Dariusz Adamski, Mirosław Kutyłowski

Prawne aspekty wykorzystania technologii cyfrowych w komunikacji urząd-obywatel

Kwartalnik Prawa Publicznego 5/1/2, 165-181

2005

KWARTALNIK PRAWA PUBLICZNEGO
ROK V • NR 1-2/2005 • UKSW - WARSZAWA • TNOiK - TORUŃ • ISSN 1642-9591

Dariusz Adamski, Mirosław Kutyłowski***

PRAWNE ASPEKTY WYKORZYSTANIA TECHNOLOGII CYFROWYCH W KOMUNIKACJI URZĄD-OBYWATEL

1. Wstęp

Zastosowanie zaawansowanych technologii informacyjnych w administracji publicznej i kontaktach z obywatelem jest nieuchronnością. Państwa, które nie usprawnią swej działalności w tym zakresie, będą przegrywały w międzynarodowej konkurencji gospodarczej.

Jednym z podstawowych warunków dla prawidłowego wykorzystania nowoczesnych rozwiązań informatycznych w sferze publicznej jest sprzyjające im środowisko prawne. Warto przyjrzeć się więc bliżej jego charakterystyce tam, gdzie dotyczy ono kontaktów urząd–obywatel, a także podjąć próbę oceny sposobu, w jaki odpowiada na potrzeby rzeczywistości, zarówno na płaszczyźnie technologicznej, jak i ekonomicznej. Dać to powinno administracji publicznej asumpt do wyboru takiej drogi implementacji technologii informacyjnej, która zwiększy efektywność działań urzędników, pozwalając na uniknięcie raf i mielizn, które stały się bardzo charakterystycznym rysem polskiej informatyzacji. Podkreślić należy przy tym, że wadliwa informatyzacja może przynieść efekt odwrotny do zamierzonego – zwiększenie kosztów i zawodności obiegu informacji oraz zmniejszenie efektywności procedur.

* Dr Dariusz Adamski – adiunkt na Wydziale Prawa, Administracji i Ekonomii, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Uniwersytet Wrocławski

** Prof. dr hab. Mirosław Kutyłowski – Instytut Matematyki i Informatyki, Politechnika Wrocławska

2. Ustawa o podpisie elektronicznym (EPU)

Jednym z podstawowych mechanizmów przewidzianych przez obowiązujące obecnie ustawodawstwo, który służyć ma propagowaniu technologii informacyjnych w kontaktach urząd–obywatel, jest art. 58 ust. 2 ustawy o podpisie elektronicznym (dalej: EPU)[1]. Na jego mocy organy władzy publicznej umożliwić mają, w terminie 4 lat od dnia wejścia w życie ustawy[2], tak zwanym „odbiorcom usług certyfikacyjnych" wnoszenie podań i wniosków oraz innych czynności w postaci elektronicznej, w przypadkach gdy przepisy prawa wymagają składania ich w określonej formie lub według określonego wzoru.

Definicja pojęcia odbiorcy usług certyfikacyjnych ustalona została w art. 3 pkt 18 EPU. Stwierdza się w nim, że status ten ma jakikolwiek podmiot prawa, któremu usługi certyfikacyjne świadczone są na podstawie umowy lub polityki certyfikacji[3] w przypadkach usług innych niż wydawanie certyfikatów[4] (por. art. 3 pkt 18 EPU). Jedynie aspekt funkcjonalny owej definicji – usługa certyfikacyjna – pozwala ustalić cechy charakterystyczne kategorii odbiorców usług certyfikacyjnych. Tytuł prawny jej świadczenia (umowa lub polityka certyfikacji) oraz zakres potencjalnych odbiorców usług (jakikolwiek podmiot prawa) ujęte są bowiem nader szeroko.

Kategoria usług certyfikacyjnych zdefiniowana została w art. 3 pkt 13 EPU. Składają się na nią: wydawanie certyfikatów (o których szerzej mowa będzie nieco dalej), znakowanie czasem[5] oraz, dość enigmatycznie określone, inne usługi związane z podpisem elektronicznym. W pierwszej kolejności wskazać należy na udostępnianie zaświadczeń certyfikacyjnych[6], list CRL i ARL[7] oraz odpowiedzi OCSP[8]. Kategoria

---

[1] Dz.U. 2001, Nr 130, poz. 1450 z późn. zm.

[2] Czyli z dniem 16.8.2006 r. Ustawa weszła bowiem w życie 16.8.2002 r., tj. po upływie 9 miesięcy od dnia ogłoszenia (co wynika z jej art. 59 ust. 1).

[3] Polityka certyfikacji to szczegółowe rozwiązania dotyczące bezpieczeństwa tworzenia i stosowania certyfikatów (por. art. 3 pkt 17 EPU).

[4] Podpisujący, dołączający certyfikat do komunikatu, jest odbiorcą usługi certyfikacyjnej na podstawie umowy (o wystawienie certyfikatu). Adresatowi komunikatu usługa (poświadczenie ważności certyfikatu) świadczona jest natomiast na zasadach wynikających jedynie z polityki certyfikacji.

[5] Znakowanie czasem to, w pewnym uproszczeniu, usługa polegająca na poświadczeniu istnienia w danej chwili konkretnej struktury danych, co pozwala na łatwe wykrycie, czy były one po tej chwili modyfikowane (por. art. 3 pkt 16 EPU). Stąd

owych usług jest wszakże dużo szersza, obejmując na przykład udostępnianie oprogramowania niezbędnego do wygenerowania podpisu elektronicznego nie opartego o jakikolwiek certyfikat[9].

Usługami certyfikacyjnymi będą zatem wszystkie te, dzięki którym możliwe jest stosowanie bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem (nazywać go będziemy podpisem kwalifikowanym[10]), bezpiecznego podpisu elektronicznego nie opartego o kwalifikowany certyfikat – to jest opartego o certyfikat inny niż kwalifikowany lub w ogóle nie opartego o certyfikat (podpisy te nazywać będziemy dalej powszechnymi) oraz tych podpisów elektronicznych, które spełniają jedynie podstawowe przesłanki podpisu elektronicznego, ustanowione w art. 3 pkt 1 EPU.

Na gruncie tego ostatniego przepisu podpisem elektronicznym są przyporządkowane osobie fizycznej dane, które, będąc powiązanymi z innymi danymi (treścią dokumentu w sensie prawnym), umożliwiają identyfikację autora dokumentu. Podpis elektroniczny pozwolić ma zatem na identyfikację autora dokumentu, poprzez powiązanie z dokumentem danych przyporządkowanych tylko jego autorowi. Usługą certyfikacyjną będzie zatem nawet generowanie PIN-ów[11] dla posiadaczy rachunków bankowego. Na gruncie art. 3 pkt 1 EPU, PIN stosowany w bankomatach jest bowiem podpisem elektronicznym.

Podkreśla się niekiedy, iż otwartość katalogu usług certyfikacyjnych, wynikająca z recepcji na grunt prawa polskiego ust. 9 preambu-

---

znakowanie czasem (jednak tylko dokonane przez kwalifikowany podmiot świadczący usługi certyfikacyjne) zrównano z nadaniem oświadczeniu daty pewnej – por. art. 7 ust. 2 EPU.

[6] Na gruncie prawa polskiego certyfikat (w sensie technologicznym) wskazuje klucz publiczny danego odbiorcy usług certyfikacyjnych i potwierdza fakt posiadania przez niego określonego statusu prawnego – por. art. 3 pkt 11 EPU.

[7] CRL (ang. *Certificate Revocation List*) to prowadzona przez podmiot świadczący usługi certyfikacyjne lista certyfikatów zawieszonych i unieważnionych, która umożliwia weryfikację ważności danego certyfikatu. ARL (ang. *Authority Revocation List*) ma bardzo zbliżony charakter, tyle tylko, że odnosi się do certyfikatów (w sensie technologicznym) wystawianym podmiotom dostarczającym usługi certyfikacyjne użytkownikom końcowym – tzw. zaświadczeń certyfikacyjnych.

[8] Ang. *Online Certificate Status Protocol*. OCSP, w przeciwieństwie do CRL, nie podaje listy zawieszonych certyfikatów, lecz informuje o statusie pojedynczego certyfikatu.

[9] Co utrudnia rozwój tego ostatniego segmentu rynku, zwłaszcza poprzez poddanie podmiotów dostarczających oprogramowanie do składania zwykłego podpisu elektronicznego zasadom odpowiedzialności odszkodowawczej, wynikającym z art. 11 EPU.

[10] Zastrzec jednak trzeba, że pojęcie to nie jest tożsame na przykład z pojęciem kwalifikowanego podpisu elektronicznego funkcjonującego w Niemczech.

[11] Osobisty Numer Identyfikacyjny (skrót od ang. *Personal Identification Number*).

ły dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[12], jest iluzoryczna[13]. Twierdzi się, iż EPU nie reguluje innych usług niż wydawanie certyfikatów i znakowanie czasem. Trudno się jednak ze stanowiskiem tym zgodzić, skoro sama EPU zastrzega, iż usługą certyfikacyjną jest jakiekolwiek świadczenie „związane z podpisem elektronicznym". Usługa ta odnosić się więc może do jakiegokolwiek podpisu elektronicznego, w tym najprostszego, niekoniecznie zaś tylko kategorii uregulowanej w EPU szczególnie mocno, czyli podpisu kwalifikowanego.

Spośród usług certyfikacyjnych najważniejszą jest wydawanie certyfikatów. Przyjrzyjmy się zatem nieco bliżej temu ostatniemu pojęciu.

Na certyfikacie może opierać się związek pomiędzy podpisem a podpisującym[14], przy czym wskazanie właściwego certyfikatu stanowi w tej sytuacji atrybut podpisu elektronicznego[15]. Certyfikat wiąże daną osobę lub urządzenie z kluczem publicznym służącym do weryfikacji komunikatu opatrzonego przez ową osobę/urządzenie kluczem prywatnym. Odgrywa on zatem rolę kluczową w procesie weryfikacji podpisu elektronicznego. Umożliwia identyfikację autora komunikatu poprzez wskazanie klucza publicznego, jaki przyznany mu został przez wystawcę certyfikatu[16]. Dodać też warto, że wydanie certyfikatu klucza publicznego ma sens praktyczny zwłaszcza wówczas, gdy nie jesteśmy w stanie z góry określić, kto będzie dokonywał weryfikacji podpisów elektronicznych w oparciu o ten certyfikat.

Szczególną pewność co do wyniku weryfikacji autorstwa komunikatu daje, w sensie prawnym, kwalifikowany podpis elektroniczny, który

---

[12] O.J. 2000, L 13/12. Ustęp ów stanowi, że definicja usług i produktów związanych z podpisem elektronicznym „nie powinna ograniczać się do wystawiania i zarządzania certyfikatami, lecz powinna zawierać wszystkie pozostałe usługi i produkty, które korzystają z podpisów elektronicznych lub są z nimi związane, takie jak usługi dotyczące rejestrowania, znakowania czasem, prowadzenia spisów, informatyczne lub konsultacyjne, związane z podpisami elektronicznymi".

[13] P. Podpłoński, P. Popis, *Podpis elektroniczny. Komentarz*, Warszawa 2004, s. 78–79.

[14] Zgodnie z art. 3 pkt 10 EPU certyfikaty to elektroniczne zaświadczenia, za pomocą których dane służące do weryfikacji podpisu elektronicznego są, po pierwsze, przyporządkowane do osoby składającej podpis elektroniczny, oraz, po drugie, umożliwiają jej identyfikację.

[15] Częsta jest również sytuacja, gdy cały certyfikat, a nie tylko jego wskazanie, dołączony zostaje do podpisu.

[16] Którym, zgodnie z art. 3 pkt 14 EPU, może być przedsiębiorca, Narodowy Bank Polski lub organ władzy publicznej.

umożliwia skojarzenie danych do weryfikacji podpisu z podpisującym, za pomocą kwalifikowanego certyfikatu[17] oraz zastosowanie bezpiecznego podpisu elektronicznego[18]. Cecha ta przełożona została na język prawny w art. 5 ust. 3 EPU. Stanowi on: „bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu zapewnia integralność danych opatrzonych tym podpisem i jednoznaczne wskazanie kwalifikowanego certyfikatu, w ten sposób, że rozpoznawalne są wszelkie zmiany tych danych oraz zmiany wskazania kwalifikowanego certyfikatu wykorzystywanego do weryfikacji tego podpisu, dokonane po złożeniu podpisu". W konsekwencji art. 5 ust. 2 EPU stanowi: „dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej". Konstrukcja ta służyć ma upowszechnieniu podpisu kwalifikowanego. Rodzi jednak szereg trudności praktycznych, odnoszących się zwłaszcza do wymogu ważności certyfikatu dla równoważności podpisu na nim opartego z podpisem własnoręcznym. Żaden kwalifikowany certyfikat nie jest bowiem ważny przez okres dłuższy niż 2 lata[19].

Art. 58 ust. 2 EPU nie wymaga takiej szczególnej pewności co do wyniku testu autorstwa. Uprawnienie statuowane tym przepisem przyznano osobom korzystającym z zaangażowania jakiejkolwiek osoby

---

[17] Jest to certyfikat spełniający wszystkie wymogi EPU dotyczące bezpieczeństwa i pewności infrastruktury podpisu elektronicznego, co gwarantowane ma być przez zastrzeżenie, iż wydawać go mogą jedynie podmioty o statusie kwalifikowanych podmiotów świadczących usługi certyfikacyjne – por. art. 3 pkt 12 EPU. Dodajmy, że prawo wielu innych krajów europejskich ogranicza się w tym miejscu do aspektów czysto technologicznych.

[18] Bezpieczny podpis elektroniczny od strony technologicznej opiera się na asymetrycznych, zaawansowanych rozwiązaniach kryptograficznych. Fakt złożenia podpisu tożsamy jest z zastosowaniem poufnych danych – tajnego klucza – wraz z podpisywanym dokumentem, w celu utworzenia unikalnych danych cyfrowych stanowiących „podpis cyfrowy". Z kolei zweryfikowanie podpisu polega na przeprowadzeniu testu matematycznego na takim podpisie cyfrowym. W trakcie weryfikacji korzysta się z klucza publicznego – danych do weryfikacji podpisu elektronicznego. Fundamentalną cechą tego rozwiązania jest asymetria – z klucza publicznego nie jest w praktyce możliwe odtworzenie klucza prywatnego.

[19] Por. § 12 rozporządzenia Rady Ministrów z 7.8.2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. 2002, Nr 128, poz. 1094).

uwierzytelniającej oświadczenie opatrzone podpisem elektronicznym. Rozwiązanie takie stanowi logiczną konsekwencję podstawowego założenia EPU, która promować ma nowoczesne rozwiązania technologiczne. Zgodnie z nim „nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego"[20] (art. 8 EPU). Ustanowiony w tym przepisie zakaz dyskryminacji podpisów elektronicznych dotyczy każdego rodzaju podpisu, który „istnieje w postaci elektronicznej", a zatem zarówno kwalifikowanych, powszechnych, jak i pozostałych[21]. Jedynie jednak w przypadku podpisu kwalifikowanego norma ta rodzi bardzo trudne do obalenia domniemanie złożenia podpisu przez osobę, której nazwisko widnieje na certyfikacie (domniemanie autorstwa)[22]. Domniemanie to bazuje nie tyle na większej pewności technologii identyfikacji autora dokumentu w przypadku opatrzenia go podpisem kwalifikowanym, co raczej na uczestnictwie w procesie identyfikacji godnego zaufania podmiotu trzeciego.

Z samej istoty statusu organów administracji publicznej wynika wszakże, iż gwarantują one, w konsekwencji władczego charakteru ich relacji z jednostką, pewność dokonywanej przez nie autoryzacji podpisów elektronicznych, jeśli to one świadczą usługi certyfikacyjne[23]. Racjonalnie więc, choć wbrew najnowszym trendom, o których będzie mowa nieco dalej, przyjęto, iż na gruncie prawa administracyjnego ułatwiona powinna zostać wymiana korespondencji elektronicznej nawet wów-

[20] Stąd za niedopuszczalną uznać należy stosowaną niekiedy przez organy administracji publicznej interpretację EPU, według której jedynym dopuszczalnych przez polskie prawo sposobem sygnowania urzędowej korespondencji elektronicznej jest podpis kwalifikowany. Interpretacja taka przeczy zarówno brzmieniu, jak i celowi owego aktu.

[21] Odmiennie, co do tej ostatniej kategorii, lecz wbrew wykładni literalnej, systemowej i logicznej art. 8 EPU, P. Podpłoński, P. Popis, *Podpis elektroniczny. Komentarz*, Warszawa 2004, przyp. 70, s. 198–199.

[22] Co wprost wynika z przepisów art. 6 EPU. Podkreślić należy, że nie statuują one całkowitej niezaprzeczalności autorstwa. Niezaprzeczalny jest jedynie fakt złożenia podpisu za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny (art. 6 ust. 3 EPU), nie zaś posłużenia się nimi przez uprawnionego.

[23] Stąd, dla przykładu, normy zawarte w austriackiej ustawie e-Government (*Bundesgesetz ueber Regelung zur Erleichterung des elektronischen Verkehrs mit oeffentlichen Stellen*), które weszły ostatnio w życie, sankcjonują szereg odstępstw od wymogów ustawy o podpisie elektronicznym w relacjach pomiędzy instytucjami publicznymi a osobami fizycznymi.

czas, gdy nie opiera się ona na, preferowanym w EPU, podpisie kwalifikowanym.

W tym momencie warto poświęcić kilka uwag, spychanym nieco na margines EPU, tym technologiom podpisu elektronicznego, które nie wymagają korzystania z usług certyfikacyjnych. Przypomnijmy bowiem – nie każdy podpis elektroniczny weryfikowany musi być certyfikatem.

Zawarte w art. 3 pkt 1 EPU, i omówione nieco wcześniej, przesłanki najprostszej postaci podpisu elektronicznego wypełnia już chociażby wpisanie danych osoby, od której pochodzi dokument, pod jego treścią edytowaną w postaci elektronicznej. W systemach zamkniętych podpis elektroniczny stanowią też hasła jednorazowe[24] i wielorazowe – tzw. PIN, jeśli związane są z kartą lub urządzeniem, którego numer seryjny powiązany jest z daną osobą. Taki sam skutek będzie miało stosowanie PINu (ze swojej istoty powtarzalnego) oraz innych danych (np. logujących do serwera) przyznanych konkretnej osobie. We wszystkich wskazanych przypadkach spełniony zostaje warunek ich przyporządkowania konkretnej osobie fizycznej.

W żadnym jednak z powyższych przypadków identyfikacja nie będzie się odbywała w oparciu o certyfikat. Ani same hasła, ani dane, z którymi są one powiązane (np. nr tokena, login), nie przyporządkowują z osobna danych służących do weryfikacji podpisu elektronicznego osobie składającej podpis. Brak jest więc jednego zaświadczenia umożliwiającego identyfikację składającego podpis. Ustanowiona w art. 3 pkt 10 EPU definicja certyfikatu nie zostanie zatem w tych przypadkach wypełniona.

Mimo jednak, że we wskazanych przypadkach zwykłe podpisy elektroniczne nie są związane z certyfikatami, korzystający z nich należą do kategorii „odbiorców usług certyfikacyjnych". W każdym przypadku korzystają bowiem z „usług związanych z podpisem elektronicznym", co, jak wskazano nieco wyżej, przemawia za istnieniem „usługi certyfikacyjnej".

Zakreśliwszy zakres odbiorców usług certyfikacyjnych przyjrzeć się warto kolejnemu elementowi konstrukcyjnemu art. 58 ust. 2 EPU. Mianowicie, odbiorcy usług certyfikacyjnych uzyskać mają możliwość wnoszenia podań i wniosków w postaci elektronicznej.

Postać elektroniczna to kategoria, co prawda, nie zdefiniowana jednoznacznie w EPU, ma jednak bezsprzecznie szeroki zakres.

---

[24] Generowane mogą być one zarówno przez tzw. token, jak i w innych technologiach – przez karty-zdrapki.

W pierwszej kolejności nie jest ona tym samym, czym oświadczenie w postaci elektroniczne opatrzone podpisem elektronicznym. Jak wskazano jednak już wcześniej, nawet wypełnienie formularza znajdującego się na stronie internetowej urzędu oznaczać będzie złożenie podpisu elektronicznego, jeśli wypełniający go poda swoje dane, pozwalające na jego identyfikację[25]. Z kolei udostępnianie tego typu formularzy stanowi świadczenie usług certyfikacyjnych, związane jest bowiem z takim właśnie, najprostszym podpisem elektronicznym.

Praktyczna stosowalność art. 58 ust. 2 pozostaje pod znakiem zapytania, i to nie tylko ze względu na wciąż ograniczoną informatyzację urzędów publicznych. Powodem o podłożu prawnym jest to, że Minister Gospodarki wciąż nie wydał, wbrew delegacji zamieszczonej w art. 58 ust. 3 EPU, rozporządzenia, które określałoby warunki techniczne i bezpieczeństwa udostępniania formularzy i wzorów, o których mowa w art. 58 ust. 2 EPU. A pamiętać należy, że art. 58 ust. 2 EPU dotyczy jedynie sytuacji, gdy przepisy prawa wymagają określonej formy lub wzoru wnoszonego pisma.

W ten sposób mechanizm wynikający z art. 58 ust. 2 EPU pozostaje w uśpieniu. Rozwój kanałów elektronicznej komunikacji pomiędzy urzędem a interesantami następuje zatem poza jego normami. Co ciekawe, w praktyce bazuje się tu na rozwiązaniach najprostszych. Coraz więcej miejskich stron internetowych udostępnia wzory formularzy potrzebnych do załatwienia spraw urzędowych[26]. Do ich wypełnienia i wniesienia tak sporządzonego podania wystarcza bazowa technologia internetowa, czyli rozwiązanie najprostsze i najtańsze. Jak się wydaje, jest ono dotychczas wystarczająco bezpieczne, brak bowiem doniesień prasowych o interesantach niezadowolonych z udostępnionych im ułatwień[27].

Oczywiście w tym przypadku postępowanie administracyjne staje się jedynie częściowo zinformatyzowane. Lepsza wydaje się jednak informatyzacja fragmentaryczna, lecz użyteczna i opłacalna, niż całościowa, ale niemożliwa do praktycznego wdrożenia. A tak zapewne byłoby, jeśli możliwość wnoszenia podań i wniosków w postaci elektronicznej miałyby tylko te osoby, których podpisy weryfikowane byłyby

---

[25] Ten sposób komunikacji z obywatelem został dopuszczony na przykład przez Generalnego Inspektora Ochrony Danych Osobowych w Polsce.

[26] Najdalej zaawansowane prace w tym zakresie poczynił gdański Urząd Miasta – www.gdansk.pl

[27] W przyszłości zagrożeniem dla tego typu rozwiązań mogą stać się ataki typy „denial of service" polegające na zasypywaniu urzędów przez korespondencję elektroniczną generowaną automatycznie i mającą charakter spamu.

przy pomocy certyfikatu (zwłaszcza kwalifikowanego). Większość interesantów jedynie sporadycznie ma potrzebę kontaktu z urzędem, co zmniejsza dla nich atrakcyjność certyfikatów. Nie zapominajmy też, że certyfikaty ważne są tylko przez ograniczony okres czasu, opłaty za nie należy uiszczać bez względu na to, jak często się z nich korzysta, a samo uzyskanie certyfikatu wymaga dopełnienia szeregu formalności.

3. Ustawa o informatyzacji

Powyższe uwagi stanowią dobry punkt wyjściowy do oceny poprawek, jakie wprowadzić ma do kodeksu postępowania administracyjnego[28] art. 36 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (dalej: PPIU)[29]. Jej art. 36 pkt 5 w dwojaki sposób zmienia art. 63 k.p.a., dotyczący sposobu wnoszenia podań w procedurze administracyjnej.

Pierwszy wydaje się bardzo logiczny. Otóż na mocy PPIU powstać ma możliwość wnoszenia podań również za pośrednictwem „formularza umieszczonego na stronie internetowej właściwego organu administracji publicznej, umożliwiającego wprowadzenie danych do systemu teleinformatycznego", czyli przy wykorzystaniu połączenia *on-line* z organem administracyjnym[30]. Art. 63 § 1 k.p.a. w obecnym kształcie umożliwia przy tym już, zgodnie z zasadą ograniczonego formalizmu tego etapu procedury, wnoszenie podań zarówno za pomocą (zwykłej) poczty elektronicznej, jak i dalekopisu czy telefaksu[31].

Gdyby zatem nie kolejna zmiana art. 63 k.p.a., powstałoby stosunkowo elastyczne rozwiązanie, dobrze wpisane w rozpowszechniającą się praktykę elektronicznego wypełniania formularzy udostępnianych przez organy administracji publicznej. Tak jednak się nie stało,

---

[28] Ustawa z 14.6.1960 r. Kodeks postępowania administracyjnego, Dz.U. 2000, Nr 98, poz. 1071 z późn. zm.

[29] Zgodnie z art. 64 pkt 2 PPIU przepis ten ma wejść w życie po upływie 7 miesięcy od dnia ogłoszenia ustawy.

[30] Art. 36 pkt 5 lit. a zmieniający art. 63 § 1 k.p.a.

[31] Lepszym co prawda wyjściem od dodania nowego sposobu wnoszenie podań byłoby raczej zastąpienie określenia odnoszącego się do poczty elektronicznej szerszym pojęciem „postaci elektronicznej". Jest ono bardziej elastyczne, obejmując jednocześnie swoim zakresem zarówno pocztę elektroniczną, jak i komunikację *on-line*. Łatwiej sprostać może wymogom zmian technologicznych, będąc rozwiązaniem neutralnym technologicznie. Otwiera zatem możliwość korzystania z nowych protokołów komunikacji, które powstać mogą na przykład na bazie telefonii UMTS.

ze względu na wprowadzenie do art. 63 k.p.a. nowego § 3a (na mocy art. 36 pkt 5 lit. b PPIU)[32]. Stanowi on „podanie wniesione w formie dokumentu elektronicznego[33] powinno być opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, przy zachowaniu zasad przewidzianych w przepisach o podpisie elektronicznym"[34].

Tym samym prawodawca wymaga uwierzytelnienia podania wnoszonego elektronicznie przy użyciu rozwiązania, które jest, ze względów organizacyjno-prawnych, najbardziej kosztowne, przynajmniej w kształcie przyjętym w EPU[35]. Zignorowane zostały w ten sposób wnioski z powszechnej praktyki, bazującej na rozwiązaniach najprostszych. Zrezygnowano też ze stopniowania bezpieczeństwa systemu zabezpieczeń w zależności od wagi czynności prawnej.

Wprowadzając omawianą poprawkę prawodawca uznał, że technologia informacyjna służyć ma nie tyle łatwiejszemu i tańszemu kontaktowi z urzędem, co zagwarantowaniu wiarygodności podpisu składanego przez interesanta[36]. Przedstawione rozwiązanie legislacyjne

---

[32] Dodany do tekstu PPIU niejako na finiszu prac w Sejmie – drukiem nr 3456 z 17.11.2004 r.

[33] Zgodnie z art. 3 pkt 2 PPIU dokumentem elektronicznym ma być stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych. Co ciekawe, informatycznym nośnikiem danych jest także materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci analogowej (art. 3 pkt 1), co krytykowane było podczas prac w komisji sejmowej – por. wystąpienie posła T. Jarmuziewicza podczas czytania projektu PPIU na 96 posiedzeniu Sejmu 19.1.2005 r.

[34] Druga część tego przepisu stanowi, iż na podanie składać się mają „dane w ustalonym formacie, zawarte we wzorze podania określonym w odrębnych przepisach, jeżeli te przepisy nakazują wnoszenie podań według określonego wzoru". Zwróćmy uwagę, iż delegacja tego rodzaju, odmiennie do tej, jaka wynika z art. 58 ust. 3 EPU i omówiona została nieco wcześniej, dotyczy standaryzacji w podstawowym zakresie (format danych), abstrahując od dalej idących wymogów (całość warunków technicznych i bezpieczeństwa). Wydaje się, iż, odstępując od tendencji do omnipotencji regulacyjnej, legislator stworzył w ten sposób warunki bardziej sprzyjające skutecznemu unormowaniu kwestii najistotniejszych.

[35] Nieprzypadkowo art. 47a ustawy z 13.10.1998 r. o systemie ubezpieczeń społecznych (Dz.U. 1998, Nr 137, poz. 887), ma, na mocy art. 40 pkt 5c PPIU, zostać znowelizowany tak, by (po bardzo co prawda długim *vacatio legis*, wynoszącym w tym przypadku 39 miesięcy – por. art. 60 w zw. z art. 64 pkt 3 PPIU) wprowadzić obowiązek sygnowania podpisami kwalifikowanymi dokumentów przekazywanych ZUS przez płatników, w miejsce obowiązujących dziś podpisów powszechnych.

[36] Nadaje się tym samym bardzo restrykcyjne znaczenie poglądom doktryny, iż „podanie może być wnoszone przez stronę z wykorzystaniem tylko tych środków łączności, które pozwalają stwierdzić, że wnosi je określona osoba i jest możliwe stwierdzenie autentyczności jej żądania" – B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2000, s. 284.

oznacza, iż w przypadku komunikacji bazującej na technologii internetowej wymaga się uwiarygodnienia nadawcy nie tylko nieporównywalnie dalej idącego niż w przypadku telefaksu (który jest uznanym przez art. 63 § 1 k.p.a. środkiem wnoszenia podań), lecz nawet w porównaniu z podpisem własnoręcznym. Logika promowania rozwiązania wystarczająco bezpiecznego ustąpiła zatem logice przymuszenia do korzystania z rozwiązania najbardziej bezpiecznego (i najbardziej kosztownego) ze wszystkich.

Wobec przedstawionej zmiany drugorzędne znaczenie mają inne modyfikacje k.p.a., wynikające z PPIU. Mimo wszystko warto im poświęcić kilka zdań.

PPIU wprowadza możliwość doręczania pism organu administracji publicznej[37] również za pośrednictwem środków komunikacji elektronicznej[38], jeśli strona[39] o takie doręczenie wystąpiła lub wyraziła na nie zgodę[40]. Podkreślmy – doręczenie elektroniczne jest dopuszczalne, nie zaś obowiązkowe. Organ administracyjny ma zatem możliwość odmówić wnioskowi strony, zwłaszcza jeśli nie posiadałby wystarczających środków technicznych aby mu zadośćuczynić[41]. Rozwiązanie takie trudno nazwać optymalnym z punktu widzenia dynamiki procedury, wydaje się jednak być jedynym możliwym do zrealizowania w praktyce.

Kolejną zmianę w k.p.a., proponowaną w projekcie PPIU, stanowi wymaganie, w przypadku elektronicznego[42] doręczenia, by organ

---

[37] „Pismem będzie wezwanie, zawiadomienie, protokół, każdy inny dokument, jak również sporządzona na piśmie decyzja czy jej odpis, odpis ugody, postanowienie"- B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2000, s. 284.

[38] Zgodnie z art. 2 pkt 5 ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204 z późn. zm.) – dalej: EDUU, do której w tej mierze odsyła PPIU, środki komunikacji elektronicznej to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności poczta elektroniczna.

[39] O ile racjonalnym wydaje się wyłączenie z kręgu osób, którym pisma doręczane mogą być elektronicznie, świadków, osób posiadających przedmiot oględzin lub tych, które trzeba zawiadomić o rozprawie administracyjnej (ponieważ mogą się one nie spodziewać otrzymania pisma tą drogą), to nie można tego samego powiedzieć o wyłączeniu owego sposobu dokonywania doręczeń pism przeznaczonych dla przedstawicieli stron, ich pełnomocników albo biegłych.

[40] Nowy art. 39^1 k.p.a., ustanowiony przez art. 36 pkt 1 PPIU.

[41] Niepożądana byłaby natomiast rozszerzająca interpretacja dopuszczalności nie czynienia zadość wnioskowi strony z innych powodów. PPIU nie przewiduje jednak żadnych mechanizmów eliminujących ową ewentualność.

[42] W istocie PPIU, podążając za terminologią EDUU, określa je mianem doręczenia za pomocą środków komunikacji elektronicznej.

administracji publicznej, dla skuteczności takiego doręczenia, uzyskał, w ciągu 7 dni od daty wysłania pisma, jego potwierdzenie[43].

Odnosząc się do owego przepisu zauważyć należy najpierw, iż korespondencja elektroniczna umieszczana jest na serwerze pocztowym, do którego dostęp ma użytkownik Internetu. Później dopiero przeniesiona może zostać przez jej adresata na urządzenie końcowe (np. komputer osobisty) przy pomocy stosownego oprogramowania (klienta pocztowego). Do rozstrzygnięcia pozostaje zatem to, kiedy następuje doręczenie (a zatem co ma zostać potwierdzone) – w chwili znalezienia się dokumentu na serwerze pocztowym, czy w urządzeniu końcowym. Wydaje się, iż właściwym jest pierwsze rozwiązanie. Strona ma przecież świadomość, iż pisma mogą jej być doręczane elektronicznie, skoro się na taką formułę doręczenia zgodziła. Powinna zatem liczyć się z koniecznością monitorowania swojego konta pocztowego (zawartości serwera). Za rozwiązaniem takim przemawia również to, iż przeglądanie poczty elektronicznej możliwe jest bezpośrednio w Internecie, bez konieczności jej przenoszenia na urządzenie końcowe. Poza tym, przy sytuacji odwrotnej do omawianej, tj. przy elektronicznym składaniu podań przez interesantów, datę doręczenia stanowi „dzień wprowadzenia żądania do systemu teleinformatycznego[44] organu administracji publicznej"[45]. Powinno być to równoznaczne z dotarciem korespondencji na odpowiedni serwer wewnątrz urzędu, choć niekoniecznie do odpowiedzialnego urzędnika. W komunikacji zwrotnej przyjęty powinien zatem zostać model analogiczny.

Z przedstawionych uwag wynika, iż faktem, który ma zostać potwierdzony, jest dostarczenie pisma w postaci elektronicznej do systemu teleinformatycznego odbiorcy. Zbyt daleko idącym byłoby zatem utożsamianie potwierdzenia tak rozumianego doręczenia z potwierdze-

[43] Nowy art. 46 § 3 k.p.a., ustanowiony przez art. 36 pkt 2 PPIU.

[44] Zgodnie z art. 2 pkt 3 EDUU, do której w tej mierze odwołuje art. 3 pkt 3 PPU, systemem teleinformatycznym jest „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego".

[45] Nowy art. 61 § 3a k.p.a., ustanowiony przez art. 36 pkt 4 PPIU. Wydaje się, iż bardziej racjonalnym byłoby uzupełnienie owej normy, na wzór art. 61 § 2 ustawy z 23.4.1964 r. kodeks cywilny (Dz.U. 1964, Nr 16, poz. 93 z późn. zm.), o stwierdzenie: „w taki sposób, żeby organ ten mógł zapoznać się z jego treścią". Nie można bowiem zupełnie wykluczyć niebezpieczeństwa awarii serwera pocztowego już po chwili, gdy znalazła się na nim wiadomość, ale zanim adresat się z nią zapoznał. Wówczas, według proponowanej regulacji, podanie zostałoby doręczone, pomimo iż adresat nie miał możliwości się z nim zapoznać. To natomiast odbiega od modelu wynikającego z zaakceptowanej przez prawodawcę w k.p.a. teorii doręczenia.

niem otwarcia korespondencji elektronicznej. To drugie odpowiada bowiem potwierdzeniu zapoznania się z dokumentem, nie zaś jego doręczenia. A przypomnijmy – prawodawca wymaga jedynie potwierdzenia doręczenia, zgodnie z modelem utrwalonym we wszystkich rodzajach polskich procedur prawnych.

Prostsze rozwiązanie, nie dające jednak pewności co do tego, iż korespondencja elektroniczna dotarła do adresata, proponowali autorzy pierwotnej wersji PPIU[46]. Optowali oni za następującą zmiana brzmienia art. 46 § 3 k.p.a.: „w przypadku doręczenia pisma za pomocą środków komunikacji elektronicznej, doręczenie jest skuteczne, jeżeli w terminie 2 dni od dnia wysłania pisma organ administracji publicznej nie otrzyma informacji o błędzie w doręczeniu pisma, nie wynikającym z działania systemu teleinformatycznego używanego przez ten organ". Komisja Nadzwyczajna do rozpatrzenia omawianej ustawy dokonała jednak zmiany na brzmienie aktualne jeszcze w trakcie prac poprzedzających drugie czytanie w Sejmie[47]. Zacytowane rozwiązanie byłoby bowiem co prawda najprostszym i najmniej kłopotliwym do wdrożenia, jednocześnie jednak dawałoby najmniejszą pewność, że pismo doszło do adresata. W szczególności, doręczenie, w sensie prawnym lecz nie faktycznym, mogłoby mieć miejsce w przypadku wadliwie skonfigurowanego systemu pocztowego, gdzie wiadomości zostałyby usunięte[48] lub nie dostarczane przez protokół obsługi poczty elektronicznej.

Potwierdzenie doręczenia ma także decydujące znaczenie dla określenia, kiedy pismo trafiło do adresata. Z zasady, co prawda, w środowisku komunikacji elektronicznej doręczenie korespondencji następuje zazwyczaj niemal natychmiast po jej wysłaniu albo nie następuje w ogóle. Nie można jednak całkowicie wykluczyć sytuacji odmiennej.

Uwaga ta ma znaczenie dla interesów strony wówczas, gdy doręczenie jest początkiem terminu na dokonanie innej czynności procesowej. Nie odnosi się natomiast do sytuacji, gdy to (elektroniczne) złożenie pisma stanowi czynność procesową, która dokonana ma zostać w określonym terminie. Aby dostosować reguły procedury administracyjnej do tego przypadku, art. 36 pkt 3 PPIU modyfikuje art. 57 § 5 k.p.a. Na mocy owej nowelizacji na pisma wysłane w formie dokumen-

---

[46] Pierwotny projekt ustawy o informatyzacji działalności niektórych podmiotów realizujących zadania publiczne, przedłożony przez Radę Ministrów 26.8.2003 r., druk nr 1934, art. 31 ust. 2.

[47] Por. jej sprawozdanie z 4.3.2004 r., druk nr 2452, brzmienie art. 34 pkt 2.

[48] Omyłkowe usunięcie mogłoby mieć miejsce choćby poprzez zbyt restrykcyjne stosowanie oprogramowania antyspamowego.

tu elektronicznego rozciągnięto ogólnie obowiązującą w tym zakresie zasadę, zgodnie z którą do dochowania terminu wystarczy wysłanie pisma w terminie (nie jest więc konieczne, by doszło ono w tym czasie do adresata)[49].

4. Podsumowanie

Przedstawiona analiza uzmysławia, iż prawodawca coraz wyraźniej zauważa potencjał, jaki dla relacji urząd – obywatel ma technologia informacyjna[50]. Sposób, w jaki decyduje się wyjść naprzeciw związanym z tym wyzwaniom charakteryzuje jednak wciąż fragmentaryczność, mała spójność i brak konsekwencji[51]. Przede wszystkim wyraźne jest jednak preferowanie nie tych rozwiązań, które będą najbardziej ekonomiczne, zwiększając efektywność działania administracji

[49] Dodatkowe postanowienie wskazanego przepisu, zgodnie z którym dla dochowania terminu konieczne jest uzyskanie poświadczenia przedłożenia pisma do organu administracji publicznej, rozumieć należy zatem jako statuujące obowiązek po stronie urzędu, nie zaś wnoszącego pismo.

[50] Por. np. plany budowy Elektronicznej Platformy Usług Administracji Publicznej (e-PUAP), które stanowią część koncepcji „Wrota Polski". Bliższe informacje na temat obydwu tych dokumentów uzyskać można z http://www.mnii.gov.pl. Na poziomie normatywnym por. natomiast np. § 5 rozporządzenia Rady Ministrów z 8.1.2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków, (Dz.U. 2002, Nr 5, poz. 46), które stanowi, że „skargi i wnioski mogą być wnoszone pisemnie, telegraficznie lub za pomocą dalekopisu, telefaksu, poczty elektronicznej, a także ustnie do protokołu". Poczta elektroniczna uznawana jest także za środek komunikacji równy innym w instrukcjach kancelaryjnych obowiązujących organy władzy publicznej – por. np. § 5, 11 i 32 rozporządzenia Prezesa Rady Ministrów z 18.12.1998 r. w sprawie instrukcji kancelaryjnej dla organów samorządu województwa (Dz.U. 1998, Nr 160, poz. 1073 z późn. zm.), rozporządzenia Prezesa Rady Ministrów z 18.12.1998 r. w sprawie instrukcji kancelaryjnej dla organów powiatu (Dz.U. 1998, Nr 160, poz. 1074 z późn. zm.) i rozporządzenia Prezesa Rady Ministrów z 22.12.1999 r. w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych (Dz.U. 1999, Nr 112, poz. 1319 z późn. zm.) lub § 4, 10 i 31 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 18.12.1998 r. w sprawie instrukcji kancelaryjnej dla zespolonej administracji rządowej w województwie (Dz.U. 1998, Nr 161, poz. 1109 z późn. zm.).

[51] Czego dowodem może być brzmienie § 54 ust. 5 powołanego w przyp. poprz. rozporządzenia w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych. Stanowi on: „korzystanie z dostępu do światowych sieci informatycznych (typu Internet) jest możliwe wyłącznie w wydzielonych i nie podłączonych do wewnętrznej sieci informatycznej urzędu stanowiskach komputerowych". Identyczny zapis znajduje się we wszystkich instrukcji wskazanych w przyp. poprz. (w ostatnim przypadku – w § 48 ust. 5, we wcześniejszych – w § 54 ust. 5).

i redukując koszty związane z załatwianiem spraw urzędowych, lecz tych, na których wzbogacić się mogą, choćby potencjalnie, podmioty pośredniczące.

Mechanizm ten szczególnie zauważalny jest przy kwestii fundamentalnej – autoryzacji, podpisywania pism wymienianych w trakcie postępowania.

Oprócz PPIU, kwalifikowany podpis elektroniczny jest rozwiązaniem wyraźnie preferowanym również na gruncie aktów stanowiących *lex specialis* wobec k.p.a.[52] Szczególnie zastanawiające jest jednak to, że poprawka do PPIU dotycząca obowiązku opatrywania podań wnoszonych w formie dokumentu elektronicznego kwalifikowanym podpisem elektronicznym zgłoszona została niemal w tym samym czasie, gdy zlikwidowany został, głównie ze względów ekonomicznych, centralny element infrastruktury klucza publicznego – tzw. root[53] – powstały na mocy EPU. Nie jest również jasne, czy koncepcja infrastruktury klucza publicznego oparta o normę ISO X.509 – w istocie realizowanego przez normy prawne w państwach Unii Europejskiej – ma w ogóle szansę sukcesu. Coraz bardziej słyszalne są głosy, iż „doświadczenia europejskie każą wątpić, czy koncepcja certyfikatów kwalifikowanych ma szansę praktycznej realizacji"[54].

Logicznie nasuwającym się wnioskiem jest, że zadekretowanie konieczności stosowania owej technologii w komunikacji pomiędzy obywatelem a urzędem stanowi próbę uratowania rynku kwalifikowanego podpisu elektronicznego. Innymi słowy, to popyt na technologię informacyjną dostosować się ma do preferowanej podaży. Tego rodzaju gra jest nader ryzykowna i przynieść może skutek odwrotny do zamierzonego – pogłębić nieefektywność zarządzania funduszami publicznymi (jeśli komunikacja nie będzie oparta na technologii najbardziej efektywnej, lecz na jedynej dopuszczalnej prawnie) lub zniechęcić do stosowania nowoczesnych metod komunikacji (jeśli jedyne dopuszczalne rozwiązanie uznane zostanie przez potencjalnych użytkowników za zbyt drogie). Próby takie są jednocześnie najbardziej zabójcze dla samych podmiotów świadczących usługi certyfikacyjne. Zade-

---

[52] Dla przykładu, art. 82 ust. 2 ustawy z 29.1.2004 r. – prawo zamówień publicznych (Dz.U. 2004, Nr 177, poz. 19 z późn. zm.) postanawia „ofertę składa się, pod rygorem nieważności, w formie pisemnej albo, za zgodą zamawiającego, w postaci elektronicznej, opatrzoną bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu".

[53] Szerzej por. P. Gamdzyk, *Root e-podpisu w NBP*, „Computerworld", 18.1.2005 r., s. 11; *Rynek odrzuca kwalifikowany e-podpis*, „Teleinfo", 24.1.2005 r., s. 10.

[54] P. Gamdzyk, *Czekanie na e-podpis*, „Computerworld", 30.11.2004 r., s. 9.

kretowanie korzystania wyłącznie z najdroższych rozwiązań spowoduje zapewne budowę złożonej infrastruktury po stronie urzędów, zaś obywatele, z przyczyn ekonomicznych, komunikować się będą z urzędem w sposób tradycyjny.

Uwagi te dotyczą zresztą korzystania, przez organy władzy publicznej, ze wszelkich usług certyfikacyjnych świadczonych przez przedsiębiorstwa prywatne. ZUS, stosujący takie właśnie rozwiązanie, wydaje rokrocznie ok. 8 mln zł na usługi certyfikacji powszechnych podpisów elektronicznych składanych przez płatników składek[55].

Wydaje się więc, że stosowanie bezpiecznego podpisu elektronicznego i budowanie pewności w elektronicznym obiegu informacji między urzędem a obywatelem ulegnie dalszemu zahamowaniu. Powtórzone zostają błędy popełnione we wdrażaniu infrastruktury klucza publicznego w Polsce na potrzeby handlu elektronicznego[56].

Z drugiej strony, praktyka funkcjonowania komunikacji elektronicznej w sektorze bankowym wskazuje, że możliwe są proste, tanie i stosunkowo niezawodne rozwiązania, proporcjonalne do zamierzonych celów[57].

Nie oznacza to jednak, że prawo dopuścić powinno możliwość stosowania tylko takich rozwiązań. W sferze nowych technologii (i nie tylko) jego rolą jest określenie elastycznych i prostych ram, umożliwiających rozwój i udoskonalanie istniejących rozwiązań. Najbardziej temu modelowi odpowiadałoby uzupełnienie art. 14 § 1 k.p.a., który stanowi: „sprawy należy załatwiać w formie pisemnej", o określenie „lub w postaci elektronicznej"[58] i dodanie normy tworzącej mechanizm w sposób ogólny gwarantujący stosowny standard bezpieczeństwa[59]. Odpowia-

---

[55] Za J. Ochab, *Ważna zmiana w ustawie o informatyzacji*, „Computerworld", 20.1.2005 r., cytującym uzasadnienie jednej z poprawek zgłoszonych w trakcie prac nad ustawą.

[56] Jednym z takich błędów w implementacji infrastruktury klucza publicznego było powstanie centralnego roota, którego działalność pochłonęła kilkadziesiąt milionów złotych ze środków NBP, zaś funkcjonalność ograniczyła się do wydania zaświadczeń certyfikacyjnych czterem kwalifikowanym podmiotom świadczącym usługi certyfikacyjne.

[57] Niemniej jednak, wobec szybkiego rozwoju bankowości elektronicznej, dostrzec należy nieuchronność stosowania bezpiecznego podpisu elektronicznego w szeregu sytuacji, zwłaszcza w rozliczeniach międzybankowych.

[58] Rozwiązanie takie bazowałoby na art. 7 ust. 1 ustawy z 29.8.1997 r. prawo bankowe (Dz.U. 2002, Nr 72, poz. 665 z późn. zm.). Przepis ten stanowi: „Oświadczenia woli związane z dokonywaniem czynności bankowych mogą być składane w postaci elektronicznej".

[59] Np. bazując na art. 7 ust. 2 prawa bankowego, powołanego w przyp. 58, zgodnie z którym „dokumenty związane z czynnościami bankowymi mogą być sporządzane na

dałoby to jednemu z aksjomatów prawidłowo działającego systemu prawa, bardzo trafnie uchwyconemu przez jednego z najlepiej zaznajomionych z tematyką podpisu elektronicznego prawników europejskich, prof. J. Dumortier. Stwierdził on: „tu nie trzeba fundamentalizmu, lecz pragmatyki. W niektórych państwach prawo regulujące te kwestie jest tak ścisłe, że nie pozostawia żadnego pola manewru, żadnego wyboru. Tymczasem zgodnie z regułami sztuki prawo powinno być tak elastyczne i tak proste, jak to tylko możliwe"[60].

Najgorsze jest natomiast w omawianym obszarze (i nie tylko) prawo kazuistyczne, nakładający na dynamicznie się rozwijającą sferę zbyt opięty kaganiec regulacyjny[61]. Niestety, prawem takim jest obecnie EPU i rozporządzenia wydane do tej ustawy. Rozwiązania takie, dekretując konieczność korzystania z konkretnych rozwiązań technologicznych, na drugi plan spychają potrzeby ich odbiorców i interes publiczny.

---

elektronicznych nośnikach informacji, jeżeli dokumenty te będą w sposób należyty utworzone, utrwalone, przekazane, przechowywane i zabezpieczone. Usługi związane z zabezpieczeniem tych dokumentów mogą być wykonywane przez banki, spółki tworzone przez banki z innymi podmiotami, a także przedsiębiorstwa pomocniczych usług bankowych". Bardziej szczegółowo kwestię tę reguluje, wydane na podstawie art. 7 ust. 4 prawa bankowego, rozporządzenie Rady Ministrów z 26.10.2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji (Dz.U. 2004, Nr 236, poz. 2364).

[60] Wywiad zamieszczony w „Computerworld", 15.6.2004 r., s. 12–13.

[61] Zupełnym nieporozumieniem wydają się opinie takie, jak prezentowana przez (byłego już) prezesa firmy Centrast: „rynek podpisu elektronicznego musi bowiem być doregulowany, tak aby ścisłe rozwiązania legislacyjne pozwoliły na zbudowanie jednolitego, stabilnego rynku" – za P. Gamdzyk, *Po co nam podpis*, „Computerworld", 15.6.2004 r., s. 12. Co ciekawe, Centrast, pełniący kluczową rolę w budowie infrastruktury dla kwalifikowanego podpisu elektronicznego, został zlikwidowany na początku 2005 r.