

PODPIS ELEKTRONICZNY W PRAWIE AMERYKAŃSKIM

W Stanach Zjednoczonych Ameryki powstały nie tylko standardy szyfrowania symetrycznego i asymetrycznego służące konstrukcji najbardziej zaawansowanego rodzaju podpisu elektronicznego. Kraj ten był także kolebką idei specjalnego ujęcia podpisu elektronicznego w ramy prawne. Pierwsza kompleksowa ustawa o podpisie elektronicznym powstała właśnie w Stanach Zjednoczonych Ameryki w 1995 roku w stanie Utah (*The Digital Signature Act* z dnia 9 marca 1995 roku).

Charakterystyka regulacji podpisu elektronicznego w prawie amerykańskim powinna uwzględniać dwie ogólne kwestie. Po pierwsze, specyficzny jest system prawa amerykańskiego. Okoliczność, że jest to sztandarowy przykład systemu *common law*, nie jest w badanym zagadnieniu znacząco doniosła, co wynika z uregulowania podpisu elektronicznego prawem stanowym (pisanym). W tym kontekście należy jedynie zważyć, że kierując się istotą prawa stanowego w systemie *common law*, można by oczekiwać szczegółowej i obszernej regulacji, co jednak nie jest trafnym przypuszczeniem. Donioślejszą cechą systemu prawa amerykańskiego w tej materii jest podział na prawo federalne i prawo stanowe, jako konsekwencji związkowego charakteru państwa. Jak powszechnie wiadomo, poszczególne stany mają uprawnienia ustawodawcze, co rzutuje w szczególny sposób na regulację podpisu elektronicznego: wprowadzanie regulacji prawnej podpisu elektronicznego do systemu prawa amerykańskiego, historycznie rzecz ujmując, polegało na wprowadzeniu początkowo regulacji tylko na poziomie stanów, a dopiero następnie na szczeblu federalnym. Przy czym należy mieć na uwadze, że wprowadzenie regulacji stanowych następowało od 1999 roku w oparciu o tzw. prawo wzorcowe, stąd regulacje te, przynajmniej teoretycznie nie powinny się między sobą znacząco różnić, a wręcz mogą być identyczne.

Drugą kwestią, na którą należy zwrócić uwagę, jest dostrzegalne podobieństwo pomiędzy regulacją prawną podpisu elektronicznego w prawie amerykańskim oraz w UNCITRAL *Model Law on Electronic Signatures* z 2001 roku (zwanej dalej „ustawą modelową UNICITRAL”). Podobieństwo to jest dostrzegalne zwłaszcza odnośnie do prawa federalnego. Przypuszczać można, że jest to efekt przygotowywania tych projektów legislacyjnych mniej więcej w tym samym czasie. Choć ustawa modelowa UNICITRAL powstała rok później niż ustawa federalna USA, to ze względu na odmienności procedury stanowienia prawa, a tym samym czas ich trwania, trudno nawet jednoznacznie wskazać, który z tych aktów był wzorcem dla drugiego. W każdym razie wiodącym założeniem obu regulacji jest niemożność odmówienia skuteczności czynnościom prawnym tylko dlatego, że zostały dokonane w postaci elektronicznej.

Źródła prawa

Regulacja podpisu elektronicznego występuje w prawie stanowym i federalnym, jak również w tzw. prawie wzorcowym. Chronologicznie wymieniając, należy wskazać wpieryw na *Uniform Electronic Transaction Act* z dnia 29 lipca 1999 roku (zwany dalej „UETA”) wraz z adoptującym ten akt do porządku prawnego powszechnie obowiązującego ustawodawstwem stanowym. Poczynić należy uwagę co do charakteru prawnego UETA. Nie jest to prawo obowiązujące, a jedynie prawo wzorcowe, z którego poszczególne stany mogą korzystać, dlatego UETA można określić jako ustawę jednolitą lub wzorcową. UETA, podobnie jak inne *Uniform Act*, jest efektem prac *National Conference of Commissioners on Uniform State Laws*, dzięki której działalności niwelowane są rozbieżności w ustawodawstwie poszczególnych stanów².

Na poziomie prawa federalnego aktem regulującym podpis elektroniczny jest *Electronic Signatures in Global and National Commerce Act* z dnia 24 stycznia 2000 roku (zwany dalej „E-sign Act”). Ustawa ta podpisana została przez prezydenta USA w dniu 30 czerwca 2000 roku, a weszła w życie 1 października tamtego roku. W dalszej części opracowania szczególna uwaga zwrócona zostanie na regulację w prawie federalnym, uzupełnioną o wskazania postanowień UETA. Wynika to z okoliczności, że regulacja E-sign Act jest znacząco podobna do UETA, aczkolwiek nie są to akty całkowicie identyczne³. Bliżej nie będzie charakteryzowane ustawodawstwo poszczególnych stanów, gdyż można przyjąć ogólne założenie, że ustawodawstwo stanowe teoretycznie powinno odpowiadać postanowieniom UETA i nie powinno być niezgodne z E-sign Act. Przy czym kwestia relacji E-sign Act do regulacji stanowych jest skomplikowana i wzbudza wątpliwości w doktrynie amerykańskiej. Chodzi tutaj o kwestie tzw. *Preemption Clause* (sec. 102 i nt E-sign Act), która, jak podnosi się czasem w literaturze, doprowadziła do sytuacji, że prawo federalne w tym zakresie stało się „*patchwork quilt*” (pol. narzutą, co wyrażać ma pewną niespójność prawną) na niejednolite prawo stanowe⁴.

Technologiczna neutralność

Zasadniczą cechą regulacji amerykańskiej, na gruncie prawa federalnego i wzorcowego, jest technologiczna neutralność (ang.

² Dotąd UEAT i mplementowały wszystkie stany poza stanem Illinois, New York i Washington (zob. informacje na stronie internetowej: <http://www.ncsl.org/default.aspx?tabid=13484>, data wejścia 7.04.2010 r.).

³ Por. S. E. Blythe, *Digital Signature Law of The United Nations, European Union, United Kingdom and Unites States: promotion of growth in e-commerce with enhanced security*, *Richmond Journal of Law and Technology* 2005, Winter, s. 39-40; G. L. Berenstein, Ch. E. Campbell, *Electronic contracting: The current state of the law and best practices*, *Journal of Proprietary Rights* 2002, September, s. 2-3.

⁴ Zob. S. E. Blythe, *Digital...*, s. 41-43 i 50; G. L. Berenstein, Ch. E. Campbell, *Electronic...*, s. 1-2.

¹ mgr Łukasz Goździaszek – doktorant w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

technology neutral), czyli niewskazywanie żadnej konkretnej technologii, z którą powiązany został jakikolwiek rodzaj podpisu elektronicznego. Nie oznacza to jednak, że prawo amerykańskie jest zupełnie liberalne i elastyczne w zakresie podpisu elektronicznego. Jak będzie później wskazane, wymagane jest, aby podpis elektroniczny był wiarygodny. Jednak regulacja amerykańska nie wskazuje, jaka technologia zapewnia ową wiarygodność i właśnie w tym tkwi istota technologicznej neutralności. Takie ujęcie przez ustawodawcę materii w zasadzie wyklucza możliwość prawnego wyodrębnienia rodzajów podpisu elektronicznego, co jednak nie oznacza, że w konkretnych okolicznościach „pozorny” podpis elektroniczny nie będzie zrównany w skutkach prawnych z podpisem własnoręcznym (ang. *manual signatures*). Należy tutaj mieć również na uwadze, że praktyka amerykańska za niebudzący żadnych wątpliwości uznaje podpis elektroniczny wykorzystujący szyfrowanie asymetryczne. Inaczej zagadnienie to przedstawia się na gruncie ustawodawstwa stanowego, gdzie często obok pojęcia *electronic signature* występuje *digital signature*. Pierwszy rodzaj podpisu elektronicznego można określić „zwykłym”, natomiast drugi „podpisem cyfrowym” jako ściśle powiązany z szyfrowaniem asymetrycznym. Definityjne wyodrębnienie dwóch rodzajów podpisu czy dokładniej, prawnego uregulowania podpisu cyfrowego będącego szczególnym rodzajem podpisu elektronicznego, nie jest jednak najczęściej powiązane ze zróżnicowaniem skutków prawnych skorzystania z tych podpisów.

Technologiczną neutralność przedstawia się czasami jako zakaz dyskryminacji jakichkolwiek technik „uwiarygodniających” podpis, jednak takie sformułowanie jest o tyle dwuznaczne, że pojęcia niedyskryminacji najczęściej używa się w kontekście niedyskryminacji podpisu elektronicznego w stosunku do podpisu własnoręcznego. Przyjęcie zasady technologicznej neutralności implikuje możliwość umówienia się stron między sobą co do techniki (metody) elektronicznego podpisywania. Tak więc, jeśli strony w umowie postanowią, że daną technikę uważają za wiarygodną, wtedy żadna ze stron nie będzie mogła podnieść, że dany podpis elektroniczny nie wywołuje skutku prawnego. Co więcej, jak się wydaje, w niektórych przypadkach wystarczy sam kontekst i analiza otoczenia do stwierdzenia wiarygodności podpisu elektronicznego.

Podpis elektroniczny w „prawie cywilnym materialnym”

Kwestia stosowania podpisu elektronicznego wpłynęła również na zmianę postanowień *Uniform Commercial Code* z 1952 roku (zwanego dalej „UCC”), czyli aktu pełniącego w pewnym zakresie rolę amerykańskiego wzorcowego kodeksu czynności handlowych (odmienne ustawodawstwo cywilne ma stan Luizjana). Jest to akt obszerny i skomplikowany, gdzie w zasadzie każdy z jedenastu artykułów posługuje się specyficzną siatką pojęciową, co często wyraźnie ukazane jest wprost przez zamieszczenie na wstępie artykułów słowniczek pojęć ustawowych. Dlatego uwagi dalej czynione nie mają charakteru ogólnego, odnoszącego się do całego UCC. Co istotne, akt ten zawiera również przepisy dotyczące relacji z regulacją E-sign Act (zob. § 1-108, § 2-108. (4) i § 7-103. (c) UCC).

W kontekście podpisu elektronicznego doniosłe znaczenia mają zmiany poczynione w artykule 9 UCC dotyczącym *Secured Tran-*

sactions (pol. prawne zabezpieczenia transakcji, wiarytelności). Wraz z upowszechnieniem transakcji dokonywanych drogą elektroniczną zmieniono tam określenie *writing* (pol. pismo) na *record* (pol. zapis), z czym z kolei łączyła się zmiana *sign* (pol. podpis) na *authenticate* (pol. poświadczenie). Aktualnie § 9-102. (a). (7) UCC stanowi, że *authenticate* znaczy podpisać się (lit. A cytowanego przepisu) lub stworzyć, lub użyć symbolu (hasła, znaku), zakodować lub w inny podobny sposób przetworzyć *record* w całości lub w części, z zamiarem poświadczającej osoby, aby zidentyfikować poświadczającą osobę oraz uwiarygodnić *record* poprzez wskazanie zatwierdzenia treści zapisu (lit. B cytowanego przepisu). Z legislacyjnego punktu widzenia pojęcie *authenticate* wzbogaca zakres dotychczasowych desygnatów pojęcia *sign*, przy czym identyczna jest rola (funkcja) *authenticate* i *sign*. Należy tutaj zważyć, że UCC posługuje się często pojęciem *record authenticated*. Natomiast *record* to zgodnie z § 9-102. (a). (69) UCC, informacja zapisana na materialnym nośniku (środku) lub przechowywana na elektronicznym, lub innym nośniku (środku) i dostępna w dostrzegalnej formie. Pojawia się zasadnicze pytanie o stosunek *authentication* do *electronic signature*. Za oficjalnym komentarzem do UETA⁵ należy powtórzyć, że *authentication* zazwyczaj ma węższe znaczenie i cel niż *electronic signature* w rozumieniu UETA. Jakkolwiek *authentication* „tworzy” *electronic signature* w rozumieniu UETA, czyli skutki prawne wywołane *authentication* są niejako absorbowane na grunt regulacji *electronic signature*.

Inne ujęcie definityjne w zakresie podpisu występuje w art. 2 i 7 UCC. Zgodnie z § 2-103.(1).(p) i § 7-102.(a).(11) UCC podpis to wyrażenie intencji poświadczenia lub użycie zapisu (ang. *record*) poprzez stworzenie, lub użycie materialnego symbolu albo połączenie lub logiczne powiązanie z zapisem elektronicznym dźwięku, symbolu lub procesu. Natomiast § 2-103.(1).(m) i § 7-102.(a).(10) UCC ustanawiają definicję *record* w identycznym brzmieniu jak § 9-102.(a).(69) UCC.

Definicja podpisu elektronicznego (ang. *electronic signature*)

Sec.106.(5) E-sign Act i sec.2.(8) UETA stanowi, że podpis elektroniczny oznacza elektroniczny dźwięk, symbol lub proces, dołączony lub logicznie powiązany z umową, lub innym *record* i stworzony lub użyty przez osobę z zamiarem podpisania *record*. Z kolei sec.106.(2) E-sign Act i sec.2.(5) UETA stanowi, że *electronic* znaczy odnoszący się do technologii (o właściwości) elektronicznej, cyfrowej, magnetycznej, bezprzewodowej, optycznej, elektromagnetycznej lub innej mającej podobne właściwości. *Record* to zgodnie z sec.106.(9) E-sign Act oraz sec.2.(13) UETA informacja, która jest zapisana na materialnym nośniku (środku) lub jest przechowywana na nośniku elektronicznym lub innym, przy czym jest możliwe jej odtworzenie w dostrzegalnej formie. Natomiast sec.106.(4) E-sign Act i sec.2.(7) UETA stanowi, że *electronic record* to umowa lub inny zapis stworzony, wygenerowany, wysłany, zakomunikowany, przekazany, otrzymany lub zgromadzony na nośniku elektronicznym. Jest to więc szczególny rodzaj *record*, obejmujący m.in. dane zgromadzone na dysku komputera lub dyskietce wiadomości poczty głosowej oraz

⁵ Jak się wydaje, przepisom prawa wzorcowego w USA zawsze towarzyszy oficjalny komentarz. W przypadku UETA zob. <http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/uet99.htm>, dostęp na dzień 7.04.2010 r.

nagrania audio i wideo. Należy mieć na uwadze, że regulacje amerykańskie opierają się na zgodzie obu stron do dokonywania czynności z zastosowaniem podpisu elektronicznego. Jednak ustalenie, czy strony wyrażają taką zgodę, następuje nie tylko w oparciu o wprost wyrażone oświadczenie w tym kierunku, ale również może wynikać z kontekstu sytuacji, jak też innych okoliczności towarzyszących danej czynności⁶.

W zasadzie klasyfikacja podpisów elektronicznych jest możliwa tylko w oparciu o kryteria nawiązujące do zagadnień technologicznych. Jeśli regulacje konstruuje się w ten sposób, że nie preferuje się żadnego rozwiązania technologicznego, nie jest możliwe wskazanie konkretnych rodzajów podpisu elektronicznego. Na gruncie prawa federalnego oraz prawa wzorcowego regulację amerykańską można w tej kwestii scharakteryzować poprzez negatywne wskazanie, że nie wyodrębnia się obok zwykłego podpisu elektronicznego jakiejś szczególnej (zaawansowanej) jego formy. Za podpis elektroniczny, któremu należy przydać doniosłe skutki prawne, należy uznać każdy podpis elektroniczny, który jest wiarygodny, tj. możliwa jest identyfikacja poświadczającego oraz zamiaru, jaki mu przyświecał przy podpisywaniu (w sensie „zamiaru poświadczenia”). Jak wcześniej wspomniano kwestia ta inaczej wygląda na gruncie prawa stanowego, na co wpływ miało choćby to, że regulacje stanowe często uchwalono wcześniej niż E-sign Act i UETA – najczęściej prawodawstwo stanowe datowane jest na drugą połowę lat dziewięćdziesiątych XX wieku. W związku z tym w regulacjach tych pojawia się pojęcie podpisu cyfrowego jako podpisu elektronicznego wykorzystującego technologię szyfrowania asymetrycznego. Uchwalenie E-sign Act, a zwłaszcza powstanie prawa wzorcowego UETA, spowodowało nowelizację dotychczasowych przepisów, jednak nie zawsze było to równoznaczne z prawną eliminacją instytucji podpisu cyfrowego. Częstym przypadkiem jest egzystowanie obok siebie regulacji podpisu elektronicznego i podpisu cyfrowego, przy czym skorzystanie z tych podpisów pociąga za sobą identyczne skutki prawne. Ogólnie można stwierdzić, że prawo poszczególnych stanów nie jest w pełni spójne pomiędzy sobą. Przykładowo w stanie Kalifornia, gdzie implementacji UETA, czy szerzej ujmując recypowania kwestii podpisu elektronicznego do systemu prawnego, dokonano poprzez zmianę *California Civil Code* z dnia 16 września 1999 r., kiedy to statuowano definicję podpisu elektronicznego (zob. § 1633.2. (h) tego aktu), jak również wyraźnie uregulowano skutki prawne skorzystania z tego podpisu (zob. § 1633.7. (a) tego aktu). W zasadzie powtórzono w tym zakresie postanowienia UETA⁷. Podobnie § 103 i § 303. (d) *Pennsylvania Electronic Transactions Act* z 16 grudnia 1999 r. Z kolei *New York Electronic Signatures Act* z dnia 25 stycznia 1999 r. stanowi o dwóch rodzajach podpisu: *digital and electronic signatures*, przy czym nie zróżnicowano skutków prawnych ich zastosowania. Natomiast *Illinois Electronic Commerce Security Act* z 14 sierpnia 1998 r. ustanawia aż trzy rodzaje podpisów: *electronic signa-*

*tures, secure electronic signatures and digital signatures*⁸. W prawie stanu Floryda spotykamy poniekąd dwoistą regulację. Przepisy sec. 668.001-668.006 *Florida Electronic Signature Act*, odnoszą się ogólnie do *electronic signatures*, zaś sec. 668.50 dotyczy wyłącznie UETA. Zgodnie z sec. 668.003. (3) *Florida Electronic Signature Act* podpis cyfrowy (*digital signatures*) to rodzaj podpisu elektronicznego, który przekształca wiadomość używającą szyfrowania asymetrycznego tak, że osoba mająca wiadomość i publiczny klucz sygnatariusza może dokładnie ustalić: (a) czy przekształcenie zostało dokonane z użyciem prywatnego klucza, który odpowiada publicznemu kluczowi sygnatariusza; (b) czy wiadomość była zmieniana, odkąd dokonano przekształcenia. Para kluczy oznacza „zestaw” składający się z prywatnego klucza i jego odpowiednika – klucza publicznego. Szyfrowanie asymetryczne jest algorytmem lub seriami algorytmów, które określają parę kluczy. Natomiast, zgodnie z pkt 4 przytoczonego przepisu, elektroniczny podpis oznacza jakiegokolwiek litery lub znaki, które zostały ujawnione elektronicznie lub w podobny sposób, wykonane lub użyte przez stronę z zamiarem poświadczenia pisma. Pismo jest podpisane elektronicznie, jeśli podpis elektroniczny jest logicznie powiązany z tym pismem. W przepisie dotyczącym skutków prawnych posłużenia się podpisem elektronicznym (faktycznie zrównanie go z podpisem tradycyjnym) nie ma mowy o szczególnych skutkach złożenia podpisu cyfrowego, jest mowa o podpisie elektronicznym, którego jednym z rodzajów jest podpis cyfrowy⁹.

W kontekście rodzajów podpisu elektronicznego omówienia wymaga kwestia poświadczania (podpisu lub umowy) przez notariusza lub inny organ władzy publicznej. Zgodnie z sec.101. (g) E-sign Act i sec.11 UETA, zadość temu wymogowi czyni złożenie podpisu elektronicznego przez właściwą osobę poświadczającą. Jak podniesiono w oficjalnym komentarzu do UETA, nie oznacza to jednak zwolnienia osoby poświadczającej z innych obowiązków, których musi dopełnić przy poświadczaniu. Chodzi tutaj zwłaszcza o obowiązek identyfikacji np. strony umowy, który często realizowany będzie poprzez osobisty kontakt tej strony i osoby poświadczającej¹⁰.

Podmioty uprawnione do posługiwania się podpisem elektronicznym

Podobnie jak ustawa modelowa UNICITRAL, prawo amerykańskie dopuszcza szeroki krąg podmiotów mogących posługiwać się podpisem elektronicznym, co w zasadzie oznacza nieograniczenie użytkowania podpisu elektronicznego wyłącznie do osób fizycznych. Mianowicie regulacje amerykańskie posługują się kategorią *person* na określenie w zasadzie każdego podmiotu prawa lub podmiotu handlowego, wymieniając przykładowo w sec.106. (8) E-sign Act oraz sec.2. (12) UETA: osoby indywidualne (*individual*), spółki, zarząd powierniczy, stowarzyszenia (*corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture*) i podmioty publiczne (*governmen-*

⁶ Por. w tym zakresie rozważania Z. Radwańskiego na gruncie prawa polskiego: Z. Radwański, *Elektroniczna forma czynności prawnej*, Monitor Prawniczy 2001, nr 22, s.1113; Z. Radwański, Uwagi ogólne o zakresie stosowania formy elektronicznej w prawie cywilnym, *Rozprawy prawnicze. Księga pamiątkowa Profesora Maksymiliana Pazdana*, Kraków 2005, s. 1306; Z. Radwański, w: *System Prawa Prywatnego: Prawo cywilne – część ogólna. T. 2*, Z. Radwański (red.), Warszawa 2008, s. 171.

⁷ Por. A. Ambroziewicz, *Podpis elektroniczny – pojęcie i funkcje w obrocie*, Przegląd Sądowy, 1, 2001, s. 106.

⁸ G. J. Ferguson, O. J. Armas, *Enforcing electronic contracts in The Americas*, *International Company and Commercial Law Review* 1999, Spe, s. 102 i nt.

⁹ Sec. 668.004 *Florida Electronic Signature Act*: Unless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature.

¹⁰ L. Plimpton, *The Arizona Electronic Transactions Act*, *Arizona Attorney* 2000, 11, s. 39.

tal agency, public corporation). Zauważyć jednak należy, że prawo amerykańskie przywołuje, w kontekście podpisu elektronicznego, specyficzną kategorię *person*, jaką są konsumenci, których, zwłaszcza E-sign Act (zob. sec.101. (c)) szczególnie chroni poprzez m.in. zaostrenie wymogów co do ich zgody na stosowanie wobec nich środków komunikacji elektronicznej. Sec.106. (1) E-sign Act stanowi, że konsumentem jest osoba indywidualna, która w drodze umowy nabywa produkt lub usługę użytku osobistego, rodziny lub celów gospodarstwa domowego, jak również pełnomocnika takiej osoby.

Szerokie zakreślenie ram podmiotowych nie oznacza, że podpis elektroniczny w rozumieniu E-sign Act znajduje zastosowanie do wszystkich czynności prawnych. E-Sign Act nie ma zastosowania do elektronicznych transakcji obejmujących: testamenty, kodycyłe i testamentowe zarządy powiernicze; przysposobienia, rozwody i inne sprawy rodzinne; do regulacji UCC, wyjąwszy §§ 1-107,2-206 i Artykuły 2 i 2A; i inne wskazane w przepisach E-sign Act. Podobnie jest w przypadku UETA¹¹.

Skutki prawne opatrzenia danych podpisem elektronicznym

Przepis sec.101. (a). (1) E-sign Act stanowi, że podpisowi, umowie lub innemu zapisowi związanemu z *transaction* nie mogą zostać odmówione skutki prawne (obowiązanie, moc prawna i wykonalność) tylko dlatego, że są sporządzone w formie elektronicznej. Dalej pkt (2) mówi, że umowie związanej z *transaction* nie mogą zostać odmówione skutki prawne (obowiązanie, moc prawna i wykonalność) tylko dlatego, że podpis elektroniczny lub elektroniczny zapis został użyty w takiej formie. Należy również wskazać, że zgodnie z sec.106. (13) E-sign Act, *transaction* to czynność lub zespół czynności odnoszących się do prowadzenia działalności gospodarczej, czynności konsumenckich lub innych handlowych zdarzeń prawnych między dwoma lub więcej osobami, dokonującymi jakiegokolwiek z następujących czynności: (A) sprzedaż, najem, wymiana, udzielenie licencji lub innej czynności (i) mającej za przedmiot majątek, w tym dobra materialne i niematerialne; (ii) usługi; (iii) oraz jakiegokolwiek kombinacje powyższych; (B) sprzedaż, najem, wymianę licencji lub inną czynność związaną z własnością lub kombinacją powyższych.

Przepisy sec.7 UETA zawierają podobne postanowienia. I tak lit. (a) stanowią, że zapis lub podpis nie może zostać uznany za niewywołujących skutków prawnych tylko dlatego, że jest w formie elektronicznej. Lit. (b) stanowi z kolei, że umowa nie może zostać uznana za niewywołującą skutków prawnych tylko dlatego, że elektroniczny zapis został użyty w takiej formie. W myśl lit. (c), jeżeli wymagane jest sporządzenie zapisu na piśmie, elektroniczny zapis spełnia taki warunek. Lit. (d) stanowi zaś, że jeżeli prawo wymaga podpisu, podpis elektroniczny czyni zadość takiemu wymogowi. Szczęólnego rozważania wymagają przywołane lit. (c) i (d). Jak podnosi się w oficjalnym komentarzu do UETA, celem tych przepisów jest uprawomocnienie dokonywania zapisów elektronicznych i podpisów elektronicznych jako ekwiwalentów pisma, przydając tym pierwszym moc równoważną zapisom papierowym i podpisom własnoręcznym. Przepis sec.13 UETA ponadto stanowi odnośnie różnego typu procedur, że dowód w postaci zapisu lub podpisu nie może zastać odrzu-

cony tylko z powodu formy elektronicznej. E-sign Act nie zawiera wprost postanowień odnośnie zrównania pod względem skutków prawnych formy elektronicznej z formą pisemną, jak to stanowi sec.7. (c) i (d) UETA, jednak z brzmienie sec.101. (c). (1) E-sign Act odwołującego się do lit. (a) tego przepisu, można wywieść zrównanie formy elektronicznej z formą pisemną (*"the use of an electronic record to provide or make available such information satisfies the requirement that such information be in writing"*).

Należy również zwrócić uwagę na regulację dotyczącą elektronicznego agenta (*electronic agent*), której zadaniem jest wyjaśnienie ewentualnych wątpliwości pojawiających się w sytuacji, gdy wszystkie strony transakcji nie uczestniczą bezpośrednio w jej zawarciu, a czynności niejako bezpośrednio, w imieniu tych osób, dokonuje elektroniczny agent. Zgodnie z sec.101. (h) E-sign Act, umowie lub innemu zapisowi odnoszącemu się do transakcji nie mogą zostać odmówione skutki prawne (obowiązanie, moc prawna i wykonalność) tylko dlatego, że została stworzona lub doręczona przez jednego lub więcej elektronicznych agentów (pośredników), tak długo jak czynności elektronicznego agenta są przypisane związanej z nim osobie. Przepisy UETA natomiast wiążą pojęcie elektronicznego agenta z transakcją automatyczną (*automated transaction*) – regulacji tej poświęcona jest sec.14 UETA, *automated transaction* została zaś zdefiniowana w sec.2. (2) UETA.

Pojęcie elektronicznego agenta wyjaśnione jest w sec. 106. (3) E-sign Act i sec.2. (6) UETA stanowiących, że jest to program komputerowy lub jakiegokolwiek automat, który niezależnie inicjuje czynność lub odpowiada przy sporządzaniu elektronicznego zapisu, lub wykonuje go w całości, lub części, bez wglądu lub ingerencji osoby w czasie tej czynności lub odpowiedzi. Sec.2. (3) UETA zawiera ponadto definicję programu komputerowego.

Weryfikacja podpisu elektronicznego

Neutralność technologiczna powoduje, że nie ma w prawie federalnym i wzorcowym wskazanej żadnej konkretnej technologii, która umożliwiałaby weryfikację nadawcy lub treści zapisu elektronicznego. W związku z tym nie ustanowiono szczególnego rodzaju podpisu elektronicznego. Można jedynie powołać się na praktykę. Według wytycznych *American Bar Association* certyfikat to wiadomość, która co najmniej: a) identyfikuje wydawcę certyfikatu, b) nazywa i identyfikuje podpisującego, c) zawiera klucz publiczny podpisującego, d) określa okres ważności, e) jest cyfrowo podpisana przez wydawcę certyfikatu¹².

W prawodawstwie niektórych stanów, jak wcześniej omówiono, występuje obok podpisu elektronicznego – podpis cyfrowy, który wykorzystując technologie szyfrowania asymetrycznego, wymaga istnienia instytucji *certificate* (pol. certyfikatu). Przykładem jest prawo stanu Floryda, gdzie sec. 668.003. (1) *Florida Electronic Signature Act* stanowi, że *certificate* oznacza komputerowy zapis, który: (a) identyfikuje *certification authority* (pol. jednostkę certyfikacyjną), (b) identyfikuje składającego, (c) zawiera publiczny klucz składającego, (d) jest cyfrowo podpisany przez *certification*

¹¹ S. E. Blythe, *Digital...*, s. 32-33; G. L. Berenstein, Ch. E. Campbell, *Electronic...*, s. 2.

¹² J. Gawel, M. Świerczyński, *Podpis elektroniczny*, *Kwartalnik Prawa Prywatnego* 2001, 1, s. 199.

authority. Zgodnie z pkt 2 *certification authority* oznacza osobę, która wydaje *certificate*.

Sec. 2. (14) UETA definiuje pojęcie procedury bezpieczeństwa, czyli postępowania podjętego w celu weryfikacji, że elektroniczny podpis, zapis lub świadczenie pochodzi od określonej osoby lub w celu wykrycia zmian i błędów w informacji zapisanej elektronicznie. Postępowanie obejmuje użycie algorytmów lub innych kodów, identyfikujących słów, numerów, szyfrów, rozmowy zwrotnej lub inne.

Według oficjalnego komentarza do UETA procedura bezpieczeństwa może zostać zastosowana, aby zweryfikować elektroniczny podpis, zweryfikować tożsamość nadawcy lub zapewnić integralność elektronicznego zapisu. Definicja nie wskazuje jakiegokolwiek szczególnej technologii służącej. Pozwala to wykorzystać takie sposoby, które strony wybiorą, lub które są im nakazane regulaminowo, co z kolei zwiększa stopień elastyczności stosunków pomiędzy stronami i jednocześnie uwzględnia ewentualny przyszły rozwój technologiczny. Statuowana w UETA definicja jest względnie szeroka. Procedura bezpieczeństwa nie jest obowiązkowa, jest jedynie metodą wykazania źródła lub zawartości zapisu elektronicznego lub podpisu elektronicznego. Procedura bezpieczeństwa może być technologicznie bardzo wyszukana, tak jak np. szyfrowanie (kryptografia) asymetryczne. Jednak może być również skrajnie prosta, przykładowo wykorzystując rozmowę telefoniczną potwierdzającą tożsamość wcześniejszego nadawcy przez inny kanał komunikacji. Każdy z tych przykładów jest metodą potwierdzania tożsamości osoby lub dokładności wiadomości.

Podsumowanie

Regulacja podpisu elektronicznego w prawie amerykańskim jest o tyle skomplikowana i w pewnym zakresie niejasna, że obowiązują jednocześnie, niejako obok siebie, przepisy prawa federalnego i prawa stanowego. Co do tego ostatniego sytuacja znacznie uprościła się wskutek coraz większego rozpowszechnienia, a tym samym implementacji postanowień UETA, będących w tej mierze prawem wzorcowym. Cechą regulacji federalnej (E-sign Act) i UETA, podobnie jak w przypadku ustawy modelowej UNICITRAL, jest ścisłe trzymanie się zasady technologicznej neutralności. Niemniej w prawie stanowym spotkać można wciąż obowiązujące pozostałości po regulacjach powstałych jeszcze przed E-sign Act i UETA, które nierzadko szeroko odwołują się do koncepcji podpisu cyfrowego. Wydaje się jednak, że choć sytuacja prawna jest w tej mierze strukturalnie skomplikowana, to jednak nie stanowi to „zapory” dla wykorzystywania podpisu elektronicznego w obrocie gospodarczym.