Damian Klimas*
ORCID: 0000-0002-7908-9241
Uniwersytet Wrocławski

DOI: 10.19195/1733-5779.26.5

Skan linii papilarnych jako podpis elektroniczny

JEL Classification: K24, Cyber Law

Słowa kluczowe: eIDAS, podpis elektroniczny, skan linii papilarnej, odcisk palca, QES, AES

Keywords: eIDAS, electronic signature, fingerprint, QES, AES

Abstrakt: Niniejszy artykuł podejmuje problematykę regulacji dotyczącej składania elektronicznych oświadczeń (woli, wiedzy, zgody) przy użyciu skanu linii papilarnej. Autor stara się odnaleźć właściwe ramy prawne dla skanu linii papilarnej jako podpisu elektronicznego na gruncie rozporządzenia eIDAS, które obowiązuje od 1 lipca 2016 roku. Analizie poddane zostały wymogi prawne oraz techniczne dotyczące podpisów elektronicznych, zaawansowanych podpisów elektronicznych oraz kwalifikowanych podpisów elektronicznych, a także konsekwencje prawne takiej determinanty.

Fingerprint as electronic signature

Abstract: Presented article addresses the issue of regulation concerning the submission of electronic statements (statements of intent, a statement knowledge or consent) using a scan of a fingerprint understood as an electronic signature. The author tries to find the appropriate framework for the fingerprint scan as an electronic signature under eIDAS Regulation, which is applicable since 1 July 2016. Article analyses the technical and legal requirements for electronic signatures, advanced electronic signatures and qualified electronic signatures, as well as the legal consequences of such determinants.

* Opiekun naukowy (Scientific Tutor) — Jacek Gołaczyński

Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne 26, 2018

Wstęp

Przedmiotowy artykuł, przy którego tworzeniu zastosowano metodę dogmatyczno-formalną, ma na celu przybliżenie problematyki regulacji dotyczącej składania elektronicznego oświadczenia (oświadczenia woli, oświadczenia wiedzy lub wyrażenia zgody) poprzez skan linii papilarnych lub inaczej — odcisk palca. Uwierzytelnianie za pomocą skanu linii papilarnych jest często wykorzystywane jako zabezpieczenie w elektronicznych urządzeniach mobilnych wysokiej klasy, takich jak smartfony, tablety czy laptopy. Dzięki takiemu rozwiązaniu można relatywnie szybko i bezpiecznie odblokować ekran w smartfonie czy zalogować się do systemu po włączeniu komputera. W porównaniu do wpisywania ciągu znaków składających się z liter i cyfr, stanowiących hasło, taka możliwość wydaje się zdecydowanie wygodniejsza. Niemniej jednak wykorzystanie tego typu urządzeń do składania oświadczeń nie ma bezpośredniej i szczegółowej regulacji prawnej.

Umożliwienie dokonywania czynności prawnych na odległość, za pomocą środków komunikacji elektronicznej, z jednej strony stworzyło przestrzeń do liberalizacji formy czynności prawnej, lecz z drugiej pozostawiło pewną lukę. W praktyce umowa zawierana za pomocą środków komunikacji elektronicznej najczęściej jest umową, w której trudno zweryfikować jej drugą stronę. Jest to istotne szczególnie przy zobowiązaniach o wysokiej wartości, gdyż nierzadko dochodzi do próby oszukania potencjalnego kontrahenta. Stosunki prawne zawierane za pośrednictwem środków komunikacji elektronicznej w Unii Europejskiej są co do zasady bezpieczne, niemniej jednak stosowanie narzędzi umożliwiających wzajemną identyfikację stron umowy jest często koniecznością, szczególnie przy transakcjach wysokiej wartości. Ponadto skala oszustw internetowych doprowadziła do stworzenia internetowych poradników dla poszkodowanych[1]. Jako przykład można przywołać często stosowane tak zwane oszustwo nigeryjskie (ang. Nigerian scam, 419 scam — od numeru artykułu w kodeksie karnym Nigerii[2] typizującego to przestępstwo) inicjowane kontaktem przez środki komunikacji elektronicznej (najczęściej e-mail), polegające na próbie przekonania potencjalnego kontrahenta-ofiary do transferu znaczącej kwoty środków finansowych podmiotowi, w istocie fikcyjnemu, na przykład poprzez sfałszowanie potwierdzenia przelewu z jednego z krajów afrykańskich (najczęściej Nigerii) celem wyłudzenia przedmiotu świadczenia umowy sprzedaży (często na aukcjach internetowych)[3].

Jak wskazano, jest to jedynie egzemplifikacja problemu, którego skalę trudno zmierzyć. Nie wszystkie ofiary bowiem chcą nagłaśniać tego typu przypadki, Policja i służby specjalne wskazują na znikomą wykrywalność sprawców takich

[1] http://paragraf415.republika.pl (dostęp: 24.01.2017).

[2] Criminal Code Act, Chapter 77. Laws of the Federation of Nigeria 1990, http://www.nigeria-law.org/Criminal%20Code%20Act-Tables.htm (dostęp: 24.01.2017).

[3] http://www.policja.pl/pol/kgp/bwik/bsk/cyberprzestepczosc/39219,Jak-uniknac-quotoszustwa-nigeryjskiegoquot.html (dostęp: 24.01.2017).

przestępstw[4]. Z tego względu (jak i zapewne wielu innych) prawodawca europejski uznał, że budowanie zaufania do środowiska on-line jest kluczowe dla rozwoju gospodarczego i społecznego. Brak zaufania, spowodowany w szczególności brakiem pewności w transakcjach elektronicznych, sprawia, że zarówno konsumenci, jak i przedsiębiorcy oraz przedstawiciele organów administracji publicznej nie podejmowali takiego ryzyka bądź starali się go unikać.

Uwierzytelnianie transakcji elektronicznych

W celu zwiększenia zaufania do transakcji elektronicznych w Unii Europejskiej prawodawca europejski uchwalił Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (dalej „rozporządzenie eIDAS")[5]. W ten sposób zapewniono wspólną podstawę bezpiecznej interakcji elektronicznej między stronami umów elektronicznych, co w założeniu ma podnieść efektywność publicznych i prywatnych usług on-line, e-biznesu i e-handlu w Unii.

Problem ten został zauważony zdecydowanie wcześniej. Legislacyjne podstawy omawianej problematyki podpisu elektronicznego zostały określone już w modelowej ustawie UNCITRAL dotyczącej zagadnień prawnych związanych z Elektronicznym Przekazem Danych (*Electronic Data Interchange*), która została opracowana przez Komisję Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego, a następnie zaaprobowana przez Zgromadzenie Ogólne ONZ w 1996 roku[6]. Prace w ramach Unii Europejskiej doprowadziły zaś do wydania Dyrektywy Parlamentu Europejskiego nr 1999/93/ WE z dnia 13 grudnia 1999 roku w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[7].

Odcisk palca w kodeksie cywilnym

Polski prawodawca dostrzegł możliwość wykorzystania odcisku palca w celu oświadczenia woli w art. 79 KC[8], umożliwiając osobom niemogącym pisać zachowanie formy pisemnej. I tak osoba niemogąca pisać może złożyć oświadcze-

---

[4] *Ibidem*.

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE Seria L 257/73, s. 73–114).

[6] A. Cieśliński, *Wspólnotowe prawo gospodarcze*, t. 2, Warszawa 2007, s. 789.

[7] Dyrektywa Parlamentu Europejskiego nr 1999/93/ WE z dnia 13 grudnia 1999 roku w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.Urz. WE L 13 z 19 stycznia 2000 r.).

[8] Ustawa z dnia 23 kwietnia 1964 roku — Kodeks cywilny (tekst jedn. Dz.U. z 2016 r., poz. 380 ze zm.); dalej „KC".

nie woli w formie pisemnej w ten sposób, że uczyni na dokumencie tuszowy odcisk palca, a obok tego odcisku osoba przez nią upoważniona wypisze jej imię i nazwisko oraz złoży swój podpis, albo w ten sposób, że zamiast składającego oświadczenie podpisze się osoba przez niego upoważniona, a jej podpis będzie poświadczony przez notariusza, wójta (burmistrza, prezydenta miasta), starostę lub marszałka województwa z zaznaczeniem, że został złożony na życzenie osoby niemogącej pisać.

Dochowanie formy pisemnej czynności prawnej co do zasady wymaga złożenia na dokumencie podpisu własnoręcznego. Zważywszy jednak, że nie wszyscy mają możliwość złożenia własnoręcznego podpisu, polski prawodawca wprowadził formę zastępczą, która jest w tym przypadku równoważna formie pisemnej. Niemniej wskazany już przepis reguluje sposób składania oświadczeń woli w formie pisemnej przez osoby niemogące pisać (na przykład osoba niepełnosprawna, której ręce są całkowicie lub częściowo niewładne)[9]. Przepis ten nie ustanawia zatem uniwersalnej formy zastępczej, lecz jedynie warunkową, którą może wykorzystać indywidualnie określona grupa osób, w konkretnych wypadkach. Ponadto w ten sposób odcisk palca jest składany w postaci tuszowej na papierze, a nie w postaci elektronicznej poprzez skan linii papilarnych.

Niemniej jednak art. 60 KC przewiduje możliwość ujawnienia woli osoby dokonującej czynności prawnej w postaci elektronicznej, a w art. 78^1 § 1 KC uszczegóławia, w jaki sposób zachować elektroniczną formę czynności prawnej (poprzez złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym). Z powodu zdecydowanie większej, jak się wydaje, użyteczności wykorzystywania w szerokim zakresie skanu linii papilarnej dalsza część artykułu zostanie poświęcona tej właśnie formie.

Problematyka usług zaufania w Unii Europejskiej

Zanim podejmę tematykę założoną wprowadzeniem, kilka słów poświęcę na pobieżne wprowadzenie do problematyki (elektronicznych) usług zaufania w Unii Europejskiej ze szczególnym uwzględnieniem podpisów elektronicznych. Jest to konieczne, gdyż zdezaktualizowały się rozprawy naukowe ujmujące podpisy elektroniczne hasłowo[10]. Ponadto mimo wielu rozważań w artykułach naukowych[11] (a nawet monografiach[12]) podniesione przez przedstawicieli doktryny tezy nie

[9] P. Sobolewski, *Komentarz do art. 79*, [w:] *Kodeks cywilny. Komentarz*, red. K. Osajda, Warszawa 2017, Legalis.

[10] P. Fajgielski, *Podpis elektroniczny. Świadczenie usług drogą elektroniczną*, [w:] *Leksykon obywatela*, red. B. Szmulik, S. Serafin, Warszawa 2008, s. 1193–1198.

[11] P. Stańczyk, *Prawne i ekonomiczne aspekty podpisu elektronicznego*, Poznań 2001; D. Szostek, *Prawne aspekty podpisu elektronicznego*, [w:] *Handel elektroniczny. Prawne problemy*, red. J. Barta, R. Markiewicz, Warszawa 2005, s. 177 n.

[12] J. Janowski, *Podpis elektroniczny w obrocie prawnym*, Warszawa 2007; D. Szostek, *Nowe ujęcie dokumentu w prawie prywatnym, ze szczególnym uwzględnieniem dokumentu elektronicz-*

zdążyły w dużej mierze ująć w swych ramach nowej regulacji, która obowiązuje od 1 lipca 2016 roku. Jeśli zaś rozważania te już ujmują ową regulację, mają ogólny charakter[13] lub dotyczą dość szczegółowych zagadnień, często związanych z elektroniczną czynnością prawną na gruncie prawa cywilnego materialnego lub procedurą cywilną[14].

Aktem prawnym, który nadaje ramy podpisom elektronicznym w Unii Europejskiej, jest rozporządzenie Parlamentu Europejskiego i Rady (EU) nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[15]. W tym miejscu warto wspomnieć, że w celu zlikwidowania kolizji regulacyjnych pomiędzy prawem unijnym w zakresie podpisów elektronicznych (rozporządzeniem eIDAS) a prawem polskim uchwalono ustawę z dnia 5 września 2016 roku o usługach zaufania oraz identyfikacji elektronicznej[16], która weszła w życie 7 października 2016 roku.

Istotne jest spostrzeżenie, że podpis elektroniczny stanowi jedną z kilkunastu rodzajów usług zaufania regulowanych w rozporządzeniu eIDAS. Zgodnie z art. 3 pkt 16 rozporządzenia eIDAS usługa zaufania oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:

a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami;

b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych;

c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

---

nego, Warszawa 2012; M. Marucha-Jaworska, *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Warszawa 2015.

[13] P. Polański, *Europejskie prawo handlu elektronicznego. Mechanizm regulacji usług społeczeństwa informacyjnego*, Warszawa 2014.

[14] *Informatyzacja postępowania cywilnego*, red. J. Gołaczyński, D. Szostek, Warszawa 2016; D. Szostek, J. Gołaczyński, *Wpływ rozporządzenia eIDAS na polskie prawo prywatne. Wybrane zagadnienia*, [w:] *Media elektroniczne. Współczesne problemy prawne*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2016; A. Kościółek, *Wpływ rozporządzenia eIDAS na skuteczność elektronicznych pism procesowych w postępowaniu cywilnym*, [w:] *Media elektroniczne. Współczesne problemy prawne*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2016; A. Zalesińska, *Wpływ informatyzacji na założenia konstrukcyjne procesu cywilnego*, Warszawa 2016.

[15] Rozporządzenie Parlamentu Europejskiego i Rady (EU) Nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz.UE.L Nr 257, s. 73).

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

Podpis elektroniczny w rozporządzeniu eIDAS a skan linii papilarnej

Jako usługa elektroniczna, podpis elektroniczny oferowany jest przez dostawcę usług zaufania[17], który co do zasady jest przedsiębiorcą. Rozporządzenie eIDAS rozróżnia trzy rodzaje podpisów elektronicznych, a więc także trzy różne definicje podpisów elektronicznych w zależności od ich charakteru. „Zwykły" podpis elektroniczny oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które są użyte przez podpisującego jako podpis[18]. Definicja ta jest bardzo szeroka i może ujmować podpisanie się palcem (lub rysikiem) na tablecie lub touchpadzie w pliku tekstowym lub graficznym, to jest w dokumencie elektronicznym[19], lub stopkę w e-mailu. Do rozważenia byłaby także koncepcja, która zaliczałaby do „zwykłych" podpisów elektronicznych także logowanie się do różnego rodzaju serwisów społecznościowych czy forów internetowych, gdy przecież posługujemy się danymi, aby podpisać się pod innymi danymi. Dobrym przykładem jest serwis społecznościowy Facebook, który umożliwia publikowanie treści różnej formy (tekst, obraz, wideo, dźwięk) pod własnym imieniem i nazwiskiem, gdyż polityka serwisu utrudnia stosowanie tak zwanego *fake accounts*. Warto w tym miejscu wskazać, że w doktrynie można spotkać odważną tezę, jakoby podpis własnoręczny można było złożyć bezpośrednio w dokumencie elektronicznym, a podpis taki pozwalałby na dochowanie formy pisemnej uregulowanej w art. 78 § 1 KC[20].

Kolejnym rodzajem podpisu elektronicznego jest zaawansowany podpis elektroniczny (dalej również: AES). Prawodawca europejski ujął jego definicję w oparciu o „zwykły" podpis elektroniczny, nakładając jednakże dodatkowe wymogi, które zaawansowany podpis elektroniczny musi spełniać[21]. AES:

a) jest unikalnie przyporządkowany podpisującemu;

b) umożliwia ustalenie tożsamości podpisującego;

c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą;

---

[17] Artykuł 3 pkt 19 rozporządzenia eIDAS stanowi, że dostawca usług zaufania oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

[18] Artykuł 3 pkt 10 rozporządzenia eIDAS.

[19] Artykuł 3 pkt 35 rozporządzenia eIDAS stanowi, że dokument elektroniczny oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne.

[20] Szerzej o podpisie własnoręcznym w dokumencie elektronicznym D. Szostek, *Nowe ujęcie dokumentu w polskim prawie prywatnym, ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej*, Warszawa 2012, s. 77 n.

[21] Artykuł 3 pkt 10 rozporządzenia eIDAS stanowi, że zaawansowany podpis elektroniczny oznacza podpis elektroniczny, który spełnia wymogi określone w art. 26 tego rozporządzenia.

d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna[22].

Jak zatem można spostrzec, taki podpis jest zdecydowanie bezpieczniejszy. Unikalność przyporządkowania podpisującemu oznacza, że nikt inny nie może się posługiwać takim podpisem. Taką unikalność w dużej mierze dostarcza właśnie skan linii papilarnej. Umożliwia on również ustalenie tożsamości podpisującego, jeśli wcześniej ta tożsamość została zarejestrowana. Oczywiście podpisujący musiałby wcześniej zeskanować swoje linie papilarne kilkanaście lub kilkadziesiąt razy na skanerze linii papilarnych, a następnie podać swoje dane, jednakże po takim uwierzytelnieniu następcze ustalenie tożsamości jest niemalże w stu procentach pewne[23]. Złożenie podpisu przy użyciu danych służących do składania podpisu elektronicznego, którego podpisujący może z dużą dozą pewności użyć pod wyłączną kontrolą, jest jednak wymogiem dość problematycznym. Oczywiście własnych palców możemy użyć w zasadzie pod swoją wyłączną kontrolą, niemniej należy podkreślić, że specjaliści do spraw bezpieczeństwa podkreślają, że stosunkowo łatwo skopiować odcisk palca, a w następstwie dokonać próby „oszukania" skanera linii papilarnych. Nie jest bowiem tajemnicą, że odciski własnych palców pozostawiamy wszędzie, od szklanki, przez klamkę od drzwi, aż po klawiaturę komputera. Abstrahując jednak od kwestii bezpieczeństwa, należy uznać, że wymóg wynikający z art. 26 lit. c rozporządzenia eIDAS będzie spełniony. Ostatni wymóg można zabezpieczyć technicznie odpowiednim oprogramowaniem, które zapewni, że dokument elektroniczny nie zostanie zmodyfikowany po naniesieniu na niego podpisu (skanu linii papilarnych).

Zważywszy na poczynioną krótką analizę stanu prawnego, należy uznać, że skan linii papilarnych może z całą stanowczością (po odpowiednim dostosowaniu) stanowić zaawansowany podpis elektroniczny.

Kwalifikowany podpis elektroniczny a skan linii papilarnej

Ostatnim rodzajem podpisów elektronicznych uregulowanych w rozporządzeniu eIDAS są kwalifikowane podpisy elektroniczne. Zgodnie z art. 3 pkt 12 tego rozporządzenia kwalifikowany podpis elektroniczny (dalej również QES) oznacza zaawansowany podpis elektroniczny (AES), który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie.

---

[22] Artykuł 26 rozporządzenia eIDAS.

[23] Należy oczywiście zasygnalizować, że w wypadku skanowania linii papilarnych zdarzają się problemy wynikające z rodzaju powierzchni, która jest skanowana. Powierzchnia palca z łatwością może się zabrudzić, zakurzyć, zatłuścić czy zmoczyć, co może wpłynąć negatywnie na skuteczność procesu skanowania, niezależnie od jakości i poziomu zaawansowania urządzenia skanującego.

Zgodnie z załącznikiem I do rozporządzenia eIDAS kwalifikowane certyfikaty podpisów elektronicznych zawierają następujące informacje:

a) wskazanie — co najmniej w postaci pozwalającej na automatyczne przetwarzanie — że dany certyfikat został wydany jako kwalifikowany certyfikat podpisu elektronicznego;

b) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz

— w odniesieniu do osoby prawnej: nazwę i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem;

— w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby;

c) co najmniej imię i nazwisko podpisującego lub jego pseudonim; jeżeli używany jest pseudonim, fakt ten jest jasno wskazany;

d) dane służące do walidacji podpisu elektronicznego, które odpowiadają danym służącym do składania podpisu elektronicznego;

e) dane dotyczące początku i końca okresu ważności certyfikatu;

f) kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania;

g) zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania;

h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący zaawansowanemu podpisowi elektronicznemu lub zaawansowanej pieczęci elektronicznej, o których mowa w lit. g);

i) miejsce usług, z którego można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu;

j) w wypadku gdy dane służące do składania podpisu elektronicznego powiązane z danymi służącymi do walidacji podpisu elektronicznego znajdują się w kwalifikowanym urządzeniu do składania podpisu elektronicznego, odpowiednie wskazanie tego faktu co najmniej w postaci pozwalającej na automatyczne przetwarzanie.

Nie dokonując rozbudowanej analizy załącznika I do rozporządzenia eIDAS, należy uznać, że przedstawione dane nie są trudne do uzyskania, a technika pozyskiwania skanu linii papilarnej nie uniemożliwia ich zawarcia. Wydaje się więc, że załącznik I do rozporządzenia eIDAS nie stanowi bariery prawnej dla uznania skanu linii papilarnej w określonych sytuacjach za kwalifikowany podpis elektroniczny.

Kwalifikowane urządzenia do składania podpisu elektronicznego a skan linii papilarnej

Zgodnie z punktem 1 załącznika II do rozporządzenia eIDAS kwalifikowane urządzenia do składania podpisu elektronicznego zapewniają — dzięki właściwym środkom technicznym i proceduralnym — co najmniej:

a) zagwarantowanie w racjonalny sposób poufności danych służących do składania podpisu elektronicznego, użytych do złożenia podpisu elektronicznego;

b) w praktyce tylko jednorazowe wystąpienie danych służących do składania podpisu elektronicznego, użytych do złożenia podpisu elektronicznego;

c) uniemożliwienie, z racjonalną dozą pewności, pozyskania danych służących do składania podpisu elektronicznego, użytych do złożenia podpisu elektronicznego, oraz skuteczną ochronę podpisu elektronicznego przed sfałszowaniem za pomocą aktualnie dostępnych technologii;

d) możliwość skutecznej ochrony, przez osobę uprawnioną do składania podpisu, danych służących do składania podpisu elektronicznego, użytych do złożenia podpisu elektronicznego, przed użyciem ich przez innych.

W wypadku załącznika II do rozporządzenia eIDAS warto przeanalizować wymogi w nim określone. Należy podkreślić, że trudno na łamach niniejszego artykułu dokonać analizy różnych urządzeń skanujących linie papilarne, szczególnie zważywszy na charakter samego artykułu jako tekstu stricte prawnego. Niezależnie od tego wydaje się, że wymogi zawarte w literach a) oraz d) przywołanego załącznika mogą być spełnione przez niemalże każde urządzenie skanujące linie papilarne, jeśli chodzi o sam proces takiego „podpisu". Ze względu na treść litery a) oraz d), poufność tych danych, a także możliwość skutecznej ich ochrony leży po stronie podpisującego i charakter linii papilarnych niejako ją zapewnia.

Litera b) wymaga jednorazowego wystąpienia danych służących do złożenia podpisu, co w zasadzie uniemożliwia zastosowanie skanu linii papilarnych, gdyż w każdym przypadku ich skanowania będą one znajdowały się w tym samym miejscu, co poprzednio. Niemniej odpowiednio zaprogramowane urządzenie w założeniu mogłoby pozwolić na pobranie skanu jedynie określonej części linii papilarnej i przypisanie jej w taki sposób, aby nie była użyta ponownie. Kombinacji różnych części takich skanów istnieje z pewnością skończona ilość, niemniej przy odpowiednim zaprogramowaniu wydaje się możliwe spełnienie również tej przesłanki. Uniemożliwienie, z racjonalną dozą pewności, pozyskania danych służących do składania podpisu elektronicznego, użytych do złożenia podpisu elektronicznego, oraz skutecznej ochrony podpisu elektronicznego przed sfałszowaniem za pomocą aktualnie dostępnych technologii jest natomiast niezmiernie trudne w stosunku do odcisku palca, zważywszy na sygnalizowaną już łatwość w jego pobraniu i skopiowaniu. Nie jest to jednak przyczyna dotycząca urządzenia do składania podpisu elektronicznego, a zatem należy uznać, że również litera c) punktu pierwszego załącznika II do rozporządzenia eIDAS nie będzie barierą prawną w uznaniu skanu linii papilarnej za kwalifikowany podpis elektroniczny.

Zgodnie z punktem 2 załącznika II kwalifikowane urządzenia do składania podpisu elektronicznego nie zmieniają danych, które mają być podpisane, ani nie uniemożliwiają przedstawienia tych danych podpisującemu przed złożeniem podpisu. Ponadto dane służące do składania podpisu elektronicznego mogą być

generowane lub zarządzane w imieniu podpisującego wyłącznie przez kwalifikowanego dostawcę usług zaufania[24].

Ponadto na podstawie punktu 4 załącznika II, bez uszczerbku dla pkt 1 lit. d), kwalifikowani dostawcy usług zaufania, zarządzający danymi służącymi do składania podpisu elektronicznego, w imieniu podpisującego mogą kopiować dane służące do składania podpisu elektronicznego wyłącznie w celu utworzenia kopii zapasowej, pod warunkiem że spełnione są następujące wymogi:

a) bezpieczeństwo skopiowanych zbiorów danych musi być na tym samym poziomie, co w wypadku oryginalnych zbiorów danych;

b) liczba skopiowanych zbiorów danych nie przekracza minimum niezbędnego do zapewnienia ciągłości usługi.

Są to wymogi leżące raczej w sferze oprogramowania, zatem nie zostaną poddane analizie na łamach niniejszego artykułu, niemniej zachowanie ich nie wydaje się niemożliwe, również w odniesieniu do skanu linii papilarnych.

Wnioski

Bez najmniejszych wątpliwości skan linii papilarnych jest „zwykłym" podpisem elektronicznym w znaczeniu art. 3 pkt 10 rozporządzenia eIDAS, czyli danymi w postaci elektronicznej dołączonymi lub logicznie powiązanymi z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis. Biorąc pod uwagę przedstawioną analizę, z dużą dozą pewności można uznać, że skan linii papilarnej przy dochowaniu należytych standardów bezpieczeństwa może stanowić zaawansowany podpis elektroniczny. Skan linii papilarnej spełnia bowiem następujące wymogi: jest unikalnie przyporządkowany podpisującemu; umożliwia ustalenie tożsamości podpisującego; jest składany przy użyciu danych służących do składania podpisu elektronicznego, którego podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

Wydaje się, iż skan linii papilarnej mógłby stanowić kwalifikowany podpis elektroniczny gdyby spełnił wymogi kwalifikowanego podpisu elektronicznego uregulowanego w art. 26 rozporządzenia eIDAS, dopełnione załącznikami I oraz II do rozporządzenia eIDAS. Niemniej wymagałoby to znaczących nakładów na system teleinformatyczny i dopracowanie oprogramowania w odpowiedni, zabezpieczający wszelkie wymogi regulacyjne, sposób.

Omawiane kwestie są tak istotne, ponieważ uznanie skanu linii papilarnej za podpis elektroniczny w rozumieniu rozporządzenia eIDAS, a w szczególności uznanie linii papilarnej za kwalifikowany podpis elektroniczny niesie z sobą da-

[24] Punkt 3 załącznika II do rozporządzenia eIDAS. Warto podkreślić, że w wypadku skanu linii papilarnych takie generowanie lub zarządzanie w imieniu podpisującego nie jest konieczne.

leko idące następstwa w sferze prawa materialnego oraz procesowego, zarówno w prawie prywatnym, jak i w prawie publicznym. Należy nadmienić, że na podstawie art. 25 ust. 1 rozporządzenia eIDAS 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 kwalifikowanych podpisów elektronicznych.

Co jeszcze ważniejsze, na podstawie art. 25 ust. 2 rozporządzenia eIDAS kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu. Jego użycie „zastępuje" zatem podpis tradycyjny, czyli wywołuje skutki prawne podpisu własnoręcznego i można go stosować w każdym wypadku, gdy jest wymagany podpis własnoręczny, chyba że przepis szczególny stanowi inaczej. Użycie kwalifikowanego podpisu elektronicznego doprowadza do uzyskania przymiotów autentyczności i integralności podpisywanych danych — innymi słowy: podpisanie się (wskazanie od kogo dany dokument pochodzi) i zastrzeżenie, że jakakolwiek zmiana w tym dokumencie jest niemożliwa lub że zmiana (fałszerstwo) jest rozpoznawalne.

Ponadto zgodnie z art. 25 ust. 3 rozporządzenia eIDAS kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich. Innymi słowy, podpisując się skutecznie w Polsce, możemy zawrzeć umowę w czasie rzeczywistym z kontrahentem na przykład z Francji. Ponadto możemy wnioskować o usługi publiczne w różnych państwach członkowskich, na przykład o wydanie dowodu rejestracyjnego pojazdu z wnioskiem o przesłanie pod wskazany adres.

Niestety, w polskich przepisach prawa nie określono, do jakich czynności dopuszczalne jest użycie zaawansowanego podpisu elektronicznego. Niemniej nie wydaje się, że na gruncie prawa polskiego uznawanie skanu linii papilarnej za zaawansowany podpis elektroniczny jest prawnie irrelewantne. Należy bowiem mieć na względzie sytuację, która z dużą dozą prawdopodobieństwa może przytrafić się podczas postępowania dowodowego, gdy biegły, uznając skan linii papilarnej za zaawansowany podpis elektroniczny, nadaje mu przymioty między innymi autentyczności i integralności[25], które z kolei stanowią relatywnie wysoką wartość dowodową.

Bibliografia

Literatura przedmiotu

Cieśliński A., *Wspólnotowe prawo gospodarcze*, t. 2, Warszawa 2007.
Handel elektroniczny. Prawne problemy, red. J. Barta, R. Markiewicz, Warszawa 2005.
Informatyzacja postępowania cywilnego, red. J. Gołaczyński, D. Szostek, Warszawa 2016.

[25] Zgodnie z wymogami stawianymi w art. 26 rozporządzenia eIDAS.

Janowski J., *Podpis elektroniczny w obrocie prawnym*, Warszawa 2007.
Kodeks cywilny. Komentarz, red. K. Osajda, SIP Legalis.
Leksykon obywatela, red. B. Szmulik, S. Serafin, Warszawa 2008.
Marucha-Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Warszawa 2015.
Media elektroniczne. Współczesne problemy prawne, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2016.
Polański P., *Europejskie prawo handlu elektronicznego. Mechanizm regulacji usług społeczeństwa informacyjnego*, Warszawa 2014.
Stańczyk P., *Prawne i ekonomiczne aspekty podpisu elektronicznego*, Poznań 2001.
Szostek D., *Nowe ujęcie dokumentu w prawie prywatnym, ze szczególnym uwzględnieniem dokumentu elektronicznego*, Warszawa 2012.
Zalesińska A., *Wpływ informatyzacji na założenia konstrukcyjne procesu cywilnego*, Warszawa 2016.

Akty Prawne

Criminal Code Act, Laws of the Federation of Nigeria 1990.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE Seria L 257/73, s. 73–114).
Dyrektywa Parlamentu Europejskiego nr 1999/93/ WE z dnia 13 grudnia 1999 roku w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz. Urz. WE Seria L 13 z 19 stycznia 2000 r.).
Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r., poz. 1579).
Ustawa z dnia 23 kwietnia 1964 roku — Kodeks cywilny (tekst jedn. Dz.U. z 2016 r., poz. 380 ze zm.).

Źródła internetowe

http://paragraf415.republika.pl
http://www.policja.pl/pol/kgp/bwik/bsk/cyberprzestepczosc/39219,Jak-uniknac-quotoszustwa-nigeryjskiegoquot.html

Fingerprint as electronic signature

Summary

Without a doubt scanned fingerprint should be understood as electronic signature within the meaning of Article 3 point 10 Regulation eIDAS as data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Given the observation made above, with a high degree of certainty, it can be assumed that a scan of the fingerprint with the observance of appropriate safety standards can provide an advanced electronic signature. Scan fingerprint, meets the following requirements: it is uniquely linked to the signatory; it is capable of identifying the signatory; it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

It seems that scans the fingerprint line could provide a qualified electronic signature if he has complied with the qualified electronic signature regulated in art. 26 Regulation eIDAS, which are supposed to Annexes I and II to Regulation eIDAS. However, this would require a significant investment in proper ICT system in order to meet all regulatory requirements.

The weight of these considerations is important to the extent that the recognition of fingerprint scan as electronic signature within the meaning of Regulation eIDAS, and in particular the recognition of the fingerprint line by a qualified electronic signature entails far-reaching consequences in the field of substantive and procedural law. And both in private law and public law fields. It should be noted that under article 25 paragraph. 1 of eIDAS Regulation an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

What's even more important, on the basis of art. 25 paragraph. 2 Regulation eIDAS qualified electronic signature has the legal effect equivalent to a handwritten signature. Therefore, its use may "replace" traditional, physical signature, which "produces" legal effect of traditional signature, and it can be used whenever required handwritten signature, unless a specific provision states otherwise. The use of qualified electronic signature brings to obtain the qualities of authenticity and integrity of the signed data.

In addition, in accordance with article 25 paragraph 3 of eIDAS regulation a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States. In other words, using QES in Poland, we can sign a contract in real time with the counterparty, e.g. from France. In addition, one may request public services in different Member States, e.g. for the issuance of the registration certificate of the vehicle.

Unfortunately Polish law does not specify to which activities is acceptable to use an advanced electronic signature. However, it does not seem that under the Polish law the recognition of fingerprint scan as advanced electronic signature is legally irrelevant. It should be bear in mind the situation that very likely can happen during the evidentiary proceedings, where expert witness recognise the fingerprint scan as the advanced electronic signature gives it attributes of authenticity and integrity, which in turn represent a relatively high value as the evidence.