

Realizacja zasady wzajemnego uznawania na gruncie eIDAS

Karolina Pawiłowicz¹

Możliwość pełnej realizacji zasady wzajemnego uznawania na gruncie rozporządzenia Parlamentu Europejskiego i Rady (UE) 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/WE² (eIDAS) jest zagadnieniem bardzo istotnym, w szczególności z perspektywy prawidłowego funkcjonowania jednolitego rynku cyfrowego. Dodatkowo pozytywnie wpływa na możliwości identyfikacji elektronicznej obywateli UE w innych państwach członkowskich, w dużym stopniu ułatwiając im komunikację z organami administracji publicznej. Jako problem badawczy w niniejszym artykule należy wskazać rozważanie na temat możliwości pełnej realizacji i efektywnej implementacji zasady wzajemnego uznawania, mając na uwadze zakres jej zastosowania, cele oraz konstrukcję prawną.

Uwagi wstępne

Rozporządzenie eIDAS ma na celu zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług *online*, e-biznesu i e-handlu w UE³. Stworzenie jednakowych dla całej UE ram prawnych rozwiązań informatycznych, pozwalających na wiarygodne określenie tożsamości osób fizycznych i jednostek organizacyjnych ma zapewnić budowanie zaufania do środowiska *online*⁴. Jednym z ważniejszych mechanizmów mającym na celu realizację powyższych celów jest wprowadzona w eIDAS zasada wzajemnego uznawania systemów identyfikacji elektronicznej (dalej jako: zasada wzajemnego uznawania). W niniejszym artykule zostaną przedstawione najważniejsze założenia wskazaniem zasady wraz z nakreśleniem oprócz aspektów pozytywnych, także elementów problematycznych w implementacji zasady w praktyce w poszczególnych państwach członkowskich.

Znaczenie zasady

Na mocy eIDAS wszystkie państwa członkowskie zostały zobowiązane do wzajemnego uznawania systemów e-identyfikacji wprowadzonych przez pozostałe państwa członkowskie. Ma to zapewnić obywatelom jednego państwa członkowskiego możliwość dostępu do elektronicznego systemu prowadzonego przez administrację publiczną innego państwa członkowskiego poprzez identyfikację przeprowadzoną za pomocą swojego krajowego systemu. Znaczenie wprowadzonej zasady jest doniosłe, w szczególności w kontekście konieczności implementacji jednolitego rynku cyfrowego. Do tej pory⁵ obywatele UE nie byli uprawnieni do korzystania z krajowych metod e-identyfikacji w celu uwierzytelnie-

nia w innym państwie członkowskim, ponieważ metody te nie były automatycznie uznawane na terytorium całej UE⁶. Wzajemnie uznawane środki identyfikacji elektronicznej ułatwiają transgraniczne świadczenie licznych usług na rynku wewnętrznym⁷, a także ułatwiają bezpośredni kontakt obywateli z organami administracji publicznej⁸.

Analizując znaczenie zasady wzajemnego uznawania, należy także spojrzeć na pozytywne aspekty wywodzące się z szerszej implementacji jednolitego rynku cyfrowego. Wskazuje się, że jednolity rynek cyfrowy pobudza gospodarkę, zmniejsza wpływ działalności ludzkiej na środowisko i poprawia jakość życia dzięki handlowi elektronicznemu i administracji elektronicznej, stając się także coraz bardziej powszechnym⁹. Dodatkowo, dostęp online do informacji i treści to efektywny kanał dystrybucji. Efektywność osiągnięta jest poprzez: niskie koszty wysyłania, udostępniania i otrzymywania informacji oraz ułatwiony, natychmiastowy i wszechobecny dostęp do informacji, a więc występują pozytywne skutki zarówno w zakresie redukcji czasu, jak

¹ Autorka jest doktorantką Kolegium Nauk Prawnych Szkoły Doktorskiej Uniwersytetu Wrocławskiego. ORCID: 0000-0002-2184-7847.

² Dz.Urz. UE L Nr 257, s. 73; dalej jako: eIDAS.

³ Motyw 2 eIDAS.

⁴ PARP Grupa PFR, Rozporządzenie eIDAS. Nowe ramy prawne elektronicznej gospodarki i z informatyzowanych urzędów, <https://www.parp.gov.pl/component/content/article/53930:rozporzadzenie-eidas-nowe-ramy-prawne-elektronicznej-gospodarki-i-z-informatyzowanych-urzedow> (dostęp z 5.3.2021 r.).

⁵ Na gruncie obowiązywania dyrektywy 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, Dz.Urz. L Nr 13, s. 12; dalej jako: dyrektywa 1999/93/WE.

⁶ M. Siemaszkiewicz, Rozporządzenie eIDAS – Nowe ramy prawne w zakresie identyfikacji elektronicznej i usług zaufania w Unii Europejskiej, Przegląd Prawa i Administracji 2016, Nr 107, s. 213.

⁷ Motyw 9 eIDAS.

⁸ M. Siemaszkiewicz, Rozporządzenie eIDAS..., s. 213.

⁹ Parlament Europejski, Noty tematyczne o Unii Europejskiej. Jednolity rynek cyfrowy, <https://www.europarl.europa.eu/factsheets/pl/sheet/43/powszechny-jednolity-rynek-cyfrowy> (dostęp z 5.3.2021 r.).

i kosztów finansowych¹⁰. Na marginesie wskazuje się także, że europejski jednolity rynek cyfrowy odegrał zasadniczą rolę w podtrzymaniu funkcjonowania gospodarki UE i w wspieraniu mieszkańców UE w czasie kryzysu związanego z COVID-19¹¹. W szczególności należy mieć na uwadze sytuacje, w których bezpośredni dostęp do administracji publicznej dla obywateli został ograniczony np. poprzez znaczące ograniczenie pracy urzędów. Mając na uwadze poczynione powyżej refleksje, instytucje unijne zostały postawione przed koniecznością stworzenia oraz efektywnej implementacji mechanizmu wzajemnego uznawania środków identyfikacji elektronicznej na terytorium UE, a co za tym idzie – odejścia od rozwiązań dyrektywy 1999/93 na rzecz dalej idącej interoperacyjności¹².

Uregulowanie zasady wzajemnego uznawania w ramach eIDAS

Rozporządzenie eIDAS stanowi, że jeżeli zgodnie z prawem krajowym lub zgodnie z krajową praktyką administracyjną dostęp do usługi *online* świadczonej przez podmiot sektora publicznego w jednym państwie członkowskim wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, w tym pierwszym państwie członkowskim na potrzeby transgranicznego uwierzytelnienia dla tej usługi *online* uznaje się środek identyfikacji elektronicznej wydany w innym państwie członkowskim. Tym samym eIDAS wprowadza jednak wiele aspektów warunkujących możliwość wzajemnego uznawania¹³. Można wyróżnić trzy warunki. Po pierwsze, środek identyfikacji elektronicznej musi być wydany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję na podstawie art. 9. Innymi słowy, taki środek identyfikacji elektronicznej musi więc zostać notyfikowany. Uznania dokonuje się nie później niż 12 miesięcy po opublikowaniu przez Komisję wykazu. Po drugie, poziom bezpieczeństwa środka identyfikacji elektronicznej odpowiada poziomowi bezpieczeństwa równemu lub wyższemu od poziomu bezpieczeństwa wymaganego przez odpowiedni podmiot sektora publicznego na potrzeby dostępu do tej usługi *online* w pierwszym państwie członkowskim, pod warunkiem że poziom bezpieczeństwa tego środka identyfikacji elektronicznej odpowiada średniemu lub wysokiemu poziomowi bezpieczeństwa. Wreszcie po trzecie, odpowiedni podmiot sektora publicznego korzysta ze średniego lub wysokiego poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi *online*. W przypadku środka identyfikacji elektronicznej, który odpowiada niskiemu poziomowi bezpieczeństwa, środek może być uznany przez podmioty sektora publicznego na potrzeby transgranicznego uwierzytelnienia dla usługi *online* świadczonej przez te podmioty. Należy

podkreślić fakultatywność takiego uznania, która zostanie szczegółowo omówiona w dalszej części artykułu.

Dodatkowo ustawodawca *expressis verbis* wskazał, że kwalifikowane podpisy elektroniczne i pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie oraz kwalifikowane elektroniczne znaczniki czasu wydane w jednym państwie członkowskim są tak samo uznawane we wszystkich państwach członkowskich, oczywiście pod warunkiem spełnienia wytycznych zawartych w eIDAS oraz aktach wykonawczych przez kwalifikowanych dostawców usług zaufania¹⁴. W ramach omawianej problematyki ma ona jednak mniejsze znaczenie, ponieważ po pierwsze, dotyczy ona szczegółowych rozwiązań technicznych, a nie rozwiązania systemowego (z jakim mamy do czynienia na gruncie art. 6 eIDAS) dotyczącego szeroko uregulowanej tematyki wzajemnego uznawania systemów identyfikacji elektronicznej; oraz po drugie, była już częściowo uregulowana w poprzednim stanie prawnym. Zasada wzajemnego uznawania kwalifikowanych podpisów elektronicznych znalazła się w dyrektywie 1999/93/WE, a uregulowanie i rozszerzenie tej zasady w eIDAS stanowi jej kontynuację¹⁵.

Implementacja przy wykorzystaniu interoperacyjności

Po przedstawieniu samej konstrukcji prawnej zasady wzajemnego uznawania należy przejść do analizy jej implementacji i jej realizacji w praktyce. Samo uznanie jest bowiem dopiero pierwszym krokiem długiego procesu mającego na celu możliwość korzystania z tej zasady w praktyce, na której drodze znajdują się przeszkody techniczne. Wskazuje się, że poszczególne państwa członkowskie znajdują się obecnie w innych stadiach zaawansowania w odniesieniu do działalności własnych systemów identyfikacji elektronicznej¹⁶. Należy także wskazać, że poszczególne państwa rozwijają swoje systemy w inny sposób, mając na uwadze własne potrzeby czy własne możliwości implementacji. Obecnie państwa członkowskie zostały postawione przed obowiązkiem technicznego dopuszczenia użytkowników z innych państw członkowskich, co na pewno trzeba będzie odzwierciedlić w technicznym działaniu poszczególnych systemów, rozszerzając możliwości dostępu do systemu i identyfikacji użyt-

¹⁰ Parlament Europejski, Dyrekcja Generalna ds. Polityk Wewnętrznych (DG IPOL), *Streaming and Online Access to Content and Services*, Bruksela 2014, s. 23–24.

¹¹ *Ibidem*.

¹² M. Siemaszkiewicz, *Rozporządzenie eIDAS...*, s. 213.

¹³ Art. 6 eIDAS.

¹⁴ Art. 27, art. 37, art. 41 ust. 3 eIDAS; M. Marucha-Jaworska, *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Lex/el. 2017.

¹⁵ M. Marucha-Jaworska, *Rozporządzenie eIDAS...*, Lex/el. 2017.

¹⁶ M. Siemaszkiewicz, *Rozporządzenie eIDAS...*, s. 213.

kowników. Ze względu na opisane wyżej zróżnicowanie od strony technicznej taka implementacja w zależności od systemu może być zadaniem łatwiejszym, trudniejszym, mniej czy bardziej kosztownym.

Naprzeciw omówionej problematyce wychodzi art. 12 eIDAS wprowadzający ramy interoperacyjności. Wskazuje się, że krajowe systemy identyfikacji elektronicznej notyfikowane na podstawie art. 9 ust. 1 muszą być interoperacyjne. Wprowadzone ramy interoperacyjności spełniają następujące kryteria: są neutralne pod względem technologicznym i nie dyskryminują żadnych konkretnych krajowych rozwiązań technicznych w zakresie identyfikacji elektronicznej w danym państwie członkowskim, są zgodne, w miarę możliwości, z europejskimi i międzynarodowymi standardami, ułatwiają wdrożenie zasady uwzględniania ochrony prywatności już w fazie projektowania oraz zapewniają, aby dane osobowe były przetwarzane zgodnie z dyrektywą 95/46/WE. W ramach omawianego przepisu na państwa członkowskie został nałożony obowiązek wzajemnej współpracy, obejmującej m.in. wymianę informacji, doświadczeń i dobrych praktyk w zakresie systemów identyfikacji elektronicznej, w szczególności wymogów technicznych związanych z interoperacyjnością i poziomami bezpieczeństwa, wzajemną ocenę systemów identyfikacji elektronicznej objętych eIDAS oraz analizę istotnych zmian w sytuacji w sektorze identyfikacji elektronicznej.

Początkowo, w literaturze wypowiadano się krytycznie na temat uregulowania interoperacyjności, wskazując na jego niedoprecyzowanie stanowiące przeszkodę w osiągnięciu odpowiedniego poziomu interoperacyjności w praktyce¹⁷. Należy mieć jednak na uwadze art. 12.8 eIDAS, w którym znalazło się upoważnienie dla Komisji do przyjęcia aktów wykonawczych w sprawie ram interoperacyjności. W następstwie Komisja 8.9.2015 r. wydała rozporządzenie wykonawcze (UE) 2015/1502 z 8.9.2015 r. w sprawie określenia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie identyfikacji elektronicznej¹⁸ określające wymogi techniczne i operacyjne w celu zapewnienia wyższego i bardziej realnego stopnia interoperacyjności systemów identyfikacji elektronicznej. Należy także wspomnieć o pozostałych aktach wprowadzonych przez Komisję w tym zakresie. Decyzja wykonawcza Komisji (UE) 2015/296¹⁹ odnosi się do współpracy państw członkowskich w celu osiągnięcia interoperacyjności i bezpieczeństwa systemów identyfikacji elektronicznej. Decyzja określa metody wymiany informacji i tworzy Sieć Współpracy w celu ułatwienia współpracy w tym zakresie. Natomiast rozporządzenie wykonawcze Komisji (UE) 2015/1501 z 8.9.2015 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 wewnętrznym²⁰ tworzy platformę

umożliwiającą praktyczną łączność między środkami identyfikacji elektronicznej z różnych państw członkowskich w celu wspierania interoperacyjności. Dodatkowo została uchwalona Decyzja wykonawcza Komisji (UE) 2015/1984²¹, która określa okoliczności, formaty i procedury powiadamiania, stanowiąc, że zgłoszenie systemów identyfikacji elektronicznej przez państwa członkowskie jest warunkiem wstępnym wzajemnego uznawania środków identyfikacji elektronicznej. Ciekawym rozwiązaniem, wprowadzonym stosunkowo niedawno (otwarte do 2.10.2020 r.), są konsultacje społeczne w sprawie przeglądu przepisów dotyczących identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Konsultacje przeprowadzane przez Komisję miały na celu zebranie opinii od szerokiego kręgu zainteresowanych stron i obywateli w celu oceny eIDAS²².

Nie należy także zapominać o serii projektów pilotażowych zrealizowanych przez Komisję w celu ułatwienia implementacji wzajemnego uznawania elektronicznej identyfikacji – STORK, STORK 2.0, e-SENS, CEF. Podstawowym założeniem STORK (*Secure Identity across Borders linked*) jest zbudowanie modułowej infrastruktury technologicznej na szczycie krajowej infrastruktury eID²³. Interoperacyjne rozwiązanie STORK opiera się na rozproszonej architekturze, która toruje drogę do pełnej integracji e-usług UE, uwzględniając specyfikację i infrastrukturę obecnie istniejącą w państwach członkowskich UE. Celem projektu jest uproszczenie formalności administracyjnych poprzez zapewnienie bezpiecznego dostępu online do usług publicznych oraz ich przetestowanie w rzeczywistych warunkach²⁴. Rozwiązanie było pilotowane przez 18 państw członkowskich i krajów stowarzyszonych UE z ponad 25 transgranicznymi usługami tożsamości w ramach eGovernment przez 18 miesięcy. Po sukcesie STORK projekt STORK 2.0 rozszerza interoperacyjność eID na reprezentację elektroniczną i mandaty elektro-

¹⁷ P. Parycek, G. Lentner, Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study, Transforming Government: People, Process and Policy 2016, Nr 10, s. 6.

¹⁸ Dz.Urz. UE L Nr 235, s. 7.

¹⁹ Decyzja wykonawcza Komisji (UE) 2015/296 z 24.2.2015 r. w sprawie uzgodnień proceduralnych dotyczących współpracy państw członkowskich w zakresie identyfikacji elektronicznej, Dz.Urz. UE L Nr 53, s. 14.

²⁰ Dz.Urz. UE L Nr 235, s. 1.

²¹ Decyzja wykonawcza Komisji (UE) 2015/1984 z 3.11.2015 r. określająca okoliczności, formaty i procedury powiadamiania, Dz.Urz. UE L Nr 289, s. 18.

²² Komisja Europejska, Digital identity and trust: Commission launches public consultation on the eIDAS Regulation, <https://ec.europa.eu/digital-single-market/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation> (dostęp z 5.3.2021 r.).

²³ Komisja Europejska, eID Documentation, <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Background+of+eID> (dostęp z 5.3.2021 r.).

²⁴ Komisja Europejska, Instytut Perspektywicznych Studiów Technologicznych, The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies, Luxembourg 2010, s. 33.

niczne, tym razem angażując 57 partnerów z 19 europejskich państw członkowskich i stowarzyszonych. Projekt pilotuje zaktualizowaną europejską platformę interoperacyjności eID w kluczowych obszarach, takich jak bankowość elektroniczna, e-zdrowie, usługi publiczne dla biznesu oraz e-learning i kwalifikacje akademickie²⁵. Natomiast celem e-SENS (Electronic Simple European Networked Services) jest ułatwienie wdrażania transgranicznych cyfrowych usług publicznych za pomocą ogólnych i nadających się do ponownego wykorzystania komponentów technicznych, poprzez konsolidację i ulepszanie rozwiązań opracowanych w innych dużych projektach pilotażowych. E-SENS kontynuował pilotaż rozwiązania eID opracowanego przez STORK w kilku dziedzinach, w tym w e-zdrowiu, e-sprawiedliwości, e-rolnictwie i e-zamówieniach²⁶. Co do CEF (*Connecting Europe Facility*) jest to kluczowy instrument służący promowaniu wzrostu gospodarczego, zatrudnienia i konkurencyjności poprzez ukierunkowane inwestycje infrastrukturalne na szczeblu europejskim. Jeśli chodzi o eID, CEF obejmuje ulepszenia wynikające z programów pilotażowych, przygotowuje je w materiał eksploatacyjny wraz z materiałami pomocniczymi i udostępnia rozwiązanie do wdrożenia przez państwa członkowskie. W tym obszarze CEF przejął rolę „produkcji” i wspierania wprowadzenia łączności elektronicznej dla państw członkowskich. Obejmuje opracowanie pakietu usług, w tym komponentów oprogramowania typu open source, dokumentacji, szkoleń i wsparcia. W marcu 2017 r. CEF przejął wszystkie funkcje i obowiązki eSENS²⁷.

Problematyka realizacja zasady wzajemnego uznawania w praktyce – proces notyfikacji

Utworzenie systemu wzajemnego uznawania systemów elektronicznej identyfikacji w UE wymaga niewątpliwie wysokiego stopnia współpracy. Aby zapewnić pełną realizację, państwa członkowskie muszą wzajemnie ufać swoim systemom identyfikacji elektronicznej, co nie jest do końca oczywiste. Wychodząc naprzeciw, eIDAS wprowadza procedurę wzajemnej oceny. Państwa członkowskie są proszone o wzajemne informowanie się o systemie identyfikacji elektronicznej, który zamierzają zgłosić. Państwo członkowskie mające obawy dotyczące bezpieczeństwa odnośnie do systemu, który został zgłoszony lub który jest w trakcie powiadamiania, może zażądać informacji związanych z problemem dotyczącym bezpieczeństwa²⁸. W tym wypadku wprowadzone rozwiązanie jednak tylko częściowo dotyka problemu wzajemnego zaufania, ponieważ odnosi się wyłącznie do przypadków, w których poszczególne państwa członkowskie chcą dokonać notyfikacji swoich systemów. Należy jednak wskazać, że chęć takiej notyfikacji nie jest już jednak tak oczywista. Obecnie²⁹

Komisja Europejska wskazuje, że 18 systemów zostało notyfikowanych, a dwa systemy znajdują się w fazie prenotyfikacji³⁰. Mając na uwadze powyższe dane, można stwierdzić, że rzeczywiście duża liczba systemów została notyfikowana i pewnie jest to kwestią czasu czy możliwości technicznych, zanim inne państwa dołączą do tej listy. Niemniej jednak alarmujące dane w zakresie procesu notyfikacji dostarczają badania instytucji unijnych dotyczące innych systemów eID, co do których państwa nie wyraziły zamiaru notyfikacji w ramach eIDAS. Wskazuje się, że takich systemów jest 28, z czego jedynie siedem systemów jest w fazie rozwoju; pozostałe systemy są już w użytku³¹.

Na problematyczne unormowanie systemu notyfikacji wskazuje się także w literaturze. Podkreśla się, że zgłoszenie jest możliwe wyłącznie wtedy, gdy program spełnia określone kryteria i nie jest obowiązkowy dla państw członkowskich. Przeszkodą we wzajemnym uznawaniu jest to, że nie wszystkie środki identyfikacji państw członkowskich mają ten sam poziom bezpieczeństwa. Państwa członkowskie, które dysponują bezpieczniejszymi środkami dostępu do usług online, nie chcą akceptować mniej bezpiecznych środków innych państw członkowskich. Mogłoby to nawet doprowadzić do powstrzymania się państw członkowskich od zgłaszania systemów identyfikacji elektronicznej, blokując możliwość wzajemnego uznawania takich systemów³². Przedstawiony powyżej argument dotyczyłby w szczególności bardziej rozwiniętych państw członkowskich. Mając na uwadze dane przedstawione powyżej, część z nich jednak zdecydowała się na notyfikację swoich systemów. Należałoby także spojrzeć na tę problematykę z perspektywy mniej rozwiniętych państw członkowskich. W przypadku takich państw należy pamiętać, że po pierwsze, być może omawiane systemy nie zostały jeszcze w pełni wprowadzone, a po drugie, dostosowanie obecnych systemów, aby udostępnić do nich dostęp użytkownikom spoza danego kraju, może być bardzo kosztowne.

²⁵ Komisja Europejska, STORK | Take your e-identity with you, everywhere in the EU, <https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu> (dostęp z 5.3.2021 r.).

²⁶ Komisja Europejska, eID Documentation, <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Background+of+eID> (dostęp z 5.3.2021 r.).

²⁷ Komisja Europejska, eID Documentation, <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Background+of+eID> (dostęp z 5.3.2021 r.).

²⁸ J. Dumortier, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), <https://ssrn.com/abstract=2855484> (dostęp z 5.3.2021 r.).

²⁹ Stan na 14.1.2021 r.

³⁰ Systemy identyfikacji elektronicznej notyfikowane na podstawie art. 9 ust. 1 eIDAS. Swoje systemy zgłosiły państwa takie jak: Czechy, Szwecja (prenotyfikacja), Estonia, Włochy (dwa systemy), Holandia (dwa systemy), Dania, Portugalia (prenotyfikacja oraz dwa systemy), Hiszpania, Łotwa, Niemcy, Słowacja, Chorwacja, Belgia (dwa systemy), Luxemburg, Litwa.

³¹ Komisja Europejska, eID Documentation, <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview> (dostęp z 5.3.2021 r.).

³² C. Cuijpers, J. Schroers, eIDAS as guideline for the development of a pan European eID framework in FutureID, Bonn 2014, s. 7.

Wskazuje się, że obowiązek uznawania notyfikowanych systemów innych krajów powinien wzmocnić dążenie państw członkowskich do zapewnienia poprzez notyfikację efektywnego uznawania własnych mechanizmów elektronicznej identyfikacji w interesie obywateli korzystających z procedur w pozostałych państwach członkowskich³³. Mając właśnie na uwadze interes obywateli, należy wskazać, że obecny stan nie jest dla poszczególnych obywateli zjawiskiem do końca pozytywnym. Obecnie część obywateli UE jest w stanie korzystać z systemów identyfikacji elektronicznej, natomiast dla drugiej części ten dostęp jest ograniczony, właśnie m.in. przez brak notyfikacji systemów. Można postawić także tezę, że taka sytuacja może nosić znamiona dyskryminacji, skoro od 2021 r. jedynie 55% ludności UE może korzystać ze swoich krajowych elektronicznych dokumentów tożsamości w całej UE³⁴.

Takie zróżnicowanie można także zauważyć przy systemach identyfikacji elektronicznej odpowiadających niskiemu poziomowi bezpieczeństwa. Tak jak już zostało wcześniej wskazane środkiem taki, który jest wydawany w ramach systemu identyfikacji elektronicznej wymienionego w wykazie publikowanym przez Komisję na podstawie art. 9 eIDAS i który odpowiada niskiemu poziomowi bezpieczeństwa, może być uznany przez podmioty sektora publicznego na potrzeby transgranicznego uwierzytelniania dla usługi *online* świadczonej przez te podmioty³⁵. Wskazuje się, że mimo iż w celu zapewnienia wzajemnego uznawania podpisów elektronicznych konieczny jest wysoki poziom bezpieczeństwa, w niektórych przypadkach, akceptowane powinny być również podpisy elektroniczne o niższym poziomie bezpieczeństwa³⁶. Z jednej strony wprowadzenie takiego rozwiązania jest uzasadnione, mając na uwadze zasadę wzajemnego zaufania, jednak należy także wskazać, że takie uregulowanie zostawia pewną lukę i swego rodzaju dobrowolność działania państw członkowskich w odniesieniu do systemów o niższym poziomie bezpieczeństwa, co w konsekwencji również może prowadzić do zróżnicowania sytuacji obywateli poszczególnych państw członkowskich.

Znaczenie efektywnej realizacji zasady wzajemnego uznawania charakteryzuje się dużą doniosłością prawną, ze względu na to, że jej efekty będą wychodzić także poza ramy eIDAS. Omawiane uregulowanie jest bowiem bazą i podstawą dla działania innych systemów w ramach szeroko pojętego rynku usług elektronicznych. Brak efektywnego działania zasady wzajemnego uznawania negatywnie odbije się także na innych systemach korzystających z uregulowania wprowadzonego eIDAS. Czołowym przykładem będzie zastosowanie zasady wzajemnego uznawania w ramach transgranicznej opieki zdrowotnej³⁷. Zapewnienie wzajemnego uznawania jest niezbędne, aby ułatwić przenoszalność danych w transgranicznej opiece zdrowotnej czy zapewnić możliwość działania systemów takich jak eRecepta na

poziomie transgranicznym. Wymaga to stworzenia bezpiecznych i wiarygodnych ram identyfikacji elektronicznej. Usługi w zakresie e-zdrowia muszą bowiem zapewniać, że wymiana dokumentacji medycznej pacjentów i związanych z nią informacji jest przekazywana w bezpieczny sposób oraz dostęp do nich ma wyłącznie upoważniony pracownik służby zdrowia zgodnie z wolą i zgodą pacjenta. Ponadto dostawcy usług opieki zdrowotnej często wymagają jednoznacznej i szybkiej identyfikacji pacjenta w celu potwierdzenia, że posiada on odpowiednie ubezpieczenie na pokrycie kosztów leczenia³⁸.

Podsumowanie

Analiza przeprowadzona w niniejszym artykule ma na celu ocenę stopnia realizacji zasady wzajemnego uznawania na gruncie eIDAS. Założeniem jest praktyczne umożliwienie kontaktowania się na poziomie europejskim z urzędami i sądami państw członkowskich z wykorzystaniem środków identyfikacji elektronicznej oraz usług zaufania³⁹. Pojawiają się także dyskusje o efektywności decyzji wprowadzenia omawianej regulacji prawnej w formie rozporządzenia, zamiast w formie dyrektywy. Mimo że można argumentować, iż rozporządzenie może zapewnić szybsze rozwiązanie, gdyż nie jest uzależnione od krajowej transpozycji przez państwa członkowskie, poleganie na aktach wykonawczych sprawia, że po przyjęciu rozporządzenia minie trochę czasu, zanim jego pełny zakres i skutki staną się jasne. W międzyczasie może to zahamować postęp w dziedzinie identyfikacji elektronicznej i usług zaufania, ponieważ wielu uczestników rynku czeka na większą pewność prawa⁴⁰.

Należy pamiętać, że eIDAS w dużym stopniu opiera się także na zasadzie wzajemnego zaufania, jednak z drugiej strony nie wszystkie państwa członkowskie są w stanie w pełni ją implementować np. ze względów technologicznych lub wyrażają chęć pełnej jej realizacji. Problematycznym aspektem pozostaje obecna sytuacja zróżnicowania poszczególnych obywateli UE pod względem możliwości posługiwania się krajowymi metodami identyfikacji w UE. Pytanie jednak, czy uregulowanie wprowadzone przez

³³ M. Marucha-Jaworska, Rozporządzenie eIDAS..., Lex/el. 2017.

³⁴ Komisja Europejska, Digital identity and trust: Commission launches public consultation on the eIDAS Regulation, <https://ec.europa.eu/digital-single-market/en/news/digital-identity-and-trust-commission-launches-public-consultation-eidas-regulation> (dostęp z 5.3.2021 r.).

³⁵ Art. 6.2 eIDAS.

³⁶ Motyw 48 eIDAS.

³⁷ Motyw 10 eIDAS.

³⁸ A. Stasis, L. Demiri, E. Chaniotaki, eIDAS – Electronic Identification for Cross Border eHealth, *International Journal of Reliable and Quality E-Healthcare* 2018, Nr 2, s. 51–52.

³⁹ M. Marucha-Jaworska, Rozporządzenie eIDAS..., Lex/el. 2017.

⁴⁰ J. Dumortier, Regulation (EU) No 910/2014..., s. 6.

ustawodawcę unijnego w obecnym kształcie jest w stanie w ogóle zapewnić pełną możliwość realizacji zasady, mając na uwadze swobodę w zakresie decyzji dot. notyfikacji. Oczywiście taka sytuacja może być wynikiem procesu implementacji, bardzo trudne bowiem byłoby jednocześnie wprowadzenie możliwości dla wszystkich obywateli UE i w takim wypadku byłaby to rzecz oczywiście naturalna,

jednak pod warunkiem jej czasowości. Nie może się jednak okazać (a niestety może się to zdarzyć w wyniku takiego, a nie innego uregulowania procesu notyfikacji), że będzie to punkt końcowy albo punkt uzależniony jedynie od dobrej woli państw członkowskich. W takim wypadku nie będzie można więc mówić o pełnej realizacji zasady wzajemnego uznawania.

Słowa kluczowe: zasada wzajemnego uznawania, systemy identyfikacji elektronicznej, jednolity rynek cyfrowy.

Realization of the principle of mutual recognition under the eIDAS Regulation

The possibility of full implementation of the principle of mutual recognition based on Regulation of the Parliament and of the Council No. 910/2014 of 23 July 2014 in the matter of electronic identification and trust services regarding electronic transactions on a domestic market and the repeal of Directive 1999/93/EC (eIDAS) is a very important issue, in particular, from the perspective of proper functioning of the single digital market. Additionally, it positively influences the possibilities of electronic identification of EU citizens in other Member States, greatly facilitating their communication with the public administration. The research problem discussed in this article is the consideration of the possibility of full realization and effective implementation of the principle of mutual recognition, bearing in mind the scope of its application, objectives and legal regulation.

Key words: principle of mutual recognition, electronic identification systems, digital single market.



Bezpieczeństwo danych

ksiegarnia.beck.pl
Zadzwoń: 81 46 13 300
E-mail: kontakt@beck.pl

C.H.BECK