Identyfikacja elektroniczna w UE – od dyrektywy do rozporządzenia

Agata Burek[1]

Intensywny rozwój komunikacji elektronicznej przyczynił się do zapoczątkowania zawierania umów elektronicznych, do czego niezbędne są bezpieczne, godne zaufania i skuteczne mechanizmy identyfikacji elektronicznej, tzn. takie, w których przesyłane dane nie są dostępne dla osób niepożądanych, oraz takie, w których bez problemu można zidentyfikować strony umowy, a złożone przez nich oświadczenia woli wywołują odpowiednie skutki prawne. W tym momencie pojawiło się miejsce na stworzenie odpowiednich regulacji prawnych. Pierwsze powstały pod koniec XX w., w tym dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[2]. Po latach okazało się, że dyrektywa ta nie spełniła wystarczająco swoich głównych założeń. Celem niniejszego opracowania jest wskazanie, dlaczego tak się stało, a tym samym wskazanie powodów, dla których UE postawiła na nową regulację: rozporządzenie Parlamentu Europejskiego i Rady Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[3], które jako akt ujednolicenia prawa jest nową nadzieją na rozpowszechnienie transakcji elektronicznych na terytorium UE.

Uwagi wstępne

Prężny rozwój technik komunikacji elektronicznej coraz intensywniej wpływa na kwestie gospodarcze i społeczne współczesnego życia. Internet umożliwił permanentny oraz obojętny terytorialnie kontakt pomiędzy podmiotami na całym świecie. Wraz z postępem nieograniczonej komunikacji odczuwana potrzeba anonimowości użytkowników sieci teleinformatycznych straciła na znaczeniu. Obecnie wzrosła nie tylko potrzeba rozpoznawalności, ale również zabezpieczenia swojej tożsamości, ochrony przed podszyciem się. Co więcej, brak pozytywnego potwierdzenia swojej tożsamości drugiemu podmiotowi rodzi problemy w rozwoju wielu możliwości, jakie daje nam komunikacja elektroniczna. Mowa tutaj o czynnościach życia codziennego, jak zakupy online, zawieranie umów elektronicznych czy rezerwacja biletów, które w naturalny sposób przeszły ze świata pozawirtualnego w rzeczywistość wirtualną. Podobnie wygląda kwestia kontaktu z organami administracji publicznej podczas wyrabiania dowodu osobistego czy zakładania działalności gospodarczej. Każda czynność elektroniczna powinna być odpowiednio zabezpieczona przed udostępnieniem zawartych w jej ramach danych niepożądanym osobom trzecim. Podstawą rozwoju e-usług jest zaufanie przez użytkowników do używanych w jej ramach narzędzi (oprogramowania), a także do tożsamości drugiej strony oraz autentyczności i integralności danych[4]. Bazę transakcji elektronicznych powinny stanowić też łatwe mechanizmy ich obsługi. Uwidoczniła się potrzeba identyfikacji, uwierzytelnienia i autoryzacji swojej tożsamości. Identyfikacja to nic innego jak utożsamienie – przypasowanie danych do podmiotu, np. nicku, do konkretnej osoby. Uwierzytelnianie natomiast ma na celu weryfikację podanej tożsamości i jest jednym z najbardziej kluczowych komponentów bezpiecznych transakcji elektronicznych. W momencie gdy tożsamość użytkownika będzie potwierdzona, następuje autoryzacja, czyli proces polegający na odmówieniu albo przyznaniu dostępu do systemu[5]. Wszystkie wymienione elementy istnieją nie tylko w świecie e-usług. Są tak samo stosowane w transakcjach tradycyjnych[6], np. w banku uwierzytelniamy się za pomocą złożenia podpisu zgodnego ze wzorem albo po uprzednim okazaniu dowodu osobistego. Następnie przechodzimy proces autoryzacji, otrzymując dostęp do danych na naszym koncie. W transakcjach tradycyjnych komponenty te są już tak naturalne, że prawie niewyczuwalne. Dopiero w sytuacji e-usług nabierają one większego znaczenia.

Jednak, co staje się, gdy już otrzymamy taki dostęp? Tutaj rozpoczyna się rola prawa, którego zadaniem jest określenie: skutków stosowania narzędzi elektronicznych, przesłanek, które wyznaczą skuteczność złożenia oświadczenia woli, czy takie oświadczenie będzie miało moc dowodową, a także dokonanie systematyki pojęciowej.

[1] Autorka jest studentką kierunku prawo na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] Dz.Urz. UE L Nr 13, s. 12–20; dalej jako: dyrektywa 1999/93/WE.

[3] Dz.Urz. UE L Nr 257, s. 73–114; dalej jako: rozporządzenie eIDAS.

[4] *J. Muszyński*, Identyfikacja, uwierzytelnianie i autoryzacja, http://www.computerworld.pl/news/Identyfikacja-uwierzytelnianie-i-autoryzacja,299422.html (dostęp z 1.4.2017 r.).

[5] *A. Smoliński*, Sposoby zabezpieczeń systemów IT jako ewolucja konwencjonalnych metod zabezpieczeń, s. 12.

[6] *T. Mielnicki* (red.), Identyfikacja i uwierzytelnienie w usługach elektronicznych, Przewodnik Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013, s. 6.

Od dyrektywy do rozporządzenia

Identyfikacja elektroniczna zaczęła być regulowana pod koniec XX w. Pierwsze akty prawne dotyczyły podpisu cyfrowego i zostały ustanowione w Stanach Zjednoczonych Ameryki. Między innymi była to ustawa o podpisach cyfrowych stanu Utah z 9.3.1995 r.[7]. W ślad za regulacjami amerykańskimi poszedł prawodawca wspólnotowy, który uchwalił dyrektywę 1999/93/WE. Celem podpisu elektronicznego miało być zagwarantowanie zaufania do transakcji elektronicznych i ich rozpowszechnianie.

Wspólnoty Europejskie nie pozostawiły tej materii regulacjom krajowym, ponieważ w rozpowszechnieniu transakcji elektronicznych widziały rozwój rynku wewnętrznego. Dlatego pojawiła się potrzeba standaryzacji prawa dotyczącego identyfikacji elektronicznej. Gdyby regulowały to poszczególne prawa krajowe, skutki stosowania danych e-usług miałyby zasięg tylko w danym państwie. Nie tylko powodowałoby to ograniczenie rozwoju e-handlu na rynku wewnętrznym, ale powstałyby również różnice technologiczne i terminologiczne.

Początkowo zdecydowano, że dyrektywa, która jest instrumentem harmonizacji, będzie wystarczająca. Przypomnijmy, że celem takiej regulacji miało być ustanowienie jasnych ram wspólnotowych dla podpisów elektronicznych, co skutkowałoby wzmocnieniem ogólnej akceptacji nowych technologii[8]. Założeniem prawodawcy wspólnotowego było rozpowszechnienie mechanizmu podpisu cyfrowego na terenie UE oraz swobodny, transgraniczny przepływ produktów i usług, pochodzących z handlu elektronicznego i skuteczność prawna podpisu cyfrowego. Dzięki regulacjom omawianej dyrektywy ułatwiony miał być kontakt obywateli UE z władzami innych państw członkowskich w dziedzinach takich jak: podatki, wymiar sprawiedliwości, zamówienia publiczne, ubezpieczenia społeczne i ochrona zdrowia[9]. Kluczowe było również nadanie podpisowi elektronicznemu mocy dowodowej przed sądami, co miało budzić poczucie bezpieczeństwa, w sytuacji gdy niezbędne będzie domaganie się swoich praw przed organami sprawiedliwości. Reasumując, dyrektywa 1999/93/WE miała na celu rozpowszechnienie stosowania podpisu elektronicznego poprzez zapewnienie bezpieczeństwa i zaufania do transakcji elektronicznych.

Komisja UE została zobowiązana do sporządzenia sprawozdania dla Parlamentu Europejskiego i Rady, sprawdzającego wykonanie dyrektywy 1999/93/WE[10]. Dokument ten powstał 15.3.2006 r. Bazę sprawozdania stanowiło studium sporządzone przez zewnętrznych konsultantów oraz nieformalne konsultacje z zainteresowanymi z 2003 r. Przeprowadzono je w celu zebrania praktycznych uwag. Sprawozdanie miało kompleksowo zbadać problemy, z jakimi boryka się identyfikacja elektroniczna w UE – nie tylko teoretycznie, ale też ze względu na obowiązującą praktykę.

Sprawozdanie potwierdziło, że dyrektywa 1999/93/WE sprostała swojemu zadaniu i zrealizowała większość swoich celów. Akt ten implementowało do krajowego porządku prawnego 25 państw członkowskich, co uznano za systematyzujący status prawny podpisu elektronicznego. Jednakowoż stwierdzono, że podpisy elektroniczne nie spopularyzowały się na terytorium UE w takim stopniu, jak zakładano. Od razu można zauważyć tutaj sprzeczność. Podstawowym celem dyrektywy 1999/93/WE było rozpowszechnienie podpisu elektronicznego. Miał on usprawniać handel na rynku wewnętrznym. Obiektywnie należy uznać, że skoro w omawianym sprawozdaniu stwierdzono, że podpisy cyfrowe, zwłaszcza zaawansowane oraz zaawansowane oparte na kwalifikowanym certyfikacie i złożone za pomocą bezpiecznego urządzenia, nie były stosowane na taką skalę, jak zakładano, to dyrektywa 1999/93/WE nie spełniła swojego zadania. Wśród elementów, które złożyły się na taki rezultat, można wymienić:

– komplikacje techniczne, związane z technologią PKI, w których jest stosowany czynnik zaufania podmiotowi trzeciemu, przy zawieraniu transakcji nieznanych sobie stron;
– brak regulacji wymogów usług weryfikacji podpisu elektronicznego przez podmioty świadczące usługi certyfikacyjne oraz ustaleń dotyczących wzajemnego uznawania się przez podmioty świadczące usługi certyfikacyjne, co doprowadziło do wykreowania odmiennych regulacji prawnych w poszczególnych państwach;
– brak interoperacyjności technicznej na poziomie krajowym i międzynarodowym, skutkujący powstaniem niewspółgrających ze sobą systemów;
– droga i skomplikowana archiwizacja dokumentów opatrzonych podpisem elektronicznym.

Chociaż zaawansowane formy podpisu elektroniczne nie przyjęły się w praktyce na tak dużą skalę, jak oczekiwano, to w wielu państwach członkowskich powstały inne mechanizmy bazujące na podpisie elektronicznym w prostszych formach. Wyszczególnić można dwa przeważające przykłady. Pierwszy to usługi bankowości elektronicznej, w której stosuje się hasła jednorazowe. Przyporządkować je można definicji zwykłego podpisu elektronicznego. Drugim zastosowaniem jest elektroniczny dostęp do administracji publicznej, czyli krajowy system identyfikacji. Często funkcjonują one na podstawie kart identyfikacyjnych, umożliwiających identyfikację, uwierzytelnianie i podpisywanie. Świetnym przykładem jest

[7] *M. Marucha-Jaworska*, Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym, Warszawa 2015, s. 46.

[8] Zob. motyw 4 preambuły dyrektywy 1999/93/WE.

[9] *M. Marucha-Jaworska*, Rozporządzenie eIDAS. Zagadnienia prawne i techniczne, Warszawa 2017, s. 20–21.

[10] Art. 12 dyrektywy 1999/93/WE.

Platforma Usług Administracji Publicznej – ePUAP. Jednak pod regulacją dyrektywy 1999/93/WE krajowe systemy identyfikacji nie były uznawane na terytorium UE poza państwem pochodzenia. Ani bankowość elektroniczna, ani krajowe systemy identyfikacji nie były regulowane prawem wspólnotowym, a zdecydowanie wyparły proponowane przez tę dyrektywę instytucje. Zastanawiające jest, czy popularność krajowych systemów identyfikacji oraz e-bankowości nie unaoczniły słabości dyrektywy 1999/93/WE. Skoro obywatele UE używają identyfikacji elektronicznej, to znaczy, że są nią zainteresowani, ale proponowane przez prawodawcę wspólnotowego mechanizmy nie spełniają oczekiwań użytkowników. To, co ich interesuje, to łatwość dostępu i obsługi oraz niskie koszty użytkowania. Można nawet stwierdzić, że najprostsze mechanizmy (zabezpieczania, szyfrowania) wystarczyły, by użytkownicy e-usług poczuli do nich zaufanie.

Pomimo powstałych problemów Komisja podkreśla pozytywny wpływ dyrektywy 1999/93/WE na rynek wewnętrzny, ponieważ uregulowano status prawny podpisu elektroniczne, w tym podstawowe zasady jego dopuszczalności. Jednak powstałe trudności należy usunąć za pomocą różnych inicjatyw[11]. Dla przykładu w maju 2010 r. sporządzono komunikat Komisji Europejskiej „Europejska Agenda Cyfrowa", gdzie założono cel zbudowania zaufania i zapewnienia bezpieczeństwa w środowisku internetowym za pomocą modernizacji przepisów dotyczących podpisu elektronicznego[12]. Dodatkowo Rada Europejska w paru konkluzjach z 2011 r. podniosła potrzebę transgranicznych transakcji elektronicznych, a także bezpiecznej identyfikacji elektronicznej i uwierzytelniania. W konkluzjach pozostawiono Komisji utworzenie jednolitego rynku cyfrowego. We wszystkich działaniach organów UE, które miały zapoczątkować zmianę dyrektywy 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, kładzie się nacisk na zapewnienie bezpieczeństwa i zaufania do transakcji elektronicznych, co można uzyskać dzięki: zwiększeniu pewności prawa, wprowadzeniu regulacji nadzoru, zapewnieniu wzajemnego uznawania krajowych systemów identyfikacji elektronicznej czy powiększeniu zakresu usług zaufania. Z opisanych inicjatyw organów UE wynika jedno – w ciągu pięciu lat od publikacji sprawozdania Komisji z wykonania dyrektywy 1999/93/WE nie było żadnego rzeczywistego działania mającego na celu zmianę prawa w zakresie identyfikacji elektronicznej. Dopiero w Akcie o Jednolitym Rynku Cyfrowym postawiono na modyfikacje tej dyrektywy[13]. W trakcie swojej prezydencji, tzw. w drugiej połowie 2011 r., Rzeczpospolita Polska rozpoczęła europejską dyskusję prowadzącą do opracowania nowej regulacji w sprawie identyfikacji elektronicznej na rynku wewnętrznym. Tym razem miało być to rozporządzenie. Istotną rolę odegrało Ministerstwo Gospodarki, które zorganizowało konferencję pt. *Boosting trust in the digital single market: the role of e-signature*. Podczas wydarzenia podjęto tezę, że w zakres europejskiego rynku cyfrowego wchodzi wspólny system identyfikacji elektronicznej, który należy stworzyć. Komisja Europejska 4.6.2012 r. opublikowała projekt rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE. Przyczyny powstania nowego aktu przedstawione przez Komisję nie różniły się od poglądu przedstawionego w sprawozdaniu z wykonania tej dyrektywy. Oficjalnie nikt nie uznał, że była to zła regulacja. Stwierdzono natomiast, że nowa regulacja ma rozszerzać dorobek dyrektywy. Ostatecznie rozporządzenie eIDAS zostało uchwalone 23.7.2014 r. W podstawowej części, która stanowi większość jego przepisów, weszło do stosowania 1.7.2016 r. Jedno z uznawanych za jego główne założenie, czyli uznawanie krajowych systemów eID przez państwa członkowskie UE (wzajemne uznawanie), ma być stosowane od 29.9.2018 r.

Dyrektywa to instrument harmonizacji prawa[14]. Jej adresatem są państwa członkowskie, którym pozostawia się swobodę wyboru środków i form, za pomocą których ma zostać osiągnięty cel dyrektywy zgodnie z art. 288 akapit 3 Traktatu o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana)[15]. Państwa członkowskie są jednak zobowiązane do transponowania regulacji dyrektywy do prawa krajowego. Prowadzi to do stworzenia wspólnych podstaw w konkretnej materii, ale jednocześnie powoduje powstanie różnic między regulacjami państw[16]. Porządki prawne państw członkowskich zbliżają się w ten sposób do siebie, ale nie są identyczne, jednolite. Akty prawne państw członkowskich, które implementują dyrektywę mogą, w pewnym zakresie, od siebie odbiegać.

Rozporządzenie, odmiennie od dyrektywy, jest instrumentem ujednolicenia prawa. Do jego głównych cech należy ogólność i abstrakcyjność. Jako akt o ogólnym charakterze skierowany jest do szerokiego kręgu adresatów, w tym: organów UE i państw członkowskich, osób fizycznych czy osób prawnych oraz instytucji. Oznacza to, że konstruuje również prawa i obowiązki skierowane do jednostek[17]. Rozporządzenie, po wejściu w życie, wiąże w całości i – co bardzo ważne – jest bezpośrednio stosowane[18]. Eliminuje się w ten sposób potrzebę transponowania przepisów rozporządzenia do po-

[11] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady, Sprawozdanie z wykonania dyrektywy 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, Bruksela 15.3.2006 r.

[12] Europejska agenda cyfrowa: kluczowe inicjatywy, Bruksela 19.5.2010 r., http://europa.eu/rapid/press-release_MEMO-10-200_pl.htm (dostęp z 1.4.2017 r.).

[13] 12 projektów dla jednolitego rynku na 2012 r.: wspólnie na rzecz nowego wzrostu gospodarczego, IP/11/46, Bruksela 13.4.2011 r., http://europa.eu/rapid/press-release_IP-11-469_pl.htm (dostęp z 1.4.2017 r.).

[14] *J. Barcz*, Instytucje i prawo Unii Europejskiej. Podręcznik dla kierunków prawa, zarządzania i administracji, Warszawa 2015, s. 232.

[15] Dz.Urz. UE C Nr 202; dalej jako: TFUE.

[16] *J. Barcz*, Instytucje i prawo…, s. 232–233.

[17] *Ibidem*, s. 230.

[18] Zob. art. 288 akapit 2 TFUE.

rządków krajowych, ponieważ automatycznie stają się ich częścią, a zakres prawny regulowany rozporządzeniem nie może być już stanowiony przez organy państw członkowskich[19]. Tym samym państwa członkowskie nie posiadają kompetencji zmiany przepisów, które są dla nich kłopotliwe. Rozporządzenie jest bardzo skutecznym instrumentem ujednolicenia prawa na terenie UE, ponieważ intensywnie ingeruje w prawa krajowe, ma szeroki zasięg terytorialny i podmiotowy[20].

Powyższe rozważania teoretyczne można przełożyć na omawiane zagadnienie, dyrektywa 1999/93/WE, będąca instrument harmonizacji, spowodowała różnice między regulacjami państw członkowskich w zakresie identyfikacji elektronicznej. Do głównych zalicza się: odmienności terminologiczne, różnice w funkcjonowaniu nadzoru[21] oraz niejednakowe wymogi, które muszą spełnić podmioty świadczące usługi elektroniczne, a także wymogi samego podpisu elektronicznego. Rozporządzenie stawia jednolite warunki uwierzytelniania oraz wymogi dla dostawców usług zaufania. Ujednolicenie standardów stawianych identyfikacji elektronicznej ułatwia wprowadzenie wzajemnego uznawania krajowych systemów identyfikacji elektronicznej przez państwa członkowskie oraz daje duże szanse na rozpowszechnienie się transgranicznych transakcji elektronicznych.

Cele rozporządzenia eIDAS

Warto przyjrzeć się celom, jakie stawia sobie nowa regulacja, mająca zapewnić bezpieczeństwo i zaufanie w kwestii transakcji elektronicznych. Prawodawca unijny stanowi, że rozporządzenie eIDAS ma poszerzać oraz umacniać dorobek uchylonej dyrektywy. Celem nie jest zmienienie całego istniejącego porządku prawnego dotyczącego identyfikacji elektronicznej. Pod rządami dyrektywy nie powstały odpowiednie ramy transgraniczne i międzysektorowe, ułatwiające funkcjonowanie bezpiecznych transakcji elektronicznych, ale nie oznacza że takich ram nie w ogóle nie było[22]. Dopiero późniejsze komplikacje, które dotyczyły praktycznego stosowania zawartych w regulacji mechanizmów, oraz sam charakter dyrektywy spowodowały, że podpis elektroniczny nie rozpowszechnił się jako narzędzie służące do zawierania umów elektronicznych w takim stopniu, jak zakładano. Twierdzi się, że było to spowodowane za małym poczuciem bezpieczeństwa wśród potencjalnych użytkowników usług elektronicznych. W ten sposób wyklarował się naturalny cel nowego rozporządzenia – ulepszenie i ujednolicenie ram prawnych dla podpisów elektronicznych oraz ustanowienie nowych usług, które jednocześnie spełnią warunek bezpieczeństwa i zaufania.

Jednym z najbardziej istotnych celów eIDAS jest wprowadzenie reguł dotyczących korzystania z usług zaufania i identyfikacji elektronicznej na rynku wewnętrznym[23]. Krajowe systemy identyfikacji elektronicznej dotychczas nie były regulowane przez przepisy wspólnotowe. Regulacje takie powstały w poszczególnych państwach członkowskich w ramach krajowej administracji publicznej. Brakowało instytucji, która umożliwiałaby korzystanie z owych systemów w każdym państwie członkowskim[24]. Dlatego eIDAS kładzie duży nacisk na zapewnienie wzajemnego uznawania notyfikowanych systemów identyfikacji elektronicznej na terytorium UE. Takie bariery transgraniczne mają zostać uchylone przynajmniej w zakresie usług publicznych[25]. Obywatel ma w ten sposób zyskać możliwość kontaktowania się z sądami oraz urzędami państw członkowskich za pomocą środka identyfikacji elektronicznej pochodzącego z jego kraju. Zasada wzajemnego uznawania ma dodatkowo objąć poszczególne kwalifikowane usługi zaufania, co spowodować może rozwój dostawców usług zaufania, którzy posiądą możliwość wyjścia ze swoimi usługami poza rynek krajowy[26].

Rozporządzenie eIDAS zakłada neutralność technologiczną, co powinno służyć popularyzowaniu umów elektronicznych na rynku wewnętrznym[27]. Założenie otwartości na rozwój technologiczny wynika z bardzo szybkiego tempa zmian w tej dziedzinie[28]. Gdyby w ciągu najbliższych lat powstały lepsze, łatwiejsze, a przede wszystkim bezpieczniejsze mechanizmy szyfrowania tożsamości, ich wprowadzenie na rynek nie powinno być ograniczone przez prawo. Nowe technologie będą musiały spełniać jedynie wymogi zawarte w Rozporządzeniu eIDAS[29].

Kolejny cel eIDAS to przyznanie mocy dowodowej poszczególnym narzędziom, tj. podpisy elektroniczne. Uchylona dyrektywa dawała im co prawda taką moc, ale Komisja w swoim sprawozdaniu stwierdziła, że nie wyklarowało się orzecznictwo umożliwiające jednoznaczne uznawanie podpisów elektronicznych w praktyce[30]. Dostawcy usług zaufania również wyrażają zdanie, że sądy nie w każdym przypadku dopuszczały takie dowody. Obwinia się w tej kwestii nieścisłości prawne[31]. Teraz wprost istnieją przepisy zabraniające

[19] *J. Barcz*, Instytucje i prawo…, s. 231–232.
[20] *M. Marucha-Jaworska*, Rozporządzenie eIDAS…, s. 33.
[21] *Ibidem*, s. 23.
[22] Motyw 3 preambuły eIDAS.
[23] Forum eIDAS_PL Forum wymiany wiedzy w zakresie Rozporządzenia eIDAS w Polsce, Webinar Forum eIDAS_PL 1 z 26.11.2015 r., https://www.youtube.com/watch?v=BnRr27v9Aqo.
[24] *P. Polański*, Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego, Warszawa 2014, s. 337.
[25] Motyw 12 preambuły eIDAS.
[26] Forum eIDAS_PL Forum wymiany wiedzy w zakresie Rozporządzenia eIDAS w Polsce, Webinar Forum eIDAS_PL 1 z 26.11.2015 r., https://www.youtube.com/watch?v=BnRr27v9Aqo.
[27] Motyw 27. preambuły eIDAS.
[28] Motyw 26. preambuły eIDAS.
[29] Motyw 27. preambuły eIDAS.
[30] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady…, s. 6.
[31] Forum eIDAS_PL Forum wymiany wiedzy w zakresie Rozporządzenia eIDAS w Polsce, Webinar Forum eIDAS_PL 1 z 26.11.2015 r., https://www.youtube.com/watch?v=BnRr27v9Aqo.

odmowy mocy dowodowej podpisom elektronicznym i innym podobnym narzędziom w postępowaniu sądowym na terytorium UE[32].

Rozporządzenie eIDAS pozostawia pewne kwestie do regulacji państwom członkowskim. Te bowiem zostały zobowiązane do wyznaczenia organu nadzoru[33], który będzie sprawowany nad kwalifikowanymi dostawcami usług zaufania. W ramach swoich kompetencji krajowy organ nadzoru sporządza i publikuje tzw. list zaufania, informacje o kwalifikowanych dostawcach usług zaufania w swoim kraju[34]. Sankcje za naruszenie regulacji wprowadzonej przez eIDAS również należy ustalić w ramach swojego państwa[35]. Pomimo że rozporządzenie, jako akt, charakteryzuje się bezpośrednim stosowaniem i co do zasady niemożliwe jest transponowanie regulacji rozporządzeń w postaci ustaw krajowych, to w pewnych przypadkach wymagane jest uchwalenie aktu prawa krajowego, np. w sytuacji wprowadzenia specjalnych instytucji krajowych[36]. Wspomniany wcześniej nadzór usług zaufania jest instytucją potrzebującą takiej regulacji. Każde państwo członkowskie posiada odrębną, swoją strukturę administracji publicznej, dlatego do jego kompetencji należy wybór odpowiedniego podmiotu, który sprawować będzie nadzór usług zaufania.

Podsumowanie

Reasumując, głównym celem eIDAS jest ujednolicenie rynku cyfrowego UE za pomocą ustanowienia szczegółowych przepisów oraz jednolitych standardów uwierzytelniania, w tym możliwości wzajemnego uznawania systemów identyfikacji elektronicznej. Skutkiem nowej regulacji ma być zapewnienie poczucia bezpieczeństwa i zaufania na rynku transakcji elektronicznych wśród ich użytkowników.

Ostateczna ocena celów rozporządzenia eIDAS możliwa jest dopiero po analizie instytucji w nim zawartych, a przede wszystkim po obserwacji funkcjonowania nowych mechanizmów w praktyce. Wtedy możliwe będzie stwierdzenie, czy założone i zamierzone cele zostały spełnione, czy pozostały tylko niezrealizowanymi ideami.

[32] Motyw 22. preambuły eIDAS.
[33] Motyw 30. preambuły eIDAS.
[34] Art. 22 eIDAS.
[35] Art. 16 eIDAS.
[36] *J. Barcz*, Instytucje i prawo…, s. 231.

Słowa kluczowe: identyfikacja elektroniczna, podpis elektroniczny, umowy elektroniczne, dyrektywa, rozporządzenie, transakcje elektroniczne, system identyfikacji elektronicznej, Unia Europejska (UE)

Electronic ID in EU – from directive to regulation

The intensive development of electronic communication has initiated the conclusion of electronic contracts for which secure, trustworthy and effective electronic identification mechanisms are necessary. I.e. those in which the data sent are not available to third parties and those in which the parties to the contract can be identified without difficulty, and their declarations of will bring legal effects. At this point, the need arose to create appropriate legal regulations. The first ones were created at the end of the 20th century, including Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. After many years, it turned out that the Directive, as an act of law harmonization, did not meet its main objectives, and also ceased to fit modern electronic identification solutions. That is why the European Union has set a new regulation: Regulation no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions which, as the act of harmonizing the law, is a new hope for the dissemination of electronic transactions on the territory of the European Union.

Keywords: electronic identification, electronic signature, electronic contracts, directive, regulation, electronic transactions, electronic identification system, European Union.