Prawo Budżetowe Państwa i Samorządu **4(12)/2024**
ISSN 2300-9853 DOI: http://dx.doi.org/10.12775/PBPS.2024.021
Data wpływu: 18 lipca 2025 r. Data akceptacji: 15 grudnia 2025 r.

ANNA WÓJTOWICZ-DAWID
Uniwersytet Rzeszowski
anwojtowicz@ur.edu.pl
ORCID: 0000-0003-3437-3289

Podpis elektroniczny – wybrane zagadnienia

An electronic signature – selected issues

Streszczenie. Cyfryzacja zamówień publicznych stanowi jeden z najbardziej zaawansowanych obszarów transformacji cyfrowej administracji publicznej. Całość procedur związanych z udzielaniem zamówień publicznych – w tym przygotowanie dokumentacji, składanie i podpisywanie ofert oraz wykonywanie czynności procesowych przez zamawiających i wykonawców – realizowana jest w formie lub postaci elektronicznej z wykorzystaniem wyspecjalizowanych narzędzi teleinformatycznych. Od 2021 r. obowiązek stosowania formy lub postaci elektronicznej, obejmujący również kwalifikowany podpis elektroniczny, stał się elementem konstrukcyjnym postępowań prowadzonych na podstawie przepisów dotyczących zamówień publicznych. Wykonawcy zostali tym samym zobligowani do sporządzania dokumentów i oświadczeń w formie lub postaci elektronicznej oraz do posługiwania się podpisem elektronicznym w kontaktach z zamawiającym. Celem artykułu jest analiza roli i pozycji uczestników stosunku zamówieniowego w warunkach dynamicznie rozwijającego się społeczeństwa informacyjnego oraz identyfikacja problemów praktycznych związanych ze składaniem

oświadczeń woli przy użyciu podpisu elektronicznego. Opracowanie obejmuje również próbę uporządkowania podstawowych pojęć oraz wskazanie najistotniejszych zagadnień interpretacyjnych dotyczących elektronicznej formy czynności prawnych w postępowaniu o udzielenie zamówienia. W zakończeniu przedstawiono postulaty *de lege ferenda*, odwołujące się do potrzeby dalszego doprecyzowania ram prawnych podpisu elektronicznego, który – obok funkcji identyfikacyjnej i uwierzytelniającej – pełni także istotną rolę w zapewnianiu integralności danych i ochronie uczestników postępowania przed nieuprawnionym dostępem oraz kradzieżą tożsamości.

Słowa kluczowe: zamówienia publiczne; cyfryzacja; digitalizacja; podpis elektroniczny.

Abstract. The digitalisation of public procurement is one of the most advanced areas of digital transformation in public administration. All procedures related to public procurement – including a preparation of documentation, submission and signing of bids, and performing procedural activities by contracting authorities and contractors – are carried out in an electronic form, using specialised IT tools. Since 2021, an obligation to use electronic form or format, including qualified electronic signatures, has become a structural element of proceedings conducted under the Public Procurement Law. Contractors are thus obliged to prepare documents and statements in an electronic format and to use electronic signatures in their dealings with the contracting authority. The aim of this article is to analyse a role and position of participants in contractual relationships in a context of a dynamically developing information society and to identify practical problems related to a submission of declarations of a will of using electronic signatures. The study also attempts to clarify basic concepts and identify the most important interpretative issues concerning the electronic form of legal acts in procurement proceedings. The conclusion presents proposals *de lege ferenda*, referring to a need to further clarify a legal framework for electronic signatures, which, in addition to their identification and authentication functions, also play an important role in ensuring data integrity and protecting participants in the proceedings against unauthorised access and identity theft.

Keywords: public procurement; digitisation; digitalisation; electronic signature.

1. Wprowadzenie

Cyberbezpieczeństwo, cyfryzacja, digitalizacja, AI są to zagadnienia, które stają się rzeczywistością funkcjonowania administracji publicznej. Publikacje naukowe, materiały informacyjne wskazują szereg danych związanych z powszechnie postępującą cyfryzacją niemalże każdej sfery naszego życia. Cyfrowe postrzeganie działań podejmowanych w otaczającej nas rzeczywistości pozwala na sformułowanie tezy, że jeśli całej planety jeszcze nie ma w chmurze, nastąpi to dość szybko. Rosnąca popularyzacja cyfryzacji pozwala realizować więcej zadań zdalnie, wkraczając w codzienność funkcjonowania administracji publicznej. Jedną z czynności ściśle związaną postępującą cyfryzacją i digitalizacją w administracji publicznej jest korzystanie z podpisów cyfrowych.

Celem artykułu jest przedstawienie prawnych, technologicznych oraz praktycznych aspektów podpisu elektronicznego. Praca zmierza do wykazania stopnia bezpieczeństwa, skuteczności oraz potencjalnych ryzyk związanych z użytkowaniem podpisu elektronicznego, jak również do wskazania rekomendacji ustawowych dla poprawy praktyki tej instytucji.

Zamówienia publiczne to sfera funkcjonowania administracji publicznej, w której możemy mówić o pełnej cyfryzacji. Wynika to wprost z obowiązujących przepisów z zakresu zamówień publicznych. Proces cyfryzacji (ang. *full digitalization of public procurement*) został zapoczątkowany na poziomie unijnym wraz z przyjęciem dyrektywy 2014/24/UE w sprawie zamówień publicznych[1]. Zgodnie z art. 22 ust. 1–6 tej dyrektywy państwa członkowskie zostały zobowiązane do zapewnienia, by cała komunikacja w postępowaniu o udzielenie zamówienia odbywała się za pomocą środków komunikacji elektronicznej, wprowadzając pełną elektronizację procedury przetargowej jako zasadę (tzw. *e-procurement by default*).

Polski ustawodawca wdrożył ten obowiązek w ustawie Prawo zamówień publicznych[2], w szczególności w art. 61–67 p.z.p. zgodnie z moty-

[1] Dyrektywa Parlamentu Europejskiego i Rady nr 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE Tekst mający znaczenie dla EOG (Dz.Urz. UE L 94 z 28.03.2014 r., s. 65).

[2] Ustawa z dnia 11 września 2019 r. (tekst jedn. Dz.U. z 2024 r. poz. 1320 ze zm.), dalej: p.z.p.

wem 52 dyrektywy 2014/24/UE wskazują, że w postępowaniu o udzielenie zamówienia publicznego komunikacja między zamawiającym a wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej. Ustawa nie przewiduje równoległego trybu papierowego, a wszystkie czynności proceduralne (publikacja ogłoszeń, składanie ofert, wezwania, komunikacja, otwarcie ofert, JEDZ, e-podpisy, KIO) odbywają się w środowisku cyfrowym. Prowadzenie postępowania, składanie i podpisywanie ofert, dokonywanie czynności w ramach prowadzonego postępowania odbywa się w pełni poprzez korzystanie z narzędzi elektronicznych. Wykonawcy zobowiązani są do cyfrowego przygotowywania i używania sporządzonych dokumentów. Cyfryzacja, a co się z tym wiąże korzystanie z podpisu elektronicznego, od początku 2021 roku stała się obligatoryjna w zakresie stosowania procedur opartych na p.z.p. Zgodnie z art. 63 ust. 2 p.z.p. w postępowaniu o udzielenie zamówienia publicznego lub konkursie o wartości mniejszej niż progi unijne ofertę wniosek o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia lub w konkursie, oświadczenie, o którym mowa w art. 125 ust. 1 p.z.p., składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem kwalifikowanym. zaufanym lub podpisem osobistym. Zgodnie zaś z art. 63 ust. 1 p.z.p., w postępowaniu o udzielenie zamówienia lub konkursie o wartości równej lub przekraczającej progi unijne ofertę wniosek o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia lub w konkursie, wniosek, o którym mowa w art. 371 ust. 3 p.z.p., oraz oświadczenie, o którym mowa w art. 125 ust. 1 p.z.p., składa się, pod rygorem nieważności, w formie elektronicznej. W każdym z wyżej wymienionych przypadków mamy do czynienia z występowaniem podpisu elektronicznego.

Na gruncie prawa cywilnego forma czynności prawnych jest rozumiana szeroko. Obejmuje formy pisemne, elektroniczne i inne sposoby ujawnienia woli. Forma pisemna jest historycznie utrwalona, natomiast forma elektroniczna została wprowadzona znacznie później, wraz z ekspansją środków komunikacji na odległość.

Celem niniejszego opracowania jest zdefiniowanie roli i możliwości stron czynności prawnych w szybko zmieniającym się społeczeństwie

informacyjnym oraz analiza problemów praktycznych związanych z podpisem elektronicznym. Artykuł zawiera wnioski *de lege ferenda* co do efektywności i bezpieczeństwa tej formy potwierdzania oświadczenia woli.

2. Cyfryzacja a digitalizacja

Pojęcia digitalizacji i cyfryzacji są często stosowane zamiennie, jednakże ich znaczenie głównie w kontekście nauk o zarządzaniu, administracji publicznej czy prawa jest odmienne. Rozróżnienie wskazanych pojęć ma istotne znaczenie praktyczne w zakresie sposobu implementacji polityk publicznych, w tym strategii transformacji cyfrowej administracji oraz procesów udzielania zamówień publicznych.

Digitalizacja jest pojęciem węższym od cyfryzacji i odnosi się do procesu przekształcania informacji analogowej w postać cyfrową. Jak wskazuje N. Negroponte, digitalizacja oznacza „zamianę atomów na bity", czyli przeniesienie treści, danych, obrazów, dźwięków czy dokumentów do formatu cyfrowego, możliwego do przetwarzania przez komputery[3].

OECD definiuje digitalizację jako konwersje danych lub dokumentów z formy fizycznej do formy cyfrowej[4]. Digitalizacja, która ma charakter operacyjno-techniczny, jest etapem wstępnym transformacji cyfrowej, umożliwiającym późniejsze wykorzystanie technologii informatycznych w szerszym kontekście organizacyjnym i społecznym[5].

D. Śledziewska i R.W. Kozłowski definiują digitalizację jako proces techniczny, którego głównym celem jest zastąpienie analogowych form zapisu i komunikacji formą cyfrową, umożliwiając ich dalsze przetwarzanie[6]. Podnoszą oni iż „na oznaczenie zjawisk, które Bloomberg określa mianem digitalizacji, używa się raczej pojęcia cyfryzacji: pisze się o cy-

---

[3] N. Negroponte, *Being Digital*, Nowy Jork 1995, s. 11.

[4] OECD, *Measuring Digital Transformation: A Roadmap for the Future*, Paris 2019: OECD Publishing; https://www.oecd.org/en/publications/measuring-the-digital-transformation_9789264311992-en.html (dostęp: 15.05.2025 r.).

[5] R. Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*, Londyn 2014, s. 35.

[6] D. Śledziewska, R. W. Kozłowski, *Gospodarka cyfrowa. Jak technologie zmieniają świat*, Warszawa 2020, s. 67 i n.

fryzacji procesów, cyfryzacji edukacji, cyfryzacji firm. Zamieszanie pojęciowe pogłębia fakt, że Komisja Europejska konsekwentnie używa pojęcia digityzacji w rozumieniu cyfryzacji”[7]. W tym sensie digitalizacja jest fundamentem, ale nie synonimem cyfryzacji[8].

Cyfryzacja to pojęcie szersze, obejmujące społeczne, gospodarcze i instytucjonalne skutki wdrażania technologii cyfrowych. Według Komisji Europejskiej cyfryzacja oznacza „integrację technologii cyfrowych z procesami gospodarczymi i społecznymi w celu ich modernizacji, optymalizacji i innowacji”[9].

Digitalizacja stanowi niezbędny warunek, lecz niewystarczający element cyfryzacji. Cyfryzacja natomiast jest etapem prowadzącym do głębszej transformacji cyfrowej, rozumianej jako zmiana paradygmatu działania administracji, gospodarki i nauki. Rozróżnienie obu pojęć ma fundamentalne znaczenie dla terminologii prawniczej i strategicznej.

3. Podpisy cyfrowe a podpisy elektroniczne

Niezbędnym elementem analizy kwestii podpisu elektronicznego jest ustalenie zakresu pojęciowego oraz wskazanie, czym jest podpis elektroniczny, a czym podpis cyfrowy. Choć oba pojęcia mogą się wydawać synonimami i niekiedy błędnie są jako synonimy używane, podpis elektroniczny niekoniecznie musi być podpisem cyfrowym.

Wprowadzenie podpisu elektronicznego do polskiego systemu prawnego stanowiło część procesu informatyzacji administracji publicznej i budowy zaufania do obrotu elektronicznego w ramach wspólnego rynku Unii Europejskiej. Pierwsze regulacje dotyczące podpisu elektronicznego

---

7 Tamże, s. 67.

8 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Cyfryzacja europejskiego przemysłu. Pełne wykorzystanie możliwości jednolitego rynku cyfrowego, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52016DC0180, (dostęp: 15.05.2025 r.).

9 OECD, *Measuring Digital Transformation: A Roadmap for the Future*, Paris 2019: OECD Publishing; https://www.oecd.org/en/publications/measuring-the-digital-transformation_9789264311992-en.html (dostęp: 15.05.2025 r.).

wprowadziła Dyrektywa 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram dla podpisów elektronicznych[10], która ustanowiła pojęcie „bezpiecznego podpisu elektronicznego" (ang. *advanced electronic signature*) o równoważnej mocy prawnej z podpisem własnoręcznym. Dyrektywa ta miała charakter technologicznie neutralny i stanowiła ramy dla krajowych systemów certyfikacji podpisu elektronicznego. Jej głównym celem było umożliwienie transgranicznego uznawania podpisów cyfrowych w obrocie prawnym i administracyjnym w UE[11].

Polska implementowała przepisy dyrektywy 1999/93/WE ustawą z dnia 18 września 2001 r. o podpisie elektronicznym[12], która weszła w życie 16 sierpnia 2002 r. Był to pierwszy akt normatywny w polskim prawie, który zrównywał podpis elektroniczny z podpisem własnoręcznym, o ile spełniał warunki „bezpiecznego podpisu elektronicznego weryfikowanego za pomocą kwalifikowanego certyfikatu"[4]. Ustawa wprowadzała pojęcia takie jak: podpis elektroniczny, bezpieczny podpis elektroniczny, certyfikat kwalifikowany, kwalifikowany podmiot świadczący usługi certyfikacyjne.

Kolejnym etapem było przyjęcie Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku[13]. Rozporządzenie to, obowiązujące bezpośrednio we wszystkich państwach członkowskich od 1 lipca 2016 r., uchyliło wcześniejszą dyrektywę 1999/93/WE i stworzyło jednolity europejski

---

[10] Dyrektywa 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram dla podpisów elektronicznych (Dz.Urz. L 13 z 19.01.2000, s. 12).

[11] Szerzej: M. Marucha-Jaworska, Rozporządzenie eIDAS. Zagadnienia prawne i techniczne, Wolters Kluwer, Warszawa 2017.

[12] Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. 2001 nr 130, poz. 1450).

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku oraz uchylające dyrektywę 199/93/WE (Dz.Urz. UE L 257 z 28.08.2014 r., s. 73), dalej: rozporządzenie eIDAS, będące akronimem od angielskiego *electronic Identification, Authentication and trust Services*).

system identyfikacji elektronicznej i usług zaufania (*trust services*). Na gruncie rozporządzenia eIDAS wprowadzono pojęcie kwalifikowanego podpisu elektronicznego (*qualified electronic signature* – QES), który: „ma skutek prawny równoważny podpisowi własnoręcznemu" (art. 25 ust. 2 eIDAS).

Polski ustawodawca dostosował krajowy porządek prawny do eIDAS ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej[14], która uchyliła ustawę z 2001 r. i wprowadziła system nadzoru nad dostawcami kwalifikowanych usług zaufania, powierzony Narodowemu Centrum Certyfikacji (NCCert) w strukturze NBP oraz Ministerstwu Cyfryzacji. Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[15] podpis elektroniczny został uznany za podstawowy środek uwierzytelniania i podpisywania dokumentów elektronicznych w systemach teleinformatycznych administracji. W kolejnym etapie wprowadzono system ePUAP (Elektroniczna Platforma Usług Administracji Publicznej) jako narzędzie składania podań, wniosków i oświadczeń opatrzonych podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym[16]. Znowelizowane zostały obowiązujące przepisy, w tym przepisy Kodeksu postępowania administracyjnego[17] (art. 63 § 3a k.p.a.), dopuszczając wnoszenie podań drogą elektroniczną pod warunkiem opatrzenia ich kwalifikowanym podpisem elektronicznym lub podpisem zaufanym[18]. Zgodnie z art. 63 § 1 Kodeksu postępowania administracyjnego „Podania utrwalone w postaci elektronicznej wnosi się na adres do doręczeń elektronicznych lub za pośrednictwem konta w systemie teleinformatycznym organu administracji publicznej". Kolejnym krokiem była pełna cyfryzacja zamówień publicznych – ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych

[14] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r., poz. 1579).

[15] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, (Dz.U. z 2024 r., poz. 1463).

[16] M. Wierzbowski, *Administracja publiczna w dobie cyfryzacji*, Warszawa 2019, s. 118.

[17] Ustawa z dnia 14 czerwca 1960 r. (tekst jedn. Dz.U. z 2024 r., poz. 572 ze zm.), dalej: k.p.a.

[18] Por. art. 63 § 3a k.p.a.

nakazująca, by wszystkie oświadczenia i dokumenty w postępowaniach o udzielenie zamówienia publicznego były opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym (art. 63 ust. 2 p.z.p.).

Podpis elektroniczny może składać się z wszystkiego, od wpisania swojego nazwiska na dole wiadomości e-mail, zeskanowanego podpisu, kliknięcia przycisku „Akceptuję", powiązanych danych biometrycznych, takich jak odciski palców czy korzystanie z platformy podpisu elektronicznego. Musi on odpowiadać standardom, dając możliwość przeprowadzenia niezależnej weryfikacji. Pojęcie podpisu elektronicznego jest szersze od podpisu cyfrowego i obejmuje wszystkie technologie zastępujące podpis odręczny w środowisku elektronicznym, pozwalając na identyfikację osoby ją składającej. Opiera się on na użyciu technologii, która wiąże podpis z tożsamością osoby podpisującej i godziną jej podpisania. Podpis elektroniczny może być procesem dołączonym, elektronicznym symbolem lub dźwiękiem do wiadomości, umowy lub dokumentu, który może być użyty do uzyskania zgody lub zatwierdzenia dokumentów elektronicznych lub formularzy.

Podpis cyfrowy jest rodzajem podpisu elektronicznego, jednakże istnieją określone różnice pomiędzy tymi instrumentami. Podpis cyfrowy wiąże się z informatycznym zastosowaniem kryptografii w celu zapewnienia autentyczności wiadomości elektronicznych oraz integralności treści tych informacji. Dotyczy więc technologii uwierzytelniania osoby składającej podpis. Odnosi się on do technologii szyfrowania używanej w e-biznesie i handlu elektronicznym, w tym w aplikacjach do podpisu elektronicznego.

Wskazując na różnice między pojęciem podpisu elektronicznego a podpisu cyfrowego, wymienia się:

1. podpisy cyfrowe są opatrzone datą, a data i godzina podpisu elektronicznego może być z nim powiązana, ale umieszczane osobno,
2. podpisy cyfrowe spełniają standardy i zwiększają bezpieczeństwo dzięki zastosowaniu metod szyfrowania kryptograficznego. W przeciwieństwie do tego podpisy elektroniczne nie zależą od standardów i są stosunkowo mniej bezpieczne,

3. mechanizm uwierzytelniania używany w podpisie elektronicznym nie jest zdefiniowany i używa adresu e-mail osoby podpisującej, numeru PIN telefonu itd. Natomiast podpis cyfrowy obejmuje metodę uwierzytelniania za pomocą identyfikatora cyfrowego ID,
4. podpis cyfrowy zapewnia bezpieczeństwo dokumentu cyfrowego, natomiast podpis elektroniczny służy do weryfikacji dokumentu cyfrowego,
5. w podpisie cyfrowym sprawdzanie poprawności podpisu jest wykonywane przez zaufane urzędy certyfikacji, podczas gdy nie jest tak w przypadku podpisu elektronicznego,
6. podpisy elektroniczne są podatne na manipulację, podpisy cyfrowe zaś są wysoce zabezpieczone i oferują dowody manipulacji.

Konwencjonalne podpisy, jakimi posługujemy się w obrocie gospodarczym, służą do oznaczenia tożsamości i zamiaru w odniesieniu do tego oświadczenia, pod którym są składane, a ich podstawowym celem jest wskazanie tożsamości czy też właściciela oświadczenia.

Wskazując na różnice tych dwóch instytucji, należy wskazać, iż każdy podpis cyfrowy jest podpisem elektronicznym, lecz nie każdy podpis elektroniczny jest podpisem cyfrowym.

Rozporządzenie eIDAS stanowi podstawowy akt prawny regulujący kwestie podpisu elektronicznego w Unii Europejskiej. Celem rozporządzenia jest ujednolicenie przepisów dotyczących identyfikacji elektronicznej, podpisu elektronicznego oraz innych usług zaufania, a także zapewnienie spójnych zasad funkcjonowania transakcji elektronicznych na jednolitym rynku UE.

Regulacja ta ma na celu wyeliminowanie niespójności i ograniczenie barier w transgranicznym uznawaniu podpisów elektronicznych, a tym samym zwiększenie zaufania między uczestnikami rynku wewnętrznego. Rozporządzenie eIDAS gwarantuje, że dokumenty opatrzone kwalifikowanym podpisem elektronicznym będą uznawane i akceptowane we wszystkich państwach członkowskich Unii Europejskiej, co stanowi

wspólną podstawę dla bezpiecznej interakcji elektronicznej pomiędzy obywatelami, przedsiębiorcami i administracją publiczną[19].

W rezultacie rozporządzenie przyczynia się do podniesienia efektywności usług publicznych i prywatnych świadczonych online, a także do rozwoju e-biznesu i e-handlu w skali całej Unii Europejskiej[20].

W doktrynie prawa podnosi się, iż pojęcie transakcji należy rozumieć szerzej niż tylko transakcje handlowe. Jest to instytucja zbliżona do słowa „proces" w jego potocznym rozumieniu, czyli przebieg następujących po sobie i powiązanych przyczynowo-skutkowo określonych zmian[21].

Celem rozporządzenia eIDAS nie jest ingerowanie w systemy zarządzania tożsamością elektroniczną i w powiązane z nimi infrastruktury ustanowionej w państwach członkowskich. Jego celem jest zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania na potrzeby dostępu do transgranicznych usług online oferowanych przez państwa członkowskie[22].

Podpisy elektroniczne w ramach eIDAS obejmują wszelkie dane w formie elektronicznej, które są dołączone do innych danych w formie elektronicznej lub logicznie z nimi powiązane i które są wykorzystywane przez podpisującego do złożenia podpisu – art. 3 pkt. 10 eIDAS. Jednocześnie eIDAS rozróżnia zaawansowany podpis elektroniczny (zgodnie z art. 3 pkt 11 eIDAS oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26), oraz kwalifikowany podpis elektroniczny. Zgodnie z art. 3 pkt 12 eIDAS oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego; oprócz wszystkich innych standardowych wymagań wymaga również posiadania osobistego certyfikatu cyfrowego.

---

19 Szerzej na ten temat m.in.: P.P. Polański, *Towards the single digital market for e-identification and trust services*, „Computer Law & Security Review" 2015 nr 31, s. 774–775; J. Dumortier, N. Vandezande, *Trust in the proposed EU regulation on trust services?*, „Computer Law & Security Review" 2012, nr 28, s. 568.

20 Motyw 2 rozporządzenia eIDAS.

21 Ł. Goździaszek, *Identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym Unii Europejskiej. Komentarz*, Legalis 2019, *komentarz do art. 1 rozporządzenia eIDAS*.

22 Motyw 5 rozporządzenia eIDAS.

Certyfikat cyfrowy jest bezpiecznym, osobistym i unikalnym poświadczeniem tożsamości elektronicznej, które musi być wydane podpisującemu w formie, którą może on zachować pod swoją kontrolą.

Rozporządzenie eIDAS reguluje sferę świadczenia usług zaufania. Jak słusznie wskazuje I. Jóźwiak, wspólną cechą usług zaufania wprowadzonych przez eIDAS jest ich ukierunkowanie na wyeliminowanie anonimowości podmiotów dokonujących czynności drogą elektroniczną i „jednoczesne uwiarygodnienie ich działań poprzez m.in. uwierzytelnienie tożsamości" podmiotu dokonującego czynności, „zapewnienie integralności (niezmienności) treści składanych oświadczeń woli, potwierdzenie czasu dokonania czynności"[23].

Nie ma wymogu stosowania określonego rodzaju technologii przy kwalifikowaniu podpisu elektronicznego w ramach eIDAS. Rozporządzenie eIDAS przewiduje możliwość wykorzystania niekwalifikowanego podpisu elektronicznego, który nie jest oparty o certyfikat kwalifikowany. Dostawcy usług związanych z podpisami elektronicznymi niekwalifikowanymi nie są zobowiązani do spełniania wszystkich wymogów określonych dla kwalifikowanych dostawców usług zaufania w rozumieniu rozporządzenia eIDAS. Z tego względu podpis elektroniczny niekwalifikowany nie posiada co do zasady mocy prawnej równoważnej podpisowi własnoręcznemu, w przeciwieństwie do kwalifikowanego podpisu elektronicznego, którego skutki prawne są zrównane z podpisem odręcznym na podstawie art. 25 ust. 2 rozporządzenia eIDAS.

Podpis elektroniczny niekwalifikowany może wywoływać skutki prawne w relacjach cywilnoprawnych, o ile strony wyraźnie uzgodniły dopuszczalność takiej formy komunikacji lub podpisu (art. 60 i 78^1 § 1 Kodeksu cywilnego). W praktyce jest on stosowany do uwierzytelniania dokumentów niewymagających zachowania formy pisemnej pod rygorem nieważności, takich jak umowy zlecenia, umowy sprzedaży, zapytania ofertowe czy dokumenty funkcjonujące w wewnętrznym obiegu organizacyjnym danego podmiotu.

[23] I. Jóźwiak, *Odpowiedzialność dostawców usług zaufania – wybrane aspekty*, „Człowiek w cyberprzestrzeni" 2018, nr 3, s. 37.

W kontekście administracyjnym i zamówień publicznych podpis niekwalifikowany znajduje zastosowanie w szczególności w postępowaniach poniżej progów unijnych, w których zamawiający dopuszcza użycie podpisu osobistego (zgodnego z art. 3 pkt 14 ustawy o dowodach osobistych[24]) lub podpisu zaufanego (ustanowionego na podstawie art. 3 pkt 14 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej[25]). Obie te formy podpisu są uznawane przez prawo krajowe za wystarczające w kontaktach z administracją publiczną, o ile przepisy szczególne nie wymagają użycia podpisu kwalifikowanego.

Podpis elektroniczny niekwalifikowany, choć nie zapewnia domniemania autentyczności i integralności danych w takim zakresie jak podpis kwalifikowany, stanowi użyteczne i prawnie dopuszczalne narzędzie w obrocie prawnym, zwłaszcza w sferze wewnętrznej komunikacji instytucjonalnej i w postępowaniach o mniejszej wadze prawnej lub finansowej.

4. Podpis elektroniczny w systemie prawa polskiego

Pierwsze regulacje prawne dotyczące podpisu elektronicznego pojawiły się w Stanach Zjednoczonych jako regulacje stanowe w 1995 r. Amerykańska ustawa federalna weszła w życie w 2000 r.[26] W Unii Europejskiej pierwsze regulacje dotyczące podpisu elektronicznego zostały zawarte w dyrektywie Parlamentu i Rady Unii Europejskiej w sprawie wspólnotowych ram w zakresie podpisów elektronicznego nr 1999/93/WE z 13 grudnia 1999 r.[27]

---

[24] Ustawa z dnia 6 sierpnia 2010 r. (tekst jedn. Dz.U. z 2022 r., poz. 671 ze zm.).

[25] Dz.U. z 2024 r., poz. 1725.

[26] Utah Code Annotated 1953, Volume 5A, 1998 Replacement, Title 39 to 46, Lexis Law Publishing; zob. szerzej: M. Marucha, *Nowa ustawa o podpisie elektronicznym*, „Monitor Prawniczy" 2002, nr 2, s. 73 oraz M. Marucha-Jaworska, *Podpis elektroniczny*, Warszawa 2002, s. 77.

[27] Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.Urz. UE L 13 z dnia 19.01.2000 r, s. 12).

Pierwsze regulacje podpisu elektronicznego w prawie polskim zawarte zostały w ustawie o podpisie elektronicznym z dnia 18 września 2001 r.[28], która – wraz z pakietem aktów wykonawczych – weszła w życie 16 sierpnia 2002 r., tworząc podwaliny do budowy kwalifikowanej infrastruktury klucza publicznego. Przesłanką, jaką kierował się polski ustawodawca, było stworzenie podwalin udrożnienia obiegu elektronicznych dokumentów w obrocie administracyjno-prawnym oraz handlowym. Ministerstwo Gospodarki jako inicjator tej regulacji wskazywało na cele, jakim ma podpis elektroniczny służyć, wskazując na podpisywanie pism i decyzji administracyjnych przez urzędy, podpisywanie faktur elektronicznych, zarejestrowanie działalności gospodarczej, składanie deklaracji celnych i podatkowych oraz zgłoszenie ubezpieczenia społecznego (system PUE ZUS). Przedmiotowa ustawa obowiązywała do 2016 r. i została uchylona ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

W Unii Europejskiej przyjęcie rozporządzenia eIDAS było kolejnym krokiem do kształtowania regulacji w zakresie korzystania z podpisu elektronicznego. W rozporządzeniu eIDAS ustanowiono ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług potwierdzonych doręczeń elektronicznych, usług certyfikacyjnych do celu uwierzytelniania witryn internetowych. Wejście w życie rozporządzenia eIDAS spowodowało uchylenie polskiej ustawy o podpisie elektronicznym z 2001 r. oraz ustanowienie ustawy o usługach zaufania. Obecnie w systemie prawa polskiego obowiązuje ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej[29] regulująca kwestie certyfikacji podpisu elektronicznego. Ustawa ta jest efektem wejścia życie rozporządzenia eIDAS, które wprowadziło we wszystkich krajach Unii Europejskiej nowy porządek prawny w obszarze usług zaufania oraz identyfikacji elektronicznej. Jest doprecyzowaniem tych obszarów regulacji, które prawodawca unijny pozostawił niedookreślone lub w których wprost odesłał do

[28] Tekst jedn. Dz.U. 2013 poz. 262 ze zm., uchylona z dniem 7 października 2016 r.
[29] Tekst jedn. Dz.U. z 2024 r. poz. 422, dalej: u.o.u.z.

prawa krajowego, zachowując zasadę, iż przedmiotowe doprecyzowanie nie stoi na przeszkodzie osiągnięciu celów rozporządzenia[30].

Na podstawie przepisów u.o.u.z. wydane zostały następujące akty wykonawcze:

1. rozporządzenie Ministra Cyfryzacji z 5 października 2016 r. w sprawie krajowej infrastruktury zaufania (Dz.U. poz. 1632); rozporządzenie Ministra Cyfryzacji z 6 września 2019 r. w sprawie wysokości kwot odpowiedzialności podmiotu odpowiedzialnego za system identyfikacji elektronicznej (Dz.U. poz. 1710);
2. rozporządzenie Rady Ministrów z 6 listopada 2018 r. w sprawie zakresu danych i dokumentów niezbędnych do przeprowadzenia postępowania w celu dokonania oceny korporacyjnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej lub podmiotu wydającego środki identyfikacji elektronicznej w tym systemie (Dz.U. poz. 2207);
3. rozporządzenie Ministra Finansów z 15 października 2018 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia odpowiedzialności cywilnej podmiotu odpowiedzialnego za system identyfikacji elektronicznej (Dz.U. poz. 2009);
4. rozporządzenie Ministra Rozwoju i Finansów z 19 grudnia 2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania (Dz.U. z 2017 r. poz. 13).

5. Czym jest podpis elektroniczny w systemie prawa?

Omawianie zagadnienia podpisu elektronicznego należy rozpocząć od wskazania, czym jest w systemie prawa polskiego podpis elektroniczny.

SN w uchwale z 30 grudnia 1993 roku[31] wskazał, że podpis oznacza szereg znaków graficznych, które według prawideł pewnego systemu

[30] A. Romaszewski, W. Trąbka, M. Kielar, K. Gajda, *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej, cz. 1*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2016, nr 42, s. 25.

[31] III CZP 146/93, „Orzecznictwo Sądu Najwyższego Izba Cywilna" 1994, nr 5, poz. 94.

pisania tworzą obraz brzmienia danego nazwiska, a które zamieszczono na dokumencie za pomocą techniki oddającej indywidualne właściwości piszącego. W świetle tego orzeczenia, jak wskazuje K. Pawłowska, podpis jest znakiem graficznym zapisanym w sposób trwały, np. tuszem czy atramentem[32]. Słusznie podnosi ona, iż w ocenie SN podpis własnoręczny może złożyć tylko osoba umiejąca czytać i mogąca pisać.

Art. 3 pkt 1 ustawy o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262, z 2014 r. poz. 1662 oraz z 2015 r. poz. 1893) wskazywał, że podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Podpis elektroniczny wykorzystywany jest do podpisywania dokumentów i oświadczeń woli elektronicznych. Dokument elektroniczny zaś, w przeciwieństwie do dokumentu tradycyjnego, nie ma formy materialnej.

Wskazana w art. 3 pkt 1 nieobowiązującej już ustawy o podpisie elektronicznym definicja podpisu elektronicznego zawierała w sobie dwa domniemania prawne:

1. domniemanie odnoszące się do osoby określonej w certyfikacie, wskazujące, iż osoba wskazana w certyfikacie jest osobą składającą podpis elektroniczny,
2. domniemanie prawdziwości znakowania czasem – znakowanie czasem wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego. Czyli podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi.

Pomimo tego, iż przywołany przepis nie obowiązuje już, w ocenie autorki wskazane domniemania należy uznać za obowiązujące, jako domniemania faktyczne, wynikające z istoty kwalifikowanego podpisu elektronicznego.

Elektroniczny podpis cyfrowy, podobnie jak dokument elektroniczny, jest ciągiem bitów, czyli zer (0) i jedynek (1). Podpis jest weryfiko-

[32] K. Pawłowska, *Podpis elektroniczny w porównaniu z podpisem własnoręcznym*, „e-Biuletyn" 2007, nr 4, s. 1.

wany przy użyciu informacji podanej do wiadomości publicznej przez nadawcę, zwanej publicznym kluczem nadawcy.

Jak słusznie wskazuje P. Świtał, podpis elektroniczny to narzędzie, którego podstawowym celem jest zagwarantowanie tożsamości, autentyczności i integralności przy wymianie informacji drogą elektroniczną. Podnosi on, iż podstawowym celem korzystania z podpisu elektronicznego jest zapewnienie unikalności oznaczania dokumentu w taki sposób, że na podstawie tego oznaczenia można zagwarantować identyfikację osoby, która dokonała czynności podpisania oraz niezaprzeczalność podpisania przez nią dokumentu[33].

Szczególnym rodzajem podpisu elektronicznego jest tzw. bezpieczny podpis elektroniczny. Zgodnie z art. 5 ustawy o podpisie elektronicznym bezpieczny podpis elektroniczny weryfikowany jest przy pomocy kwalifikowanego certyfikatu i wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu.

Oświadczenie woli w formie elektronicznej jest złożone innej osobie z chwilą, gdy wprowadzono je do środka komunikacji elektronicznej w taki sposób, że osoba ta mogła zapoznać się z jego treścią. Dla skutków prawnych oświadczenia złożonego z wykorzystaniem podpisu elektronicznego znaczenie ma nie chwila rzeczywistego zapoznania się adresata z treścią, a moment, w którym wystąpiła możność zapoznania się z jego treścią – art. 61 § 2 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny[34].

W praktyce podpisywanie dokumentu podpisu elektronicznego polega na udziale osoby generującej taki podpis w zainicjowaniu procesu podpisywania i jego zakończenia. Jest to więc czynność faktyczna, w efekcie której dochodzi do wygenerowania podpisu elektronicznego pod danym dokumentem czy oświadczeniem woli w formie elektronicznej.

---

33 P. Świtał, *Podpis elektroniczny – wybrane aspekty prawne*, „Studenckie Zeszyty Naukowe" 2013, nr 23, s. 107.

34 Tekst jedn. Dz.U. z 2024 r., poz. 1061.

6. Cechy podpisu elektronicznego

Zgodnie z regulacjami eIDAS wprowadzenie usług zaufania[35] oznacza, iż ona:

1. może dotyczyć tworzenia, weryfikacji lub walidacji podpisów elektronicznych, a także znaczników czasu lub pieczęci, usług rejestrowanych doręczeń elektronicznych oraz certyfikatów wymaganych przy tych usługach,
2. obejmuje tworzenie, weryfikację oraz walidację certyfikatów, które służą do uwierzytelniania stron internetowych,
3. jest zachowanie (konserwacja) podpisów elektronicznych, pieczęci lub powiązanych z nimi certyfikatów[36].

Katalog kwalifikowanych usług zaufania wymienionych w art. 3 pkt 16 eIDAS ma charakter zamknięty[37].

Rozporządzenie eIDAS w art. 3 pkt 1 i 2 definiuje pojęcie identyfikacji elektronicznej jako „proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną", umożliwiających rozpoznanie podmiotu, następujące za pośrednictwem środka identyfikacji elektronicznej, który „oznacza materialną bądź niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online". Oznacza to, iż identyfikacja elektroniczna to deklaracja tożsamości, zaprezentowanie unikalnej cechy identyfikującej osobę (lub rzeczy), forma elektronicznego „przedstawienia się" osoby składającej podpis elektroniczny.

Analizując zagadnienie podpisu elektronicznego, można wyodrębnić jego cechy:

---

35 Zgodnie z art. 3 pkt 16 eIDAS jest to usługa elektroniczna (zasadniczo świadczona za wynagrodzeniem, czyli odpłatna), której celem jest tworzenie, weryfikacja, walidacja i konserwacja podpisów elektronicznych, pieczęci elektronicznych, certyfikatów uwierzytelnienia witryn internetowych.

36 A. Monarcha-Matlak, *Usługi zaufania i identyfikacja elektroniczna*, „Acta Iuris Stetinensis" 2018, nr 3, s. 144.

37 M. Marucha-Jaworska, *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Warszawa 2017, s. 49; A. Anusz, *Ochrona konsumentów w świetle rozporządzenia eIDAS*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020, nr 2, s. 102.

1. pewność – odbiorca informacji, otrzymując dokument wysłany drogą elektroniczną i podpisany podpisem elektronicznym, nabywa pewności co do osoby składającej podpis,
2. integralność – otrzymany dokument lub oświadczenie woli podpisane podpisem elektronicznym nie uległa najmniejszej zmianie,
3. uwierzytelnienie – oświadczenie podpisane podpisem elektronicznym potwierdza autentyczność dokumentu i tożsamość jego nadawcy w sposób trudny do podrobienia, możliwy do weryfikacji osoby składającej e-podpis i trwale połączony z dokumentem,
4. poufność – polega na takim zaszyfrowania dokumentu, że dane w nim zawarte odczyta tylko osoba, do której wiadomość została wysłana,
5. stemplowanie znakiem czasu – w tworzeniu e-dokumentów cechą podpisu elektronicznego jest ich stemplowanie znakiem czasu, czyli podpis elektroniczny przypisuje dokumentom dokładny czas ich powstania i złożenia oświadczenia woli.

Złożenie kwalifikowanego podpisu elektronicznego niesie za sobą skutki prawne poprzez uznanie takiego podpisu za równoważny podpisowi własnoręcznemu, jeśli jest:

1. przyporządkowany wyłącznie do osoby składającej e-podpis,
2. sporządzany za pomocą bezpiecznych urządzeń będących pod kontrolą tej osoby,
3. powiązany z danymi, do których został dołączony.

W kontekście skuteczności prawnej kwalifikowanego podpisu elektronicznego kluczowe znaczenie ma kwalifikowany certyfikat podpisu elektronicznego, wydawany posiadaczowi przez kwalifikowanego dostawcę usług zaufania po przeprowadzeniu procedury weryfikacji tożsamości zgodnej z wymogami określonymi w art. 24 ust. 1 lit. d rozporządzenia eIDAS. Certyfikat ten potwierdza przyporządkowanie klucza publicznego do określonej osoby, której tożsamość została uprzednio zweryfikowana, a tym samym zapewnia domniemanie autentyczności podpisu oraz integralności danych podpisanych w formie elektronicznej.

Nie mniej istotnym elementem systemu jest klucz prywatny, stanowiący techniczny odpowiednik podpisu własnoręcznego, który umożliwia składanie podpisów elektronicznych w sposób jednoznacznie przypisany

do właściciela certyfikatu. Klucz ten powinien być przechowywany i używany w warunkach gwarantujących jego bezpieczeństwo, w szczególności z wykorzystaniem kwalifikowanego urządzenia do składania podpisu elektronicznego (QSCD – Qualified Signature Creation Device), spełniającego wymagania art. 29 rozporządzenia eIDAS. Zapewnienie integralności i poufności klucza prywatnego jest warunkiem zachowania wiarygodności całego mechanizmu zaufania oraz podstawą domniemania prawnego, iż podpis został złożony przez osobę, dla której certyfikat został wydany.

7. Certyfikat cyfrowy

Certyfikat cyfrowy jest elektronicznym zaświadczeniem, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowywane do określonej osoby i potwierdzają jej tożsamość. Wydawany jest przez kwalifikowanego dostawcę usług zaufanych.

Autentyczność podpisu elektronicznego można sprawdzić, jeśli znany jest klucz publiczny organu certyfikującego. Klucz ten znajduje się na certyfikacie wystawionym dla organu certyfikującego przez organ wyższej instancji – Narodowe Centrum Certyfikacji (National Certification Center, dalej jako NCCert). Narodowe Centrum Certyfikacji to główny urząd certyfikacji w polskiej infrastrukturze zaufania. Nie jest ono kwalifikowanym dostawcą usług zaufania, ma swoją rolę w procesie wydawania certyfikatów dostawców usług zaufania. Certyfikaty te są wykorzystywane w transakcjach elektronicznych i mają na celu potwierdzenie tożsamości osób fizycznych lub prawnych oraz zapewnienie bezpiecznego podpisywania dokumentów elektronicznych.

Zgodnie z art. 10 u.o.u.z. zadaniami NCCest jest:

1. tworzenie i wydawanie kwalifikowanym dostawcom usług zaufania certyfikatów służących 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 in-

nych usług zaufania świadczonych przez kwalifikowanych dostawców;
2. publikowanie certyfikatów, o których mowa w pkt 1;
3. publikowanie listy unieważnionych certyfikatów, o których mowa w pkt 1;
4. tworzenie dane do opatrywania pieczęcią elektroniczną certyfikatów, o których mowa w pkt 1, oraz certyfikatów do weryfikacji tych pieczęci, zwanych dalej „certyfikatami narodowego centrum certyfikacji".

Celem NCCert jest zapewnienie właściwych standardów bezpieczeństwa, poufności i integralności w dziedzinie elektronicznych usług zaufania. Na stronie internetowej NCCert publikowane są: skrót danych służących do walidacji danych powiązanych z certyfikatem NCCert wystawionym w 2016 r. (NCCert2016) oraz skrót danych służących do walidacji danych powiązanych z certyfikatem NCCert wystawionym w 2009 r. (NCCert2009), a także aktualne certyfikaty NCCert (Certyfikat Narodowego Centrum Certyfikacji wystawiony w 2016 r. oraz 2009 r.).

Art. 14 u.o.u.z. kształtuje obowiązki przy wydawaniu kwalifikowanego certyfikatu podpisu elektronicznego. Wskazuje, iż kwalifikowany dostawca usług zaufania, wydając kwalifikowany certyfikat podpisu elektronicznego, jest obowiązany:
1. uzyskać od osoby ubiegającej się o certyfikat potwierdzenie przyporządkowania do niej danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie,
2. poinformować osobę ubiegającą się o certyfikat o procedurze zgłaszania żądań unieważnienia kwalifikowanego certyfikatu.

Zgodnie z art. 19 u.o.u.z. dostawca usług zaufania jest obowiązany posiadać politykę świadczenia usługi. Stanowi ona nazwany zestaw reguł, w szczególności takich jak polityka certyfikacji, określający zasady świadczenia usługi, odpowiedzialność stron, zasady postępowania z danymi i mający zastosowanie do określonego kręgu podmiotów lub zastosowań, o wspólnych dla tego kręgu wymaganiach bezpieczeństwa, opracowywany na podstawie norm lub standardów określających wymagania dla polityk świadczenia usług. Kwalifikowany dostawca usług zaufania jest obowiązany posiadać plan zakończenia działalności oraz zastosować

ten plan do zakończenia działalności. Jego obowiązkiem jest również zapewnienie możliwość całodobowego zgłaszania żądań unieważnienia kwalifikowanych certyfikatów. W tym miejscu należy od razu wskazać, iż dostawca usług zaufania jest podmiotem świadczącym swoje usługi komercyjnie. Opracowana polityka świadczenia usług jest gwarantem, że system działa prawidłowo, to znaczy, że każdy jego uczestnik jest „znany i rozpoznawalny", zaś składane przez niego oświadczenia są wiążące na gruncie przepisów prawa[38]. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 2021 r.[39] uznał, że polityka świadczenia usługi stanowi nazwany zestaw reguł, w szczególności takich jak polityka certyfikacji, określający zasady świadczenia usługi, odpowiedzialność stron, zasady postępowania z danymi i mający zastosowanie do określonego kręgu podmiotów lub zastosowań, o wspólnych dla tego kręgu wymaganiach bezpieczeństwa, opracowywany na podstawie norm lub standardów określających wymagania dla polityk świadczenia usług.

Przywołany art. 19 u.o.u.z. kształtuje trzy obowiązki kwalifikowanego dostawcy usług:

1. konieczność posiadania polityki świadczenia usługi,
2. konieczność posiadania planu zakończenia działalności, jak również jego zastosowanie,
3. zapewnienie możliwości całodobowego zgłaszania żądań unieważnienia kwalifikowanych certyfikatów.

Niezrealizowanie któregokolwiek z nich przez kwalifikowanego dostawcę usług może stanowić dla ministra właściwego do spraw informatyzacji podstawę do podjęcia działań nadzorczych, wynikających z art. 30 u.o.u.z.. Istotne jest, aby w tym miejscu podkreślić, iż ustawodawca nie definiuje pojęcia nadzoru. Dodatkowo zgodnie z art. 12a ust. 1 pkt 13 ustawy z o działach administracji rządowej[40] dział informatyzacja obejmuje sprawy nadzoru nad świadczeniem usług zaufania w rozumieniu przepisów o usługach zaufania. Obecnie ministrem właściwym do spraw informatyzacji, kierującym działem administracji rządowej informatyza-

[38] Wyrok WSA w Warszawie z 22 kwietnia 2021 r., VII SA/Wa 2089/20, LEX nr 3184763.
[39] Tamże.
[40] Ustawa z dnia 4 września 1997 r., Dz.U. z 2022 r. poz. 2512 ze zm.

cja, jest Minister Cyfryzacji (zob. § 1 rozporządzenia Prezesa Rady Ministrów z 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji[41]).

Minister jest uprawniony jest do wydania decyzji o odebraniu kwalifikowanemu dostawcy usług zaufania statusu kwalifikowanego. Taka decyzja nakłada na kwalifikowanego dostawcę usług obowiązek przekazania odpowiednich dokumentów i danych ministrowi właściwemu do spraw informatyzacji, gdy żaden inny kwalifikowany dostawca usług nie przejął działalności kwalifikowanego dostawcy, który utracił status kwalifikowanego.

Wskazany nadzór regulowany jest rozporządzeniem eIDAS, zgodnie z którym obejmuje on działania *ex ante* i *ex post*, służące zapewnieniu, by kwalifikowani dostawcy usług zaufania i świadczone przez nich usługi zaufania spełniały wymogi prawne wynikające z tego rozporządzenia.

Korzystanie z podpisów elektronicznych sprawia, że zarządzanie dokumentami, składanie oświadczeń woli, transakcje przebiegają szybciej i nie wymagają fizycznej obecności w określonym miejscu. Istnieje jednakże szereg zagrożeń, z jakimi obecnie mamy do czynienia, a które wiążą się z kradzieżą podpisu elektronicznego. Zjawisko podszywania się pod inną osobę w środowisku cyfrowym, określane w literaturze specjalistycznej mianem *spear phishingu*, stanowi jeden z najbardziej niebezpiecznych i zarazem trudnych do wykrycia typów ataków socjotechnicznych. Jego istotą jest precyzyjne ukierunkowanie działań sprawcy na konkretny podmiot – najczęściej osobę pełniącą funkcje decyzyjne, mającą dostęp do systemów teleinformatycznych lub dysponującą znaczącymi zasobami organizacyjnymi bądź finansowymi. Celem takiego ataku jest nie tylko uzyskanie informacji, ale także wymuszenie określonych działań, w szczególności wywołanie skutków prawnych poprzez złożenie oświadczenia woli.

W praktyce *spear phishing* wiąże się z bezprawnym użyciem danych identyfikujących inną osobę, w tym także danych uwierzytelniających wykorzystywanych do składania podpisu elektronicznego. Skutek takiego działania

[41] Dz.U. poz. 2720.

jest szczególnie doniosły prawnie: osoba trzecia może złożyć oświadczenie woli, które – z uwagi na obecność weryfikowalnych atrybutów podpisu elektronicznego – jest przez odbiorcę traktowane jako pochodzące od osoby wskazanej w certyfikacie lub identyfikatorze elektronicznym.

Rozporządzenie eIDAS oraz przepisy krajowe dotyczące usług zaufania opierają się na założeniu, że poprawnie zweryfikowany podpis elektroniczny daje podstawę do przypisania autorstwa oświadczenia osobie, której dane widnieją w certyfikacie. Jest to swoiste domniemanie autentyczności odzwierciedlone w konstrukcji prawnej podpisu elektronicznego jako instrumentu identyfikacji.

Spear phishing ujawnia nie tylko słabości techniczne systemów ochrony tożsamości cyfrowej, lecz również istotne luki w regulacjach dotyczących przypisania skutków prawnych oświadczeń składanych w procesach informatycznych. W połączeniu z rosnącą automatyzacją procedur administracyjnych oraz pełną cyfryzacją postępowań cywilnoprawnych problem ten nabiera charakteru systemowego. Rozwiązania wymagają zarówno precyzyjnego ukształtowania obowiązków w zakresie nadzoru nad środkami identyfikacji elektronicznej, jak i stworzenia klarownych zasad alokacji ryzyka pomiędzy podmiotami korzystającymi z usług zaufania.

Podkreślenia wymaga fakt, iż zgodnie z rozporządzeniem eIDAS środki nadzorcze wobec niekwalifikowanych dostawców usług zaufania powinny zostać zastosowane przez organ nadzoru jedynie wtedy, gdy zostanie on poinformowany (przez samego dostawcę usług zaufania, przez inny organ nadzoru czy też w drodze zgłoszenia od użytkownika lub na podstawie własnego dochodzenia), że niekwalifikowany dostawca usług zaufania nie wypełnia wymogów rozporządzenia eIDAS[42]. Oznacza to, iż do chwili uzyskania takiej informacji organ nadzorczy nie ma podstaw do podejmowania władczych działań w stosunku do niekwalifikowanego dostawcy usług nadzorczych. Niesie to ze sobą ryzyko korzystania z podpisu elektronicznego niekwalifikowanego w sposób, który może naruszać interes właściciela takiego podpisu bądź osób trzecich. Aby zro-

[42] Szerzej: M. Ciorgoń-Urbańska, *Komentarz do art. 27* [w:] B. Kwiatek, A. Skóra (red.), *Usługi zaufania oraz identyfikacja elektroniczna. Komentarz*, Warszawa 2024.

zumieć powagę takiego stanu, należy wskazać, iż podpis elektroniczny będzie miał status podpisu „nieważny" w przypadku: upływu terminu ważności certyfikatu, unieważnienia certyfikatu, zmiany w treści dokumentu po jego podpisaniu. Oznacza to, iż w przypadku niekwalifikowanego podpisu elektronicznego możliwe są sytuacje, gdy dochodzi do jego kradzieży, zastosowania przez osobę nieuprawnioną i pomimo tego wywołuje on skutki prawne przewidziane określonymi przepisami prawa.

W art. 27 ust. 2 u.o.u.z. uregulowano zakres nadzoru ministra nad dostawcami usług zaufania, obejmujący wyszczególnione w nim zadania nadzorcze. Katalog uprawień ministra ma charakter otwarty, co oznacza, że poza wyszczególnionymi w nim zadaniami organ nadzoru może podejmować również inne działania nadzorcze, między innymi wynikające z krajowych regulacji. Należy również podkreślić, że zakres oraz rodzaj możliwych do zastosowania środków nadzorczych wobec kwalifikowanych dostawców usług zaufania jest szerszy niż wobec niekwalifikowanych dostawców usług zaufania, co wynika bezpośrednio z reguły ustanowionej w art. 17 ust. 3 rozporządzenia eIDAS. Pozwala to ustawodawcy krajowemu na kształtowanie przepisów krajowych w sposób zapewniający maksymalne bezpieczeństwo w zakresie posługiwania się podpisem elektronicznym.

Minister ds. cyfryzacji jest organem, który ma kompetencje do stwierdzenia, że kwalifikowany dostawca usług zaufania prowadzi działalność niezgodnie z przepisami o usługach zaufania i podjąć działania przewidziane przepisami prawa. Wskazane przez przepisy prawa uprawnienia nadzorcze ministra ds. cyfryzacji wiążą się z działaniami ściśle wynikającymi z przepisów prawa i w trybach w nich określonych. Oznacza to, iż skutki podejmowanych działań są oddalone w czasie, zwiększając przez to ryzyko wystąpienia zagrożeń związanych z niewłaściwym bądź nielegalnym korzystaniem z podpisu elektronicznego.

8. Wnioski

Konkludując, w ocenie autorki pojawia się konieczność zwiększenia bezpieczeństwa korzystania z podpisu elektronicznego poprzez wprowadzenie przez ustawodawcę narzędzi zabezpieczających uczestników obrotu gospo-

darczego, np. poprzez wprowadzenie wymogu stosowania dodatkowego narzędzia weryfikacji składania podpisu elektronicznego. Jeśli dojdzie do nieuprawnionego przejęcia kopii danego podpisu elektronicznego bądź określona osoba użyje jej do podpisania dokumentów w sposób bezprawny, będzie musiała pamiętać, iż zobowiązana będzie dodatkowo do przedstawienia obiektywnego dowodu legalności. Tego typu praktyka jako forma zabezpieczenia podpisu elektronicznego wprowadzona została w bankowości elektronicznej. Brak dodatkowego potwierdzenia wywołuje skutek w postaci braku uznania złożonego podpisu elektronicznego. Zastosowanie takiego uwierzytelniania dwuskładnikowego zmniejsza prawdopodobieństwo, iż nieupoważniona osoba korzysta z bezprawnie pozyskanego narzędzia do składania podpisu elektronicznego osoby trzeciej. Zwiększa to pewność, że tylko uprawnione osoby podpisują dane oświadczenie.

Istotnym jest w ocenie autorki wprowadzenie szybkich i efektywnych narzędzi nadzorczych uprawniających ministra ds. cyfryzacji do skutecznego zawieszania ważności certyfikatów potwierdzających podpis elektroniczny do czasu podjęcia ostatecznej decyzji w zakresie odebrania uprawnień zaufanemu dostawy. Taka praktyka zawieszania ważności podpisu elektronicznego zwiększa bezpieczeństwo obrotu gospodarczego.

Korzystanie z podpisu elektronicznego jest coraz bardziej dostrzegane w naszym życiu – przyspiesza działania, ogranicza biurokrację, pozwala na prowadzenie określonych działań bez wychodzenia z domu. Szczególnie pandemia COVID-19 przyspieszyła jego używanie w codziennej praktyce administracji publicznej. Nie wolno jednakże zapominać o ryzykach, jakie niesie ze sobą korzystanie z podpisu elektronicznego. Jednym z najpoważniejszych zagrożeń związanych z podpisem elektronicznym jest możliwość jego podrobienia. Stąd też używanie podpisu elektronicznego wymaga wysokiej odpowiedzialności za stan oprogramowania w urządzeniu, z którego korzystamy do podpisu.

Coraz większa liczba dostawców zaufanych umożliwia wystawienie kwalifikowanego certyfikatu podpisu elektronicznego bez potrzeby weryfikacji tożsamości w trakcie spotkania bezpośredniego, zastępując je weryfikacją w trakcie połączenia wideo. Usługi takie dostępne są zarówno u dostawców zagranicznych, jak i krajowych. W ocenia autorki tego typu

praktyka powinna być ustawowo zakazana jako zwiększająca prawdopodobieństwo „podrobienia" podpisu elektronicznego.

Technologie stosowane przy podpisach elektronicznych podlegają nieustannie doskonaleniu. Stosowanie zaś takich podpisów staje się coraz łatwiejsze i wymaga coraz mniej wiedzy technologicznej, jednak należy być świadomym podstawowych zasad ich działania. Należy pamiętać, iż nawet jeśli ustawodawca stworzy regulacje chroniące uczestników obrotu gospodarczego, konieczna jest stała aktualizacja wiedzy na temat podpisów elektronicznych.

Bibliografia:

Anusz A., *Ochrona konsumentów w świetle rozporządzenia eIDAS*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2020, nr 2, s. 101–110, DOI: 10.7172/2299-5749.IKAR.2.9.8.

Ciorgoń-Urbańska M., *Komentarz do art. 27* [w:] B. Kwiatek, A. Skóra (red.), *Usługi zaufania oraz identyfikacja elektroniczna. Komentarz*, Wolters Kluwer, Warszawa 2024.

Dumortier J., Vandezande N., *Trust in the proposed EU regulation on trust services?*, „Computer Law & Security Review" 2012, nr 28, s. 568–576.

Goździaszek Ł., *Identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym Unii Europejskiej. Komentarz*, Legalis 2019, *komentarz do art. 1 rozporządzenia eIDAS*.

Jóźwiak I., *Odpowiedzialność dostawców usług zaufania – wybrane aspekty*, „Człowiek w cyberprzestrzeni" 2018, nr 3, s. 36–54.

Kitchin R., *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*, Sage, Londyn 2014.

Marucha M., *Nowa ustawa o podpisie elektronicznym*, „Monitor Prawniczy" 2002, nr 2, s. 67–74.

Marucha-Jaworska M., *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Wolters Kluwer, Warszawa 2017.

Marucha-Jaworska M., *Podpis elektroniczny*, Prawo i Praktyka Gospodarcza, Wydawnictwo Prawo i Praktyka Gospodarcza, Warszawa 2002.

Monarcha-Matlak A., *Usługi zaufania i identyfikacja elektroniczna*, „Acta Iuris Stetinensis" 2018, nr 3, s. 143–162, DOI: 10.18276/ais.2018.23-08.

Negroponte N., *Being Digital*, Alfred A. Knopf, Nowy Jork 1995.

Pawłowska K., *Podpis elektroniczny w porównaniu z podpisem własnoręcznym*, „e-Biuletyn" 2007, nr 4, s. 1–10.

Polański P.P., *Towards the single digital market for e-identification and trust services*, „Computer Law & Security Review" 2015, nr 31, s. 773–781, DOI: https://doi.org/10.1016/j.clsr.2015.09.001.

Romaszewski A., Trąbka W., Kielar M., Gajda K., *Wprowadzenie usług zaufania zgodnych z rozporządzeniem UE eIDAS w aspekcie systemów informacyjnych opieki zdrowotnej (cz. 1)*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2016, nr 42, s. 24–40.

Śledziewska D., Kozłowski R.W., *Gospodarka cyfrowa. Jak technologie zmieniają świat*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2020.

Świtał P., *Podpis elektroniczny – wybrane aspekty prawne*, „Studenckie Zeszyty Naukowe" 2013, nr 23, s. 104–116.

Wierzbowski M., *Administracja publiczna w dobie cyfryzacji*, Wydawnictwo C.H. Beck, Warszawa 2019.