Ignacy Sitnicki

Krótki komentarz do kierunków założeń ustawy o podpisie elektronicznym

Palestra 46/1-2(529-530), 40-46

2002

Ignacy Sitnicki

KRÓTKI KOMENTARZ DO KIERUNKÓW ZAŁOŻEŃ USTAWY O PODPISIE ELEKTRONICZNYM[1]

L. KIERUNKI I TOK PROCESU LEGISLACYJNEGO

W dniu 18 września 2001 r. Sejm uchwalił ustawę o podpisie elektronicznym[2]. Adopcja do polskiego systemu prawnego zasad stosowania jednej z zaawansowanych technologii obrotu poprzez Internet stała się faktem[3]. Sam proces tworzenia ustawy był dość skomplikowany i trudny. Wystarczy przypomnieć, ile kontrowersji budził projekt przygotowany przez Ministerstwo Spraw Wewnętrznych i Administracji[4] oraz jakie emocje towarzyszyły opracowaniu drugiego, opartego na innej koncepcji, poselskiego projektu ustawy o podpisie elektronicznym[5]. Powstał bowiem zasadniczy problem, czy obydwie inicjatywy, rządowa i poselska, wychodzące z różnych założeń odnośnie do definicji, funkcjonowania i infrastruktury bezpieczeństwa podpisu elektronicznego, dadzą się ze sobą pogodzić?

Jednak dzięki sprawnemu kierowaniu pracami legislacyjnymi przez posła Karola Działoszyńskiego[6], obydwie propozycje stały się bazą wyjściową do opracowania jednolitego projektu ustawy o podpisie elektronicznym. Prace w komisjach sejmowych zakończono w zaplanowanym terminie[7], a Sejm przyjął przedstawiony projekt ustawy. Ustawa różni się w sposób istotny od przygotowanych wcześniej: wstępnego[8] i rządowego (opracowanego przez MSWiA) projektów. W kilku istotnych punktach różni się także od projektu poselskiego. Przede wszystkim *zrezygnowano* z technologicznie zależnego modelu podpisu elektronicznego (chodziło w tym przypadku o podpis cyfrowy). Zrezygnowano ze ścisłego nadzoru nad podmiotami świadczącymi usługi w zakresie podpisów elektronicznych, jaki w założeniach miał sprawować minister właściwy do spraw wewnętrznych. Zrezygnowano również z niepotrzebnie rozbudowanej struktury systemu kontroli usług certyfikacyjnych. Ustawodawca nie zdecydował się jednak na utworzenie wyspecjalizowanej instytucji regulującej rynek tych usług. Przy konstruowaniu ustawy wybrano zatem wariant adekwatnej kontroli jakości i bezpieczeństwa korzystania z usług w zakresie podpisów elektronicznych. Przy tworzeniu ustawy odstąpiono jednak od pomysłu całkowitej neutralności technologicznej, kładąc nacisk na gwarancyjną funkcję podpisu elektronicznego. W ustawie znowelizowano art. 60[9] oraz art. 78 k.c.

II. ZAŁOŻENIA USTAWY O PODPISIE ELEKTRONICZNYM

Celem ustawodawcy było takie ukształtowanie funkcji podpisu elektronicznego, aby: 1) stosowanie podpisu elektronicznego spełniało warun ki określone w ustawie, 2) określone zostały skutki prawne jego stosowania, 3) ukształtowane zostały zasady świadczenia usług certyfikacyjnych, 4) wykształcone zostały infrastruktura oraz reguły nadzoru nad podmiotami świadczącymi usługi certyfikacyjne.

Podstawowym założeniem ustawy było zrównanie skutków prawnych podpisu elektronicznego z podpisem własnoręcznym i szerszym otwarciem ograniczonych dotychczas możliwości rozwoju e-businessu[10]. Trzeba jednak zaznaczyć, iż ustawodawca miał do wyboru wariant bardziej lub mniej permisywny, jeśli chodzi o granice zastosowania podpisu elektronicznego. W literaturze wyróżnia się zazwyczaj dwa przeciwstawne modele regulacji prawnych dotyczących stosowania technologii podpisu elektronicznego: model technologicznie otwarty i model technologicznie zależny[11]. Pierwszy zakłada przyznanie skutków prawnych podpisu własnoręcznego podpisowi elektronicznemu w każdej postaci, nie określając *ex lege* warunków, jakie powinna spełniać metoda podpisu elektronicznego, drugi przyznaje takie skutki jedynie podpisowi elektronicznemu spełniającemu warunki określonej technologii (np. podpis cyfrowy)[12]. Pierwszy jest zatem wariantem technologicznie neutralnym[13] (bezwzględnie otwartym), drugi technologicznie zamkniętym. W ustawie zastosowano model mieszany, zgodnie zresztą z założeniami Dyrektywy Unii Europejskiej z 13 grudnia 1999 r. Taki model mieszany uznać można za model względnie otwarty (definiujący warunki podpisu elektronicznego gwarantujące jego pewny i bezpieczny charakter) w odróżnieniu do modelu bezwzględnie otwartego (neutralnego), który nie preferuje żadnej szczególnej metody podpisu elektronicznego, ale nie jest też w praktyce nigdzie zalecany. Decydując się na przyjęcie modelu mieszanego (względnie otwartego), miano na uwadze w pierwszym rzędzie imperatyw bezpieczeństwa stosowanej metody oraz cel jakim jest budowanie zaufania do korzystania z technologii, która daje pełne gwarancje poufności i integralności przesyłanych drogą elektroniczną informacji. Warunkami dającymi takie gwarancje są zakreślone ustawą wymagania dla podpisu elektronicznego zdeterminowane poprzez warunki, iż podpis elektroniczny jest przyporządkowany wyłącznie do osoby składającej ten podpis, jest on sporządzany za pomocą urządzeń i danych podlegających wyłącznej kontroli osoby składającej podpis elektroniczny oraz jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna. Tego rodzaju podpis ustawodawca określił jako „bezpieczny podpis elektroniczny". Definicja taka jest próbą pogodzenia modelu neutralnego technologicznie z modelem zależnym technologicznie. Na dzień dzisiejszy bezpieczną technologią podpisu elektronicznego jest metoda podpisu cyfrowego oparta na zasadzie asymetrycz-

nych kluczy szyfrujących i deszyfrujących (prywatnego i publicznego). Nie jest wykluczone, iż opracowane zostaną inne metody podpisu elektronicznego, spełniające warunki definicji „bezpiecznego podpisu elektronicznego". Jeśli chodzi o zasady świadczenia usług certyfikacyjnych, dopuszczono zasadę swobodnego akcesu do rynku tych usług, z tym zastrzeżeniem, iż wyodrębniono wśród podmiotów świadczących te usługi grupę podmiotów wpisanych do rejestru. Wpis do rejestru ma spełniać zadanie *sui generis* gwarancji co do jakości i nadzoru nad oferowanymi usługami w zakresie podpisów elektronicznych. Jednakże zgodnie ze standardami europejskimi, tego swoistego przymusu akredytacyjnego nie wprowadzono, choć sam wpis do rejestru ma istotne odniesienie do mocy podpisu elektronicznego.

Nadzór nad podmiotami świadczącymi usługi certyfikacyjne powierzono ministrowi właściwemu do spraw gospodarki. Ustawodawca znalazł w tym zakresie rozwiązanie częściowo łagodzące spór, czy nadzór i kontrolę przypisać ministrowi właściwemu do spraw wewnętrznych, czy zupełnie nowej instytucji będącej wyspecjalizowanym regulatorem rynku usług certyfikacyjnych.

III. GRANICE BEZPIECZEŃSTWA STOSOWANIA USTAWY

Ustawa ustanawia adekwatnie szerokie ramy stosowania podpisu elektronicznego tak w wymiarze technologicznym, jak i obszarów jego wykorzystania.

Ustawa jest otwarta na implementowanie różnych technologii podpisu elektronicznego[14]. W praktyce, za bezpieczną metodę podpisu elektronicznego uważa się metodę podpisu cyfrowego opartą na systemie Infrastruktury Klucza Publicznego – PKI[15]. Regulacja ustawowa nie wyłącza możliwości wdrożenia zupełnie innych bezpiecznych metod podpisu elektronicznego (np. metod biometrycznych). W każdym razie, w ślad za Dyrektywą Unii Europejskiej z 13 grudnia 1999 r., ustawa polska rozróżnia zwykły (*sensu largo*) „podpis elektroniczny" w postaci danych elektronicznych, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny[16] oraz zaawansowany (*sensu stricto)* „bezpieczny podpis elektroniczny" wywołujący takie same skutki prawne (wszak pod pewnymi warunkami) jak podpis własnoręczny, gwarantujący integralność przesyłanych danych[17]. Obecnie w praktyce warunki takie spełnia podpis cyfrowy z kluczem publicznie znanym. Jest oczywiście sprawą otwartą zastosowanie w przyszłości także innych metod podpisu elektronicznego, ustawa bowiem nie definiuje tego rodzaju podpisu jako podpisu cyfrowego. Tymczasem jednak inne metody podpisu (w tym symetryczne metody kodowania) będą mogły być stosowane, o ile strony to zaakceptują.

Usługi certyfikacyjne może świadczyć każdy podmiot na podstawie umowy. Umowa taka pod rygorem nieważności powinna zostać sporządzona na piśmie. Ponadto ustawa kreuje kategorię akredytowanych i kwalifikowanych podmiotów świadczących usługi certyfi-

kacyjne. Regulacja struktury i hierarchii podmiotów świadczących usługi certyfikacyjne oparta została na koncepcji zaufanej trzeciej strony (*Trusted Third Party*) jako podmiotu pośredniczącego między kontrahentami w Internecie, dającego pełną gwarancję zachowania poufności i integralności przesyłanych drogą elektroniczną danych. Można oczywiście dyskutować nad modelem struktury i hierarchii podmiotów świadczących usługi w zakresie podpisów elektronicznych. Jednakże nie ulega wątpliwości, że poziom takiego zaufania musi być budowany poprzez środki weryfikacji i kontroli usług świadczonych przez podmiot pełniący rolę osoby zaufania publicznego. Stopień złożoności zarówno struktury, jak i weryfikacji oraz kontroli podmiotów świadczących usługi certyfikacyjne wydaje się być dość wysoki. Jednakże przy konstruowaniu tych przepisów ustawodawca musiał bardzo uważnie wsłuchać się w głos opinii specjalistów, w szczególności matematyków-kryptologów, osób wdrażających technologie internetowe, przedstawicieli banków oraz resortu spraw wewnętrznych. Aby powiązać jakość świadczonych usług z gwarancjami bezpieczeństwa stosowania oferowanych technologii, w ustawie wprowadzono system certyfikatów, od certyfikatu zwykłego jako elektronicznego zaświadczenia, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny po certyfikat kwalifikowany, posiadający silniejszą moc gwarancyjną i wiążący ze swoją treścią szersze skutki prawne niż certyfikat zwykły. Hierarchizacja podpisów i certyfikatów jest jedynie konsekwencją przyjęcia modelu mieszanego odnośnie do technologii podpisów elektronicznych i nadzoru nad usługami w tym zakresie.

IV. FUNKCJE USTAWY

Ustawa o podpisie elektronicznym spełnia funkcje: 1) systemową – statującą skutki prawne podpisu elektronicznego w postaci zaawansowanej (bezpieczny podpis elektroniczny) równe skutkom prawnym podpisu własnoręcznego, 2) technologiczną – umożliwiającą zastosowanie różnorodnych metod podpisu elektronicznego, 3) regulacyjną – zakładającą swobodny dostęp do usług w zakresie podpisów elektronicznych oraz określającą zasady wpisu do rejestru podmiotów świadczących usługi certyfikacyjne, 4) ochronną i gwarancyjną – normującą zasady nadzoru i kontroli podmiotów świadczących usługi certyfikacyjne oraz dającą gwarancje bezpieczeństwa stosowania podpisów elektronicznych, integralności przesyłania danych oraz zaufania do usług z tym związanych. Ustawa zawiera również przepisy karne, które są *sui generis* katalogiem reguł gwarantujących częściową (dotyczącą podpisu elektronicznego) ochronę obrotu *via* Internet.

Funkcja systemowa ustawy opiera się na rozwiązaniu, że jedynie bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu wywołuje pełne skutki prawne równoważne skutkom prawnym podpisu własnoręcznego. Również dane w

postaci elektronicznej opatrzone takim podpisem odpowiadają dokumentom na papierze opatrzonym podpisem własnoręcznym. Inne sposoby podpisywania w drodze elektronicznej będą miały wyłączoną bądź ograniczoną moc dowodową.

Funkcja technologiczna zakłada system otwarty, z tym że jest to system względnie otwarty, zakładający pełne skutki prawne podpisu jedynie dla kategorii bezpiecznego podpisu elektronicznego. Właściwie każde rozwiązanie technologiczne może odpowiadać definicji bezpiecznego podpisu elektronicznego, o ile spełnia warunki określone w ustawie. Ustawa umożliwia tworzenie drzew certyfikatów oraz znakowanie czasem.

Funkcja regulacyjna ustawy zakłada wolny i konkurencyjny rynek usług w zakresie podpisów elektronicznych. Rozwiązania ustawy respektują zalecenie Dyrektywy 1999/93/EC, by nie ograniczać konkurencyjności rynku usług certyfikacyjnych. Natomiast wolny akces do tego rodzaju usług jest zasadą. Uwzględniono także zalecenie dobrowolności akredytacji. Jednak z uwagi na zdeterminowanie bezpieczeństwa stosowanych technologii podpisów elektronicznych przez spełnienie warunków gwarantujących jakość stosowanych metod, usługi te podzielono na „niekwalifikowane", czyli bez wpisu podmiotu do rejestru, który je świadczy i usługi kwalifikowane poprzez wpis do rejestru. System taki ma zapewnić pewność i wysoką jakość obrotu elektronicznego, inaczej rynek usług certyfikacyjnych, nieregulowany w jakimkolwiek stopniu, mógłby załamać, a nie rozwinąć obrót elektroniczny.

Funkcja gwarancyjna i ochronna ustawy wiąże się ściśle z funkcjami poprzednimi, a ponadto określa system nadzoru i kontroli nad usługami w zakresie podpisów elektronicznych, a także buduje prawnokarne środki ochrony bezpiecznego korzystania z tych usług. W ustawie odstąpiono zarówno od propozycji ścisłego nadzoru i reglamentowania usług certyfikacyjnych, jak i od zasady dwustopniowej kontroli tych usług i podmiotów je świadczących.

Ustawa o podpisie elektronicznym z pewnością doczeka się wielu polemik i komentarzy (pierwsze próby już są czynione). Z pewnością jest to ustawa w dużym stopniu pionierska i stąd gorące kontrowersje budziła już na etapie opracowywania założeń do niej. Zanim jednak rozgorzeją dyskusje na tle szczegółowych rozwiązań ustawy i ich odniesienia do innych regulacji prawnych, warto przeanalizować główne kierunki założeń oraz intencji ustawodawcy, bowiem stopień złożoności i skomplikowania unormowanej materii wart jest głębszej refleksji.

Przypisy

[1] Publikacja niniejsza jest próbą generalnej rekapitulacji wyniku prac legislacyjnych nad ustawą o podpisie elektronicznym i omówieniem tych podstawowych zadań, jakie ustawodawca postawił przed dość przecież pionierską regulacją. Nie jest zamiarem autora szczegółowe analizowanie przepisów ustawy, gdyż ustawa sama w sobie jest aktem prawnym wymagającym gruntownej analizy. Tym niemniej, warto odnotować, że ustawa doczekała się jeszcze w toku prac legislacyjnych nad nią recen-

zji krytycznych (patrz: J. A. Stefanowicz, A. Szałamacha, *Kto uwłaszczy się na podpisie elektronicznym,* Polityka z 14–1 5 sierpnia 2001 r. dodatek „Prawo co dnia"), choć poziom ogólności zaprezentowanych wniosków czyni przedwczesnym podjęcie polemiki. Celem niniejszej syntetycznej refleksji nad założeniami ustawy jest nadanie ewentualnej polemice pewnych kierunków odpowiadających specyfice regulacji odnoszących się do podpisu elektronicznego. Por. także W. Cellary, T. Piątek, *Klucze do przyszłości*, Rzeczpospolita, Prawo co dnia, 20 października 2001 r.

[2] Ustawa wejdzie w życie w terminie po upływie 9 miesięcy od dnia ogłoszenia (z wyjątkiem kilku przepisów) – ustawa została opublikowana w Dzienniku Ustaw z 15 listopada 2001 r., Nr 130, poz. 1450.

[3] W dniu 11 października 2001 r. ustawa została podpisana przez Prezydenta RP, przy czym prezydent podpisał ustawę także poprzez złożenie podpisu elektronicznego.

[4] Por. m.in. cykl publikacji l. Sitnickiego i M. Srebrnego pt. *„Algorytmy dla nowej gospodarki",* Rzeczpospolita z 8, 9 i 10 lutego 2001 r. (Prawo co dnia).

[5] Podstawowym założeniem projektu poselskiego było dostosowanie go do wytycznych ONZ w sprawie handlu elektronicznego oraz rozwiązań dyrektywy Unii Europejskiej 1999/93nEC z 13 grudnia 1999 r.

[6] Poseł Działoszyński przewodniczył specjalnej podkomisji sejmowej ds. podpisu elektronicznego, działającej w ramach Komisji Transportu i Łączności. Współprzewodniczył komisji poseł Stefan Macner. M.in. dzięki wysiłkom obu posłów prace nad połączonym projektem przebiegały sprawnie.

[7] Autor niniejszej publikacji brał udział w charakterze zaproszonego eksperta w pracach podkomisji ds. podpisu elektronicznego. W pracach podkomisji oprócz parlamentarzystów i osób reprezentujących Rząd udział brali przedstawiciele nauki, zarówno matematycy-kryptolodzy z PAN (prof. Marian Srebrny, dr Andrzej Borzyszkowski), jak i prawnicy (prof. Zbigniew Radwański), a także przedstawiciele organizacji bankowych, sektora IT (dyr. Paluszyński z TP Internet), zainteresowanych resortów administracji rządowej oraz notariatu.

[8] Pod auspicjami NBP został opracowany tzw. wstępny projekt ustawy o podpisie elektronicznym. Projekt ten był w zasadzie propozycją tez wyjściowych do możliwej konstrukcji regulacji dot. podpisu elektronicznego – por. l. Sitnicki, *Uwagi nad niektórymi założeniami wstępnego projektu ustawy o podpisie elektronicznym,* „Palestra" Nr 11 –12/2000.

[9] W brzmieniu nadanym ustawą „z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnią jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej (oświadczenie woli)" – art. 60 k.k.

[10] Wypada w tym miejscu zauważyć, iż dynamika rozwoju e-businessu uległa pewnemu zahamowaniu w skali globalnej, co było związane z wycofaniem się inwestorów z giełdy NASDAQ i spadkiem wartości wielu wiodących firm Nowej Gospodarki, takich jak Cisco Systems, Oracle, Sun Microsystems i innych, nie mówiąc już o załamaniu się sektora tzw. dot.comów. Mimo wszystko wyżej wymienione korporacje oraz takie firmy sektora IT jak Microsoft, SAP czy Cap Gemini, nadal zaliczane są do największych światowych przedsiębiorstw, a gospodarka wykorzystująca w szerokim zakresie Internet uznawana jest za ten rodzaj działalności ekonomicznej, której globalny rozwój jest nieunikniony.

[11] Por. A. Ambroziak, *Podpis elektroniczny – pojęcie i funkcje w obrocie,* Przegląd Sądowy Nr 1/ 2001.

[12] Niektóre ustawodawstwa wprost odnosiły swoje regulacje do kategorii podpisu cyfrowego, por. ustawa stanu Utah, niemiecka ustawa SigG oraz dekret hiszpański. Gwoli ścisłości należy zauważyć, że były to pionierskie rozwiązania w przedmiocie podpisów elektronicznych. Regulacje powstałe później posługują się już kategorią podpis elektroniczny, podkreślając otwarty dla technologii charakter regulacji.

[13] *Por. W.* Kocot, *Elektroniczna forma oświadczeń woli,* PPH Nr 3/2001.

[14] Obecnie najczęściej wymienia się metodę podpisu cyfrowego, polegającą na szyfrowaniu i deszyfrowaniu algorytmami asymetrycznymi oraz metody biometryczne, takie jak odczytywanie obrazu linii

papilarnych, kształtu ludzkiej czaszki czy siatkówki tęczówki. Metody biometryczne nie mają jak dotąd szerszego zastosowania w praktyce i wiele z nich jest jeszcze na etapie badań.

[15] *Public Key Infrastructure* – metoda ogłoszona po raz pierwszy w połowie lat 70 XX wieku przez dwóch matematyków-informatyków amerykańskich Martina Hellmana i Whitfielda Diffie, Metoda *PKI* oparta jest na parze asymetrycznych kluczy kodujących i dekodujących, prywatnego i publicznego. Pierwszy znany jest wyłącznie podpisującemu, drugi dostępny jest publicznie i służy do identyfikacji i weryfikacji podpisującego. Pierwsza publiczna prezentacja systemu przez dr. Martina Hellmana miała miejsce w roku 1976.

[16] Por. art. 2 ust. 1 Dyrektywy 1999/93/EC w brzmieniu: *„For the purpose of this Directive: 1. «electronic signature» means data in electronic form which are attached* to or *logically associated with other electronic data and which serve as a method of authentication"*.

[17] Gwarancjami „bezpieczeństwa" tego rodzaju podpisu są warunki, jak następuje: 1. podpis taki jest przyporządkowany wyłącznie osobie go składającej, 2. jest on sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego, 3. jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.