludzi przy zatrudnianiu oraz przy promocji czy awansu. Jednak warto wspomnieć już teraz, że AI Act wymaga od dostawców takowych algorytmów, aby czuwali nad tym, jak działają ich programy. Wszystko po to, by nie doszło do ich spaczenia, co mogłoby stworzyć podobną sytuację jak z przytaczanym już wcześniej algorytmem wykorzystywanym swego czasu przez platformę Amazon.

Kolejnym użyciem, które zawiera się w kategorii wysokiego ryzyka, jest ocenianie ludzi pod względem przyjęcia na uniwersytet. Również w tym przypadku, jak w poprzednim, AI Act wymaga od dostawców ciągłej administracji po to, by nie dochodziło do nadużyć czy dyskryminacji na tle rasowym, czy płci. Najważniejszym zapisem jest jednak wpisanie do tej kategorii używanie AI dla infrastruktury krytycznej oraz Policji. Można zakładać, że poziom administracji takiego algorytmu będzie zdecydowanie wyższy niż w przypadku oceny ludzi starających się o przyjęcie do pracy oraz że zaufanie do takiego algorytmu będzie mocno ograniczone. Deweloperzy tej technologii są zobligowani do serii testów, które wyeliminują jakąkolwiek stronniczość w ocenianiu danych, na jakie będzie wystawiony algorytm. Tu również pojawia się wymóg obecności człowieka po drugiej stronie algorytmu, który będzie w stanie go „naprawić", jeśli ten zacznie wychylać się ze swoją oceną gdzieś poza ramy przyjęte przez te określone w akcie ramy użycia.

Trzecią i czwartą kategorię stanowią tzw. użycie limitowane oraz minimalne. Oba wykorzystywane są w działaniach, podczas których trudno zrobić krzywdę człowiekowi. Mowa tu m.in. o rozwiązaniach jak *Chatbot* czy filtr spamu. W takiej sytuacji deweloperzy tej technologii zobowiązani są, by każdorazowo powiadamiać użytkownika, że rozmawia ze sztuczną inteligencją. Dodatkowo zalecane jest, by deweloperzy wytworzyli w tej kwestii swój własny kod etyki. Jednak presja na tym wyszczególnionym aspekcie użytkowania sztucznej inteligencji nie jest wysoka.

Antropocentryzm w AI Act

AI Act nazywany jest legislacją „na próbę", co samo w sobie nie jest złe w żaden sposób. Nie wiemy jeszcze, jakie są granice użycia AI w różnych gałęziach przemysłu, więc AI Act wydaje się naprawdę dobrym aktem prawa, który nada ton późniejszym obostrzeniom oraz bada to, w jaki sposób AI może być użytkowane, by sprawić, żeby życie było lepsze.

Zastanawia jednak fakt podejścia prawodawców do tego przedmiotu regulacji. Jest to akt, który reguluje wykorzystywanie sztucznej inteligencji przez pryzmat człowieka. Bo to do niego odnoszą się wszelkie ewentualne konsekwencje nieplanowanych działań sztucznej inteligencji.

Oczywiste jest, że w regulacji prawnej przede wszystkim chodzi o to, żeby nikomu nie stała się krzywda przez legalne użytkowanie tego typu programów. Jednak wątpliwości może budzić jakość danych zgromadzonych przez legislatorów na podstawie ustawy, której centrum stanowi człowiek.

Jednocześnie zastanawia, dlaczego regulacje nie odnosiły się do konkretnych kwestii związanych ze sztuczną inteligencją. Nie zabroniono tworzyć oprogramowania mogącego spełniać przesłanki kategorii nieakceptowalnej, ale zabroniono jej używać. Może to doprowadzić do sytuacji, gdy przy różnej legislacji oprogramowanie, które w Europie nie może być wykorzystywane, jest w niej jednocześnie produkowane.

[10] *I. Asher Hamilton*, Trump targeting Black voters in 2016 shows Facebook's microtargeting is a danger to democracy, experts say, https://www.businessinsider.com/trump-targeting-black-voters-facebook-2016-deterrence-experts-comment-2020-9 (dostęp 14.1.2023 r.).

AI w ujęciu prawa kontynentalnego oraz *common law*

Prawo kontynentalne istotnie różni się od *common law*, a różnice te mogą stanowić przeszkodę w przypadku ograniczania rozwoju szkodliwych nowych technologii. Pierwszą i kluczową odmiennością jest tu tempo legislacji. Zdecydowanie wolniej będą tworzyć się akty, na które obywatel może się powołać w starciu sądowym z deweloperami sztucznej inteligencji. Mimo używania wykładni intencjonalnej najczęściej preferowanej przez UE wciąż zdecydowanie szybszy rozwój nowych technologii, w tym AI, może doprowadzić do sytuacji, w której ta technologia będzie używana do łamania pewnych praw, a jednocześnie będzie wciąż legalna.

W systemie *common law* sytuacja ma się zgoła inaczej, jeśli obywatel może przed sądem powołać się na wyrok innego sądu. Wystarczy jeden wyrok skazujący, by to jedno wykorzystanie tej nowej technologii zostało do pewnego stopnia ograniczone, a na pewno, by obywatel mógł bronić swoich praw w efektywniejszy sposób.

Polityczność kręgosłupa AI oraz czy i jakie prawa mogą na tym ucierpieć

Prawodawcy, jak wszyscy politycy, odpowiadają przed swoim suwerenem, jakim są ludzie. Można zatem zakładać, że takie podejście będzie miało swoje odzwierciedlenie w aktach prawa, które z rąk takich prawodawców wychodzą. Zatem uzasadnioną obawą jest, że prawa, których opis łatwiej zamknąć w prostych słowach, będą determinowały to, na co pozwolimy deweloperom sztucznej inteligencji.

Nikt nie poskarży się, że spowolnienie rozwoju AI narusza jego prawa ekonomiczne, kiedy zobaczy, że źródłem tych ograniczeń jest wolność i bezpieczeństwo każdego Europejczyka. Jednak stanowi to aspekt, nad którym warto się zastanowić. Jeśli prawo będzie tworzone pod medialny wydźwięk, możemy doprowadzić do sytuacji, w której nie będziemy w stanie korzystać z tej technologii w pełni jej potencjału. Ważne jest, by znaleźć złoty środek między ograniczaniem a wytyczaniem optymalnego kursu, który, choć już widoczny w zalążku, powinien być rozwijany w przyszłości dla najlepszej efektywności algorytmów sztucznej inteligencji. Nie możemy również poddawać się emocjom, które od początku towarzyszą tej technologii.

Czy legislacja na naszym aktualnym poziomie wiedzy jest legislacją trafną?

Na ten moment legislacja oparta na ryzyku w użyciu jest rozsądna. Nie znamy jeszcze wszelkich możliwości sztucznej inteligencji, a jej wszechstronność działa na niekorzyść regulacji mających ją ograniczać. Dlatego dobrze, że powstał akt prawa, który (choć nie jest wolny od wad) normuje najbardziej krytyczne sposoby użytkowania tej technologii.

Oczywiste jest, że pojawią się wkrótce sposoby wykorzystania jej do rzeczy, które – gdybyśmy o nich wiedzieli dziś – byłyby wyłączone z użycia, jednak złą praktyką z perspektywy rozwoju byłoby również ograniczanie jej w sposób nazbyt rozwinięty. Każda technologia ma koniec końców służyć ludziom. A AI Act jest na dobrej drodze, by zapewnić nam przyszłość, w której tymi ludźmi jesteśmy my.

Słowa kluczowe: sztuczna inteligencja, AI Act, kategorie AI Act, regulacje prawne sztucznej inteligencji, zastosowanie sztucznej inteligencji.

How intelligent is the law regulating artificial intelligence? An attempt to analyse the AI Act based on its implementation in the sphere of commercial use

The purpose of this study is to present regulations in regard to artificial intelligence, examples of its use and risks it entails. In the present article the author also brings up the subject of the AI Act, analyses the issue of artificial intelligence in the context of civil law and common law, and attempts to answer the question whether AI legislation on our current level of knowledge is accurate legislation.

Keywords: artificial intelligence, AI Act, categories of AI Act, artificial intelligence regulations, application of artificial intelligence.

Wybrane obowiązki strażników dostępu w świetle Aktu o rynkach cyfrowych z perspektywy ochrony danych osobowych

r.pr. *Krzysztof Wyderka*[1]

W ostatnich latach usługi cyfrowe, a zwłaszcza platformy internetowe odgrywają coraz ważniejszą rolę w europejskiej i światowej gospodarce. Możliwości, które stwarzają usługi platformowe w połączeniu z potencjalnymi, nieuczciwymi praktykami przedsiębiorstw świadczących te usługi, mogą niekorzystnie wpływać na konkurencję oraz prawa podstawowe użytkowników końcowych. Dostrzegalny jest również problem kontrolowania ważnych ekosystemów w gospodarce cyfrowej przez kilka dużych platform, które określane są mianem strażników dostępu (*gatekeepers*). W odpowiedzi na te wyzwania organy Unii Europejskiej ustanawiają nowe ramy prawne mające stworzyć bezpieczniejszą przestrzeń cyfrową oraz sprawiedliwe warunki działania w celu wspierania innowacji, wzrostu gospodarczego i konkurencyjności. Mając na uwadze fakt, że dane, w tym zwłaszcza dane osobowe, są kluczowym aktywem dla gospodarki cyfrowej, nowe akty prawne wprowadzają również obowiązki związane z przetwarzaniem danych osobowych. Wśród przyjętych w ostatnim czasie regulacji istotne miejsce zajmuje Akt o rynkach cyfrowych (DMA). Celem artykułu jest zidentyfikowanie wynikających z przepisów DMA kluczowych obowiązków strażników dostępu związanych z przetwarzaniem danych osobowych, określenie wzajemnych relacji pomiędzy przepisami Aktu o rynkach cyfrowych a przepisami RODO i wyzwań z nich wynikających, a także podjęcie próby wyjaśnienia wątpliwości.

Uwagi wstępne

W dniu 12.10.2022 r. w Dzienniku Urzędowym Unii Europejskiej zostało opublikowane rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z 14.9.2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych)[2]. Akt ten ma przyczynić się do zapewnienia sprawiedliwej i konkurencyjnej gospodarki cyfrowej, jednego z trzech głównych filarów strategii cyfrowej UE[3]. Ten cel, stosownie do treści art. 1 DMA, jest realizowany poprzez „ustanowienie zharmonizowanych przepisów służących zapewnieniu wszystkim przedsiębiorstwom kontestowalnych i uczciwych rynków w sektorze cyfrowym w całej Unii, na których działają strażnicy dostępu, z korzyścią dla użytkowników biznesowych i użytkowników końcowych".

Jeszcze w trakcie trwania procesu legislacyjnego w doktrynie wskazywano, że „przynależność projektowanej regulacji do określonej dziedziny prawa nie jest oczywista"[4]. Przepisy DMA przede wszystkim uzupełniają obecnie obowiązujące unijne i krajowe reguły konkurencji oraz zwalczania nieuczciwej konkurencji[5]. Zważywszy jednak, że aktywem o strategicznym znaczeniu dla gospodarki cyfrowej, dającym często przewagę konkurencyjną, są dane, w tym zwłaszcza dane osobowe, w DMA zawarto również przepisy regulujące obowiązki strażników dostępu związane z przetwarzaniem danych osobowych. Akt o rynkach cyfrowych wprowadza w szczególności ograniczenia w zakresie łączenia i wykorzystywania przez strażników dostępu danych osobowych użytkowników końcowych, reguluje uprawnienia związane z przenoszeniem i dostępem do danych, a także zawiera przepisy odnoszące się do profilowania.

Wzajemne oddziaływanie prawa ochrony danych osobowych i prawa ochrony konkurencji jest od dłuższego czasu zauważalne w treści aktów prawnych, w orzecznictwie, a także w praktyce organów antymonopolowych oraz organów ochrony danych. Wystarczy zauważyć, że przetwarzanie przez przedsiębiorców danych osobowych w sposób niezgodny z przepisami o ochronie danych osobowych może stanowić okoliczność o istotnym znaczeniu dla ustalenia naruszenia prawa ochrony konkurencji czy prawa ochrony konsumentów[6]. Dostęp do danych osobowych, ich zbieranie, łączenie

[1] Autor jest członkiem Okręgowej Izby Radców Prawnych w Warszawie. ORCID: 0000-0002-8793-1902. Przedstawione w artykule opinie stanowią wyraz osobistych poglądów autora i nie powinny być utożsamiane ze stanowiskiem żadnej organizacji lub instytucji, z którą autor był lub jest powiązany.

[2] Dz.Urz. UE L Nr 265, s. 1; dalej jako: DMA lub Akt o rynkach cyfrowych.

[3] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final 2020/0374 (COD), s. 3.

[4] *M. Namysłowska*, Zwalczanie nieuczciwych praktyk handlowych między przedsiębiorcami w prawie Unii Europejskiej. W poszukiwaniu modelu ochrony, Warszawa 2022, s. 536.

[5] Zob. *U. Czarnomska-Bokowy*, Prawo konkurencji a projekt rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym – kto przypilnuje strażników?, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2022, Nr 1, s. 13.

[6] Zob. *I. Małobęcka-Szwast*, Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów, [w:] Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020 (red. *G. Sibiga*), MoP 2020, Nr 23, s. 92.

i analizowanie mogą sprzyjać wzmacnianiu pozycji rynkowej oraz negatywnie wpływać na konkurencję na rynkach cyfrowych, zwłaszcza w sytuacji, gdy przedsiębiorcy wykorzystują dane osobowe w sposób wykraczający poza cele, w których dane pierwotnie zebrano[7].

Nawet bez przeprowadzania pogłębionej analizy DMA możliwe jest stwierdzenie, że stosowanie tego rozporządzenia wpływa na operacje przetwarzania danych osobowych związane ze świadczeniem podstawowych usług platformowych. Treść niektórych przepisów oraz zastosowane konstrukcje, omówione w dalszej części artykułu, potwierdzają istnienie silnych związków między prawem ochrony danych osobowych a prawem ochrony konkurencji[8]. Doniosłe znaczenie w tym kontekście mają wzajemne relacje pomiędzy przepisami DMA a przepisami 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 (ogólnego rozporządzenia o ochronie danych)[9].

Zgodnie z motywem 12 DMA rozporządzenie to powinno mieć zastosowanie bez uszczerbku dla przepisów wynikających z innych aktów prawa UE regulujących niektóre aspekty świadczenia usług objętych DMA, w tym w szczególności przepisów RODO. Ponadto na podstawie art. 8 ust. 1 DMA, strażnicy dostępu są zobowiązani zapewnić, aby wdrożenie środków zapewniających przestrzeganie ich obowiązków ustanowionych w DMA było zgodne m.in. z przepisami RODO. Stosowanie jednak równocześnie przepisów obydwu rozporządzeń w niektórych wypadkach może okazać się problematyczne. Celowe jest zatem zbadanie obowiązków strażników dostępu związanych z przetwarzaniem danych osobowych oraz określenie wzajemnych relacji pomiędzy przepisami DMA a przepisami RODO, a także zidentyfikowanie wynikających z nich problemów interpretacyjnych i praktycznych oraz sformułowanie potencjalnych rozwiązań.

Strażnicy dostępu oraz podstawowe usługi platformowe

Kluczowe znaczenie dla ustalenia zakresu zastosowania przepisów DMA mają pojęcia strażnika dostępu oraz podstawowej usługi platformowej. W świetle definicji zawartej w art. 2 DMA strażnikiem dostępu jest „przedsiębiorstwo świadczące podstawowe usługi platformowe, które wskazano na podstawie art. 3". Jako strażnik dostępu może natomiast zostać wskazane przedsiębiorstwo, które łącznie spełnia trzy wymogi określone w art. 3 ust. 1 DMA. Przepisy DMA ustanawiają przy tym wzruszalne domniemania spełnienia przez przedsiębiorstwo poszczególnych wymogów warunkujących wskazanie go przez Komisję Europejską jako strażnika dostępu.

Pierwszym wymogiem jest wywieranie znaczącego wpływu na rynek wewnętrzny UE. Domniemywa się, że wymóg ten jest spełniony, jeżeli przedsiębiorstwo „uzyskało roczny obrót w Unii wynoszący co najmniej 7,5 mld euro w każdym z ostatnich trzech lat obrotowych lub jeżeli jego średnia kapitalizacja rynkowa lub równoważna rzeczywista wartość rynkowa wynosiła co najmniej 75 mld euro w ostatnim roku obrotowym oraz świadczy tę samą podstawową usługę platformową w co najmniej trzech państwach członkowskich". Drugie kryterium stanowi świadczenie podstawowej usługi platformowej będącej ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych. Spełnienie tego wymogu domniemywa się, jeżeli przedsiębiorstwo „świadczy podstawową usługę platformową, z której w ostatnim roku obrotowym korzystało co najmniej 45 mln aktywnych miesięcznie użytkowników końcowych mających siedzibę lub miejsce pobytu w Unii oraz co najmniej 10 000 aktywnych rocznie użytkowników biznesowych z siedzibą w Unii". Trzeci wymóg polega na zajmowaniu przez przedsiębiorstwo ugruntowanej i trwałej pozycji w zakresie prowadzonej przez siebie działalności lub możliwości przewidzenia, że zajmie taką pozycję w niedalekiej przyszłości. Domniemywa się jego spełnienie, jeżeli progi dotyczące drugiego wymogu zostały osiągnięte w każdym z ostatnich trzech lat obrotowych.

Przedsiębiorstwo, które osiągnęło progi pozwalające uznać spełnienie wymogów kwalifikujących je jako strażnika dostępu, jest zobowiązane do bezzwłocznego powiadomienia o tym Komisji. Wraz z powiadomieniem przedsiębiorstwo może jednak przedstawić argumenty podważające domniemania. Istotne jest również, że Komisja może w dowolnym momencie, na wniosek lub z własnej inicjatywy, ponownie rozpatrzyć, zmienić lub uchylić decyzję o wskazaniu przedsiębiorstwa jako strażnika dostępu. Ponadto Komisja regularnie, co najmniej raz na trzy lata, dokonuje przeglądu w celu ustalenia, czy strażnicy dostępu spełniają wymogi określone w art. 3 ust. 1 DMA, a także sprawdza, przynajmniej co roku, czy nowe przedsiębiorstwa świadczące podstawowe usługi platformowe spełniają te wymogi. Obowiązkiem Komisji jest również publikowanie i aktualizowanie na bieżąco wykazu strażników dostępu oraz wykazu podstawowych usług platformowych.

[7] Zob. *L. Taylor*, *H. Mukiri-Smith*, *T. Petročnik*, *L. Savolainen*, *A. Martin*, (Re)making data markets: an exploration of the regulatory challenges, Law, Innovation and Technology 2022, vol. 14, iss. 2, s. 379.

[8] Zob. *J. Tielemans*, The EU's DMA and DSA: Why this should be of interest to privacy pros, https://iapp.org/news/a/developments-on-the-dma-and-dsa-why-this-should-be-of-interest-to-privacy-professionals/ (dostęp 5.5.2023 r.).

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

Akt o rynkach cyfrowych zawiera w art. 2 pkt 2 szeroki katalog podstawowych usług platformowych. Obejmuje on usługi pośrednictwa internetowego, wyszukiwarki internetowe, internetowe serwisy społecznościowe, usługi platformy udostępniania wideo, usługi łączności interpersonalnej niewykorzystujące numerów, systemy operacyjne, przeglądarki internetowe, wirtualnych asystentów, usługi przetwarzania w chmurze, a także internetowe usługi reklamowe, w tym sieci reklamowe, giełdy reklamowe i inne usługi pośrednictwa w zakresie reklam, świadczone przez przedsiębiorstwo, które świadczy dowolne podstawowe usługi platformowe.

Ograniczenia przetwarzania danych osobowych użytkowników końcowych

Akt o rynkach cyfrowych wprowadza ograniczenia w zakresie przetwarzania przez strażników dostępu danych osobowych użytkowników końcowych. Dotyczą one niektórych czynności oraz podstaw prawnych, na których może opierać się przetwarzanie. W art. 5 ust. 2 DMA ustanowiono katalog czynności przetwarzania, które co do zasady nie mogą być dokonywane przez strażnika dostępu, chyba że występuje jedna z określonych podstaw prawnych. W ten sposób ograniczono dopuszczalność przetwarzania przez strażników dostępu danych osobowych użytkowników końcowych w stosunku do zasad ogólnych wynikających z przepisów RODO.

Stosownie do treści art. 6 ust. 1 RODO przetwarzanie danych osobowych jest zgodne z prawem, gdy istnieje co najmniej jedna spośród sześciu wymienionych w tym przepisie podstaw prawnych. Tymczasem czynności przetwarzania określone w art. 5 ust. 2 DMA mogą opierać się jedynie na czterech podstawach prawnych. Stanowią je zgoda oraz przesłanki uregulowane art. 6 ust. 1 lit. c, d i e RODO, tj. niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze, niezbędność do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a także niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W konsekwencji podstawą prawną realizacji czynności przetwarzania wymienionych w art. 5 ust. 2 DMA nie może być niezbędność do zawarcia umowy ani prawnie uzasadniony interes.

Wśród czterech czynności, których zgodnie z art. 5 ust. 2 DMA co do zasady nie może dokonywać strażnik dostępu, jako pierwszą wymieniono przetwarzanie do celów świadczenia internetowych usług reklamowych danych osobowych użytkowników końcowych, którzy korzystają ze świadczonych przez osoby trzecie usług wykorzystujących podstawowe usługi platformowe strażnika dostępu (art. 5 ust. 2 lit. a DMA). Rozwiązanie to ma w zamierzeniu unijnego prawodawcy niwelować potencjalną przewagę konkurencyjną uzyskiwaną przez strażników dostępu w związku z przetwarzaniem danych osobowych pochodzących od znacznie większej liczby użytkowników niż w wypadku innych przedsiębiorstw[10]. Przyjęta ostatecznie w toku prac legislacyjnych treść art. 5 ust. 2 lit. a DMA wzbudza jednak wątpliwości z perspektywy wyrażonej w RODO zasady ograniczenia celu przetwarzania[11]. Brzmienie tego przepisu, m.in. w angielskiej wersji językowej, może bowiem sugerować istnienie jednego, ogólnego celu przetwarzania danych polegającego na świadczeniu usług reklamowych[12]. Tymczasem funkcjonowanie reklamy internetowej w praktyce wiąże się z realizacją wielu czynności przetwarzania służących różnym celom. W konsekwencji istnieje potencjalnie możliwość podejmowania próby wykorzystania przez strażników dostępu treści art. 5 ust. 2 lit. a DMA jako argumentu uzasadniającego pozyskiwanie jednej, ogólnej zgody na przetwarzanie danych osobowych użytkownika końcowego w wielu różnych celach. Taka praktyka wzbudzałaby natomiast kontrowersje w kontekście wymogów dotyczących zgody wynikających z art. 7 RODO.

Zasadniczo, w świetle DMA nie jest ponadto dopuszczalne łączenie przez strażnika dostępu danych osobowych pochodzących z danej podstawowej usługi platformowej z danymi osobowymi pochodzącymi z innych podstawowych usług platformowych lub z dowolnych innych usług świadczonych przez strażnika dostępu lub z danymi osobowymi pochodzącymi z usług świadczonych przez osoby trzecie (art. 5 ust. 2 lit. b DMA). Akt o rynkach cyfrowych co do zasady zabrania również strażnikom dostępu logowania użytkowników końcowych do innych usług świadczonych przez strażnika dostępu, po to by łączyć dane osobowe (art. 5 ust. 2 lit. d DMA). Łączenie danych osobowych stanowi bowiem źródło uzyskiwania przez strażników dostępu przewagi konkurencyjnej[13]. Jednakże wprowadzenie zakazu w tym zakresie może niekorzystnie wpływać na bezpieczeństwo platform internetowych oraz realizację wynikającego z art. 32 ust. 1 RODO obowiązku wdrażania odpowiednich środków technicznych i organizacyjnych, zapewniających właściwy stopień bezpieczeństwa przetwarzania danych osobowych. Łączenie oraz porównywanie niektórych elementów danych służy bowiem wykrywaniu zagrożeń i zapobieganiu oszustwom lub innym,

[10] Akt o rynkach cyfrowych, motyw 36.

[11] Zob. *F. Pop*, The Digital Markets Act: more choice and improved data protection for users?, https://www.eipa.eu/blog/the-digital-markets-act-more-choice-and-improved-data-protection-for-users/ (dostęp 5.5.2023 r.).

[12] W angielskiej wersji językowej DMA użyto liczby pojedynczej („*purpose*") *„process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper*".

[13] Akt o rynkach cyfrowych, motyw 36.

niepożądanym działaniom[14]. Z reguły przetwarzanie danych osobowych w tym celu opiera się na prawnie uzasadnionym interesie (art. 6 ust. 1 lit. f RODO). Przepisy DMA wykluczają jednak możliwość powołania się na tę podstawę. W rezultacie, w praktyce konieczne może okazać się rozważenie przez strażników dostępu oparcia czynności łączenia danych osobowych na podstawie zgody, obowiązku prawnym, przesłance ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej albo interesie publicznym.

Kolejną czynność, której co do zasady nie może dokonywać strażnik dostępu, stanowi wykorzystywanie danych osobowych pochodzących z danej podstawowej usługi platformowej w ramach innych usług świadczonych oddzielnie przez strażnika dostępu, w tym innych podstawowych usług platformowych, i odwrotnie – wykorzystywanie danych osobowych pochodzących z takich innych usług w ramach podstawowej usługi platformowej (art. 5 ust. 2 lit. c DMA). Ograniczenie to odnosi się do sytuacji, w której strażnik dostępu odgrywa podwójną rolę – przedsiębiorstwa świadczącego na rzecz swoich użytkowników biznesowych podstawową usługę platformową (np. internetowe usługi reklamowe) oraz przedsiębiorstwa konkurującego z tymi samymi użytkownikami biznesowymi w oferowaniu takich samych lub podobnych usług lub produktów na rzecz tych samych użytkowników końcowych[15]. Zakaz ustanowiony w tym przepisie ma na celu uniemożliwienie strażnikom dostępu czerpania korzyści z pełnienia podwójnej roli. Dodatkowo, na podstawie art. 6 ust. 2 DMA, konkurując z użytkownikami biznesowymi, strażnik dostępu nie może wykorzystywać niedostępnych publicznie danych wygenerowanych lub dostarczonych przez użytkowników biznesowych w ramach korzystania przez nich z podstawowych usług platformowych lub usług świadczonych wraz z podstawowymi usługami platformowymi lub wspierających takie usługi, w tym danych wygenerowanych lub dostarczonych przez klientów użytkowników biznesowych. Dane niedostępne publicznie obejmują przy tym wszelkie zagregowane i niezagregowane dane wygenerowane przez użytkowników biznesowych, w tym m.in. dane dotyczące kliknięć, zapytań, wyświetleń i dane głosowe.

Zgoda użytkownika końcowego na niektóre czynności strażnika dostępu

Kluczowy z perspektywy strażników dostępu wyjątek od zakazu realizowania czynności wymienionych w art. 5 ust. 2 DMA wiąże się z zapewnieniem użytkownikom końcowym możliwości dokonania konkretnego wyboru i wyrażenia zgody w rozumieniu przepisów RODO. Konieczne jest zatem spełnienie przez strażników dostępu wymogów wynikających z art. 4 pkt 11 oraz art. 7 RODO. Koncepcja wykorzystania zgody jako zasadniczej podstawy dokonywania niektórych czynności określonych w DMA spotkała się z krytyką przedstawicieli doktryny oraz podmiotów prezentujących swoje stanowisko w toku prac legislacyjnych. W szczególności podnoszono, że poddanie otwarcia rynku danych wymogowi wyrażenia zgody przez użytkowników końcowych utrudni realizację głównych celów DMA[16]. Ponadto wskazywano, że rozwiązanie to może sprzyjać zjawisku tzw. zmęczenia zgodą (*consent fatigue*) oraz łatwemu pozyskiwaniu przez strażników dostępu zgód użytkowników końcowych[17]. Dostrzegano również trudności o charakterze technicznym związane z wdrożeniem efektywnych procesów wycofania zgody na wielu platformach i w wielu przedsiębiorstwach. Ponadto z uwagi na wyraźną dysproporcję sił pomiędzy użytkownikiem końcowym a strażnikiem dostępu wyrażano wątpliwości dotyczące możliwości zapewnienia faktycznej dobrowolności zgody.

Wymienione ryzyka w pewnym stopniu mogą zostać ograniczone w związku z zawarciem przez unijnego prawodawcę w preambule DMA wskazań odnoszących się do procesu zarządzania zgodami użytkowników końcowych. Zwrócono w niej w szczególności uwagę na powinność proaktywnego przedstawiania przez strażnika dostępu użytkownikowi końcowemu „przyjaznego dla użytkownika rozwiązania umożliwiającego wyrażenie, zmianę lub cofnięcie zgody w sposób wyraźny, jasny i prosty”[18]. Strażnicy dostępu powinni dawać użytkownikom końcowym możliwość swobodnego decydowania o uczestnictwie w praktykach polegających na wykonywaniu czynności określonych w art. 5 ust. 2 DMA. Służyć temu ma oferowanie mniej spersonalizowanego, ale równoważnego rozwiązania, a także nieuzależnianie korzystania z podstawowej usługi platformowej lub niektórych jej funkcjonalności od uzyskania zgody użytkownika końcowego[19]. Ponadto w momencie wyrażania zgody użytkownik końcowy powinien zostać poinformowany o skutkach jej niewyrażenia, w tym o otrzymaniu mniej spersonalizowanej oferty, a także o tym, że „podstawowa usługa platformowa pozostanie niezmieniona i że żadne funkcjonalności nie zostaną usunięte”. Wyjątek dotyczy sytuacji braku możliwości wyrażenia zgody bezpośrednio w ramach podstawowej usługi

[14] Zob. *B. Bellamy, A. Simpson*, How the EU Digital Markets Act Affects GDPR, https://www.lawyer-monthly.com/2022/08/how-the-eu-digital-markets-act-affects-gdpr/ (dostęp 5.5.2023 r.).

[15] Akt o rynkach cyfrowych, motywy 46 i 47.

[16] Zob. Bridging the DMA and the GDPR – Comments by the Centre for Information Policy Leadership on the Data Protection Implications of the Draft Digital Markets Act, s. 12, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_data_protection_implications_of_the_draft_digital_markets_act__6_dec_2021_.pdf (dostęp 5.5.2023 r.).

[17] Zob. *R. Podszun*, Should Gatekeepers Be Allowed to Combine Data? – Ideas for Art. 5(a) of the Draft Digital Markets Act, GRUR International 2022, vol. 71, iss. 3, s. 199.

[18] Akt o rynkach cyfrowych, motyw 37.

[19] Akt o rynkach cyfrowych, motyw 36.

platformowej strażnika dostępu. Wówczas wymagane jest umożliwienie użytkownikom końcowym wyrażenia zgody za pośrednictwem korzystającej z podstawowej usługi platformowej usługi świadczonej przez osobę trzecią, „aby zezwolić strażnikowi dostępu na przetwarzanie danych osobowych do celów świadczenia internetowych usług reklamowych”[20].

Pewne wątpliwości wzbudza treść art. 5 ust. 2 akapit drugi DMA, a zwłaszcza zawarte w nim sformułowanie dotyczące „wyrażenia zgody do celu akapitu pierwszego”[21]. Akapit pierwszy obejmuje bowiem cztery różne czynności mogące służyć realizacji wielu celów przetwarzania danych osobowych. Dlatego też w trakcie prac legislacyjnych podnoszono, że proponowana treść art. 5 ust. 2 akapit drugi DMA tworzy lukę prawną i stawia strażników dostępu w korzystnej sytuacji, umożliwiając im pozyskiwanie jednej, ogólnej zgody obejmującej wiele czynności oraz celów przetwarzania[22]. W tym samym przepisie wyraźnie ustanowiono jednak wymóg „zapewnienia możliwości dokonania konkretnego wyboru”. Umożliwienie wyrażenia zgody wyłącznie na wszystkie czynności określone w art. 5 ust. 2 DMA byłoby zatem niewystarczające. Zważywszy, że zgoda wyrażana przez użytkownika końcowego powinna spełniać wymogi wynikające z przepisów RODO, strażnik dostępu powinien umożliwić wyrażenie zgody na poszczególne czynności przetwarzania realizowane w określonych celach. Biorąc pod uwagę możliwości techniczne, którymi dysponują podmioty posiadające status strażników dostępu, uzasadnione jest również oczekiwanie zapewnienia odpowiedniej dostępności oraz jasnego i prostego języka.

Preambuła Aktu o rynkach cyfrowych zawiera również wskazania odnoszące się do cofnięcia zgody. Przede wszystkim powinno być ono równie proste co jej wyrażenie. Ponadto „strażnicy dostępu nie powinni projektować, organizować lub obsługiwać swoich interfejsów internetowych w sposób, który w drodze wprowadzenia w błąd, manipulacji lub w inny sposób istotnie zakłóca lub ogranicza zdolność użytkowników końcowych do swobodnego wyrażenia zgody”. Akt o rynkach cyfrowych ustanawia także ograniczenia w zakresie występowania przez strażników dostępu z wnioskiem o wyrażenie zgody. W świetle art. 5 ust. 2 akapit drugi DMA, jeżeli użytkownik końcowy odmówił wyrażenia zgody lub cofnął taką zgodę, strażnik dostępu nie może występować z ponownym wnioskiem o wyrażenie zgody do tego samego celu częściej niż raz w ciągu roku.

Szczegółowe wskazania dotyczące zarządzania zgodami użytkowników końcowych zawarte w preambule DMA nie gwarantują realizacji celów Aktu o rynkach cyfrowych, ale mogą mieć istotny wpływ na stosowanie przepisów rozporządzenia. Jeszcze większe znaczenie dla zapewnienia kontestowalności rynków cyfrowych oraz ochrony danych osobowych użytkowników będzie mieć jednak praktyka organów nadzorczych.

Zapewnienie możliwości przenoszenia danych

Jednym z instrumentów sprzyjających synergii pomiędzy prawem ochrony danych osobowych a prawem konkurencji jest uprawnienie do przenoszenia danych[23]. Dotychczas istniejące mechanizmy w tym zakresie były jednak niejednokrotnie oceniane w literaturze jako niewystarczające, aby przyczynić się do przeciwdziałania monopolizacji rynków cyfrowych przez duże platformy internetowe[24]. W Akcie o rynkach cyfrowych ustanowiono obowiązek zapewnienia przez strażnika dostępu możliwości przenoszenia danych dostarczonych przez użytkownika końcowego lub wygenerowanych przez użytkownika końcowego w ramach korzystania z podstawowej usługi platformowej. Stosownie do treści art. 6 ust. 9 DMA obowiązek ten obejmuje zapewnienie nieodpłatnych narzędzi ułatwiających przenoszenie danych oraz stałego dostępu do danych w czasie rzeczywistym. Uprawnienie do przenoszenia danych może być realizowane przez użytkownika końcowego oraz upoważnione przez niego osoby trzecie. W preambule DMA wskazano, że obowiązek zapewnienia skutecznego przenoszenia danych wynikający z przepisów tego rozporządzenia stanowi uzupełnienie prawa do przenoszenia danych osobowych uregulowanego w RODO[25]. Z uwagi na pewne elementy wspólne i powiązania pomiędzy obiema konstrukcjami ich analiza ma istotne znaczenie praktyczne.

Szczególnie wyraźna różnica pomiędzy porównywanymi instytucjami dotyczy zakresu ich zastosowania. W odróżnieniu od prawa do przenoszenia danych osobowych uregulowanego w art. 20 RODO obowiązek zapewnienia możliwości przenoszenia danych wynikający z art. 6 ust. 9 DMA obejmuje dane dostarczone przez użytkownika końcowego lub wygenerowane w toku działalności użytkownika końcowego w ramach korzystania z podstawowej usługi platformowej, a zatem nie tylko dane osobowe. Ponadto prawo osoby, której dane dotyczą, zostało w art. 20 ust. 1 RODO ograniczone do danych, które osoba ta „dostarczyła administratorowi”. Stosownie do treści wytycznych Grupy Roboczej Art. 29 sfor-

[20] Akt o rynkach cyfrowych, motyw 37.

[21] W angielskiej wersji językowej DMA: „*consent given for the purposes of the first subparagraph*”.

[22] Zob. EPC & DCN statement on the DMA, https://www.epceurope.eu/post/epc-dcn-statement-on-the-dma, https://www.epceurope.eu/post/epc-dcn-statement-on-the-dma (dostęp 5.5.2023 r.).

[23] Zob. *W. Kerber, L. Specht -Riemenschneider*, Synergies between Data Protection Law and Competition Law, s. 43, https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf (dostęp 5.5.2023 r.).

[24] Zob. *I. Graef, J. Prüfer*, Governance of data sharing: A law & economics proposal, Research Policy 2021, vol. 50, iss. 9, s. 12.

[25] Akt o rynkach cyfrowych, motyw 59.

mułowanie to oznacza, że uprawnienie osoby, której dane dotyczą, ma zastosowanie do danych osobowych „aktywnie i świadomie" przekazanych przez tę osobę, a także do danych osobowych, „które wynikają z obserwacji działań użytkowników, takich jak surowe dane przetwarzane przez inteligentny licznik lub inne rodzaje podłączonych obiektów, dzienniki aktywności, historia korzystania ze strony internetowej lub działań związanych z wyszukiwaniem"[26]. Zakres prawa do przenoszenia danych osobowych nie obejmuje jednak danych wywnioskowanych i pochodnych, tworzonych przez administratora na podstawie danych przekazanych przez osobę, której dane dotyczą[27]. Takie ograniczenie nie występuje natomiast w wypadku obowiązku strażnika dostępu określonego w art. 6 ust. 9 DMA. Pewien wpływ na zakres danych objętych zakresem analizowanych instytucji ma również podstawa prawna przetwarzania danych. Prawo do przenoszenia danych zgodnie z art. 20 ust. 1 RODO znajduje zastosowanie wyłącznie, gdy przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy. Tymczasem obowiązek zapewnienia możliwości przenoszenia danych wynikający z przepisów DMA istnieje również w wypadku przetwarzania danych osobowych na innej podstawie prawnej.

Kolejne różnice dotyczą szczegółowych warunków realizacji obydwu uprawnień. W Akcie o rynkach cyfrowych wyraźnie wskazano, że możliwość przenoszenia danych powinna być zapewniona przez strażnika dostępu nieodpłatnie. Natomiast zgodnie z art. 12 ust. 5 RODO na zasadzie wyjątku, „jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań".

W preambułach obydwu rozporządzeń zawarto ponadto wskazania odnoszące się do warunków technicznych realizacji uprawnień związanych z przenoszeniem danych. Również w tym zakresie dostrzegalne są różnice. W wypadku prawa do przenoszenia danych osobowych osoba, której dane dotyczą, powinna mieć możliwość otrzymania danych osobowych „w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego i interoperacyjnym formacie oraz przesyłania ich innemu administratorowi"[28]. Ponadto w preambule RODO postuluje się zachęcanie administratorów danych do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych[29]. Grupa Robocza Art. 29 wskazuje przy tym jako dobrą praktykę rozwijanie przez administratorów środków, które przyczynią się do odpowiadania na wnioski o przeniesienie danych takich jak narzędzia do pobierania danych oraz interfejsy programowania aplikacyjnego[30]. Znacznie dalej idące wymagania techniczne sformułowano natomiast w preambule DMA odnośnie do obowiązku zapewnienia możliwości przenoszenia danych. Dane powinny być otrzymywane w formacie umożliwiającym natychmiastowe uzyskanie do nich dostępu przez użytkownika końcowego lub osobę trzecią, do której są przenoszone[31]. Przede wszystkim jednak od strażników dostępu oczekiwane jest zapewnienie możliwości „ciągłego i przebiegającego w czasie rzeczywistym swobodnego przenoszenia danych", które jest realizowane „za pomocą odpowiednich i wysokiej jakości środków technicznych, takich jak interfejsy programowania aplikacyjnego"[32].

Z uwagi na liczne różnice dotyczące zwłaszcza zakresu zastosowania oraz warunków realizacji obydwu analizowanych uprawnień trudno jest podzielić stanowisko, że obowiązek zapewnienia możliwości przenoszenia danych stanowi jedynie uzupełnienie prawa do przenoszenia danych ustanowionego w RODO. W rzeczywistości uprawnienie przysługujące użytkownikowi końcowemu na podstawie art. 6 ust. 9 DMA jest znacznie bardziej rozbudowane w stosunku do prawa wynikającego z art. 20 RODO. Wyzwaniem może być w praktyce prawidłowa interpretacja intencji użytkownika końcowego występującego z żądaniem oraz właściwe jego zakwalifikowanie przez strażnika dostępu. Potencjalne rozwiązanie tego problemu mogłoby polegać w szczególności na wdrażaniu przez strażników dostępu rozwiązań technicznych umożliwiających informowanie w przejrzysty sposób użytkownika końcowego o obydwu uprawnieniach oraz dokonywanie świadomego wyboru prawa, z którego użytkownik chce skorzystać.

Zapewnienie dostępu do danych

Kolejny obowiązek strażników dostępu, który może mieć istotne znaczenie dla zapewnienia kontestowalności rynków cyfrowych, a jednocześnie uwidacznia rolę danych, w tym danych osobowych, został ustanowiony w art. 6 ust. 10 DMA. Przepis ten reguluje zapewnienie użytkownikom biznesowym i osobom trzecim przez nich upoważnionym dostępu do danych i możliwości korzystania z nich. Obowiązek zapewnienia dostępu obejmuje dane dostarczane lub generowane w ramach korzystania przez użytkowników biznesowych oraz przez użytkowników końcowych korzystających z produktów dostarczanych lub usług świadczonych przez użytkowników biznesowych z podstawowych usług platformowych lub usług świadczonych wraz z podstawowymi usługami platformowy-

[26] Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, s. 10.
[27] *Ibidem.*
[28] RODO, motyw 68.
[29] *Ibidem.*
[30] Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, s. 3.
[31] Akt o rynkach cyfrowych, motyw 59.
[32] *Ibidem.*

mi lub wspierających takie usługi. Stosownie do treści art. 6 ust. 10 DMA dostęp ten powinien być „skuteczny, wysokiej jakości i stały", a ponadto zapewniony w czasie rzeczywistym oraz ma obejmować dane zagregowane i niezagregowane, w tym dane osobowe. Jednakże w wypadku danych osobowych strażnik dostępu jest zobowiązany zapewnić dostęp i możliwość korzystania z nich wyłącznie, gdy są one „bezpośrednio powiązane z faktem korzystania przez użytkowników końcowych z produktów lub usług" oferowanych przez użytkownika biznesowego za pośrednictwem podstawowej usługi platformowej. Ponadto warunkiem udostępniania danych osobowych jest wyrażenie na to zgody przez użytkowników końcowych.

Podobnie jak w wypadku zapewnienia możliwości przenoszenia danych, również w odniesieniu do obowiązku zapewnienia dostępu do danych, unijny prawodawca zawarł w preambule DMA wskazania dotyczące warunków realizacji tego obowiązku. Przede wszystkim nie jest dopuszczalne stosowanie przez strażnika dostępu jakichkolwiek ograniczeń, w tym w szczególności umownych, w celu uniemożliwienia użytkownikom biznesowym dostępu do danych[33]. Ponadto strażnik dostępu powinien umożliwiać użytkownikom biznesowym uzyskanie zgody użytkowników końcowych na udzielenie dostępu, jeśli jest ona wymagana. Zapewnienie stałego dostępu do danych w czasie rzeczywistym powinno być realizowane za pomocą odpowiednich środków technicznych, takich jak np. interfejsy programowania aplikacyjnego oraz zintegrowane narzędzia dla „drobnych użytkowników biznesowych"[34].

Regulacja zawarta w art. 6 ust. 10 DMA wzbudza liczne wątpliwości w kontekście ochrony danych osobowych. Ograniczenie zakresu zastosowania obowiązku zapewnienia dostępu do danych „bezpośrednio powiązanych z faktem korzystania przez użytkowników końcowych z produktów lub usług" koresponduje z uregulowaną w art. 5 ust. 1 lit. c RODO zasadą minimalizacji danych. Jednakże poważnym wyzwaniem może być w praktyce określenie, które dane są „bezpośrednio powiązane". Ponadto, wobec braku precyzyjnej regulacji w części normatywnej DMA oraz ewentualnych wskazań w jego preambule, kwestię dyskusyjną może stanowić interpretacja sformułowania „dane dostarczane lub generowane w ramach korzystania". Zwłaszcza zakres drugiej kategorii wydaje się niejasny. Nie jest bowiem oczywiste, czy zakres obowiązku udostępnienia danych obejmuje poza danymi przekazanymi przez użytkownika również np. dane wynikające z obserwacji działań użytkowników, dane wywnioskowane i pochodne, tworzone na podstawie danych przekazanych przez użytkownika końcowego[35]. Z perspektywy strażników dostępu konkurujących z użytkownikami biznesowymi niewątpliwie korzystne jest ograniczenie do minimum zbioru danych podlegających udostępnieniu. Z uwagi na sprzeczne interesy określenie zakresu danych objętych obowiązkiem udostępnienia może zatem stanowić w praktyce przedmiot sporu pomiędzy strażnikami dostępu oraz użytkownikami biznesowymi.

Potencjalnym źródłem napięć w relacjach pomiędzy strażnikami dostępu a użytkownikami biznesowymi może być również ustalenie treści i sposobu wyrażenia przez użytkowników końcowych zgody na udostępnienie danych. Trudności w tym zakresie wynikają m.in. z faktu, że udostępnienie danych na podstawie art. 6 ust. 10 DMA może obejmować różne zbiory danych i cele przetwarzania, w których dane wykorzystują użytkownicy biznesowi. Natomiast w świetle wymogów wynikających z przepisów RODO użytkownicy końcowi powinni zostać poinformowani o „tożsamości administratora oraz zamierzonych celach przetwarzania danych osobowych", a ponadto oświadczenie o wyrażeniu zgody powinno mieć „zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem"[36]. W tym kontekście dużym wyzwaniem może okazać się w praktyce wdrażanie przez strażników dostępu odpowiednich rozwiązań technicznych, umożliwiających użytkownikom biznesowym uzyskiwanie zgód spełniających wymogi ustanowione w RODO.

W art. 6 ust. 11 DMA uregulowano ponadto obowiązek zapewnienia „przedsiębiorstwu będącemu dostawcą wyszukiwarek internetowych, które jest osobą trzecią" dostępu do „danych dotyczących plasowania, zapytań, kliknięć i wyświetleń związanych z nieodpłatnym i płatnym wyszukiwaniem, wygenerowanych przez użytkowników końcowych przy wykorzystaniu jego wyszukiwarek internetowych". Ustanowiono przy tym wymóg poddania anonimizacji wszelkich danych wyszukiwania będących danymi osobowymi. Realizacja skutecznej anonimizacji danych stanowi poważny problem praktyczny, a udostępnianie danych wyszukiwania może wiązać się z ryzykiem ponownej identyfikacji osoby, której dane dotyczą. Na to ryzyko zwrócił uwagę w toku prac legislacyjnych m.in. EIOD[37], rekomendując uwzględnienie w motywach DMA wskazania, zgodnie z którymi strażnik dostępu powinien być w stanie wykazać, że zanonimizowane dane dotyczące zapytań, kliknięć i wyświetleń zostały odpowiednio przetestowane pod kątem ewentualnych zagrożeń związanych z ponowną identyfikacją[38].

W preambule DMA określono ogólne warunki dotyczące dokonywania anonimizacji danych osobowych. W szczególności wskazano, że odpowiednia anomimizacja polega na

[33] Akt o rynkach cyfrowych, motyw 60.
[34] *Ibidem*.
[35] Zob. Bridging the DMA and the GDPR..., s. 9.
[36] RODO, motyw 42.
[37] Europejski Inspektor Ochrony Danych.
[38] Zob. EDPS, Opinion 2/2021 on the Proposal for a Digital Markets Act, s. 12.

nieodwracalnej zmianie danych osobowych w taki sposób, że „informacje nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, lub gdy dane osobowe zostały zanonimizowane w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można ich zidentyfikować”[39]. Ponadto zawarto wskazanie, w świetle którego strażnik dostępu powinien zapewnić ochronę „przed zagrożeniami związanymi z deanonimizacją, za pomocą odpowiednich środków, takich jak anonimizacja takich danych osobowych, bez znacznego obniżania jakości lub przydatności danych”[40]. Treść preambuły DMA może w pewnym stopniu przeciwdziałać praktyce nadmiernego ograniczania zakresu i modyfikacji danych wyszukiwania podlegających udostępnieniu, jednak sposób realizacji anonimizacji danych może być przedmiotem sporu pomiędzy strażnikami dostępu, a dostawcami wyszukiwarek.

Informowanie o praktykach w zakresie profilowania

Akt o rynkach cyfrowych wprowadza również nowe obowiązki strażników dostępu związane z profilowaniem konsumentów. Stanowią one kolejny element złożonego systemu norm prawnych odnoszących się do transparentności algorytmicznego przetwarzania danych osobowych[41]. Poza przepisami DMA w wypadku stosowania przez strażników dostępu profilowania konieczne może okazać się również uwzględnienie m.in. obowiązków określonych w art. 13, 15 i 22 RODO, a także obowiązków dostawców usług pośrednich w zakresie przejrzystości wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)[42].

Na podstawie art. 15 ust. 1 DMA strażnik dostępu powinien w terminie sześciu miesięcy od dnia wskazania przedsiębiorstwa jako strażnika dostępu przedłożyć Komisji Europejskiej „poddany niezależnemu audytowi opis technik profilowania konsumentów, z których korzysta w odniesieniu do lub w ramach świadczonych przez siebie podstawowych usług platformowych wymienionych w decyzji o wskazaniu”. Opis ten Komisja przekazuje następnie EROD[43]. Ponadto stosownie do treści art. 15 ust. 3 DMA obowiązkiem strażnika dostępu jest publiczne udostępnienie podsumowania opisu poddanego audytowi, a także aktualizowanie opisu i podsumowania co najmniej raz w roku. Istotne znaczenie dla zawartości udostępnianego publicznie podsumowania może mieć wynikające z przepisów Aktu o rynkach cyfrowych uprawnienie strażnika dostępu „do uwzględnienia konieczności zachowania swoich tajemnic handlowych”.

Regulacja zawarta w art. 15 DMA ma na celu zapewnienie przejrzystości oraz wywieranie presji na strażników dostępu, skłaniającej ich do ograniczenia stosowania „głębokiego profilowania konsumentów”[44]. W preambule tego rozporządzenia zawarto wskazania dotyczące treści opisu założeń profilowania. Powinien on obejmować informację o przetwarzaniu danych osobowych, o celu sporządzania i wykorzystywania profilu, czasie profilowania, wpływie na usługi świadczone przez strażnika dostępu, krokach podejmowanych w celu zapewnienia użytkownikom końcowym wiedzy na temat wykorzystania profilowania, a także krokach podejmowanych w celu uzyskania ich zgody lub w celu zapewnienia im możliwości odmowy lub cofnięcia zgody[45].

Podsumowanie

Akt o rynkach cyfrowych ustanawia liczne obowiązki strażników dostępu związane z przetwarzaniem danych osobowych. Ich realizacja może w praktyce okazać się poważnym wyzwaniem i wzbudzać kontrowersje. Wynika to z faktu, że stosowanie niektórych przepisów DMA prawdopodobnie będzie napotykać problemy interpretacyjne oraz trudności o charakterze technicznym. Mogą one występować zwłaszcza w kontekście próby realizacji obowiązków strażników dostępu wynikających z DMA bez uszczerbku dla przepisów RODO. Ponadto z uwagi na nieprecyzyjność regulacji przynajmniej do momentu opublikowania wytycznych lub stanowisk organów nadzorczych, a także ewentualnych rozstrzygnięć w postępowaniu przed Trybunałem Sprawiedliwości interpretacja przepisów DMA może być przedmiotem licznych sporów pomiędzy strażnikami dostępu a użytkownikami biznesowymi i użytkownikami końcowymi.

[39] Akt o rynkach cyfrowych, motyw 61.
[40] *Ibidem*.
[41] Zob. *M. Eifert, A. Metzger, H. Schweitzer, G. Wagner*, Taming the giants: The DMA/DSA package, Common Market Law Review 2021, vol. 58, iss. 4, s. 1016.
[42] Dz.Urz. UE L Nr 277, s. 1 – tzw. Akt o usługach cyfrowych.
[43] Europejska Rada Ochrony Danych.
[44] Akt o rynkach cyfrowych, motyw 72.
[45] *Ibidem*.

Słowa kluczowe: dane osobowe, Akt o rynkach cyfrowych, strażnicy dostępu, podstawowa usługa platformowa, przenoszenie danych, profilowanie.

Selected obligations of gatekeepers in the light of the Digital Markets Act from a perspective of personal data protection

In recent years, digital services and in particular online platforms have played an increasingly important role in the European and global economy. Opportunities created by platform services, combined with potential ill practices of enterprises providing these services, can adversely affect competition and the fundamental rights of end users. There is also a perceivable problem of control of important ecosystems in the digital economy by few large platforms, which are referred to as gatekeepers. In response to these challenges, European Union bodies are setting up a new legal framework to create a more secure digital space and a fair play field to foster innovation, economic growth and competitiveness. Bearing in mind the fact that data, and in particular personal data, is a key asset for the digital economy, new legislation also establishes obligations related to the processing of personal data. Among the recently adopted regulations, the Digital Markets Act (DMA) plays an important role. The purpose of this article is to identify the key obligations of gatekeepers relating to the processing of personal data arising from the provisions of DMA, to identify the interplay between the provisions of the Digital Markets Act and the provisions of the GDPR and the challenges arising from it, and to attempt to clarify doubts.

Keywords: personal data, Digital Markets Act, gatekeepers, core platform service, data portability, profiling.

Commentary of confirmation to the judgement of the Voivodship Administrative Court in Łódź of 30 November 2021, Ref. No. I SA/Łd 699/21

Gracjan Ciupa[1]

The subject of this commentary is the judgement of the Voivodship Administrative Court (WSA) in Łódź of 30 November 2021, ref. I SA/Łd 699/21. This judgement concerns the interpretation of the Director of the National Fiscal Information of 27 July 2021. The tax authority interpreted Article 22(14) of the Personal Income Tax Act of 26 July 1991, in accordance with which it held that the purchase of electrical energy necessary for the operation of cryptocurrency mining hardware and the purchase of computer equipment for the construction of cryptocurrency mining hardware should not qualify as tax-deductible costs for the paid disposal of virtual currency. The author of the commentary takes a position in line with the judgement of the WSA, which recognizes these expenses as tax-deductible costs. The commentary presents, among other things, the author's views on the "directness" of the costs and regulations of cryptocurrencies.

Introduction

In the judgement of 30 November 2021, the Voivodeship Administrative Court in Łódź[2] ruled that expenses incurred for creation of virtual currency should be qualified as expenses incurred directly for purchasing virtual currency, and they are tax-deductible costs of its disposal for consideration in a sense of Article 22(14) of the Personal Income Tax Act of 26 July 1991[3].

Definitions used in the commentary

To avoid misunderstandings, I would like to start by defining a few terms. First of all, the term *virtual currency* used in my text is drawn from Article 2(2) point 26 of the Anti-Money Laundering Act of 1 March 2018[4] and means: "a digital image of values other than:

1) legal tender issued by the National Bank of Poland, foreign central banks or other public authorities,
2) an international unit of account established by an international organisation and accepted by individual countries belonging to or cooperating with that organisation,
3) electronic money within the meaning of the Payment Services Act of 19 August 2011,
4) a financial instrument within the meaning of the Act of 29 July 2005 on trading in financial instruments,
5) a bill of exchange or cheque".

This definition is very wide and may cause problems while using it in practice. For this commentary, it is sufficient, as it can easily be considered that cryptocurrencies are, in principle, virtual currencies. This is reflected in the explanatory memorandum to the anti-money laundering law. "The lawmakers intended to include both so-called cryptocurrencies and centralised virtual currencies within the scope of this definition"[5]. At this stage of consideration, it is worth to distinguish between virtual currency and digital money as it is known to civil law. The doctrinal definition of this concept is as follows: "digital money is a monetary value that is the electoral equivalent of cash marks. It is stored on electronic storage media and issued on a contractual basis by banks or digital money institutions in exchange for cash of a nominal value not less than that value. It is expressed in monetary units and must be exchanged for cash by the issuer upon request. The issuance of digital money takes the form of a payment instrument, i.e., a personalised device or a set of procedures agreed upon between the user and the issuer of e-money used to make a payment order"[6].

The main difference between virtual currency and digital money is that digital money must be exchanged for cash on demand. It is also worth noting that both virtual currency and digital money are not legal tenders in the territory of the Republic of Poland. As such, they do not have a legal power to write off liabilities. Consequently, their use in business transactions requires at least the implied consent of both the creditor and the debtor[7].

State of facts

The petitioner bought the necessary equipment to mine virtual currency in 2018 and he connected it on his own in

[1] Faculty of Law, Administration and Economics University of Wrocław. ORCID: 0000-0002-5687-1732.

[2] I SA/Łd 699/21

[3] Dz.U. z 2022 r. poz. 2647.

[4] Dz.U. z 2022 r. poz. 593.

[5] See: https://mycompanypolska.pl/artykul/waluta-wirtualna-a-kryptowaluta-czym-sie-roznia/7904 (access 27.12.2022).

[6] *Z. Radwański, A. Olejniczak, J. Grykiel*, Zobowiązania – część ogólna, Warszawa 2022, s. 64–65.

[7] *Ibidem.*

a way which enables him to mine virtual currency, in that case mostly Ethereum. His mining hardware gains force of approximately 110 Mh/s, requires 490W and downloads 11,76 kWh per day. As a result, his hardware mines daily about 0,006 ETH, which according to the currency exchange rates on 22 November 2021 after converting is $24. Concerning that activity, he incurred the following expenses: computer bought in 2018 worth PLN10 133,56 and value of buying electrical energy worth PLN5982,61, which is essential for mining virtual currency. The petitioner does not have a separate electricity meter but based on his voltmeter it takes a lot of electrical energy to charge the mining hardware. Obtaining virtual currency, he exchanges it for different ones, e.g. Bitcoins. He mines virtual currency to sell it, when the exchange rate is satisfactory for him. Until 30 November 2021, he did not exchange any amount of virtual currency. Since 2018 he filed a tax return using PIT-37 form because he did not conduct any economic activity. Moreover, he pointed out that because of his lack of knowledge of the opportunity to qualify expenses of mining hardware and electrical energy as tax-deductible costs, he has not deducted those expenses. What is more, he has got VAT invoices, which document the fact of buying the computer and using electrical energy.

Administrative procedures

The petitioner put a question to the Director of the National Fiscal Information: "1) Are expenses incurred in connection with mining virtual currency? (For example, buying computers destined for building virtual currency mining hardware is an expense in a sense of Article 22(14) of the Personal Income Tax Act); 2)) Are expenses incurred in connection with mining virtual currency? (For example, buying electrical energy, which is necessary for the work of mining hardware, is an expense in a sense of Article 22(14) of the Personal Income Tax Act. In the mind of the petitioner those expenses are expenses in a sense of Article 22(14) of the Personal Income Tax Act.)". The Director of the National Fiscal Information has a different opinion from the petitioner and considers the previous opinion to be wrong.

The Director of the National Fiscal Information pointed out that the revenue from trading virtual currency is the revenue of monetary capital in a sense of Article 17(1) point 11 of the Personal Income Tax Act of 26 July 1991. Moreover, he wrote that expenses incurred directly for purchasing virtual currency are a purchase price, but also a commission charged by a person broking in trading. In the decision of the Director of the National Fiscal Information, in contrast, a tax-deductible cost of virtual currency disposal for consideration is not an expense incurred indirectly. The catalogue of those expenses in that decision is closed and includes purchasing the computer, purchasing electrical energy, and the expenses of buying "cryptocurrency mining hardware", because it is impossible to determine which expense is affiliated to which revenue. Secondly, the Director of the National Fiscal Information has doubts in regard to purchasing virtual currency. The authority's second argument was that the applicant would not be purchasing virtual currency from another entity but would be performing the initial mining of the currency, which by analogy compares to manufacturing. A mined currency has never been a part of trade flows, because it had not existed before. In the opinion of the Director of the National Fiscal Administration, it was assessed that if the legislator had intended to allow the taxpayer to account for all forms of entry into possession of virtual currency he would have made an appropriate entry into the law. Therefore, the applicant referred the matter to the Voivodship Administrative Court in Łódź.

The judgement of the Voivodship Administrative Court in Łódź

The Voivodship Administrative Court in Łódź ruled that the decision of the Director of the National Fiscal Information is incorrect and considered a defiance of material law in Article 22(14) of the Personal Impact Tax Act of 26 July 1991, through a wrong explanation of that article. The Voivodship Administrative Court in that case used a linguistic form of explanation and quoted a definition of the word *directly* from the Dictionary of the Polish language. Viewed against it, there is no doubt that *directly* means without any intermediary and that the expenditure incurred by the appellant is incurred directly for its acquisition. The issue also arose as to whether mining virtual currency could be considered an acquisition within the meaning of the provision. The court concluded that according to the director's interpretation, the applicant is not purchasing the currency from another entity, but rather mining it. Thus, he may be considered to be making an acquisition, but only a primary one.

The opinion of the glossator

In my opinion, the judgment of the Voivodship Administrative Court in Łódź should be regarded as correct. At the beginning of 2019, the taxation of revenue from paid disposal of virtual currency was introduced into the Personal Income Tax Act of 26 July 1991, creating a closed catalogue of them. The Director of the National Fiscal Information certified in its Individual Interpretations that expenses for the creation of virtual currency should not be qualified as expenses incurred directly for purchasing virtual currency (Compare Individual Interpretation from 2021-07-27 (Director of the National Fiscal Information) 0113-KDIPT2-1.4011.414.2021.2.MGR and Individual Interpretation from

2020-05-15 (Director of the National Fiscal Information) 0111-KDIB1-1.4010.116.2020.1.SG). A contrary standpoint is presented by the Voivodship Administrative Courts. According to them, expenses for the creation and mining virtual currency should be qualified as expenses incurred directly for purchasing virtual currency (see the judgment of the Voivodship Administrative Court in Łódź of 21 July 2020[8]).

Given these discrepancies, I think that the most important thing is to define the meaning of words *direct* and *purchasing* used by the legislator and whether, because of this, cryptocurrency mining expenses have both characteristics.

Beginning with the directness – I believe that the expenses of cryptocurrency mining can be defined as costs that have the attribute of directness through linguistic interpretation already. Here I will use the rule of presumption of the special language and reach to the accounting. According to its principles, every cost is an expense, but not every expense is a cost. Therefore, the considerations concerning the costs will certainly regard the expenses, because the term *cost* has fewer designations than the term *expense*, and in this case, I can limit my considerations to the term of direct costs. To sum up, there are two reasons why I can replace *expense* with *cost*. First and foremost, the lawmaker mixed both of these words in Act because it defines *cost* using *expense*, for example in Article 22(14) of the Personal Impact Tax Act of 26 July 1991. I know that there is a difference between both of these words, but since the lawmaker did not contribute to differentiate it clearly, I am authorised to do something similar in my deliberations. Secondly, what I mentioned before, each cost is an expense – according to that rule, every analysis of costs involves expenses too. The most important target of that paragraph is making evident what *directness* means.

Moving on to the considerations – B. Micherda in *Podstawy rachunkowości* defines *direct costs* as "operating costs that are directly related to the product being manufactured"[9]. Given this definition, costs of purchasing computer and electrical energy are direct costs, because they are a direct connection to the product being manufactured, which in this case is cryptocurrency. This would not be possible without them. Moreover, as an analogy, in this case, the presumption of legal language and the Accounting Act of 29 September 1994[10] can be used. Admittedly, in this case, the term *direct costs* appears in connection with the concept of costs of manufacturing a product, yet in my opinion, there is no doubt that cryptocurrencies are manufactured by miners. According to this Act, direct costs include "the value of direct materials used, acquisition and processing costs directly related to production, and other costs that are incurred in bringing the product to the form and place in which it is located at the date of valuation." Accordingly, cryptocurrencies are produced by harnessing the calculating power of a computer, which in broad terms is converted into cryptocurrency. Hence, by way of analogy, this can be likened to the material from which the commodity is produced under the Accounting Act of 29 September 1994. Therefore, the electricity and the computer could be regarded as acquisition and processing costs directly related to production, and thus classified as a direct cost. In this case, the Voivodship Administrative Court used a decidedly more secure option, justifying its position with the definition from the Dictionary of the Polish Language.

Moving on to the second issue that may have caused controversy, which is the matter of purchasing virtual currency by miners. In this case, only the systemic approach gives satisfactory results. One of the principles of tax law is the ability to tax income, not revenue. Therefore, if the costs of cryptocurrency excavation could not be considered tax costs, miners would be deprived of that right, because the basis of taxation of their activity would be income, not revenue. Of course, I am aware that the systemic interpretation is not used in the first place, but according to the *In dubio pro tributario* principle and given the ambiguous standardisation of the situation of "miners" of cryptocurrencies, this is an argument in favour of considering the expenses associated with mining cryptocurrency as tax-deductible costs for their disposal against payment. This statement was shared in J. Wirski's paper *Opodatkowanie obrotu kryptowalutami na gruncie podatków dochodowych w świetle zmian od 1.01.2019 r. – zagadnienia praktyczne*[11]. In this case, the Voivodship Administrative Court referred to the situation of a person who acquired the ownership of a movable no-man's land by taking it into their possession, or a person who manufactured the movable from their materials. In this case, I also share the court's standpoint, which can be seen in the example of the definitions of *direct costs* I have cited.

Moreover, as Robert Kurek rightly points out in his work *Pieniądz prywatny – status Bitcoina w Niemczech*, the status of cryptocurrency mining hardware in Germany is much better regulated. According to the terminology there, "miners" do not purchase cryptocurrency, but mine it. Miners can be either individuals or business entities that professionally engage in this practice. Income is earned on the day the bitcoin is dug, and its value is determined by the purchase price. Individuals can take advantage of the free amount of €256. In addition, the German legislator has allowed reducing the tax base by the cost of purchasing the mining equipment and the electricity consumed, which must be documented. As the above example shows, it is possible to uniformly define the

[8] I SA/Łd 285/20, Legalis.

[9] *B. Micherda,* Podstawy rachunkowości. Aspekty teoretyczne i praktyczne, Warszawa 2022.

[10] Dz.U. z 2021 r. poz. 217.

[11] *J. Wirski,* Opodatkowanie obrotu kryptowalutami na gruncie podatków dochodowych w świetle zmian od 1.1.2019 r. – zagadnienia praktyczne, Przegląd Podatkowy 2019, Nr 1, s. 41–48.

problem which was the subject of the ruling referred to in the commentary[12]. Postulating *de lege feren*da, I hope that in the foreseeable future there will be an amendment of these provisions in our tax law system.

Furthermore, being aware that the website of the Minister of Finance is not a source of law in the formal sense[13], I would like to dwell on it for a moment. On this website, you will find the guide *Settlement from the sale of cryptocurrencies*. Admittedly, the case which is the subject of the commentary has not yet involved the sale of cryptocurrency, but the facts described there are very similar. Under the subsection *Deductible costs*, it states: "If you obtain virtual currencies through so-called digging, you may not consider as deductible costs the expenses incurred for: the purchase of equipment intended for the digging of virtual currency or the purchase of electricity consumed in connection with the use of equipment for digging"[14]. This shows that the tax administration, despite the rulings of the administrative courts that are unfavourable to it, is still keen to convince the doctrine of its position vis-à-vis deductible costs from the sale of dug-up cryptocurrency. These actions are fully justified, as each authority will, in principle, convince other authorities to adopt its point of view. However, because of the position taken by the Voivodship Administrative Court, this is very difficult, especially as there has been no change in the legal position since the ruling which is the subject of the commentary. The actions of the Ministry of Finance are only like soft law at its weakest.

In abstracto, I believe that the legislator in the above-mentioned provision presented a too general way of classifying tax-deductible costs of paid disposal of virtual currency. In my view the previous regulation was better, the wording of which is as follows: "expenses for the purchase of a computing service that will be used to mine cryptocurrencies (...) may be deductible costs if they are indeed in a causal relationship with the revenues obtained". (See Individual Interpretation from 2018-10-19 (Director of the National Fiscal Information) 0112-KDIL3-1.4011.350.2018.1.AN.). Here, it is obvious that the purchase of a computer as well as electricity is closely connected with the sale of cryptocurrency, as there is no doubt that without these tools cryptocurrency would not have been formed. Furthermore, I also take a negative view towards the definition that is used in the Impact Tax Act. It is taken from Article 2(2) point 26 of the Act on Anti-Money Laundering and Financing of Terrorism of 1 March 2018. According to this definition, "coins" from the game FIFA 23, or more precisely FIFA Ultimate Team, can be considered virtual currency. I believe that legislators should create separate detailed regulations because they are becoming an increasingly important element of economic turnover and sanctioning them along with other virtual currencies can lead to abuse.

To sum up, the judgement of 30 November 2021, ruled by the Voivodship Administrative Court in Łódź is correct and should be used to create a line of case law and line of administrative decisions.

[12] *R. Kurek*, Pieniądz prywatny – status Bitcoina w Niemczech, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu 2017, Nr 478 s. 280–290.

[13] *W. Gromski*, Formalne źródła prawa, [w:] *A. Bator* (red.), Wprowadzenie do nauk prawnych. Leksykon tematyczny, Warszawa 2016, s. 243–244.

[14] See: ttps://www.podatki.gov.pl/pit/rozliczenie-ze-sprzedazy-kryptowalut/ (access 27.12.2022).

beckakademia

HARMONOGRAM SZKOLEŃ

- Postępowanie rozpoznawcze po zmianach KPC z 9.03.2023 r.,
  2 czerwca 2023, SSO dr Łukasz Zamojski

- PAKIET 2 SZKOLEŃ KPC: Postępowanie cywilne po zmianach z 9.03.2023 r.,
  2 i 22 czerwca 2023, SSO dr Łukasz Zamojski

- Nowa ustawa o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta w praktyce,
  6 czerwca 2023, Bernadeta Skóbel

- Postępowanie restrukturyzacyjne w praktyce,
  13 czerwca 2023, SSR Cezary Zalewski

- Rewolucyjne zmiany w prawie pracy 2023 r.,
  14 czerwca 2023, dr Anna Kamińska-Pietnoczko

- Mobbing w organizacji w świetle nowych wymogów prawnych,
  16 czerwca 2023, dr Anna Kamińska-Pietnoczko

- Ochrona danych osobowych w sekretariatach sądów powszechnych – praktyczne aspekty,
  19 czerwca 2023, Katarzyna Sandecka

- Upadłość konsumencka w praktyce,
  19 czerwca 2023, SSR Cezary Zalewski

- Obowiązki profesjonalnych pełnomocników po zmianach KPC z 9.03.2023 r.,
  20 czerwca 2023, SSR Artur Żuki

- Mobbing w organizacji – zapobieganie, przeciwdziałanie, reagowanie,
  21 czerwca 2023, Iwona Kordjak

- Postępowanie cywilne po zmianach z 9.03.2023 r.,
  22 czerwca 2023, SSO Grzegorz Karaś

- Kredyty i ugody frankowe w praktyce – z uwzględnieniem wyroków TSUE z 15.6.2023 oraz najnowszego orzecznictwa SN
  28 czerwca 2023, dr Łukasz Węgrzynowski

- Zabezpieczenia umowne w praktyce – weksel, poręczenie, zastaw, gwarancje, zabezpieczenia, egzekucja,
  30 sierpnia 2023, r. pr. Katarzyna Niekrasz-Gierejko

- Kara umowna w praktyce,
  7 września 2023, SSO dr Łukasz Zamojski

- Zakładowy Fundusz Świadczeń Socjalnych 2023 w praktyce,
  11 września 2023, Marek Rotkiewicz

- Darowizna w prawie cywilnym i podatkowym w praktyce,
  12 września 2023, r. pr. Katarzyna Siwiec

- Czas pracy kierowców samochodów osobowych w jednostkach samorządu terytorialnego w praktyce
  18 września 2023, Marek Rotkiewicz

- Wycena usług księgowych i doradców podatkowych. Negocjacje i rozmowy o pieniądzach z klientem biura rachunkowego
  21 września 2023, Iwona Kordjak

Aktualna lista szkoleń i zapisy:

akademia.beck.pl

WYMOGI EDYTORSKIE:

- język publikacji: polski, angielski, niemiecki, rosyjski;
- edytor tekstu Word (format .doc lub .docx);
- styl czcionki: Times New Roman;
- wielkość czcionki: tekst główny – 12 pkt, przypis – 10 pkt;
- interlinia: 1,5 wiersza (w przypadku przypisów – 1 wiersz);
- objętość artykułu: do 30 000 tys. znaków ze spacjami;
- marginesy: standardowe – wszystkie 2,5 cm;
- przypisy dolne: odsyłaczami przypisów powinny być cyfry arabskie; odsyłacz należy umieścić bezpośrednio po fragmencie, do którego odnosi się przypis (przed kropką kończącą zdanie);
- należy dołączyć słowa kluczowe w języku polskim i angielskim;
- tytuł powinien być napisany czcionką Times New Roman 14 pkt (czcionka pogrubiona);
- tekst powinien składać się z następujących części: lid (streszczenie ok. 1500 znaków ze spacjami), uwagi wstępne, rozwinięcie (z podziałem na zatytułowane części), podsumowanie;
- do artykułu należy załączyć także lid (streszczenie) w języku angielskim (ok. 1500 znaków ze spacjami);
- śródtytuły nie powinny być numerowane, lecz pogrubione;
- należy dołączyć notę biograficzną (ok. 800 znaków ze spacjami);
- prosimy o wskazanie afiliacji.

Powoływane w przypisach pozycje bibliograficzne prosimy pisać według wzoru:

Inicjał. Nazwisko, Tytuł, ew. numer wydania, tom, część itp., miejsce i rok wydania, a następnie cytowane strony skrótem „s.", np.: *J. Kowalski*, Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku kolejnego powołania się **bezpośrednio** na cytowaną pozycję:

Ibidem, s. 15–16.

Powołanie kolejny raz, gdy cytujemy tylko jedną pozycję danego autora:

J. Kowalski, *op. cit*., s. 29–20.

Kolejne powołanie, gdy cytuje się kilka pozycji danego autora, zawiera pierwsze wyrazy tytułu, np.:

J. Kowalski, Jak pisać..., s. 28–29.

W przypadku **prac pod redakcją**, jeśli powoływana publikacja stanowi część całości:

P. Igrek, Cytowanie, [w:] *J. Kowalski* (red.), Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku publikacji w czasopismach tytuł czasopisma zastępuje nazwę wydawnictwa, po nim następuje rok (rocznik), przecinek, następnie numer (nr) w ramach rocznika ewentualnie także numer od początku wydawania pisma i numer strony:

J. Kowalski, Jak pisać przypisy?, Wiadomości Tekściarskie 2006, Nr 28 (236), s. 7.

Kilka kwestii specjalistycznych:

1. Oczekiwane oznaczenie ustawy wygląda następująco: Dz.U. z 2006 r. Nr 28, poz. 456.
2. Publikator prosimy podawać jedynie przy pierwszym przywołaniu aktu prawnego. Wówczas nazwę aktu i datę (miesiąc słownie) podajemy w tekście głównym (np. ustawa z 13.4.2003 r. o zasadach pisania artykułów), w przypisie zaś publikator (np. t.j. Dz.U. z 2006 r. Nr 28, poz. 456).
3. Zapisując artykuł, ustęp, punkt aktu prawnego, skrótów nie oddzielamy przecinkami, tak więc: art. 28 ust. 59 pkt (bez kropki!) 36, a nie: art. 28, ust. 59, pkt. 36.
4. W przypadku orzeczeń sądowych prosimy o zastosowanie następujących oznaczeń: Wyrok SN z 11.5.2011 r., I CA 123/11, OSNCP 2011, Nr 8, poz. 34. Nazwę orzeczenia i jego datę prosimy podać w tekście głównym (np. wyrok SN z 11.5.2011 r.), natomiast w przypisie publikator (I CA 123/11, OSNCP 2011, Nr 8, poz. 34).

Harmonogram publikacji:

Nr 1 – teksty do końca stycznia, druk luty/marzec
Nr 2 – teksty do końca kwietnia, druk maj/czerwiec
Nr 3 – teksty do końca lipca, druk sierpień/wrzesień
Nr 4 – teksty do końca października, druk listopad/grudzień

Osoba do kontaktu: dr *Aleksandra Klich*, e-mail: pme@beck.pl

EDITORIAL REQUIREMENTS:

- language of publication: Polish, English, German, Russian;
- text editor MS Word (.doc or .docx);
- font style: Times New Roman;
- font size: main text – 12 pts, footnote – 10 pts;
- line spacing: 1.5 line (for footnotes – 1 row);
- volume of the article: up to 30,000 characters with spaces;
- margins: standard – all 2.5 cm;
- footnotes: cross-referenced footnotes should be Arabic numerals; reference should be placed immediately after the passage to which the footnote regards (before the full stop ending a sentence);
- article must be attached with key words in Polish and English;
- the title should be written in Times New Roman 14 pts (bold);
- text should consist of following parts: lead (summary, around 1500 characters with spaces), initial comments, amplification (with a division into parts with titles), summation;
- article should also be attached with a lead (summary) in English (around 1500 characters with spaces);
- intertitles should not be numbered, but bold;
- article must be attached with a biographical note (approx. 800 characters including spaces);
- please indicate affiliation.

The referenced sources should adhere to the following style:

Initial(s). Last name, Title, edition number if applicable, volume, part, etc., place and year of publication, followed by the page(s) referred to with the 'p. (pp.)' abbreviation, e.g.: *J. Kowalski*, How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For subsequent reference made **directly** to the cited item:

Ibidem, p. 15–16.

Further reference, when several positions by a given author are being cited, include the first words of the title, e.g.:

J. Kowalski, How to..., p. 28–29.

For edited volumes, when the publication referenced forms a part of the whole:

P. Igrek, Citing, [in:] *J. Kowalski* (ed.), How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For publications in periodicals, the title of the periodical replaces the name of the publisher, followed by the year, comma, then the number (No.) within the year, possibly the consecutive number and page numbers:

J. Kowalski, How to do references?, Editorial news 2006, No. 28 (236) p. 7.

A few technical issues:

a. Expected indication of a legal act goes as follows: Journal of Laws of 2006, No. 28, item 456. The publishing body should only be provided when referring to the act for the first time. Then the name and date of the act (month – in words) shall be given in the body of the text (e.g. The Act of 13 April on the rules of writing articles), and the publishing body shall be given in the footnote (e.g. Journal of Laws of 2006, No. 28, item 456).
b. When writing article, paragraph, point of a legal act, abbreviations should not be separated by commas, that is: art. 28 par. 59 point (no full stop!) 36, not: art. 28, par. 59, pt. 36).
c. For court judgements, please use the following indications: Judgement of the Supreme Court of 11.5.2011, I CA 123/11, OSNCP 2011, No. 8, item 34. Mind that the appelative of the judgement and its date should be indicated in the main text (e.g. Judgement of the Supreme Court of 11.5.2011), and the publishing body in the footnote (I CA 123/11, OSNCP 2011, No. 8, item 34).

Publication schedule (deadlines):

No. 1 – submitting manuscripts – end of January (print – February/March)
No. 2 – submitting manuscripts – end of April (print – May/June)
No. 3 – submitting manuscripts – end of July (print – August/September)
No. 4 – submitting manuscripts – end of October (print – November/December)

Contact Person: *Aleksandra Klich* PhD, e-mail: pme@beck.pl