

PRAWO NOWYCH TECHNOLOGII

redakcja naukowa Kinga Flaga-Gieruszyńska, Jacek Gołaczyński

Aneta Małgorzata Arkuszewska, Wojciech Bożek, Błażej Gadek
Ewa Galewska, Jacek Gołaczyński, Łukasz Goździaszek
Maria Kaczorowska, Sylwia Kotecka-Kral, Hanna Matyja
Mariusz Nawrocki, Katarzyna Tomaszewska

PRAWO NOWYCH TECHNOLOGII

redakcja naukowa Kinga Flaga-Gieruszyńska, Jacek Gołaczyński

Aneta Małgorzata Arkuszewska, Wojciech Bożek, Błażej Gadek
Ewa Galewska, Jacek Gołaczyński, Łukasz Goździaszek
Maria Kaczorowska, Sylwia Kotecka-Kral, Hanna Matyja
Mariusz Nawrocki, Katarzyna Tomaszewska

Stan prawny na 1 stycznia 2021 r.

Recenzent

Dr hab. Joanna Studzińska, prof. ALK

Wydawca

Magdalena Stojek-Siwińska

Redaktor prowadzący

Adam Choiński

Opracowanie redakcyjne

Katarzyna Świerk-Bożek

Projekt okładek serii

Wojtek Kwiecień-Janikowski, Przemek Dębowski

prawolubni

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

Szanujmy prawo i własność

Więcej na www.legalnakultura.pl

Polska Izba Książki

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2021

ISBN 978-83-8223-513-5

Dział Praw Autorskich

01-208 Warszawa, ul. Przykopowa 33

tel. 22 535 82 19

e-mail: ksiazki@wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz skrótów	7
Wstęp	11
<i>Sylvia Kotecka-Kral</i> Informatyzacja usług publicznych – założenia konstrukcyjne	13
<i>Jacek Gołaczyński, Katarzyna Tomaszewska</i> Informatyzacja postępowania administracyjnego i sądowoadministracyjnego	53
<i>Błażej Gadek</i> Wybrane aspekty udziału konsumenta w handlu elektronicznym	89
<i>Ewa Galewska</i> Zwalczanie nielegalnych treści zamieszczanych przez użytkowników platform internetowych – kierunek regulacji Unii Europejskiej.....	105
<i>Łukasz Goździaszek</i> Informatyzacja postępowania cywilnego	137
<i>Hanna Matyja</i> Udzielanie świadczeń zdrowotnych w modelu telemedycyny w świetle odpowiedzialności cywilnoprawnej za szkodę wyrządzoną pacjentowi	165
<i>Wojciech Bożek</i> Informatyzacja rynku usług finansowych na przykładzie sektora usług płatniczych i bankowych	183
<i>Sylvia Kotecka-Kral</i> Informatyzacja działalności korporacji prawniczych na przykładzie postępowania cywilnego	201

<i>Mariusz Nawrocki</i> Informatyzacja postępowania karnego	227
<i>Mariusz Nawrocki</i> Informatyzacja publicznych rejestrów karnych	239
<i>Maria Kaczorowska</i> Informatyzacja rejestrów sądowych oraz jej znaczenie dla usprawnienia i zapewnienia bezpieczeństwa obrotu cywilnoprawnego	259
<i>Aneta Małgorzata Arkuszewska</i> Informatyzacja pozasądowych form rozwiązywania sporów	283
Autorzy	315

WYKAZ SKRÓTÓW

Akty prawne

k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
k.k.	– ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2020 r. poz. 1444 ze zm.)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
k.p.	– ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2020 r. poz. 1320 ze zm.)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2020 r. poz. 256 ze zm.)
k.p.c.	– ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2020 r. poz. 1575 ze zm.)
k.p.k.	– ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2020 r. poz. 30 ze zm.)
p.p.s.a.	– ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2019 r. poz. 2325 ze zm.)
pr. bank.	– ustawa z 29.08.1997 r. – Prawo bankowe (Dz.U. z 2020 r. poz. 1896 ze zm.)
pr. not.	– ustawa z 14.02.1991 r. – Prawo o notariacie (Dz.U. z 2020 r. poz. 1192 ze zm.)
r.c.i.r.z.	– rozporządzenie Ministra Sprawiedliwości z 15.10.1997 r. w sprawie ustroju i organizacji centralnej informacji o zastawach rejestrowych oraz szczegółowych zasad udzielania informacji, wydawania odpisów i zaświadczeń (Dz.U. Nr 134, poz. 893 ze zm.)
r.s.w.p.s.	– rozporządzenie Prezydenta Rzeczypospolitej Polskiej z 27.05.2019 r. w sprawie szczegółowego sposobu oraz szczegółowych warunków przekazywania skargi wraz z aktami sprawy i odpowiedzią na skargę do sądu administracyjnego (Dz.U. poz. 1003)
r.u.s.p.	– rozporządzenie Ministra Sprawiedliwości z 18.06.2019 r. – Regulamin urzędowania sądów powszechnych (Dz.U. poz. 1141 ze zm.)

r.w.d.r.z.	– rozporządzeniu Ministra Sprawiedliwości z 9.07.2019 r. w sprawie warunków organizacyjno-technicznych dotyczących formy wniosków i dokumentów oraz ich składania do sądów prowadzących rejestr zastawów i do centralnej informacji o zastawach rejestrowych, a także orzeczeń, odpisów, zaświadczeń i informacji doręczanych wnioskodawcom przez sądy oraz centralną informację za pośrednictwem systemu teleinformatycznego (Dz.U. poz. 1345)
r.w.m.	– rozporządzeniu Ministra Sprawiedliwości z 20.06.2016 r. w sprawie wysokości wynagrodzenia i podlegających zwrotowi wydatków mediatora w postępowaniu cywilnym (Dz.U. poz. 921)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)
u.i.d.p.	– ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346 ze zm.)
u.k.s.	– ustawa z 22.03.2018 r. o komornikach sądowych (Dz.U. z 2020 r. poz. 121 ze zm.)
u.k.w.h.	– ustawa z 6.07.1982 r. o księgach wieczystych i hipotece (Dz.U. z 2019 r. poz. 2204)
u.p.k.	– ustawa z 30.05.2014 r. o prawach konsumenta (Dz.U. z 2020 r. poz. 287 ze zm.)
u.p.z.p.s.	– ustawa z 13.05.2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym (Dz.U. z 2020 r. poz. 152)
u.r.p.	– ustawa z 6.07.1982 r. o radcach prawnych (Dz.U. z 2020 r. poz. 75 ze zm.)
ustawa COVID-19	– ustawa z 2.03.2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. poz. 1842 ze zm.)
ustawa o KRK	– ustawa z 24.05.2000 r. o Krajowym Rejestrze Karnym (Dz.U. z 2019 r. poz. 1158)
ustawa o KRS	– ustawa z 20.08.1997 r. o Krajowym Rejestrze Sądowym (Dz.U. z 2021 r. poz. 112 ze zm.)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
u.u.p.	– ustawa z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2020 r. poz. 794 ze zm.)
u.z.r.r.z.	– ustawa z 6.12.1996 r. o zastawie rejestrowym i rejestrze zastawów (Dz.U. z 2018 r. poz. 2017)

Czasopisma, zbiory orzecznictwa

M. Praw.	– Monitor Prawniczy
OSNC	– Orzecznictwo Sądu Najwyższego. Izba Cywilna
OSNKW	– Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
PiP	– Państwo i Prawo

Inne

ePUAP	–	Elektroniczna Platforma Usług Administracji Publicznej
KEL	–	uchwała Nadzwyczajnego II Krajowego Zjazdu Lekarzy z 14.12.1991 r. w sprawie Kodeksu Etyki Lekarskiej, https://nil.org.pl/uploaded_images/1574857770_kodeks-etyki-lekarskiej.pdf (dostęp: 15.01.2021 r.)
KRK	–	Krajowy Rejestr Karny
KRS	–	Krajowy Rejestr Sądowy
NSA	–	Naczelny Sąd Administracyjny
SA	–	Sąd Apelacyjny
SN	–	Sąd Najwyższy
WSA	–	Wojewódzki Sąd Administracyjny

WSTĘP

Prawo nowych technologii jest nową, dynamicznie rozwijającą się gałęzią prawa, która nie tylko tworzy nieznana dotąd terminologię i reguły prawne, ale również wpływa bezpośrednio na sposób kształtowania regulacji prawnych we wszystkich obszarach prawa prywatnego i publicznego. Podstawową wartością nowoczesnego prawa jest nadążanie za rozwojem technicznym i cywilizacyjnym współczesnych społeczeństw, co powoduje, że prawo nowych technologii nieustannie się poszerza i przekształca wraz z wprowadzaniem do obrotu prawnego i gospodarczego nowych rozwiązań technicznych, ze sztuczną inteligencją na czele.

Monografia stanowi odpowiedź na zapotrzebowanie na kompleksową analizę obecności prawa nowych technologii w różnych dziedzinach polskiego systemu prawnego. Do współpracy nad nią zostali zaproszeni specjaliści zajmujący się poszczególnymi aspektami funkcjonowania prawa prywatnego i publicznego, którzy w swoich analizach skupili się na elektronizacji i informatyzacji obszarów, których badaniem zajmują się na co dzień. W konsekwencji powstał niepowtarzalny zbiór analiz istotnych dla prawidłowej wykładni konstrukcji prawa cywilnego, karnego, finansowego i administracyjnego, związanych z wdrażaniem nowych technologii zarówno w zakresie funkcjonowania konstrukcji prawnych istotnych dla tych dziedzin prawa, jak i konieczności dalszego uregulowania procesu informatyzacji na potrzeby regulacji stosunków cywilnych i administracyjnoprawnych, a także odpowiedzialności karnej.

Oddane do rąk Czytelników opracowanie rozwiązuje wiele problemów interpretacyjnych odnoszących się do informatyzacji i elektronizacji obrotu prawnego i gospodarczego, w tym kształtowania w tym zakresie praw konsumenckich, funkcjonowania elektronicznych rejestrów karnych i cywilnych, a także działania organów administracji publicznej i wymiaru sprawiedliwości. Z pewnością będzie ono istotnym merytorycznym wsparciem dla praktyków zajmujących się problematyką odnoszącą się do prawa nowych technologii, przenikającego tak wiele obszarów życia społecznego.

Sylvia Kotecka-Kral

INFORMATYZACJA USŁUG PUBLICZNYCH – ZAŁOŻENIA KONSTRUKCYJNE

1. Uwagi ogólne

Rozwój społeczeństwa informacyjnego oraz technologii informacyjno-komunikacyjnych wymusza nowe spojrzenie na zarządzanie zasobami informacyjnymi pozostającymi w dyspozycji podmiotów publicznych, informatyzacja zaś jako metoda zwiększania efektywności przetwarzania danych staje się ważnym elementem zarządzania publicznego. Ogromna część usług publicznych świadczona jest w oparciu o przetwarzanie danych, jakie wpływają do podmiotów publicznych bądź jakimi dysponują podmioty publiczne. Informacja wpływa do organu administracji publicznej na przykład w postaci podania, jest uzupełniana lub weryfikowana przez gromadzenie i ocenę danych w trakcie postępowania, a rezultatem tych czynności staje się decyzja administracyjna, którą można określić mianem wypowiedzi o zgromadzonych danych. Zadaniem organu administracji publicznej jest zebranie, przetworzenie i wartościowanie danych, a następnie tworzenie, w oparciu o prawo materialne i procesowe, danych nowego typu. Wykorzystywana w tych działaniach technologia nie tworzy nowych zasad postępowania z przetwarzaną informacją, lecz pełni rolę służebną wobec reguł postępowania, określonych chociażby w Kodeksie postępowania administracyjnego. Niemniej jednak z uwagi na szybkie zmiany technologiczne oraz niedawno jeszcze funkcjonujące oparcie procedur administracyjnych (prawie) wyłącznie na zasadzie pisemności, a więc dokumentach sporządzonych zarówno przez strony postępowania administracyjnego, jak i organy administracji publicznej na nośniku, jakim jest papier, konieczne stało się wprowadzenie zmian prawnych ułatwiających czy wręcz niekiedy umożliwiających zainformatyzowanie usług publicznych.

W celu prowadzenia dalszych wywodów należy zdefiniować kilka podstawowych pojęć. Następnie zostaną omówione założenia konstrukcyjne informatyzacji usług publicznych w Polsce. Przez założenia konstrukcyjne rozumiem filary, a więc elementy „bazowe”, umożliwiające lub znacznie ułatwiające świadczenie usług publicznych za pomocą

systemów teleinformatycznych i środków komunikacji elektronicznej. Z tego powodu w niniejszym opracowaniu nie zostaną szczegółowo omówione wszelkie kwestie, jakie wiążą się z informatyzacją podmiotów realizujących zadania publiczne.

2. Pojęcie elektronicznej (z informatyzowanej) administracji publicznej

Kilkanaście lat temu w literaturze posługiwano się raczej pojęciami dotyczącymi informatyzacji administracji publicznej, a więc samych struktur organizacyjnych, niż informatyzacji usług publicznych, czyli świadczeń, jakich udzielają instytucje administracyjne, wydając na przykład decyzje.

Zagadnienie *e-government*, czyli elektronicznej (dziś powiedzielibyśmy „z informatyzowanej”) administracji publicznej, zwanej też elektronicznym rządem, e-administracją, elektronicznym zarządzaniem, a nawet elektronicznym państwem, było i jest pojmowane w sposób niejednolity zarówno w literaturze obcojęzycznej, jak i polskiej. *E-government* był nowym podejściem do zarządzania administracją publiczną, obejmującym wewnętrzne i zewnętrzne jej środowisko z wykorzystaniem nowoczesnych technologii cyfrowych. To niewątpliwie przełomowa koncepcja zarządzania administracją publiczną, związana z rewolucją społeczną, jaka łączy się z transformacją między społeczeństwem industrialnym a społeczeństwem informacyjnym. Elektroniczna administracja była definiowana jako zintegrowane działanie, zmierzające do stworzenia tańszego i efektywniejszego aparatu władzy przez zastosowanie nowoczesnych metod zarządzania państwem, dzięki którym przewidywane jest obniżenie kosztów jego funkcjonowania¹.

W sferze podmiotowej *e-government* stanowi relację między administracją publiczną a adresatami usług publicznych. Występujące modele powiązań są następujące:

- 1) *Government to Citizen* (*e-government* w stosunku do obywateli),
- 2) *Government to Business* (*e-government* w stosunku do przedsiębiorców),
- 3) *Government to Government* (relacja między strukturami publicznymi).

Na tle przedstawionych modeli komunikacji prowadzonych przez organy administracyjne powstało w nauce prawa pojęcie stosunku informacyjnego, kreujące nowy rodzaj stosunków administracyjnoprawnych, związanych przecież ze świadczeniem usług publicznych. Wyodrębnia się dwie główne płaszczyzny relacji zachodzących w badanych stosunkach – zewnętrzne (między organem a obywatelem) oraz wewnętrzne (między organami administracyjnymi)². Obecnie obok tradycyjnych sposobów nawiązania stosunku administracyjnoprawnego występuje również możliwość jego zainicjowania lub

¹ Zob. A. Hareża, *Wprowadzenie do problematyki elektronicznej administracji publicznej*, „Prawo Mediów Elektronicznych” 2011/1, s. 27 i powołana tam literatura.

² I. Lipowicz, *Administracyjnoprawne zagadnienia informatyki*, Katowice 1984, s. 116–143.

prowadzenia go na dalszym etapie postępowania przy wykorzystaniu sieci i systemów teleinformatycznych. W obu przypadkach charakter i cechy stosunku administracyjno-prawnego są tożsame. Elektroniczna postać stanowi jedynie inną metodę wykonywania praw i obowiązków, składających się na treść tych zależności.

3. Pojęcie z informatyzowanej usługi publicznej

Z zagadnieniem z informatyzowanych usług publicznych wiążą się pojęcia komputeryzacji i informatyzacji, a także cyfryzacji, digitalizacji, środków komunikacji elektronicznej, systemu teleinformatycznego, usługi i usługi publicznej.

Pojęcia komputeryzacji i informatyzacji były lub są niekiedy stosowane zamiennie, chociaż dokonanie między nimi rozróżnienia jest niezbędne. Zgodnie ze *Słownikiem informatycznym*³ „komputeryzacja” to proces wprowadzania nowoczesnych metod przetwarzania danych za pomocą komputerów oraz ich stosowanie w praktycznie wszystkich obszarach ludzkiego działania, na przykład w zarządzaniu przedsiębiorstwami i instytucjami, nauczaniu, sterowaniu procesami technologicznymi i projektowaniu. Komputeryzacja oznacza więc zastosowanie urządzeń komputerowych zarówno przez podmioty prywatne, jak i publiczne.

Jednakże szerszy obszar wykorzystania rozwiązań technologicznych służących realizacji zadań i usług publicznych przez organy administracji definiuje pojęcie „informatyzacja”. *Słownik informatyczny*⁴ określa informatyzację jako proces wprowadzania rozwiązań informatycznych, które wspomagają funkcjonowanie przedsiębiorstw i instytucji. Przez to pojęcie należy rozumieć jakościowe rozwinięcie procesów skorelowanych z wykorzystaniem postępu technologicznego i zastosowaniem komputerów o istotny aspekt organizacyjny. Zawiera on w sobie pojęcie komputeryzacji i wiąże się z możliwie najlepszym wykorzystaniem zasobów cyfrowych, oprogramowania oraz urządzeń komputerowych. Informatyzacja jest wyrazem efektywnego, zintegrowanego i kompleksowego zarządzania publicznego. Niesie ze sobą usprawnienie funkcjonowania podmiotów publicznych, zwiększając ich wydajność i potencjalne możliwości.

Warto również zdefiniować pojęcia cyfryzacji, digitalizacji i techniki cyfrowej, ponieważ one również są używane, w tym w oficjalnych rządowych programach czy dokumentach dotyczących informatyzacji usług publicznych. *Słownik języka polskiego*⁵ w zakresie pojęcia „cyfryzacja” odsyła do terminu „digitalizacja” (inny sposób zapisu to „dygitalizacja”), które definiuje jako nadawanie postaci cyfrowej danym pisanym i drukowanym, zawartym na nośnikach magnetycznych lub innych. Z kolei *Encyklopedia*

³ Hasło „informatyzacja” [w:] P. Adamczewski, *Słownik informatyczny*, Gliwice 2005, s. 102.

⁴ Hasło „cyfryzacja” [w:] P. Adamczewski, *Słownik...*, s. 81.

⁵ Hasło „dygitalizacja” [w:] <https://sjp.pwn.pl/szukaj/dygitalizacja.html>.

PWN⁶ wskazuje, że „technika cyfrowa” to zespół metod, procedur i środków służących do wytwarzania, przetwarzania, przesyłania i przechowywania w pamięci sygnałów cyfrowych. „Sygnał” jest pojęciem z zakresu telekomunikacji (a więc dziedziny nauki i techniki oraz działalności ludzkiej dotyczącej przekazywania na odległość wiadomości za pośrednictwem sygnałów, obecnie głównie elektrycznych) i oznacza czynnik będący nośnikiem wiadomości, umożliwiający jej przesyłanie na odległość lub rejestrację⁷. „Sygnał cyfrowy” to sygnał dyskretny, w przypadku którego kolejne wartości wielkości fizycznej są reprezentowane przez ciągi liczb należących do skończonego zbioru. „Sygnał binarny” z kolei jest sygnałem cyfrowym, w którym liczbami reprezentującymi wartości wielkości fizycznej są 0 i 1 (elementy binarne, bity). Warto odnotowania jest również pojęcie „dyskretyzacja sygnału”, które oznacza przekształcenie sygnału analogowego w sygnał dyskretny.

Pojęcie środków komunikacji elektronicznej definiuje ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną. „Środki komunikacji elektronicznej” to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności poczta elektroniczna (art. 2 pkt 5 u.s.u.d.e.).

Godne uwagi jest również wpisanie się idei *e-government* świadczącej usługi publiczne przy wykorzystaniu nowych technologii w nurt koncepcji administracji responsywnej, często porównywanej do administracji „współpracującej”, „partycypacyjnej”, „inkluzyjnej”, „demokratycznej” bądź „reprezentatywnej”. Obecna pozycja organów administracji publicznej uległa bowiem daleko idącej zmianie. Z tego względu organy administracji publicznej zaczynają pełnić funkcję usługodawcy jak każdy inny podmiot, decyzja administracyjna zaś – usługi. Taki stan rzeczy jest podkreślany niejednokrotnie w strategiach propagujących rozwój społeczeństwa informacyjnego, a wraz z nim – elektronicznej administracji oferującej „klientom” bogatą ofertę usług publicznych⁸. Ponieważ istotą wykorzystania nowoczesnej techniki nie jest wyposażenie urzędników w szybkie komputery i elektroniczne bazy danych, a *de facto* usprawnienie działalności organów administracji publicznej, należy mówić raczej o z informatyzowanych usługach publicznych, świadczonych przez tę administrację obywatelom i przedsiębiorcom.

Zdefiniowanie pojęcia „usługa publiczna” nie jest zadaniem łatwym. Na jej określenie używa się, czasem zamiennie jako synonimy, takich pojęć, jak na przykład usługi użyteczności publicznej, usługi świadczone w interesie ogólnym, usługi świadczone w ogólnym interesie gospodarczym, usługi powszechne, usługi użytku publicznego, usługi społeczne. Chaos terminologiczny swoje istnienie zawdzięcza także różnemu

⁶ Hasło „technika cyfrowa” [w:] <https://encyklopedia.pwn.pl/szukaj/technika%20cyfrowa.html>.

⁷ Hasło „sygnał” [w:] <https://encyklopedia.pwn.pl/szukaj/sygna%C5%82.html>.

⁸ A. Haręza, *Wprowadzenie...*, s. 30.

umocowaniu usług użyteczności publicznej w systemach prawnych poszczególnych państw członkowskich Unii Europejskiej, co prowadzi do braku harmonizacji regulacji dotyczącej usług publicznych na szczeblu unijnym. Samo pojęcie usługi jest równie szerokie, co niedookreślone. Przykładowo, zgodnie z art. 57 TFUE usługami w rozumieniu Traktatów są świadczenia wykonywane zwykle za wynagrodzeniem w zakresie, w jakim nie są objęte postanowieniami o swobodnym przepływie towarów, kapitału i osób. Usługi obejmują zwłaszcza: a) działalność o charakterze przemysłowym, b) działalność o charakterze handlowym, c) działalność rzemieślniczą, d) wykonywanie wolnych zawodów.

Usługi publiczne są w literaturze różnie definiowane i klasyfikowane. Ich istotne cechy definicyjne i klasyfikacyjne są związane z takimi kryteriami, jak między innymi: charakter praw dostępności, rodzaj podmiotu świadczącego usługi, źródła finansowania ze środków publicznych, rodzaje realizowanych zadań publicznych, rodzaje zaspokajanych potrzeb i interesów publicznych, sposób świadczenia⁹. Należy przyjąć, że usługami publicznymi są te usługi, które państwo, w ramach ciążących na nim zobowiązań, dostarcza (lub zapewnia dostarczenie) ogółowi społeczeństwa, zaspokajając minimum jego potrzeb w wymiarze ustalonym drogą umowy społecznej. Ich dostawa stanowi więc wyraz realizacji interesu publicznego i wymaga zaangażowania państwa zarówno w sensie organizacyjnym, jak i finansowym¹⁰. Inna definicja stanowi, że usługi publiczne można zdefiniować jako dobra publiczne, w stosunku do których niemożliwe jest wykluczenie kogokolwiek z korzystania z nich. Są to dobra, które niezależnie od liczby korzystających posiadają określoną wartość, której nie naruszają kolejni użytkownicy¹¹. W doktrynie do kategorii usług publicznych zalicza się więc tylko te usługi, które służą osiągnięciu celów wyższych, stanowiąc o być albo nie być wspólnoty obywateli.

Ogólna klasyfikacja przedmiotowa usług publicznych jest następująca:

1) usługi i e-usługi administracyjne:

- wydawanie dokumentów niebędących decyzjami administracyjnymi, zezwoleniami, koncesjami,
- wprowadzanie do baz danych uzyskiwanych bezpośrednio od klientów organów administracyjnych,
- wydawanie zezwoleń i decyzji w trybie zgodnym z Kodeksem postępowania administracyjnego,
- wydawanie zezwoleń i koncesji dotyczących działalności gospodarczej reglamentowanej przez państwo;

2) usługi i e-usługi społeczne:

⁹ Zob. O. Lissowski, *Usługi publiczne i usługi w interesie ogólnym – koncepcja i niektóre problemy instytucjonalne marketyzacyjnej modernizacji świadczenia usług publicznych w Unii Europejskiej*, „Zeszyty Naukowe Politechniki Poznańskiej”. Organizacja i Zarządzanie 2017/74, s. 10.

¹⁰ Zob. J. Ząbkowicz, *Rynkowe usługi użyteczności publicznej w Unii Europejskiej. W poszukiwaniu konsensu i pewności prawnej*, Warszawa 2017, s. 24.

¹¹ B. Koźuch, A. Koźuch, *Istota współczesnych usług publicznych* [w:] *Usługi publiczne. Organizacja i zarządzanie*, red. B. Koźuch, A. Koźuch, Kraków 2011, s. 34–39.

- ochrona zdrowia,
 - oświata i wychowanie,
 - kultura,
 - kultura fizyczna i rekreacja,
 - pomoc i opieka społeczna,
 - mieszkalnictwo,
 - bezpieczeństwo publiczne;
- 3) usługi techniczne:
- transport – usługi i infrastruktura,
 - zaopatrzenie w wodę i kanalizacja,
 - gospodarka odpadami oraz utrzymanie czystości i porządku,
 - cementnictwo,
 - zaopatrzenie w energię (elektroenergetyka, gazownictwo, ciepłownictwo),
 - zieleń publiczna¹².

Usługa publiczna dotyczy więc wszystkich potrzeb obywateli, obsługiwanych bezpośrednio przez instytucje publiczne albo przez instytucje niepubliczne w imieniu instytucji publicznych. Jest ona realizowana w trybie ciągłym, ma charakter powszechny, nie dyskryminujący kogokolwiek i jest realizowana po najniższych możliwych kosztach¹³.

Należy także zwrócić uwagę na relacje zewnętrzne, jakie organ administracji nawiązuje, świadcząc usługi publiczne. Przybierają one postać informacyjną, interakcyjną (z ewentualnym wyróżnieniem interakcji dwukierunkowej) oraz transakcyjną. Wskazana kolejność nie jest przypadkowa i wiąże się ze stopniem informatycznego zaawansowania świadczonej usługi publicznej. Informowanie przybiera bowiem charakter pasywny (zwłaszcza jeśli jest realizowane w trybie bezwnioskowego dostępu do informacji publicznej), natomiast interakcja związana jest z aktywnym komunikowaniem się z organem administracji publicznej. Faza transakcyjna jest uwięzieniem koncepcji z informatyzowanej usługi publicznej, gdyż najczęściej stanowi o możliwości załatwienia określonej sprawy „w całości” za pośrednictwem komunikacji elektronicznej. Usługa publiczna nie musi zakończyć się wydaniem aktu administracyjnego, lecz zawsze skutkuje nawiązaniem stosunku prawnego za pomocą środków komunikacji elektronicznej (przez system teleinformatyczny). Proces świadczenia konkretnej usługi przez organy administracji może obejmować kilka relacji, począwszy od informowania, przez nawiązanie interakcji, do fazy kończącej sprawę, czyli transakcji. Koncepcja świadczenia kompleksowych usług przez organ administracji publicznej, do którego wpłynęło określone podanie, tzw. *concept* jednego okienka (*one-stop-government*, czy też *one-stop-shop*), likwiduje tradycyjny podział organizacyjny i funkcyjny organów administracji publicznej. Ze strony klienta administracji takie rozwiązanie jest nie tylko redukcją podejmowanych czynności,

¹² Zob. B. Kożuch, A. Kożuch, *Usługi...*, *passim*; cyt za: O. Lissowski, *Usługi...*, s. 10.

¹³ G. Bliźniuk, *Usługi publiczne z perspektywy Europy*, http://www.magazynngmina.pl/index.php?option=com_k2&view=item&id=246:uslugi-publiczne-z-perspektywy-europy (dostęp: 26.08.2020 r.).

lecz również redukcją stosunków administracyjnoprawnych. Pojedyncza interakcja w jednym organie administracji publicznej wywołuje szereg interakcji, zwięzłych transakcjami między wnioskodawcą a zbiorem organów właściwych przedmiotowo i miejscowo do załatwienia żądań zawartych w podaniu. Nie jest wykluczone wydanie aktów administracyjnych przez więcej niż jeden organ¹⁴.

Ustawa o świadczeniu usług drogą elektroniczną definiuje także pojęcie „świadczenie usługi drogą elektroniczną” (art. 2 pkt 4), a nie „usługa elektroniczna”. Jest nim wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z 16.07.2004 r. – Prawo telekomunikacyjne¹⁵. Jednakże ustawa ta nie ma zastosowania do świadczenia usług przez podmioty publiczne, stanowi bowiem implementację dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)¹⁶.

Ustawa o świadczeniu usług drogą elektroniczną określa obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną, zasady wyłączania odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną, zasady ochrony danych osobowych osób fizycznych korzystających z usług świadczonych drogą elektroniczną. „Usługodawcą” z kolei to osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługi drogą elektroniczną (art. 2 pkt 6 u.s.u.d.e.).

Definicję pojęcia „system teleinformatyczny”, który jest używany do realizacji zadań publicznych, zawiera ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Jest nim zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów Prawa telekomunikacyjnego (art. 3 pkt 3 u.i.d.p.). Jest to jedno z kluczowych pojęć z zakresu informatyzacji usług publicznych.

„Zinformatyzowaną usługę publiczną” można próbować określić jako usługę udostępnianą w trybie ciągłym przez organy administracji publicznej lub inne podmioty administrujące w ramach ich kompetencji i na odległość za pomocą systemów telein-

¹⁴ A. Haręża, *Wprowadzenie...*, s. 31.

¹⁵ Dz.U. z 2019 r. poz. 2460 ze zm.

¹⁶ Dz.Urz. UE L 178, s. 1.

formatycznych. Element kosztów systemu informatycznego oraz opłat za świadczone usługi publiczne został w tej definicji pominięty. Za niektóre elektroniczne usługi publiczne, podobnie jak za usługi publiczne świadczone tradycyjnie („na miejscu”), opłata jest pobierana, ale nie powinna stanowić elementu konstrukcyjnego definicji z informatyzowanej usługi publicznej.

4. Czynniki wpływające na informatyzację usług publicznych w Polsce

4.1. Uwagi ogólne

Aby wprowadzić z informatyzowane usługi publiczne w Polsce konieczne były zmiany prawne. Należy wyróżnić dwa podstawowe założenia konstrukcyjne informatyzacji usług publicznych, które zrewolucjonizowały myślenie opartej dotąd na dokumentacji pisemnej (papierowej) administracji publicznej. Były to niewątpliwie identyfikacja elektroniczna podmiotu korzystającego z usługi publicznej oraz zdefiniowane legalnie pojęcie dokumentu elektronicznego, do którego odwołuje się także wiele ustaw regulujących świadczenie usług publicznych. Identyfikację elektroniczną i dokument elektroniczny należy określić mianem podstawowych założeń konstrukcyjnych, na których opiera się informatyzacja usług publicznych. Gdyby nie możliwość sporządzania aktów administracyjnych w formie dokumentu elektronicznego (a nawet więcej – załatwiania spraw w formie dokumentu elektronicznego; zob. art. 14 § 1 k.p.a.), a także wnoszenia pism przez obywatela czy przedsiębiorcę w formie dokumentu elektronicznego, których treść i pochodzenie potwierdzone jest podpisem elektronicznym lub inną metodą identyfikacji elektronicznej, niemożliwe byłoby wprowadzenie elektronicznych podań, elektronicznych doręczeń czy elektronicznej decyzji administracyjnej (i innych aktów administracyjnych). Opierając się na treści ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, można wyróżnić następujące założenia konstrukcyjne informatyzacji usług publicznych:

- 1) identyfikacja elektroniczna usługobiorcy;
- 2) możliwość załatwiania spraw w formie dokumentu elektronicznego;
- 3) centralne planowanie przedsięwzięć informatycznych w Programie Zintegrowanej Informatyzacji Państwa;
- 4) centralne ustalanie standardów dla systemów teleinformatycznych i rejestrów publicznych służących realizacji zadań publicznych oraz wymiany informacji w postaci elektronicznej w celu zapewnienia interoperacyjności, dostępności dla osób z dysfunkcjami, z nałożeniem na organy administracji publicznej ponownego wykorzystywania danych już raz podanych przez obywatela lub przedsiębiorcę (zob. art. 220 k.p.a.);
- 5) elektroniczna Platforma Usług Administracji Publicznej.

Wyróżnione wyżej założenia konstrukcyjne wpisują się w europejski kontekst świadczenia z informatyzowanych usług publicznych. Komisja Europejska, realizując inicjatywy zapowiedziane w Strategii Jednolitego Rynku Cyfrowego UE (*A Digital Single Market Strategy for Europe*)¹⁷, opracowała Plan Działania na rzecz eGovernment (*eGovernment Action Plan 2016–2020*)¹⁸. Dokument ten wyznacza cel w postaci usunięcia istniejących barier cyfrowych, stworzenia jednolitego rynku cyfrowego oraz powstrzymania fragmentacji, która nastąpiła w związku z modernizacją administracji publicznych. Wyróżniono w nim kompletne i spójne zasady odnoszące się do budowy elektronicznych (z informatyzowanych) usług publicznych. Są nimi w szczególności:

- 1) domyślna cyfrowość – usługi administracji publicznej powinny być z założenia cyfrowe (co obejmuje informacje nadające się do przetwarzania automatycznego), przy zachowaniu innych kanałów dla osób nieposiadających dostępu do Internetu z wyboru lub z konieczności; usługi publiczne powinny być ponadto świadczone w ramach pojedynczych punktów kontaktowych lub punktów kompleksowej obsługi i za pośrednictwem różnych kanałów;
- 2) zasada jednorazowości – administracje publiczne powinny zadbać o to, aby obywatele i przedsiębiorstwa podawały te same informacje tylko raz; urzędy administracji publicznej, jeśli jest to dozwolone, powinny ponownie wykorzystywać wewnętrznie te dane (w zgodzie z przepisami dotyczącymi ochrony danych), eliminując w ten sposób dodatkowe obciążenia dla obywateli i przedsiębiorstw;
- 3) powszechność i dostępność – administracje publiczne powinny opracować cyfrowe usługi publiczne tak, aby były one z założenia powszechne i dostosowane do różnych potrzeb, na przykład potrzeb osób starszych i osób niepełnosprawnych;
- 4) otwartość i przejrzystość – administracje publiczne powinny wymieniać się informacjami i danymi oraz zapewnić obywatelom i przedsiębiorstwom dostęp do ich danych, kontrolę nad nimi i możliwość ich poprawiania; powinny też umożliwić użytkownikom monitorowanie procesów administracyjnych, które ich dotyczą; ponadto powinny współpracować z zainteresowanymi podmiotami (takimi jak przedsiębiorstwa, badacze i organizacje *non-profit*) w zakresie projektowania i świadczenia usług;
- 5) domyślna transgraniczność – administracje publiczne powinny udostępnić odpowiednie cyfrowe usługi publiczne na poziomie transgranicznym i zapobiec dalszej fragmentacji, wspierając tym samym mobilność w ramach jednolitego rynku;
- 6) domyślna interoperacyjność – usługi publiczne powinny być opracowywane w taki sposób, aby funkcjonowały bezproblemowo w ramach jednolitego rynku i między sztywnymi strukturami organizacyjnymi w oparciu o swobodny przepływ danych i usług cyfrowych w Unii Europejskiej;

¹⁷ COM/2015/0192 final.

¹⁸ Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions *EE eGovernment Action Plan 2016–2020 Accelerating the digital transformation of government*, COM/2016/0179 final.

- 7) niezawodność i bezpieczeństwo – w przypadku wszystkich inicjatyw należy zapewnić wyższy poziom ochrony danych osobowych, prywatności i bezpieczeństwa informatycznego, niż wynikałoby to ze zwykłej zgodności z ramami prawnymi w tych dziedzinach, uwzględniając wspomniane elementy na etapie projektowania; spełnienie tych istotnych warunków może zwiększyć zaufanie do usług cyfrowych i stopień korzystania z nich.

4.2. Identyfikacja elektroniczna usługobiorcy

4.2.1. Uwagi ogólne

Przy świadczeniu usług poprzez system teleinformatyczny szczególnie istotne jest trafne zidentyfikowanie osoby korzystającej z usługi. W przeciwnym wypadku istniałoby ryzyko, że osobą faktycznie korzystającą z usługi świadczonej przez system teleinformatyczny podmiotu publicznego byłaby osoba inna niż ta, która została wskazana na potrzeby realizacji usługi, na przykład wydania decyzji administracyjnej. Ponieważ niektóre usługi publiczne mogą bezpośrednio kształtować prawa i obowiązki obywateli, taka sytuacja mogłaby w znaczącym stopniu zagrozić pewności obrotu prawnego.

Przepisy art. 20a u.i.d.p., mające kluczowe znaczenie z punktu widzenia informatyzacji usług publicznych, określają sposoby identyfikacji użytkownika systemów teleinformatycznych podmiotu publicznego, w którym udostępniane są usługi *online*. Jego obecne brzmienie zostało ukształtowane przez ustawę z 5.07.2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw¹⁹, która w tym zakresie weszła w życie 11.09.2018 r. (a w zakresie art. 20a ust. 1 pkt 2 weszła w życie 29.09.2018 r.). Uwierzytelnienie użytkownika systemu teleinformatycznego podmiotu publicznego, w którym udostępniane są usługi *online*, wymaga zatem użycia:

- 1) środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej, o którym mowa w art. 21a ust. 1 pkt 2 lit. a u.u.z.i.e.²⁰, lub
- 2) środka identyfikacji elektronicznej wydanego w notyfikowanym systemie identyfikacji elektronicznej, lub
- 3) danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi *online*.

Uwierzytelnianie z wykorzystaniem środków identyfikacji elektronicznej, o których mowa w pkt 1 i 2, zapewnia się adekwatnie do wymaganego poziomu bezpieczeństwa,

¹⁹ Dz.U. poz. 1544 ze zm.

²⁰ Ustawa z 5.09.2016 r. o usługach zaufania i identyfikacji elektronicznej (Dz.U. z 2020 r. poz. 1173 ze zm.).

o którym mowa w art. 25 u.u.z.i.e. Podmiot publiczny, który używa do realizacji zadań publicznych systemu teleinformatycznego, może umożliwiać użytkownikowi uwierzytelnienie w tym systemie także przez zastosowanie innych technologii.

Używane wyżej pojęcia „uwierzytelnienie” oraz „identyfikacja elektroniczna” nie zostały zdefiniowane w przepisach krajowych. Należy tu zatem stosować definicje z rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE²¹. Zgodnie z nimi „uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej (art. 3 pkt 5 rozporządzenia 910/2014). Z kolei „identyfikacja elektroniczna” oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną (art. 3 pkt 1 rozporządzenia 910/2014).

4.2.2. Środki identyfikacji elektronicznej wydane w krajowym systemie identyfikacji elektronicznej

4.2.2.1. Uwagi ogólne

W art. 20a ust. 1 u.i.d.p. spośród wymienionych mechanizmów uwierzytelniania w pierwszej kolejności następuje odesłanie do środków identyfikacji elektronicznej wydanych w systemie identyfikacji elektronicznej przyłączonych do węzła krajowego identyfikacji elektronicznej.

„Środek identyfikacji elektronicznej” został zdefiniowany w art. 3 pkt 2 rozporządzenia 910/2014 jako materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi *online*. W świecie cyfrowym środek identyfikacji elektronicznej pełni rolę podobną do tej, jaką spełnia dokument tożsamości w świecie realnym, jego głównym celem jest bowiem umożliwienie wiarygodnego potwierdzenia tożsamości posługującej się nim osoby, występującej w imieniu swoim lub określonego podmiotu.

Zakłada się nieodpłatność wykorzystywania środków identyfikacji elektronicznej do uwierzytelnienia w celu realizacji elektronicznych usług publicznych, zdefiniowanych przez pryzmat podmiotu świadczącego taką usługę, czyli usług *online* świadczonych przez podmiot, o którym mowa w art. 2 i art. 19c ust. 1 u.i.d.p., lub podmiot sektora publicznego, o którym mowa w art. 3 pkt 7 rozporządzenia 910/2014. Stosownie

²¹ Dz.Urz. UE L 257, s. 73.

do brzmienia wyżej wskazanego rozporządzenia przez „podmioty sektora publicznego” należy rozumieć każdy organ państwowy, regionalny lub lokalny, podmiot prawa publicznego lub stowarzyszenie utworzone przez jeden lub kilka takich organów lub jeden lub kilka takich podmiotów prawa publicznego, lub jednostkę prywatną, której co najmniej jeden z tych organów, podmiotów lub jedno z takich stowarzyszeń udzieliły upoważnienia do świadczenia usług publicznych, gdy działa ona na podstawie takiego upoważnienia (art. 3 pkt 7).

Celem rozporządzenia 910/2014 jest zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania nie tylko na wewnętrzne potrzeby krajowe, ale i na potrzeby dostępu do transgranicznych usług *online* oferowanych przez państwa członkowskie (motyw 12 preambuły rozporządzenia 910/2014). Narzędziem służącym do osiągnięcia tego celu jest korzystanie z systemu węzłów w poszczególnych krajach członkowskich Unii Europejskiej, dzięki którym możliwe jest połączenie systemów poszczególnych państw. Definicja węzła znajduje się w rozporządzeniu wykonawczym Komisji (UE) 2015/1501 z 8.09.2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym²². Zgodnie z art. 2 pkt 1 rozporządzenia 910/2014 „węzeł” to punkt przyłączenia będący częścią architektury systemu interoperacyjności identyfikacji elektronicznej, który jest wykorzystywany w procesie transgranicznego uwierzytelniania osób i który ma zdolność do rozpoznawania i przetwarzania lub przesyłania danych do innych węzłów poprzez umożliwienie sprzężenia krajowej infrastruktury identyfikacji elektronicznej jednego państwa członkowskiego z krajowymi infrastrukturami służącymi do identyfikacji elektronicznej innych państw członkowskich. Węzły umożliwiają zatem po pierwsze scalenie na potrzeby uwierzytelniania użytkowników informacji pochodzącej z poszczególnych krajowych systemów identyfikacji elektronicznej, po drugie wymianę takich informacji z analogicznymi węzłami w innych krajach członkowskich Unii Europejskiej²³.

Podwójną funkcję węzłów podkreśla również polska definicja węzła krajowego zawarta w art. 21a ust. 2 u.u.z.i.e. Zgodnie z tym przepisem „węzeł krajowy” jest rozwiązaniem organizacyjno-technicznym umożliwiającym uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi *online*, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego. Do węzła krajowego przyłączone są:

²² Dz.Urz. UE L 235, s. 1, ze sprost.

²³ Zob. G. Kubalski, M. Małowiecka, *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, Legalis 2019, art. 20a, nb 4.

- 1) systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej (art. 21a ust. 1 pkt 2 lit. a u.u.z.i.e., przywołany w treści art. 20a ust. 1 pkt 1 u.i.d.p.);
- 2) systemy teleinformatyczne, w których udostępniane są usługi *online* (art. 21a ust. 1 pkt 2 lit. b u.u.z.i.e.), a zatem te systemy, które w celu uwierzytelniania użytkowników korzystają z informacji pochodzących z systemów identyfikacji elektronicznej.

W art. 20a ust. 1 pkt 1 u.i.d.p. wskazano, że do uwierzytelniania użytkownika systemu teleinformatycznego mogą być wykorzystane wszystkie systemy identyfikacji elektronicznej bezpośrednio przyłączone do węzła krajowego. Co do zasady będą to jednak systemy krajowe. Systemy zagraniczne mogą być co prawda wykorzystywane, ale ich podłączenie do węzła krajowego następuje za pośrednictwem systemu transgranicznego.

Węzeł krajowy będzie umożliwiał uwierzytelnienie użytkowników systemów teleinformatycznych korzystających z usług *online* podmiotów publicznych, z wykorzystaniem środka identyfikacji elektronicznej wydanego w krajowym systemie identyfikacji elektronicznej przyłączonym do tego węzła albo środka identyfikacji elektronicznej wydanego w zagranicznym systemie identyfikacji elektronicznej, do którego dostęp będzie możliwy za pośrednictwem węzła transgranicznego. Został on przewidziany jako rozwiązanie organizacyjno-techniczne, łączące z jednej strony platformy, na których udostępniane są usługi publiczne i niepubliczne, a z drugiej systemy identyfikacji elektronicznej, w ramach których będą wydawane środki identyfikacji elektronicznej oraz węzeł transgraniczny. Funkcjonowanie węzła krajowego będzie zapewniał minister właściwy do spraw informatyzacji (Minister Cyfryzacji, którego zadania wykonuje obecnie Prezes Rady Ministrów)²⁴.

W celu zapewnienia bezpieczeństwa i pewności obrotu, w którym jako podmioty odpowiedzialne za systemy identyfikacji elektronicznej będą uczestniczyć także podmioty niepubliczne, przewidziano, że zgoda na przyłączenie do węzła krajowego systemu identyfikacji elektronicznej będzie wydawana przez ministra właściwego do spraw informatyzacji w drodze decyzji administracyjnej. Minister będzie mógł wydać decyzję o przyłączeniu systemu identyfikacji elektronicznej do węzła krajowego po spełnieniu warunków określonych w art. 21b u.u.z.i.e. Niespełnianie ich będzie skutkowało wydaniem decyzji o odmowie przyłączenia systemu identyfikacji elektronicznej do węzła krajowego.

Strona internetowa węzła krajowego eIDAS²⁵ została uruchomiona 9.09.2018 r. Można na niej znaleźć najaktualniejsze informacje dotyczące funkcjonowania węzła krajowego

²⁴ Zob. rozporządzenie Prezesa Rady Ministrów z 6.10.2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz.U. poz. 1716).

²⁵ <http://login.gov.pl>

oraz informacje dla integratorów – zarówno dostawców środków identyfikacji elektronicznej, jak i twórców systemów teleinformatycznych, w których świadczone są usługi *online*²⁶. Docelowo użytkownicy z informatyzowanych usług publicznych nie muszą przy logowaniu do portali administracji publicznej pamiętać wielu haseł. Do wszystkich będą mogli zalogować się za pomocą jednego, wybranego przez siebie loginu²⁷. Początkowo potwierdzanie tożsamości możliwe było tylko za pomocą profilu zaufanego, jednakże stopniowo również środków identyfikacji będzie przybywać. Logowanie jest już także możliwe przy wykorzystaniu haseł używanych do systemów bankowości elektronicznej.

Nie jest wykluczone osiągnięcie w przyszłości przez system przyłączony do węzła krajowego statusu systemu notyfikowanego.

4.2.2.2. Podpis elektroniczny

W Polsce podpis elektroniczny funkcjonuje już od kilkunastu lat i jest instytucją szeroko opisaną w literaturze, do której wypada odesłać. W ramach Unii Europejskiej, na mocy dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych²⁸, która weszła w życie 19.01.2000 r., państwa członkowskie miały obowiązek wprowadzenia w życie przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do wykonania dyrektywy w terminie do 19.07.2001 r. Dyrektywa została uchylona 1.07.2016 r. przez rozporządzenie nr 910/2014. Rozporządzenie 910/2014 stanowi część polskiego porządku prawnego i jest bezpośrednio stosowane od 1.07.2016 r. (z wyjątkami określonymi w art. 52).

Zarówno w dyrektywie 1999/93/WE, jak i rozporządzeniu 910/2014 zdefiniowano pojęcia „podpis elektroniczny” i „zaawansowany podpis elektroniczny”. Termin „kwalifikowany podpis elektroniczny” nie było zdefiniowane w dyrektywie 1999/93/WE, natomiast interpretowano je z jej postanowień, zwłaszcza z treści art. 5 ust. 1.

„Podpis elektroniczny”, według art. 3 pkt 10 rozporządzenia 910/2014, oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis. „Zaawansowany podpis elektroniczny” to podpis elektroniczny, który spełnia wymogi

²⁶ G. Kubalski, M. Małowiecka, *Ustawa...*, Legalis 2019, art. 20a, nb 4.

²⁷ Według informacji aktualnej na 18.01.2021 r. za pomocą login.gov.pl można się zalogować do 291 serwisów, w tym: platformy ePUAP, Internetowego Konta Pacjenta, Platformy Usług Elektronicznych Zakładu Ubezpieczeń Społecznych, Emp@tii Portalu Informacyjno-Usługowego, praca.gov.pl, obywatel.gov.pl, Centralnej Ewidencji i Informacji o Działalności Gospodarczej, gabinet.gov.pl, biznes.gov.pl, e-urzędu Miasta Oświęcim, Ultima Ratio Stowarzyszenia Notariuszy Rzeczypospolitej Polskiej, GSKO Urzędu Gminy w Płużnicy – zob. <https://login.gov.pl/login/services>.

²⁸ Dz.Urz. UE L 13, s. 12, ze zm.

określone w art. 26 rozporządzenia 910/2014 (art. 3 pkt 11 rozporządzenia 910/2014), a zatem: jest unikalnie przyporządkowany podpisującemu, umożliwia ustalenie tożsamości podpisującego, jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą oraz jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna. Zgodnie z brzmieniem art. 3 pkt 12 rozporządzenia 910/2014 „kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. Przymiot kwalifikacji urządzenia uzyskuje się po spełnieniu enumeratywnej listy warunków zawartych w załączniku II do rozporządzenia 910/2014 (art. 3 pkt 23 rozporządzenia 910/2014), przymiot zaś kwalifikacji certyfikatu – od strony podmiotowej, jeśli zostanie on wydany przez dostawcę usług spełniającego warunki zawarte w załączniku I do rozporządzenia 910/2014 i formalnie uznanego przez właściwy organ nadzoru (art. 3 pkt 15 rozporządzenia 910/2014).

W obu aktach prawnych – dyrektywie 1999/93/WE i rozporządzeniu 910/2014 – wskazano również na skutki prawne wykorzystania podpisu elektronicznego. Zgodnie z art. 25 rozporządzenia 910/2014 podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich. Oznacza to, że kwalifikowany podpis elektroniczny z powodzeniem może zastąpić podpis własnoręczny urzędnika na przykład na decyzji administracyjnej.

Rozporządzenie 910/2014 powinno zapewnić długoterminową konserwację informacji w celu zapewnienia prawnej ważności podpisów elektronicznych przez wydłużone okresy oraz zagwarantowania możliwości ich walidacji bez względu na przyszłe zmiany technologiczne.

Omawiając zagadnienie podpisu elektronicznego i jego ogromnego znaczenia dla rozwoju z informatyzowanych usług publicznych, należy także wskazać na krajowe akty prawne. Podpis elektroniczny był regulowany ustawą z 18.09.2001 r. o podpisie elektronicznym²⁹, która została uchylona 7.10.2016 r. przez ustawę z 5.09.2016 r. o usługach zaufania i identyfikacji elektronicznej. Ustawa o podpisie elektronicznym definiowała pojęcia „podpis elektroniczny” oraz „bezpieczny podpis elektroniczny”, pomijała zaś definicję terminu „zaawansowany podpis elektroniczny”. Ustawa o usługach zaufania i identyfikacji elektronicznej określa: 1) krajową infrastrukturę zaufania; 2) działalność

²⁹ Dz.U. z 2013 r. poz. 262 ze zm.

dostawców usług zaufania, w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych; 3) tryb notyfikacji krajowego systemu identyfikacji elektronicznej; 4) nadzór nad dostawcami usług zaufania; 5) krajowy schemat identyfikacji elektronicznej; 6) nadzór nad krajowym schematem identyfikacji elektronicznej. Jej przepisów nie stosuje się do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników. Ustawa ta służy stosowaniu rozporządzenia 910/2014.

4.2.2.3. Podpis zaufany i profil zaufany

Zgodnie z art. 20aa u.i.d.p. minister właściwy do spraw informatyzacji odpowiada za funkcjonowanie systemu teleinformatycznego, który po pierwsze zapewnia obsługę publicznego systemu identyfikacji elektronicznej, w którym wydawany jest profil zaufany i profil osobisty, a po drugie umożliwia podmiotom publicznym uwierzytelnienie osoby fizycznej przy użyciu środka identyfikacji elektronicznej (profil zaufany i profil osobisty) oraz zapewnienie osobie fizycznej możliwości opatrzenia dokumentu elektronicznego podpisem zaufanym.

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne w art. 3 pkt 14a definiuje pojęcie „podpis zaufany”. Jest nim podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający dane identyfikujące osobę, ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie, o którym mowa w art. 20aa pkt 1 u.i.d.p., obejmujące: imię (imiona), nazwisko, numer PESEL, identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony, czas jego złożenia.

Definicja podpisu zaufanego posługuje się siatką pojęciową rozporządzenia 910/2014. „Podpis zaufany” to szczególny rodzaj podpisu elektronicznego, a zatem stanowi dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis (art. 3 pkt 10 rozporządzenia 910/2014). Cechą wyróżniającą podpis zaufany pośród innych podpisów jest posłużenie się pieczęcią elektroniczną ministra właściwego do spraw informatyzacji w celu zapewnienia jego autentyczności i integralności. Zakres danych zawartych w podpisie zaufanym zasadniczo nie stanowi jego elementu definicyjnego³⁰.

Podpis zaufany może złożyć każdy, kto posiada profil zaufany. Podpis zaufany służy do podpisywania dokumentów kierowanych do podmiotów publicznych. Profil zaufany to środek identyfikacji elektronicznej zawierający zestaw danych identyfikujących

³⁰ Zob. G. Kubalski, M. Małowiecka, *Ustawa...*, Legalis 2019, art. 3, nb 33.

i opisujących osobę fizyczną, który został wydany w sposób, o którym mowa w art. 20c albo art. 20ca u.i.d.p. (art. 3 pkt 14). Pojęcie środka identyfikacji elektronicznej znajduje się w art. 3 pkt 2 rozporządzenia 910/2014. Zgodnie z przywołanym przepisem „środek identyfikacji elektronicznej” oznacza materialną (np. kartę kryptograficzną) lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi *online*. Profil zaufany jest zatem niematerialną jednostką zawierającą dane identyfikujące osobę fizyczną wydaną w polskim publicznym systemie identyfikacji elektronicznej³¹.

4.2.2.4. Podpis osobisty i profil osobisty

Artykuł 10a u.d.o.³² stanowi, że dowód osobisty umożliwia jego posiadaczowi: uwierzytelnianie w usługach *online* za pomocą profilu osobistego, składanie podpisu osobistego, potwierdzanie obecności w określonym czasie i miejscu. Dowód osobisty spełnia wymogi dla kwalifikowanego urządzenia do składania podpisu elektronicznego określone w załączniku II do rozporządzenia 910/2014.

Zgodnie z art. 2 ust. 1 pkt 9 u.d.o. „podpis osobisty” to zaawansowany podpis elektroniczny w rozumieniu art. 3 pkt 11 rozporządzenia 910/2014, weryfikowany za pomocą certyfikatu podpisu osobistego. Ustawa o dowodach osobistych definiuje i to pojęcie, stanowiąc, że „certyfikat podpisu osobistego” jest poświadczeniem elektronicznym, które przyporządkowuje dane służące do walidacji podpisu osobistego do posiadacza dowodu osobistego, potwierdzające dane tego posiadacza (art. 2 ust. 1 pkt 2).

Z dniem 4.03.2019 r. na mocy ustawy z 6.12.2018 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw³³ słowniczek pojęć znajdujący się w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne został poszerzony o pojęcie profilu osobistego (art. 3 pkt 14b). Pojęcie to zdefiniowano przez odesłanie do treści art. 2 ust. 1 pkt 10 u.d.o. w brzmieniu obowiązującym od 4.03.2019 r., zgodnie z którym „profil osobisty” to środek identyfikacji elektronicznej zawierający dane potwierdzane przez certyfikat identyfikacji i uwierzytelniania. „Certyfikat identyfikacji i uwierzytelniania” to z kolei, zgodnie z brzmieniem art. 2 ust. 1 pkt 1 u.d.o., poświadczenie elektroniczne służące do identyfikacji i uwierzytelnienia posiadacza dowodu osobistego, potwierdzające dane tego posiadacza. Będzie się on znajdował w warstwie elektronicznej dowodu osobistego (art. 12a ust. 1 pkt 2 u.d.o.).

³¹ Zob. G. Kubalski, M. Małowiecka, *Ustawa...*, Legalis 2019, art. 3, nb 32.

³² Ustawa z 6.08.2010 r. o dowodach osobistych (Dz.U. z 2020 r. poz. 332 ze zm.).

³³ Dz.U. z 2019 r. poz. 60 ze zm.

4.2.3. Środki identyfikacji elektronicznej wydane w notyfikowanym systemie identyfikacji elektronicznej

W art. 20a ust. 1 u.i.d.p. w drugiej kolejności wśród sposobów uwierzytelniania użytkownika systemu teleinformatycznego wymieniono środki identyfikacji elektronicznej wydane w notyfikowanym systemie identyfikacji elektronicznej. Systemy identyfikacji elektronicznej wymagające notyfikowania zostały określone w art. 7 rozporządzenia 910/2014, sama zaś procedura notyfikacji – w art. 9 rozporządzenia 910/2014. W praktyce jednak kluczowy dla interpretacji komentowanego przepisu jest art. 12 ust. 1 rozporządzenia 910/2014, ustanawiający obowiązek interoperacyjności krajowych systemów identyfikacji elektronicznej. Zgodnie z określającymi warunki interoperacyjności przepisami rozporządzenia 2015/1501 co do zasady notyfikowane systemy identyfikacji będą podłączone do węzłów krajowych poszczególnych państw członkowskich, a w razie potrzeby wykorzystania ich do uwierzytelnienia użytkownika będzie to następowało przez wymianę danych między węzłami transgranicznymi. W praktyce można zatem przyjąć, że środki identyfikacji elektronicznej wydane w notyfikowanym systemie informacji elektronicznej obejmują:

- 1) środki identyfikacji elektronicznej wydane w krajowym systemie informacji elektronicznej notyfikowanym Komisji Europejskiej – wówczas pokrywają się one ze środkami wymienionymi w art. 20a ust. 1 pkt 1 u.i.d.p.;
- 2) środki identyfikacji elektronicznej wydane w innym niż krajowy systemie informacji elektronicznej notyfikowanym Komisji Europejskiej – wówczas stanowią część krajowego schematu identyfikacji elektronicznej poprzez węzeł transgraniczny³⁴.

Wykaz notyfikowanych systemów identyfikacji elektronicznej jest publikowany w formie komunikatu w Dzienniku Urzędowym Unii Europejskiej serii C. Komunikat nie jest redagowany przyrostowo, lecz całościowo, a więc ogłoszeniu podlegają nie tylko nowo notyfikowane systemy, ale wszystkie, również te objęte wcześniejszymi komunikatami. Ostatni przed złożeniem niniejszej publikacji do druku komunikat został opublikowany 14.12.2020 r.³⁵ i objął systemy (wliczając w nie jeszcze Wielką Brytanię): Niemiec, Włoch (dwa systemy identyfikacji), Chorwacji, Estonii, Hiszpanii, Luksemburga, Belgii (dwa systemy identyfikacji), Portugalii (dwa systemy identyfikacji) i Wielkiej Brytanii, Czech, Holandii (dwa systemy identyfikacji), Słowacji, Łotwy, Danii, Litwy. Polska jeszcze nie notyfikowała środków identyfikacji elektronicznej.

W art. 20a ust. 1a u.i.d.p. ustanowiono dość oczywisty wymóg stosowania środków identyfikacji elektronicznej adekwatnych do wymaganego dla danego systemu tele-

³⁴ Zob. G. Kubalski, M. Małowiecka, *Ustawa...*, Legalis 2019, art. 20a, nb 5.

³⁵ Systemy identyfikacji elektronicznej notyfikowane na podstawie art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.Urz. UE C 432, s. 7).

informatycznego poziomu bezpieczeństwa. Zgodnie z art. 25 u.u.z.i.e. każdy podmiot odpowiedzialny za system teleinformatyczny, w którym udostępniane są usługi *online*, jest zobowiązany je określić. Poziomy bezpieczeństwa zostały zdefiniowane w prawie unijnym. Zgodnie z art. 8 ust. 2 rozporządzenia 910/2014 wyróżnia się trzy poziomy bezpieczeństwa:

- 1) niski poziom bezpieczeństwa – w kontekście systemu identyfikacji elektronicznej odnosi się on do środka identyfikacji elektronicznej, który zapewnia ograniczony stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest obniżenie ryzyka podszycia się lub modyfikacji tożsamości;
- 2) średni poziom bezpieczeństwa – w kontekście systemu identyfikacji elektronicznej odnosi się on do środka identyfikacji elektronicznej, który zapewnia średni stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest znaczne obniżenie ryzyka podszycia się lub modyfikacji tożsamości;
- 3) wysoki poziom bezpieczeństwa – w kontekście systemu identyfikacji elektronicznej odnosi się on do środka identyfikacji elektronicznej, który zapewnia wyższy stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby niż środek identyfikacji elektronicznej o średnim poziomie pewności i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest zapobieganie podszyciu się lub modyfikacji tożsamości.

Należy wskazać, że zapewnienie każdego z tych poziomów wymaga od dostawcy środka identyfikacji elektronicznej dostosowania systemu identyfikacji elektronicznej do odpowiednich specyfikacji i standardów technicznych, a także podporządkowania się ustalonym procedurom, których celem jest odpowiednie do deklarowanego poziomu obniżenie ryzyka podszycia się lub modyfikacji potwierdzanej tożsamości. Stąd też poziom bezpieczeństwa należy odnieść do środka identyfikacji elektronicznej w kontekście systemu identyfikacji elektronicznej, w którym ten środek jest wydawany. Niski poziom bezpieczeństwa obniża ryzyko podszycia się lub modyfikacji tożsamości, średni poziom bezpieczeństwa obniża to ryzyko znacząco, a wysoki poziom bezpieczeństwa wyklucza to ryzyko. Przyjęto, że na poziomie krajowym będą funkcjonowały trzy poziomy bezpieczeństwa odpowiadające wyżej wspomnianym poziomom bezpieczeństwa, o których mowa w rozporządzeniu 910/2014. Zakłada się, że średni poziom bezpieczeństwa jest poziomem bazowym (podstawowym), który będzie miał zastosowanie do większości usług publicznych świadczonych drogą elektroniczną. Uwierzytelnienie użytkownika systemu teleinformatycznego w celu realizacji usługi *online* będzie wymagało użycia środka identyfikacji elektronicznej na poziomie bezpieczeństwa określonym przez podmiot udostępniający tę usługę.

Z definicji zawartych w rozporządzeniu 910/2014 nie wynika, co dokładnie oznacza dany poziom bezpieczeństwa. Określa go rozporządzenie wykonawcze Komisji (UE) 2015/1502 z 8.08.2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym³⁶. Jego załącznik określa specyfikacje techniczne i procedury dotyczące niskiego, średniego i wysokiego poziomu zaufania w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach notyfikowanego systemu identyfikacji elektronicznej³⁷.

4.2.4. Dane weryfikowane za pomocą kwalifikowanego certyfikatu podpisu elektronicznego

Jako trzeci ze sposobów uwierzytelniania ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne dopuszcza uwierzytelnienie przy użyciu danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego. Jak już wspomniano, uwierzytelnianie oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej (art. 3 pkt 5 rozporządzenia 910/2014). Podmioty publiczne mogą zatem świadczyć takie z informatyzowane usługi publiczne, dla których proces uwierzytelnienia może przebiegać przy użyciu danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego. Dane te są wykorzystywane na przykład do potwierdzenia profilu zaufanego, które polega na weryfikacji zgodności danych zawartych we wniosku o jego wydanie ze stanem faktycznym, a także unieważnienia profilu zaufanego. Obu tych czynności może dokonać samodzielnie osoba fizyczna przy wykorzystaniu kwalifikowanego podpisu elektronicznego, w przypadku gdy kwalifikowany certyfikat podpisu elektronicznego zawiera dane obejmujące co najmniej imię (imiona), nazwisko i numer PESEL.

Uwierzytelnienie użytkownika systemu teleinformatycznego podmiotu publicznego, w którym udostępniane są usługi *online*, wymaga użycia danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi *online* (art. 20a ust. 1 pkt 3 u.i.d.p.).

Mianem „certyfikatu podpisu elektronicznego” określa się poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby (art. 3 pkt 14

³⁶ Dz.Urz. UE L 235, s. 7 ze sprost.

³⁷ Zob. G. Kubalski, M. Małowiecka, *Ustawa...*, Legalis 2019, art. 20a, nb 7.