Rejent * rok 11 * nr 11(127)
listopad 2001 r.

Jerzy Jacyszyn
Sebastian Zakrzewski

Podpis elektroniczny jako element systemu zabezpieczenia danych w sieci (część druga)*

I. Podpis cyfrowy a podpis własnoręczny

Aspekt prawny

W związku z rozwojem na szeroką skalę technologii informatycznej pojawia się pytanie o relację podpisu własnoręcznego do podpisu elektronicznego, a ściślej rzecz biorąc, o stosunek oświadczenia woli złożonego na nośnikach elektronicznych do wymogu zachowania formy pisemnej. W doktrynie krajowej[1] pojawiają pytania, czy oświadczenie woli złożone na nośniku elektronicznym różni się od dotychczasowych oświadczeń składanych za pomocą tradycyjnych środków przekazu, a jeżeli tak, to na czym te odmienności polegają. Na ogół jednak panuje przekonanie, że skoro art. 60 k.c. traktuje oświadczenie woli jako każde zachowanie osoby, z którego wynika zamiar przejawienia woli i wywołania określonych skutków prawnych, to nie ma przeszkód, by „elektroniczne" oświadczenia woli traktować inaczej czy też specjalnie i wydzielać im odrębne miejsce w regulacjach prawnych. Zasada ta może doznawać pewnych wyłączeń i ograniczeń, zwłaszcza wtedy, gdy w grę wchodzę czynności prawne dokonywane z udziałem notariusza. Dostrzegają taką potrzebę regulacje unijne, które

---

* Część pierwsza artykułu została opublikowana w: Rejent 2001, nr 10, s. 40-54.

[1] Zob. np. W. K o c o t, *Elektroniczna forma oświadczeń woli*, Przegląd Prawa Handlowego 2001, nr 3, s. 2 i nast.

dopuszczają wyłączenie spod działania tej reguły czynności, które dla swej ważności wymagają udziału notariusza bądź zarejestrowania przez właściwy organ, a także czynności dokonywane stosownie do norm prawa rodzinnego i spadkowego.

Z powodu niezachowania warunku własnoręczności odmawia się waloru prawnego, jeśli chodzi o dochowanie wymogów formy pisemnej, zarówno podpisowi sporządzonemu na maszynie, jak i nanoszonemu na papier metodą fotograficzną, drukarską lub inną, tzw. faksymile, odtwarzającemu podpis określonej osoby; podobnie traktuje się podpis na oświadczeniu przesłanym telefaksem, dalekopisem, radiogramem. Uwzględniając to, trzeba także przyjąć, iż przymiotu „własnoręcznego podpisu" nie posiada wpisane w dowolnym edytorze na nośnik informacji imię i nazwisko określonej osoby.

W związku z coraz powszechniejszym wykorzystywaniem w obrocie dokumentów elektronicznych proponowane są różne rozwiązania jurydyczne, które mają stworzyć nowe podstawy prawne dla oświadczeń woli składanych na elektronicznych nośnikach elektronicznych, a także pozwolą wmontować podpis elektroniczny do instrumentów prawnych równoważących znaczenie i charakter podpisu własnoręcznego.

Komisja kodyfikacyjna prawa cywilnego przekazała do opublikowania projekt zmian w kodeksie cywilnym w połowie 2000 r. Obejmuje on m.in. kwestie elektronicznych czynności prawnych – dopuszczono składanie oświadczenia woli na elektronicznym nośniku informatycznym, przewidziano również składanie ofert na elektronicznym nośniku informatycznym, ale z zastrzeżeniem, że oferta taka powinna zawierać dodatkowe informacje, określające zrozumiale i dokładnie procedurę zawarcia umowy oraz metody korygowania błędów powstałych w trakcie transmisji danych. Natomiast w stosunkach między przedsiębiorcami strony mogą ustalić inne wymagania lub z nich zrezygnować.

Warunek formy pisemnej będzie również spełniony przez posłużenie się podpisem elektronicznym zamiast własnoręcznego. Zachowanie formy pisemnej nastąpi wiec także przez złożenie oświadczenia woli na elektronicznym nośniku informatycznym, jeśli zostanie ono należycie utrwalone i zabezpieczone, a dane dołączone lub powiązane w odpowiedni sposób z podpisem elektronicznym. W tej sytuacji wydaje się, że dzieli nas tylko

krok od wprowadzenia elektronicznych nośników informatycznych oraz podpisów elektronicznych do obrotu prawnego i gospodarczego, w tym także do praktyki notarialnej. Zbliżająca się dekada „podpisów elektronicznych" staje się faktem, coraz więcej grup zawodowych, w tym prawniczych[2], podejmuje edukację w tym zakresie, stara się przygotować do stosowania podpisów elektronicznych, a także Internetu oraz innych nowych technik komunikowania się na odległość w swojej codziennej pracy.

Różnice w stosowaniu podpisów zwykłych i cyfrowych

Pojęcie **„podpis"** jest rozumiane przez nas intuicyjnie. Rozumiemy przez nie nakreślony przez człowieka, najczęściej na papierze przy użyciu środka pisarskiego, jego znak identyfikacyjny, który przeważnie odzwierciedla imię i nazwisko podpisującego. Podpis składany na dokumencie ma na celu wskazanie, że dokument należy do osoby podpisującej, że osoba podpisująca sporządziła ten dokument lub że zgadza się ona z treścią dokumentu. Ponadto podpis może być wykorzystany także jako element bezpośredniej identyfikacji danej osoby, przez porównanie jej podpisu z wcześniej ustalonym wzorcem.

Identyfikacja jest pojęciem szczególnie bliskim nauce kryminalistyki. Identyfikacja kryminalistyczna realizuje funkcje: rozpoznawczą, wykrywczą, dowodową i zapobiegawczą na potrzeby takich dziedzin, jak proces karny, czynności operacyjno-rozpoznawcze, opiniowanie i sporządzanie ekspertyz sądowych, niemniej jednak sposób rozumienia tego pojęcia ma walor uniwersalizmu. Celem identyfikacji jest ustalenie tożsamości indywidualnej lub grupowej.

Ponieważ przedmiotem naszych zainteresowań jest identyfikacja człowieka, będziemy mówić o identyfikacji indywidualnej, polegającej na wydaniu sądu, w którym stwierdzamy, że określony przedmiot, w tym wypadku podpis, posiada takie same cechy, jak przedmioty należące do określonej grupy (podpisy sporządzone przez tę samą osobę) i dlatego może być do tej grupy zaliczony[3]. Identyfikując jakiś przedmiot, należy dokonać porównania przedmiotu z innym przedmiotem bądź wzorcem. Z powyższe-

---

[2] W dniach 27-28 października 2000 r. odbyło się I Forum Radców Prawnych „Prawo a Internet", w którym wzięło udział około 300 osób, co świadczy o dużym zainteresowaniu omawianą problematyką. Szerzej na ten temat: Radca Prawny 2001, nr 1, s. 4 i nast.

[3] T. H a n a u s e k, *Kryminalistyka. Zarys wykładu*, Kraków 2000, s. 45.

go wynika, że identyfikacja jest pewnym procesem badawczym, który jest prowadzony według przyjętej efektywnej metody.

W fakcie, że do tej pory podpis był rozumiany intuicyjnie i jednoznacznie, należy upatrywać przyczyny, iż przepisy prawa nigdzie nie definiują pojęcia **podpisu**, mimo że wiele aktów prawnych się nim posługuje (kodeks cywilny, kodeks spółek handlowych, kodeks postępowania cywilnego). Najszerzej stanowi o podpisie prawo czekowe i wekslowe, które zawiera specyfikację cech dokumentu uznawanego za czek. Wśród nich wyróżnia **podpis wystawcy czeku**, stanowiąc, że musi być złożony własnoręcznie pod tekstem dokumentu. Nie musi być to podpis kaligraficzny, może być ograniczony do nazwiska wystawcy czeku. Jeżeli przyjmiemy, że podstawową funkcją podpisu jest umożliwienie identyfikacji określonej osoby, to musi on zawierać cechy, które go indywidualizują i pozwalają na jednoznaczne powiązanie go z osobą, która podpis złożyła. Wymaga to przyjęcia określonej techniki składania podpisu. Do niedawna uznawano, że własnoręczność podpisu jest najlepszym gwarantem prawdziwości oświadczenia skierowanego do innego podmiotu. Było to podyktowane także tym, że podstawowym środkiem utrwalania oświadczeń woli oraz sporządzania i przechowywania innych dokumentów był papier. Dzisiaj sytuacja nie jest już tak oczywista. Istnieje wiele technik uwierzytelniania odpowiadających przesłankom poprawnej identyfikacji (pozwalają na identyfikację, uniemożliwiają złożenie takiego podpisu przez inną osobę, podpis nie może być przeniesiony na inny dokument). Wśród nich wskazać należy techniczne metody biometrycznej identyfikacji, które są sposobami jednoznacznego rozpoznawania osób na podstawie ich cech biologicznych lub zachowań. Kwalifikuje się do nich także rozpoznawanie pisma ręcznego, w tym podpisów. Zaliczane jest ono do grupy metod dynamicznych, obok których wyróżnić można statyczne, jak identyfikacja odcisków palców czy siatkówki lub rogówki oka, oraz multimodalne, stanowiące efekt połączenia metod statycznych z dynamicznymi[4].

Ze względu na powyższe może pojawić się pytanie, który ze znanych sposobów identyfikacji może być wykorzystywany do sygnowania dokumentów. Jak do tej pory, kwestia ta pozostawiona jest obowiązującej kon-

[4] M. D e m b e c k, *Pożegnanie z hasłem i PIN. Teraźniejszość i przyszłość biometrycznych systemów identyfikacji,* Problemy Kryminalistyki 2000, nr 230, s. 66 i nast.

wencji, zaś ustawa o podpisie cyfrowym, niezależnie od tego, jaki przybierze ostateczny kształt, może stać się pierwszym aktem prawnym, który określi w sposób precyzyjny kryteria, jakim musi odpowiadać podpis używany w obrocie prawnym. Przy tej okazji można wskazać pewną różnicę, jaka zarysowuje się w podejściu do podpisu, widoczną w naukach penalnych. Dla kryminalistyki element woli składającego podpis jest bez znaczenia. Podpis jest zaliczany do kategorii śladów kryminalistycznych, która jest zdefiniowana bardzo szeroko – **śladami są wszelkie dające się ustalić w określonym wycinku rzeczywistości następstwa tych zmian, których zespół albo tworzy jakieś zdarzenie, albo jest z tym zdarzeniem ściśle powiązany**[5]. Są one następstwami jakichś zachowań, z którymi wykazują związki przyczynowo skutkowe i mają charakter materialny, a co za tym idzie, są możliwe do zbadania.

W prawie cywilnym akcentuje się, że podpis jest przede wszystkim sposobem uzewnętrznienia woli wewnętrznej. Tym samym jest dowodem złożenia oświadczenia woli, nierzadko stanowiącym jedyny jej przejaw. Dlatego też duży nacisk kładzie się na rozróżnienie, co jest podpisem, a co nim nie jest. Ze względu na to, jak poważne skutki może rodzić złożenie podpisu w sferze stosunków prawnych, duże znaczenie ma rytualność tej czynności, która podkreśla jej doniosłość i zmusza do przemyślenia zasadności samej czynności. Zwraca się uwagę, iż nierzadko elementów tych brak w transakcjach elektronicznych, w których uzewnętrznienie woli następuje przez naciśnięcie przycisku „myszy".

Psychofizjologia pisma

Często można spotkać się z twierdzeniem, że podpisy cyfrowe gwarantują dużo wyższy poziom bezpieczeństwa niż podpisy tradycyjne. Należy zastanowić się, czy jest tak w istocie. Jedynym stałym elementem sankcjonującym podpis jest jego własnoręczność. Dzięki tej właściwości podpisu, przy zastosowaniu zaawansowanych technik analizy pisma możliwe jest ustalenie tożsamości podpisującego. Prześledźmy pokrótce ten żmudny i skomplikowany proces. Pierwszą metodą badań pisma ręcznego była metoda grafologiczna, której największą zasługą było poczynienie spostrzeżenia, że cechy psychofizyczne człowieka znajdują odzwierciedlenie w jego piśmie. Rozwój procesu pisania u osób fizycznych łączy się z rozwojem

[5] T. H a n a u s e k, *op. cit*., s. 88.

ontogenetycznym, a więc z dojrzewaniem fizycznym i psychicznym. Pismo jako rodzaj mowy (zewnętrznej) związane jest ściśle z funkcjami centralnego układu nerwowego, w szczególności z określonymi funkcjami mózgu. Obecność określonych ośrodków sensorycznych i motorycznych w mózgu, umożliwiających mówienie i pisanie, nie oznacza, że zdolności te pojawiają się niejako automatycznie w procesie rozwoju. Wręcz przeciwnie, wymagają one określonego procesu, podczas którego następuje nauka prawidłowego mówienia i pisania, rozumowania, a nawet formalnego słuchania mowy innych. Obok omówionych czynników psychicznych o zdolności pisania decydują ponadto czynniki fizjologiczne związane z budową układu kostno-mięśniowego, głównie przedramienia, dłoni i palców. Czynniki te są wysoce indywidualne u każdego człowieka. Kolejnymi czynnikami indywidualizującymi pismo są: częstotliwość pisania oraz wpływy środowiska. Najbardziej typowe cechy pisma każdego człowieka ujawniają się w formie, jaką jest podpis. W formowaniu się podpisu znaczną rolę odgrywają nawyki techniczne, graficzne i ortograficzne. Proces kształtowania się podpisu przebiega szybciej niż powstawanie stałych cech pisma. Podpis pozostaje także najdłużej ze wszystkich zdolności pisania u chorego człowieka, często jest też jego ostatnią czynnością. W podpisie bowiem ujawnia człowiek swój temperament, zdolności, skłonności i usposobienie.

Niemniej jednak identyfikacyjne badania podpisów nie należą do łatwych ze względu na to, że liczba elementów graficznych jest niewielka, oraz fakt, iż czynność ich kreślenia jest zautomatyzowana, co powoduje powstanie mniej lub bardziej wyraźnych różnic pomiędzy nim a pismem zwykłym danej osoby. Komparatystyczne badania pisma obejmują cztery warstwy: graficzną, językową, treściową i techniczną, przy czym trzy pierwsze z nich są w zasadzie równoważne. W badaniach podpisów pole badania zawężone jest do warstwy graficznej i technicznej. Z tego względu liczba cech zawartych w podpisach i mogących podlegać badaniom jest generalnie znacznie mniejsza niż w piśmie, zwłaszcza gdy podpis ma postać tworu nieczytelnego. Z tego również względu metody badań pisma nie są w pełni adekwatne do badania podpisów, do których stosowane są specyficzne metody badawcze[6].

[6] Szerzej patrz A. K o z i c z a k, *Metody pomiarowe w badaniach pismoznawczych*, Kraków 1997.

Kolejnym aspektem identyfikacji osoby na podstawie jej podpisu są pewne ograniczenia wynikające z przyjętej metody badawczej. Metoda ta – wnioskowanie *per analogiam* – jest od początku tych badań niezmienna, i nie ulega zmianom wraz ze zmianą przedmiotu ekspertyzy. Biegły porównuje zarówno całość materiału badawczego, jak i jego poszczególne elementy. Dąży do ustalenia cech wspólnych lub rozłącznych. Sedno sprawy tkwi w tym, że rozumowanie *per analogiam* z punktu widzenia logiki nie może prowadzić do sądów kategorycznych. W ramach tego rozumowania należy przyjąć możliwość poznania prawdopodobnego. Umożliwia to poznanie tylko w granicach większego lub mniejszego prawdopodobieństwa. Dzisiaj mówi się, że w pewnych przypadkach rozumowanie przez analogię może zbiec się z pewnością bezwzględną. Mamy taką sytuację, gdy prawdopodobieństwo różni się od pewności o różnicę dostatecznie małą. W przypadku ekspertyzy mamy z taką sytuacją do czynienia, gdy prawdopodobieństwo wynosi np. 98%, zaś o tych 2% decydują cechy drugorzędne, które nie mogą w danym przypadku przesądzać. Te 2% może wynikać choćby z tego, że pismo ulega ciągłym zmianom, które wynikać mogą z szeregu czynników: stanu psychofizycznego osoby piszącej, jej pozycji podczas pisania, podłoża, stanu emocjonalnego, zażywania narkotyków, alkoholu, warunków środowiskowych (niskie temperatury). Z pewnością biegły nie może dostarczyć opinii kategorycznej w przypadku badania parafy.

Podczas identyfikacji w oparciu o podpis własnoręczny wykorzystywany jest fakt, że w piśmie człowieka znajdują odbicie jego własności psychofizjologiczne, które ujawniają się w piśmie bezwarunkowo, w taki sposób, że bardzo trudno jest je świadomie zafałszować, zaś ich bezbłędne podrobienie jest wysoce dyskusyjne i wymaga wyrafinowanych metod oraz wiedzy zbliżonej do tej, jaką posiada biegły pismoznawca. W obrocie elektronicznym należało znaleźć metody, które by tę cechę zastąpiły, a jednocześnie były równie pewne.

Identyfikacja na podstawie podpisu cyfrowego przebiega w zupełnie inny sposób. W podpisie nie znajdują odbicia żadne cechy na trwałe związane z podmiotem podpisującym. O kształcie podpisu cyfrowego decyduje zawartość podpisywanego dokumentu oraz wartość tajnego klucza, który powinien być znany tylko osobie podpisującej. Identyfikacja odbywa się w oparciu o sekret, który jest znany tylko sygnatariuszowi, gdyż jeśli przez deszyfrowanie otrzymujemy sensowny tekst, a nie chaotyczny ciąg bitów,

to tylko osoba znająca klucz prywatny może być jego autorem. Podpis ma więc w tym wypadku charakter dynamiczny. Będzie on niepowtarzalny dla każdego dokumentu, gdyż zmiana treści dokumentu chociażby o jeden bit pociągnie za sobą zmianę podpisu. W końcu zmianie ulegać mogą także klucze szyfrujące. Tak więc dla pewności obrotu istotne znaczenie ma powiązanie kluczy szyfrujących z podpisującym, które zapewnić mają cyfrowe certyfikaty. Dla zapewnienia pewności obrotu podpis cyfrowy musi spełniać następujące założenia:

1) jedynie osoba x może utworzyć podpis osoby x – podrobienie podpisu jest niemożliwe;

2) jednoznacznie można stwierdzić, że podpis został złożony pod określonym dokumentem;

3) kopiowanie podpisu z jednego dokumentu na drugi jest niewykonalne.

Zintegrowanie podpisu z dokumentem zapewnia niemożliwość jego przeniesienia ani skopiowania na inny dokument. Wyklucza to możliwość przerobienia czy podrobienia dokumentu elektronicznego, o co nie jest tak trudno w przypadku dokumentów papierowych. Tak więc sama technika składania podpisu cyfrowego zapewnia realizację powyższych warunków, o ile tylko klucz tajny służący do podpisywania pozostanie zabezpieczony przed nieautoryzowanym użyciem. Z tego względu – obok głosów entuzjastycznie przyjmujących możliwość operowania podpisem cyfrowym – pojawiają się także głosy wyrażające sceptycyzm co do zrównania rangi podpisu cyfrowego z odręcznym[7]. Dokonując identyfikacji, w rzeczywistości weryfikujemy jedynie fakt oznaczenia dokumentu przy użyciu klucza prywatnego, zarejestrowanego na daną osobę, a nie fakt rzeczywistego dokonania przez nią tej czynności. Wynika stąd, że obiektywne wykazanie spełnienia pierwszego warunku jest niemożliwe, ponieważ podpis może utworzyć każda osoba, która znajdzie się w posiadaniu określonego klucza prywatnego. Wnioskowanie o prawdziwości podpisu opiera się na założeniu, że właściciel klucza nie dopuści do jego upublicznienia, gdyż nie leży to w jego interesie. Kwestia ewentualnej odpowiedzialności za umyślne bądź nieumyślne naruszenie tej zasady ma znaczenie fundamentalne i wy-

[7] M. M a r u t a, *Podpis elektroniczny – zarys przyszłych regulacji prawnych*, Radca Prawny 2001, nr 2, s. 53.

maga uregulowania przez prawo podpisów cyfrowych. Należy spodziewać się także obwarowania tej kwestii odrębnymi przepisami dotyczącymi procedury certfikacyjnej. Jak widać, zagadnienie to będzie miało donośne znaczenie na gruncie prawa dowodowego.

II. Regulacje prawne w zakresie podpisu

Dokumentem, który zmobilizował zarówno rząd, jak i posłów do podjęcia prac nad podpisem elektronicznym była Dyrektywa Unii Europejskiej z dnia 19 stycznia 2000 r. (L. 13/12) o wspólnotowej infrastrukturze podpisów elektronicznych. Stała się ona od niedawna głównym aktem, na którym mają się wzorować regulacje krajowe, dotyczące podpisu elektronicznego i systemu organizacyjnoprawnego, na bazie którego będzie funkcjonowała e-gospodarka.

Wstępny projekt ustawy o podpisie elektronicznym mimo swoich mankamentów prawnych, o czym mówili sami jego twórcy, zawierał wiele niewiadomych, nie rozstrzygał też wątpliwości co do ostatecznego kształtu legislacyjnego tej ustawy; pozostawiał też na marginesie kwestie organizacyjnoprawne, w tym zwłaszcza ustalenie charakteru Krajowego Urzędu Autoryzacji; padały propozycje, by był to urząd państwowy, choć równolegle pojawiała się koncepcja firmy prywatnej, która by czuwała nad porządkiem prawnym i organizacyjnym, jaki wiąże się z infrastrukturą podpisów elektronicznych.

Pojawienie się Dyrektywy o wspólnotowej infrastrukturze podpisów elektronicznych w Unii Europejskiej w poważnym stopniu wymogło ponowne zajęcie się projektem ustawy o podpisie elektronicznym; zaowocowało także uchwałą, jaką w lipcu 2000 r. przyjął Sejm, zobowiązującą rząd do przedstawienia do końca września strategii rozwoju społeczeństwa informacyjnego w Polsce. Jednym z zadań tej strategii miało być stworzenie przejrzystych reguł prawnych i odpowiedniej infrastruktury dla podpisów elektronicznych i handlu elektronicznego (e-*commerce*).

Zdaniem osób reprezentujące tzw. kręgi rządowe, nie byliśmy zapóźnieni w opracowywaniu aktów prawnych dotyczących tej problematyki w stosunku do Unii Europejskiej. Ukazały się bowiem takie regulacje, które w dużym stopniu wprowadziły przepisy o zawieraniu umów drogą elektroniczną. Wymienia się wśród tych aktów prawnych przede wszystkich: ustawę z dnia 29 sierpnia 1997 r. – Prawo bankowe, kodeks karny, ustawę z dnia

19 listopada 1999 r. – Prawo działalności gospodarczej, ustawę z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny. Odpowiednie zapisy normatywne zostały też zaproponowane w projekcie ustawy o działalności ubezpieczeniowej, a także (o czym była wyżej mowa) w nowelizowanym kodeksie cywilnym.

Nieco inne opinie co do stanu, tempa i kierunku prac nad projektem ustawy o podpisie elektronicznym i e-gospodarki padają ze strony przedsiębiorców, osób wykonujących wolne zawody, a zwłaszcza prawników prowadzących kancelarie prawnicze, adwokatów, radców prawnych, notariuszy czy też innych osób, które korzystają z usług sieci Internetu dla potrzeb własnych oraz swoich firm.

Upowszechnienie wykorzystania dokumentów i transakcji elektronicznych i związane z tym oszczędności czasu, pieniędzy i zasobów naturalnych wymagają stworzenia infrastruktury zaufania do instytucji podpisu elektronicznego. Niezbędna jest w tym celu odpowiednia regulacja prawna, taka, która zapewni bezpieczeństwo normatywne, analogiczne do uznanej od stuleci infrastruktury opartej na dokumencie papierowym, podpisach własnoręcznych, pieczęciach i innych znakach legitymujących osoby, które się nimi posługują lub w imieniu których osoby te występują w obrocie prawnym i gospodarczym.

Nasze przygotowania do opracowania projektu ustaw o podpisie elektronicznym rozpoczęły się stosunkowo niedawno, w ubiegłym roku był gotowy wstępny projekt takiej ustawy; niewielki zespół autorów, posiłkując się przykładami z innych regulacji, a także ustaleniami unijnymi zaproponował roboczy kształt projektu ustawy. Pojawiły się też dość nieśmiałe i mało zdecydowane próby jego upowszechnienia, choć prawdę powiedziawszy, sami autorzy rzadko o nim mówili w mass mediach.

Projekt ten był pełen niewiadomych i wątpliwości, stawiał też pytania i problemy, które wychodziły poza ramy tej regulacji; co więcej, nie rozstrzygnięta była instytucjonalizacja infrastruktury podpisu elektronicznego, otwartym był problem podmiotowości instytucji sterującej całym systemem, zadawano pytanie, czy ma być to urząd państwowy, czy firma prywatna; zespół projektujący był zdania, że klarowniejszym w działaniu i bezstronnym będzie urząd, gdyż firma prywatna może być podejrzewana o prowadzenie „konkurencji w sektorze". Takie stanowisko było co najmniej dys-

kusyjne, czego nie ukrywali twórcy tego projektu. Zwracano uwagę na cechy czy też atuty, jakimi musi wyróżniać się ten urząd, wskazywano, że musi cieszyć się pełnym zaufaniem na rynku, gdyż dla rozstrzygnięcia decyzji o powołaniu takiego, a nie innego ogólnopolskiego „autoryzatora", główne znaczenie będzie miało: zachowanie pełnej niezależności, gwarancja bezpieczeństwa i poufności, niekwestionowana bezstronność. Zasady te miały być wpisane w ustawę o podpisie elektronicznym; wsparcie tych reguł znajduje się w powołanej już dyrektywie, która wprowadza zasady nadzoru nad działalnością podmiotów, których zadaniem jest wydawanie certyfikatów; podmioty te powinny być osobami godnymi zaufania. Nadzór nad działalnością tych osób odbywa się w ramach tzw. systemów akredytacyjnych, są one dobrowolne, w myśl art. 3 ust. 1 Dyrektywy. Państwa członkowskie nie uzależniają świadczenia usług certyfikacyjnych od uzyskania uprzedniego zezwolenia; państwa te mogą wprowadzić lub utrzymywać dobrowolne systemy akredytacji służące podniesieniu świadczonych usług certyfikacyjnych. Wszelkie wymogi w ramach takich systemów muszą być obiektywne, przejrzyste, proporcjonalne i nie dyskryminujące. Państwom członkowskim nie wolno ograniczać liczby akredytowanych podmiotów świadczących usługi certyfikacyjne.

Na zgłoszony rządowy projekt ustawy o podpisie elektronicznym czekał od końca ubiegłego roku poselski projekt ustawy o podpisie elektronicznym.

Oba projekty spotkały się w Sejmie; autorzy konkurencyjnych projektów ustawy o podpisie elektronicznym zapowiedzieli dość szybko współpracę przy tworzeniu jednej, kompromisowej wersji ustawy.

Pierwsze czytanie projektów w Sejmie odbyło się w połowie marca bieżącego roku. Natomiast 27 lipca ustawa o podpisie elektronicznym została przyjęta przez Sejm, a 11 października 2001 r. podpisał ją Prezydent Rzeczypospolitej Polskiej. Ustawa ta wchodzi w życie w 9 miesięcy od dnia jej ogłoszenia.

Po raz pierwszy w historii wiele krajów świata, w tym Polska, podjęło próbę zastąpienia (lub zrównania) w pewnym zakresie skutków prawnych własnoręcznego podpisu, jaki znamy od ponad czterech tysięcy lat, zespołem technik i algorytmów określanych jako „podpis cyfrowy".

Bez wątpienia ustawa o podpisie elektronicznym ma kapitalne znaczenie dla przyszłości nie tylko gospodarki, ale i nas wszystkich; podpis elektroniczny bowiem to narzędzie lub instrument, którym będziemy się posłu-

giwać w niedalekiej przyszłości na co dzień, w sprawach błahych i skomplikowanych, w trakcie czynności faktycznych i prawnych, w kwestiach prywatnych i publicznych, w czasie zawierania umów, jak i w chwili podejmowania decyzji majątkowych o różnym charakterze.

Podpis elektroniczny nie ma zatem elitarnego zastosowania, wprost przeciwnie, jeżeli ma spełnić swoje główne zadanie misyjne, jakim jest zrównanie go pod względem skutków prawnych z podpisem własnoręcznym, to nie jest to elektroniczny kaprys ani elektroniczny zawijas, ale sposób i forma wyrażania woli uczestników obrotu elektronicznego.

III. Ogólne zasady systemu certyfikacji[8]

Istota systemu certyfikacji sprowadza się do tego, że odpowiednie organy, tzw. organy certyfikacyjne (*certification authorities*), będące swoistymi jednostkami zaufania publicznego, potwierdzają autentyczność danego klucza publicznego.

Prawo do wydawania certyfikatów jest sprawą niezwykłej wagi; muszą być to bowiem osoby (podmioty) godne najwyższego zaufania; takie, które spełniają określone kryteria i cechy umiejscawiające je w gronie niekwestionowanych autorytetów organizacyjnoprawnych.

Potwierdzenie to przybiera postać kolejnego podpisu elektronicznego[9].

Certyfikatem jest to elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację osoby[10].

Podstawową funkcją certyfikatu jest zaświadczenie o powiązaniu pary kluczy (prywatnego i publicznego) z osobą uprawnioną do posługiwania się nimi.

Aby zweryfikować podpis cyfrowy, musi istnieć podmiot weryfikujący. Winien mieć on dostęp do publicznego rejestru kluczy, w którym znajduje się klucz publiczny podpisującego, oraz pewność, że odpowiada on kluczowi prywatnemu wysyłającego podpisany dokument. Ale pojawia się tutaj

---

[8] Jednym z głównych składników infrastruktury podpisu elektronicznego jest system certyfikacji.

[9] J. B a r t a, R. M a r k i e w i c z, *Internet a prawo*, Kraków 1998, s. 72.

[10] *Vide* art. 3 pkt 6 rządowego projektu ustawy o podpisie elektronicznym.

kolejny problem, a mianowicie wzajemnego zaufania stron transakcji. Przecież nie sposób domniemywać dobrej wiary stron umowy zawartej w Internecie na odległość „między nieobecnymi", często w ogóle nie znającymi się stronami. Konieczne jest w tej sytuacji powołanie odpowiedniego urzędu. Taką „instytucją zaufania" mogłoby być tzw. centrum (urząd) certyfikacji, którego zadaniem byłoby wystawianie certyfikatu, który dołączony do podpisanego dokumentu, umożliwiałby kontrahentowi weryfikację powiązanego z kluczem prywatnym klucza publicznego, przypisanego podpisującemu.

Coraz częściej legislator wprowadza do obrotu prawnego tzw. formę elektroniczną, wskazując na odchodzenie przez ustawodawcę od formy pisemnej w przypadkach, gdzie większą efektywność przynosi technika informatyczna. Jeżeli dodamy do tego możliwość przesyłania wymienionych dokumentów elektronicznych za pośrednictwem sieci komputerowych, okaże się jak niezbędną stała się ustawa o podpisie elektronicznym, która w świecie wirtualnym będzie odpowiednikiem tradycyjnej sygnatury.

Ponieważ minimalnym wymaganiem dla zachowania formy pisemnej jest złożenie własnoręcznego podpisu, jedną z kluczowych kwestii dla formy elektronicznej będzie rozstrzygnięcie problemu prawnej skuteczności podpisu cyfrowego. Trudno domniemywać możliwość stosowania podpisu elektronicznego w przypadku braku wyraźnego przepisu ustawy. Problem podpisu cyfrowego to nie tylko odpowiednio wybrane i skonstruowane metody kryptograficzne[11], ale również potrzeba sprostania funkcjom, jakie przypisuje się w prawie cywilnym podpisom, tj. funkcji gwarancyjnej, ostrzegawczej, identyfikującej i dowodowej.

Otwartym problem jest pytanie o stopień przygotowania ogniw gospodarki, instytucji prywatnych, państwowych i wielu innych do włączenia się w system podpisów cyfrowych; system ten bowiem nie ominie żadnej sfery organizacji społeczeństwa. Co może oznaczać, że nie tylko firmy prywatne, ale wszystkie organy, instytucje, administracje rządowe i samorządowe, a także inne muszą poczynić pewien wysiłek intelektualny, informacyjny,

---

[11] Sygnalizują te kwestie już od pewnego czasu polscy specjaliści, np. J. P r z e t o c k i, J. U r b a n o w i c z, A. W i t t l i n, *Czynności elektroniczne i kryptografia w pracy notariusza*, Rejent 1999, nr 100, s. 90 i nast.

organizacyjny, finansowy i kadrowy, by sprostać wyzwaniu nowych technik elektronicznych w szeroko rozumianym obrocie prawnym i gospodarczym.

Od czynności elektronicznych nie ma ucieczki, nie ma też powrotu do tradycyjnych form wyrażania oświadczeń woli; zanikać będzie bezpośredniość kontaktów klient – urzędnik w dokumentowaniu czynności prawnych, składaniu oświadczeń woli czy też w innych zdarzeniach cywilnoprawnych.

Nowy system gospodarki elektronicznej wytwarza prężną i stale rozwijającą się dziedzinę zrównywania dokumentów w formie elektronicznej z dokumentami pisemnymi, taka jest bowiem misja i rola e-podpisów.

IV. Formy zabezpieczenia podpisu cyfrowego i jego ochrony

Bezpieczeństwo podpisu cyfrowego polega na uniemożliwieniu nieautoryzowanego posługiwania się tym podpisem w imieniu innej osoby.

Bezpieczeństwo jest realizowane na trzech płaszczyznach:

– kryptograficznej,
– technicznej,
– prawnej.

Płaszczyzna kryptograficzna

Kanały komunikacyjne, szybkie i zapewniające dostępność z każdego miejsca na ziemi, mogą być podsłuchane. Szyfrowanie zapewnia, że podsłuchujący nie będzie mógł poznać treści podsłuchanej informacji. Jednocześnie dzięki odpowiedniej konstrukcji algorytmów asymetrycznych, nawet znając kryptogram i klucz publiczny, nie będzie mógł odtworzyć klucza prywatnego.

Podstawowym aspektem bezpieczeństwa jest więc odporność stosowanych algorytmów na łamanie. Stosowane obecnie algorytmy i funkcje bazują na obserwacjach zjawisk matematycznych, które nie są do końca poznane. Dla konstruowania dobrych algorytmów szyfrujących korzysta się z rezultatów dotyczących **złożoności obliczeniowej problemów**. Tak na przykład algorytm RSA wykorzystuje trudności związane z rozkładem liczb na czynniki pierwsze, zaś algorytm El Gamala trudność obliczania dyskretnych logarytmów.

Należy mieć na uwadze, że żadna metoda szyfrowania nie jest stuprocentowo pewna. Jak na razie, oba algorytmy są odporne na efektywne łamanie. Dzieje się tak dzięki temu, że przy zastosowaniu odpowiednio dużych

liczb (takich, które mają kilkaset znaków), liczba możliwych kombinacji kluczy prywatnych i publicznych jest bliska nieskończoności (100 procesorów pentium 100 potrzebowałyby roku by złamać 428- bitowy klucz RSA). Tym niemniej 512-bitowe klucze nie zapewniają już obecnie odpowiedniego bezpieczeństwa. Trzeba pamiętać jednak, że zwiększenie długości klucza o jeden bit oznacza podwojenie ilości nakładów potrzebnych do jego złamania. Uważa się, że liczby 1024-bitowe będą zapewniały odpowiedni poziom bezpieczeństwa w systemach RSA i El Gamala. To, że algorytmy nie są łatwe do złamania dzisiaj, nie oznacza, że za kilka lat nie będzie łatwiej ich pokonać, gdyż wydajność komputerów stale się zwiększa. Także postępy w teorii liczb mogą doprowadzić do odkrycia algorytmu znajdowania czynników w czasie rosnącym wielomianowo, który to algorytm będzie mógł zagrozić bezpieczeństwu RSA.

Przyszłością szyfrowania mogą się okazać systemy korzystające z krzywych eliptycznych, które umożliwiają obsługę bardzo dużych liczb, przy minimalnym zapotrzebowaniu na pamięć i niewielkich kosztach obliczeniowych.

Dodatkowym wzmocnieniem kryptograficznym podpisów cyfrowych jest stosowanie jednokierunkowych funkcji hashujących. Jednokierunkowość funkcji *f* gwarantuje, że znając jedynie *f(x),* nie można obliczyć *y* takiego, że *f(y) = x.* Można, co prawda, uzyskać pewne informacje o *y*, ponieważ niektóre bity są łatwe do wyliczenia, ale za to inne praktycznie są nie do odtworzenia. Także algorytm RSA posiada takie trudne miejsca, zwane **hard – core bit**, gdyż tę właściwość ma funkcja obliczająca ostatni bit tekstu jawnego dla argumentu składającego się z klucza publicznego RSA oraz kryptogramu.

Płaszczyzna techniczna

Nie mniej istotnym aspektem jest generowanie kluczy kryptograficznych w odpowiednich warunkach i późniejsze właściwe przechowywanie klucza prywatnego, który nie może ulec odtajnieniu.

Najprostszą metodą generowania kluczy jest posłużenie się odpowiednią aplikacją, która jest dostępna w ramach pakietu oprogramowania przeznaczonego do realizacji usług ochrony informacji w sieci. Klucze powinny być generowane na komputerze odciętym od sieci, w specjalnym serwerze sieciowym lub przy wykorzystaniu urządzenia kryptograficznego. Klucz ten jest dość dużą liczbą i może być trudny do zapamiętania. Jeżeli jest

przechowywany w systemie komputerowym, to dostęp do niego powinien być odpowiednio zabezpieczony (klucz można zabezpieczyć hasłem, które jest przechowywane w postaci zhashowanej), zaś komputer odcięty od dostępu do Internetu. Innym sposobem jest wykorzystanie do przechowywania klucza karty magnetycznej, pamięciowej lub inteligentnej[12]. Można do tego celu używać także odpowiedni *hardware* – tzw. **urządzenie kryptograficzne**, które jest układem elektronicznym, zamkniętym w specjalnej obudowie, która nie przepuszcza żadnego promieniowania elektromagnetycznego generowanego podczas jego pracy, a próba otworzenia obudowy powoduje bezpowrotną utratę zapisanych wewnątrz danych. Stosując rozbudowany system kryptograficznego zabezpieczania danych i korespondencji, wykorzystujący różne urządzenia i techniki, będziemy posiadać szereg kluczy o różnej hierarchii ważności, które muszą być odpowiednio zarządzane[13].

Kolejnym elementem jest system certyfikacji pozwalający na identyfikację właściciela klucza publicznego.

---

[12] Karta inteligentna jest wyposażona w mikroprocesor i pamięć RAM. Jest ona w stanie samodzielnie wykonywać złożone operacje, związane np. z zaszyfrowaniem o odszyfrowywaniem przechowywanego w niej klucza.

[13] Hierarchia kluczy w systemie kryptograficznym:

MASTER KEY – nigdy nie jest zmieniany i nie może być odczytany. Jego znaczenie jest fundamentalne – jest zapamiętywany przez użytkownika lub zapisywany w urządzeniu kryptograficznym. Służy do zabezpieczenia pozostałych kluczy, przechowywanych na nośnikach elektronicznych.

KLUCZE PIERWOTNE – służą do zabezpieczenia komunikacji i przechowywania danych. Powinny być często zmieniane, gdyż duża ilość szyfrowanych przez nie danych ułatwia kryptoanalizę.

KLUCZE WTÓRNE – są niezbędne ze względów technicznych. Są to klucze używane w różnych protokołach, np. dla przesyłania lub uzgadniania kluczy pomiędzy partnerami przed rozpoczęciem wymiany danych. Są rzadko zmieniane, ale i szyfrują stosunkowo rzadko, i do tego krótkie teksty.

KLUCZ SESYJNY – zalecane jest stosowanie odrębnych kluczy do szyfrowania komunikacji występującej w obrębie każdej sesji:

– ogranicza to ilość kryptogramów, które są generowane za pomocą jednego klucza, a tym samym ogranicza ilość kryptogramów, jakie przeciwnik może analizować;

– ogranicza skutki odgadnięcia klucza przez przeciwnika, jeśli sesja została już zakończona, przeciwnik nie ma możliwości przeprowadzenia aktywnego ataku, może jedynie poznać dane przekazywane w trakcie zakończonej już sesji. Wyznaczenie kluczy dla następnej sesji przebiega bowiem przy użyciu kluczy wtórnych, a nie bieżącego klucza sesyjnego.

Płaszczyzna prawna

Polski system prawny obejmuje represją prawnokarną czyny, które mają charakter „przestępstw komputerowych". Pojęcie to nie jest co prawda jeszcze ściśle zdefiniowane; na użytek prawa karnego materialnego rozumiemy pod nim sytuacje, w których system komputerowy stanowi zarówno przedmiot, jak i narzędzie zamachu. Przestępstwa komputerowe charakteryzują się swoistą specyfiką, o czym decydują następujące fakty: miejsce dokonania przestępstwa nie zawsze jest „miejscem" w potocznym tego słowa znaczeniu, istnieją duże trudności z ustaleniem sprawców przestępstw ze względu na fakt, że sieć Internet pozbawiona jest atrybutów fizycznej obecności, będących klasycznymi śladami kryminalistycznymi, jak odciski palców, głos czy wizerunek. Fakt ten znajduje swoje odzwierciedlenie w poglądzie, że zarówno prawo karne materialne, jak i procedurę karną należy wyposażyć w nowe instrumenty prawne, które umożliwią ściganie tej kategorii przestępstw[14].

Poniżej zaprezentowany został szeroki katalog przestępstw, z których nie wszystkie bezpośrednio skierowane są przeciwko dokumentom, a co za tym idzie, ich przedmiotem wykonawczym byłyby podpisy cyfrowe czy e-dokumenty. Podyktowane jest to tym, że większość cyberprzestępstw nie istnieje samodzielnie, przenikają się one i uzupełniają tak, że sprawca w chwili egzekwowania odpowiedzialności karnej podlega najczęściej kilkunastu zarzutom. W przypadku przestępstw przeciwko dokumentom elektronicznym, które przechowywane są w systemie komputerowym, najczęściej przestępstwo jest dokonywane przy użyciu Internetu, który wykorzystywany jest w celu wejścia w posiadanie informacji pozwalających na zrealizowanie przestępczego zamiaru. Skutkiem tego sprawca swoimi czynnościami przygotowawczymi realizuje stany faktyczne, wyczerpujące znamiona innych przestępstw z zakresu przestępstw komputerowych. W takim stanie sprawca będzie mógł ponieść odpowiedzialność karną nawet w sytuacji, w której niemożliwe byłoby udowodnienie mu usiłowania popełnienia przestępstwa przeciwko dokumentom elektronicznym lub przygotowania do jego popełnienia.

---

[14] J. D z i e r ż a n o w s k a, *Karnoprocesowa problematyka przestępczości komputerowej*, [w:] *Internet 2000*, Lublin 1999, s. 288.

W kodeksie karnym należy wskazać następujące rozdziały zawierające wspomniane wyżej przestępstwa komputerowe:

Rozdział XXXIII, zatytułowany „Przestępstwa przeciwko ochronie informacji", w którym dokonano kryminalizacji następujących czynów:

• art. 267 § 1 – haking;

• art. 267 § 2 – nielegalny podsłuch, inwigilacja przy użyciu urządzeń technicznych;

• art. 268 § 2 w związku z 268 § 1– naruszenie integralności zapisu informacji;

• art. 269 § 1 i 2 – sabotaż komputerowy, zakłócenie lub paraliżowanie funkcjonowania systemów komputerowych o istotnym znaczeniu dla bezpieczeństwa państwa i obywateli.

Rozdział XXXIV – przestępstwa przeciwko wiarygodności dokumentów:

• art. 270 §1 – fałszerstwo komputerowe polegające na manipulowaniu treścią dokumentu elektronicznego.

Mówienie w tym przypadku o fałszerstwie komputerowym stało się możliwe dzięki nowemu ujęciu definicji legalnej dokumentu w kodeksie karnym – art. 115 §14, która uzyskała następujące brzmienie:

„Dokumentem jest **każdy przedmiot** lub **zapis na komputerowym nośniku informacji**, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne"[15].

[15] Sformułowanie tego przepisu jest *de facto* uznawane za wysoce niefortunne, wszak żaden zapis, nawet ten na „komputerowym nośniku informacji", nie może istnieć poza przedmiotem. W nauce kryminalistyki występuje trójelementowa konstrukcja dokumentu, zgodnie z którą w skład dokumentu wchodzą: podłoże, środki kryjące związane z tym podłożem, treść intelektualna utrwalona za pomocą środków kryjących. Struktura dokumentu elektronicznego jest odmienna. Brak w niej drugiego elementu w postaci środka kryjącego. Sam nośnik ma ponad wszelką wątpliwość materialny charakter. Jest on złożoną kompilacją elementów o różnej strukturze wewnętrznej. Od tradycyjnego dokumentu różni się nie tylko materiałem, z którego zbudowany jest nośnik, ale przede wszystkim sposobem utrwalania na tym nośniku treści intelektualnej. Treść nie jest nanoszona na podłoże w tradycyjny sposób, ale jest umieszczana wewnątrz nośnika, tak że nie jest poznawalna dla człowieka bez użycia skomplikowanych narzędzi w postaci czytnika i oprogramowania. Specyfiką dokumentu elektronicznego jest to, iż nie zmieniając materii nośnika, można zmieniać treść dokumentu, która następuje przez zmianę rozkładu domen magnetycznych umieszczonych

Konsekwencją takiego ujęcia, a przynajmniej rozwianiem istniejących w tej kwestii wątpliwości, jest rozciągnięcie ochrony karnoprawnej dokumentu elektronicznego na wszystkie te czyny, w których opisie pojawia się słowo dokument.

Rozdział XX – przestępstwa przeciwko bezpieczeństwu powszechnemu:

• art. 165 § 1 ust. 4 – sprowadzenie niebezpieczeństwa dla życia lub zdrowia dla wielu osób albo mienia w znacznych rozmiarach, które jest wynikiem zakłócenia, uniemożliwienia lub wpływania w inny sposób na automatyczne przetwarzanie informacji.

Rozdział XVII – przestępstwa przeciwko Rzeczpospolitej:

• art. 130 § 2 – uprzywilejowana postać szpiegostwa; czyn ten można popełnić przez włączenie się do sieci komputerowej w celu uzyskania wiadomości, których udzielenie obcemu wywiadowi może wyrządzić szkodę Rzeczpospolitej Polskiej.

Problemem na odrębną dyskusję jest kwestia wykrywalności przestępstw tego typu, ustalania tożsamości sprawcy i zabezpieczania dowodów popełnienia przestępstwa. Niewątpliwie jest to utrudnione ze względu na ciągły i szybki rozwój samej sieci komputerowej oraz technologii z nią związanych. Sama wykrywalność przestępstw oraz uzyskiwanie dowodów ich popełnienia wymagają opracowania nowych, niekonwencjonalnych metod i technik adekwatnych do środowiska cyfrowego, w czym mogłaby pomóc współpraca kryminalistyków, prawników i specjalistów z zakresu informatyki i nowoczesnych technologii.

---

wewnątrz nośnika. Należy zadać sobie pytanie, czy te odmienności w strukturze dokumentu elektronicznego wymagają jego odmiennego traktowania na gruncie definicji legalnej. Gdyby odpowiedź miała być twierdząca, na pewno nie może być to czynione w sposób, w jaki dokonano tego w k.k., gdzie takie brzmienie definicji implikuje tezę, iż dokument elektroniczny istnieje poza przedmiotem, a co za tym idzie, ma całkowicie niematerialny charakter. Problem ten w zasadzie nie pojawia się na gruncie nauki kryminalistyki, gdzie za dokument uznajemy **każdy przedmiot, który zawiera treść mającą formę pisma, rysunku lub obrazu wykonanego ręcznie lub za pomocą odpowiedniego urządzenia.**

Podsumowanie

Pierwszym polem szerszego zastosowania podpisu elektronicznego powinno być stworzenie systemu komunikacyjnego, dającego możliwość łatwego i szybkiego kontaktu między obywatelami oraz klientami instytucjonalnymi a urzędami państwowymi, na których będzie ciążył obowiązek respektowania podpisu elektronicznego. Na przeszkodzie stanąć może jednak brak odpowiedniej infrastruktury technicznej, której rozwinięcie w skali całego kraju może zająć kilka lat. Na pewno można spodziewać się, że pakiety usług kryptograficznych, a wśród nich aplikacje realizujące funkcje podpisu elektronicznego, będą wykorzystywane do ochrony korespondencji elektronicznej, zwłaszcza mającej charakter służbowy. Pomimo tego, iż spora część sektora komercyjnego oczekuje z niecierpliwością na wejście w życie ustawy o podpisie elektronicznym, upatrując w niej szeregu korzyści pozwalających na zrewolucjonizowanie prowadzonej dotychczas działalności, zwłaszcza w sferze kontaktów z klientami, zdaje się, że ci ostatni są najmniej przygotowani na zaakceptowanie nowej technologii bez zastrzeżeń. Nie jest zaskoczeniem, iż największe obawy budzi kwestia bezpieczeństwa całego systemu, przy czym najwięcej uwagi poświęca się możliwości przeprowadzenia skutecznego ataku hakerskiego i wykorzystania zdobytych dzięki niemu informacji w celu uzyskania nieuprawnionych korzyści lub zaszkodzenia w inny sposób ofierze tego ataku. Atak taki jest faktycznie możliwy i nosi on nazwę ataku na schemat generowania podpisów. Ma on na celu uzyskanie możliwości fałszowania wiadomości przez posłużenie się cudzym podpisem, tak aby adresat uznał przerobioną lub w całości spreparowaną wiadomość za pochodzącą od tego, którego identyfikator jest do wiadomości dołączony. Atak ten może przybrać formę ataku na klucz prywatny nadawcy, funkcję skrótu, system dystrybucji kluczy. Pierwszy z tych ataków ma na celu odgadnięcie wartości klucza tajnego i polega na zebraniu możliwie najwięcej nadających się do analizy informacji o kryptosystemie będącym przedmiotem ataku, w celu wykrycia słabych punktów algorytmu, pozwalających na szybkie złamanie szyfru. Rozróżniane są różne klasy takiego ataku w zależności od ilości danych wyjściowych, jakimi dysponuje kryptoanalityk, takich jak: kryptogram, tekst jawny, dostęp do urządzenia szyfrującego. Jeśli algorytm nie posiada słabych punktów, pozostaje metoda ogólna polegająca na przeszukiwaniu całej

przestrzeni kluczy. Atak przeciwko funkcji skrótu polega na podstawieniu wiadomości, która będzie pasować do odpowiadającej autentycznej wiadomości funkcji skrótu, zaś ostatni z ataków polega na manipulacji, której skutkiem będzie uznanie klucza publicznego napastnika za klucz innej osoby. W praktyce oznaczałoby to sfałszowanie certyfikatu przypisanego do danego klucza. Przeprowadzenie któregokolwiek z tych ataków może zakończyć się hipotetycznym powodzeniem. Zabezpieczeniem przed nimi jest skonstruowanie takiego kryptosystemu, aby dla jak największej liczby klas ataków metoda taka wymagała ilości obliczeń przekraczających praktyczne możliwości.

W przypadku tradycyjnych fałszerstw, w większości przypadków można udowodnić fałszerstwo, zarówno gdy wymaga to badań pisma, jak i badań fizyko-chemicznych lub innych technicznych badań dokumentów. W celu zwiększenia ochrony i większego „powiązania" podpisu z osobą, stosuje się dodatkowe zabezpieczenia w postaci kodów PIN i kart chipowych, które chronią dostęp do urządzeń kryptograficznych[16]. Nie ulega wątpliwości, że najbezpieczniejszą formą zabezpieczenia podpisu cyfrowego byłoby jego związanie z technikami identyfikacji biometrycznej. Istnieje już wiele narzędzi realizujących kontrolę dostępu do danych bądź aplikacji, którymi są systemy oparte o rozpoznawanie linii papilarnych, geometrii dłoni, mowy czy cech charakterystycznych tęczówki oka[17]. Z pewnością wykorzystywanie systemów kryptograficznych stanowi krok milowy w dziedzinie zapewniania bezpieczeństwa dokumentom przesyłanym za pomocą sieci. Zdobycie pełnego zaufania użytkowników, a co za tym idzie, powszechne wykorzystywanie podpisu cyfrowego wymaga upływu czasu i oswojenia się przez nich z tą techniką. Przypuszczalnie z czasem możliwe będzie wykorzystanie algorytmów bezpośrednio wiążących dokument cyfrowy z cechami antropometrycznymi składającego podpis[18]. Dopiero wtedy będzie możliwe ziszczenie się wizji całkowitego wyparcia przez nowe nośniki dokumentów papierowych. Ale czy tak się stanie? Czy zostaną obszary na

---

[16] M. M a r u t a, *Podpis elektroniczny – zarys przyszłych regulacji prawnych*, Radca Prawny 2001, nr 2, s. 53 i 54.

[17] Zobacz **www.auotoid.pl**

[18] W. K o c o t, *Elektroniczna forma oświadczeń woli*, Przegląd Prawa Handlowego 2001, nr 3, s. 5.

tyle istotne, jak np. testamentowanie, gdzie nowoczesne techniki przegrają z naszym przywiązaniem do metod tradycyjnie uznawanych za najbardziej sprawdzone? Odpowiedzi na te pytania może udzielić jedynie praktyka, a ta nie dojdzie do głosu, jeśli nie będzie choćby potencjalnej możliwości skorzystania z nowego podpisu w celu wywołania skutków w sferze prawnej. Uchwalenie ustawy o podpisie elektronicznym jest do tego krokiem pierwszym i niezbędnym.