Rozdział I. Podpis elektroniczny, zapis elektroniczny, podpis i pismo w aktach międzynarodowych i wspólnotowych

§ 1. Rodzaje podpisów elektronicznych

Termin „podpis elektroniczny" jest pojęciem prawnym, a nie technicznym. W regulacjach międzynarodowych, wspólnotowych i krajowych przyjęto różne jego definicje. Obecnie zasadniczo charakteryzują się one szerokim ujęciem i technologiczną neutralnością[1]. Na skutek nadania podpisowi elektronicznemu szerokiego znaczenia, można go złożyć za pomocą licznych, a zarazem bardzo różniących się od siebie technologii. Dane elektroniczne będą stanowiły podpis elektroniczny, jeżeli zostały dołączone lub logicznie powiązane z innymi danymi obejmującymi informacje lub oświadczenie nim sygnowane, natomiast np. samo hasło, numer PIN lub podpis cyfrowy niezwiązany z żadnym oświadczeniem nie będzie podpisem elektronicznym.

I. Podpis cyfrowy

1. Istota i złożenie podpisu cyfrowego

Podpis cyfrowy (*digital signature*), nazywany również podpisem kryptograficznym lub podpisem asymetrycznym, jest ciągiem bitów, czyli zer i jedynek (w jakikolwiek sposób powiązany z innym ciągiem bitów), składających się na podpisany dokument, pozwalający na identyfikację sygnatariusza oraz zabezpieczenie autentyczności opatrzonego nim dokumentu[2]. Podpis cyfrowy opiera

[1] Przykładowo, w ustawie modelowej UNCITRAL o podpisach elektronicznych z 2001 r. podpis elektroniczny oznacza dane w formie elektronicznej, załączone do wiadomości elektronicznej albo logicznie z nią powiązane, które mogą być wykorzystane do identyfikacji podpisującego związanego z wiadomością elektroniczną i wskazują na zaaprobowanie przez podpisującego informacji zawartej w tej wiadomości.

[2] *J. Janowski*, Podpis elektroniczny w obrocie prawnym, Warszawa 2007, s. 38.

się na kryptografii asymetrycznej[3]. Do stworzenia podpisu cyfrowego wymaga się posiadania klucza asymetrycznego składającego się z dwóch kluczy, tj. prywatnego i publicznego. Pierwszy, służący do podpisania dokumentu, jest tajny i powinien być znany wyłącznie sygnatariuszowi, zresztą od tej cechy wzięła się jego nazwa. Natomiast drugi, wykorzystywany do weryfikacji podpisu, jest jawny, dostępny dla każdego, stąd też jego miano. Wskazane klucze są ze sobą ściśle związane. Podpis cyfrowy nie jest bezwarunkowo bezpieczny, lecz jedynie obliczeniowo bezpieczny. Bezpieczeństwo systemów kryptograficznych, wykorzystywanych do stworzenia podpisu asymetrycznego, opiera się na założeniu, że nie istnieje możliwość wyprowadzenia klucza prywatnego z klucza publicznego z uwagi na obecne ograniczenia mocy obliczeniowej komputerów. Sprawdzenie wszystkich dopuszczalnych kombinacji trwałoby dłużej niż okres ważności certyfikatu zawierającego klucz publiczny. Jednak ze względu na zwiększającą się moc obliczeniową komputerów z czasem niezbędne będzie wydłużanie klucza prywatnego i publicznego[4].

Złożenie podpisu cyfrowego polega na obliczeniu, na podstawie tekstu jawnego, tj. dokumentu oraz klucza prywatnego, określonego ciągu znaków. Podpis elektroniczny oznaczonego podmiotu składany pod różnymi dokumentami będzie za każdym razem inny, co odróżnia go od podpisu własnoręcznego, który w sytuacji optymalnej powinien zawsze mieć tożsamą postać. Wskazane rozwiązanie gwarantuje bezpieczeństwo podpisu cyfrowego, gdyż w przeciwnym razie nieuprawniona osoba mogłaby skopiować cudzy podpis i bezprawnie opatrywać nim oświadczenia[5].

Podpis kryptograficzny oblicza się na podstawie dwóch elementów, tj. dokumentu będącego parametrem zmiennym oraz klucza prywatnego stanowiącego parametr stały. W praktyce w celu przyspieszenia podpisywania i zmniejszenia liczby przesyłanych danych nie sygnuje się kluczem prywatnym całego dokumentu, lecz tylko jego obraz matematyczny, określany mianem skrótu lub sumą kontrolną (*hash*, *message digest*)[6]. Funkcja skrótu umożliwia na podstawie dowolnej wiadomości obliczyć ciąg znaków o stałej długości. Aktualnie stosuje

[3] Wytyczne do polityki dotyczącej kryptografii skierowane przede wszystkim do państw opracowała Organizacja Współpracy Gospodarczej i Rozwoju (OECD) w dokumencie zatytułowanym *Guidelines for Cryptography Policy*. Wskazany akt obejmuje osiem wytycznych. Szerzej na ten temat *K. Kowalik-Bańczyk*, Sposoby regulacji handlu elektronicznego w prawie wspólnotowym i międzynarodowym, Kraków 2006, s. 157–158.

[4] *K. Szaniawski*, *T. Kościelny*, Ustawa o podpisie elektronicznym, Komentarz, Kraków 2003, s. 40–41.

[5] Tamże, s. 23.

[6] *P. Polański*, Podpisy elektroniczne w prawie polskim i wspólnotowym, Rej. 2008, Nr 9, s. 85.

się dwa algorytmy funkcji skrótu, tj. SHA-1 (*Secure Hash Algorithm*), tworzący skrót o długości 160 bitów, oraz MD5 (*Message-digest Algorithm*), obliczający skrót liczący 128 bitów. Wynikowy ciąg znaków obliczany na podstawie funkcji skrótu zależy od wszystkich znaków tekstu jawnego, dlatego jakakolwiek modyfikacja dokumentu spowoduje zmianę skrótu. Odtworzenie tekstu oryginalnego na podstawie skrótu wiadomości jest obliczeniowo niewykonalne[7].

Podpisanie dokumentu odbywa się w dwóch etapach. W pierwszej kolejności należy na podstawie dokumentu obliczyć jego skrót, w drugiej zaszyfrować go algorytmem asymetrycznym za pomocą klucza prywatnego sygnatariusza[8]. Cała operacja jest wykonywana przez komputer po wybraniu przez podpisującego odpowiedniej opcji programu. Z reguły sygnatariusz przechowuje klucz prywatny na mikroprocesowej karcie kryptograficznej, jednak może go również zapisać na twardym dysku komputera lub innym elektronicznym nośniku informacji, co raczej nie powinno mieć miejsca, gdyż nie gwarantuje jego poufności. Karta kryptograficzna jest wyposażona w procesor dokonujący operacji kryptograficznych oraz pamięć, w której przechowuje się klucz prywatny, przy czym nie można go z niej odczytać ani skopiować na zewnątrz, co zapewnia jego poufność. Korzystanie z karty wymaga zaopatrzenia komputera w czytnik kart. Podpisanie dokumentu następuje wewnątrz karty kryptograficznej, nie ma więc potrzeby kopiowania klucza prywatnego do urządzenia zewnętrznego, nadto dostęp do niego chroniony jest numerem PIN (*Personal Identification Number*), który powinien być znany jedynie sygnatariuszowi[9], co ma gwarantować wysoki stopień bezpieczeństwa podpisu cyfrowego. Wszystkie wskazane zabezpieczenia służą zachowaniu tajności klucza prywatnego, gdyż w razie jego ujawnienia nieuprawnionej osobie trzeciej mogłaby ona fałszować dokumenty, bezprawnie podpisując je w imieniu prawowitego posiadacza klucza prywatnego.

Podpisanie dokumentu jest w praktyce szybkie i proste. Sygnatariusz dysponujący komputerem wyposażonym w odpowiedni interfejs użytkownika i czytnik karty kryptograficznej wkłada do niego kartę, wywołuje dokument, który ma zostać podpisany, po czym wybiera komendę „podpisać". Utworzony w ten sposób podpis cyfrowy jest plikiem danych zdatnym do bycia samodzielnie przechowywanym i przenoszonym, przy czym istnieje możliwość powiązania z nim innego pliku danych jako podpisanego nim dokumentu[10].

Podmiot dokonujący weryfikacji podpisu elektronicznego musi dysponować trzema elementami, tj. dokumentem, plikiem podpisu oraz kluczem publicznym

[7] *K. Szaniawski*, *T. Kościelny*, Ustawa o podpisie, s. 24–25.
[8] Tamże, s. 28.
[9] Tamże, s. 39–40.
[10] *J. Janowski*, Podpis elektroniczny, s. 54.

sygnatariusza[11]. Klucz publiczny jest zapisywany w elektronicznym certyfikacie wystawionym przez osoby prywatne lub przez podmioty świadczące usługi certyfikacyjne, który zamieszcza się na stronie WWW, odpowiednich serwerach lub przesyła pocztą elektroniczną[12].

Weryfikacja podpisu elektronicznego sprowadza się do porównania dwóch skrótów dokumentu. Pierwszy uzyskujemy przez obliczenie skrótu otrzymanej wiadomości (weryfikowanej), zgodnie z ogólnie znanym algorytmem. Drugi otrzymujemy poprzez przekształcenie odwrotne (odszyfrowanie) za pomocą klucza publicznego, podpisu dołączonego do pliku, który w rzeczywistości jest skrótem oryginalnego dokumentu utworzonym przez osobę podpisującą i przekształconym (zaszyfrowanym) za pomocą jej klucza prywatnego. Jeżeli obydwa skróty są jednakowe, to należy stwierdzić, że dokument nie został zmieniony po jego podpisaniu. W przypadku gdy skróty różnią się, musiała nastąpić modyfikacja dokumentu[13]. Mając na względzie powyższe, należy podkreślić, iż podpis cyfrowy zapewnia integralność dokumentu, umożliwiając ustalenie, czy miała miejsce zmiana treści dokumentu po jego sygnowaniu, nie pozwalając jednak na wykrycie, jakie modyfikacje zostały dokonane.

Klucz prywatny i publiczny może zostać samodzielnie wygenerowany przez osobę mającą zamiar posługiwania się podpisem cyfrowym za pomocą odpowiedniego oprogramowania, w szczególności publicznie dostępnego programu *Pretty Good Privacy* (PGP) albo stworzony i przyznany przez podmiot świadczący usługi certyfikacyjne. Przedmiotowe klucze stanowią jednak tylko pewne oznaczone wartości liczbowe i nie są związane z sygnatariuszem w taki sposób, by mogły go identyfikować. W celu ustalenia tożsamości podpisującego do klucza publicznego należy dodać więc dane osobowe podmiotu, dla którego oznaczony klucz publiczny i prywatny został wygenerowany, co czyni się, jak już wskazano, za pomocą certyfikatu[14].

2. Infrastruktura Klucza Publicznego

Obecnie najbardziej rozpowszechnionym systemem pozwalającym na wiarygodne i niezawodne przypisanie oznaczonej pary kluczy do określonego podmiotu jest Infrastruktura Klucza Publicznego (*Public Key Infrastructure* – PKI). Jest to konstrukcja organizacyjna i techniczna umożliwiająca jednoznaczne przyporządkowanie klucza publicznego, powiązanego z kluczem prywat-

[11] *K. Szaniawski*, *T. Kościelny*, Ustawa o podpisie, s. 30.
[12] *R. Kaszubski*, *A. Koniewicz*, Podpis elektroniczny, Glosa 2001, Nr 5, s. 3.
[13] *K. Szaniawski*, *T. Kościelny*, Ustawa o podpisie, s. 30.
[14] Tamże, s. 32.

nym, do konkretnej osoby fizycznej[15]. Na PKI składają się urzędy certyfikacji (*Certification Authority*), określane również mianem zaufanej osoby trzeciej (*Trusted Third Party*) lub jednostki certyfikacyjnej albo podmiotu świadczącego usługi certyfikacyjne, które wystawiają, zawieszają i unieważniają certyfikaty.

Infrastruktura Klucza Publicznego jest rozbudowaną strukturą hierarchiczną, na którą z reguły składają się trzy poziomy zaufanych osób trzecich. Najważniejszą jednostkę stanowi główny urząd certyfikacji (*Root Certificate Authority*), będący podstawą zaufania dla wszystkich podmiotów świadczących usługi certyfikacyjne, posługujący się wydanym i podpisanym przez siebie certyfikatem określanym mianem certyfikatu samopodpisanego (*Self Signed Certificate*), certyfikujący urzędy usytuowane niżej w hierarchii. Drugi poziom struktury tworzą pośrednie urzędy certyfikacji wystawiające certyfikaty tylko dla innych jednostek certyfikacyjnych i grupujące zaufane osoby trzecie oferujące podobny stopień zaufania i odpowiedzialności. Najniżej w hierarchii usytuowane są końcowe urzędy certyfikacji wydające certyfikaty należące do różnych klas, w zależności od stopnia ich zabezpieczenia dla podmiotów chcących posługiwać się podpisami cyfrowymi[16].

Końcowa jednostka certyfikacyjna realizuje zasadniczo dwa zadania. Po pierwsze, wystawia certyfikaty, co obejmuje wygenerowanie klucza asymetrycznego dla sygnatariusza albo sprawdzenie prawidłowości klucza przedstawionego przez niego, identyfikację i potwierdzenie tożsamości osoby ubiegającej się o certyfikat, stworzenie certyfikatu oraz opatrzenie go podpisem kryptograficznym urzędu certyfikacji. Po drugie, potwierdza ważność certyfikatu na wniosek podmiotu polegającego na podpisie elektronicznym.

Certyfikat jest elektronicznym zaświadczeniem zawierającym klucz publiczny podpisującego oraz liczne informacje, w szczególności zaś wskazanie tożsamości osoby będącej posiadaczem klucza publicznego i ewentualnie innych jej atrybutów, oznaczenie urzędu certyfikacji wydającego certyfikat czy też określenie czasu ważności certyfikatu. Jak już wyżej wskazano, jednostka certyfikacyjna ma obowiązek przed wystawieniem certyfikatu dokonać pewnej identyfikacji podmiotu ubiegającego się o niego. W rezultacie w obrocie elektronicznym certyfikat stanowi swoisty rodzaj dokumentu tożsamości[17].

Nadawca wiadomości elektronicznej podpisanej cyfrowo dołącza do niej swój certyfikat i wysyła odbiorcy, który korzystając z ogólnie dostępnego klu-

[15] *J. Janowski*, Podpis elektroniczny, s. 74.

[16] *M. Marucha-Jaworska*, Podpis elektroniczny, Warszawa 2002, s. 35–36; *J. Janowski*, Podpis elektroniczny, s. 77.

[17] *Ł. Neuman*, *M. Świerczyński*, Podpis elektroniczny – prawne i techniczne objaśnienie pojęć, MoP 2001, Nr 11, s. 592.

cza publicznego jednostki certyfikacyjnej, sprawdza, czy certyfikat rzeczywiście został wystawiony przez zaufaną osobę trzecią, czy nie upłynął okres, na który go wystawiono, wreszcie czy widnieje na liście certyfikatów zawieszonych lub unieważnionych, ustalając tym samym autentyczność i ważność certyfikatu. Następnie przechodzi on do omówionej już weryfikacji podpisu asymetrycznego. Infrastruktura Klucza Publicznego jest również wykorzystywana do szyfrowania dokumentu, gdyż ta sama para kluczy użyta w odwrotnej konfiguracji służy do utajnienia przesyłanej wiadomości[18], czyniąc ją niemożliwą do odczytania przez nieuprawnione osoby trzecie.

W literaturze wskazano pięć cech podpisu cyfrowego opartego na PKI, które zadecydowały o jego komercyjnym zastosowaniu. Wskazany podpis charakteryzuje się więc: unikalnością i niepowtarzalnością, niemożliwością podrobienia, łatwością wygenerowania i weryfikacji, jak również niedopuszczalnością wyparcia się podpisującego jego złożenia[19]. Podpis cyfrowy oparty na PKI umożliwia zaszyfrowanie przesyłanego dokumentu elektronicznego, pozwala na ustalenie tożsamości podpisującego, nadto zapewnia integralność opatrzonych nim danych. Wszystko to gwarantuje wysoki stopień bezpieczeństwa dokonywanej czynności prawnej. Sygnatariusz powinien jednak przedsięwziąć niezbędne środki ostrożności, by zapewnić poufność klucza prywatnego, gdyż w razie jego ujawnienia nieuprawnionej osobie trzeciej będzie ona mogła fałszować dokumenty.

II. Podpis mobilny

Podpis mobilny jest szczególnym rodzajem podpisu cyfrowego. Zasadnicza różnica polega na tym, że składa się go za pomocą telefonu komórkowego i karty SIM (*Subscriber Identity Module* – Moduł Identyfikacji Abonenta), a nie z wykorzystaniem komputera, czytnika kart i mikroprocesorowej karty kryptograficznej. Stosowanie podpisu mobilnego nie jest jednak obecnie szerokie, lecz z uwagi na powszechność posługiwania się telefonami komórkowymi przez podmioty prawa może w przyszłości takim się stanie.

[18] *P. Polański*, Podpisy elektroniczne, s. 86.

[19] *R. Wegenek*, *G. O'Neill*, *J. Moore*, E-Commerce, A Guide to the Law of Electronic Business, Third Edition, London 2002, s. 26.

III. Podpis biometryczny

Podpis biometryczny to digitalizacja charakterystycznej cechy biometrycznej człowieka[20], która może być jego biometryczną cechą fizyczną (tęczówka, siatkówka oka, geometria twarzy, dłoni, linie papilarne, barwa głosu, układ linii krwionośnych dłoni) lub jego biometryczną cechą behawioralną (sposób: mówienia, składania podpisu własnoręcznego, pisania na klawiaturze), pozwalająca na identyfikację osoby fizycznej. Urządzenia do badania właściwości biometrycznych mierzą określoną cechę człowieka i sprowadzają ją do formatu danych elektronicznych, co często jest określane mianem procesu digitalizacji[21], po czym są porównywane z uprzednio pobranymi danymi dotyczącymi tej cechy przechowywanymi w istniejącej bazie danych.

Wskazane urządzenia są wykorzystywane w różnych dziedzinach, w szczególności w: bezpiecznej bankowości, wymiarze sprawiedliwości, administracji publicznej do identyfikacji właścicieli paszportów lub dowodów osobistych oraz przedsiębiorstwach lub innych organizacjach jako metoda chroniąca pomieszczenia lub komputery bądź inne urządzenia przed dostępem do nich nieuprawnionych osób trzecich. Składanie podpisu biometrycznego w celu sygnowania złożonego oświadczenia woli nie jest jednak obecnie rozpowszechnione.

Podpis biometryczny pozwala na identyfikację sygnatariusza, lecz nie zapewnia integralności danych nim opatrzonych, dlatego też w literaturze proponuje się obecnie połączenie stosowania przedmiotowej sygnatury z podpisem cyfrowym. Dokument podpisany biometrycznie lub zawierający digitalizację cech biometrycznych mógłby następnie zostać opatrzony podpisem kryptograficznym, co gwarantowałoby wykrywalność jakichkolwiek zmian dokonanych w jego treści[22]. Nadto, wskazuje się, że podpis biometryczny można wykorzystać w procesie składania podpisu cyfrowego opartego na PKI zamiast numeru PIN zabezpieczającego dostęp do klucza prywatnego przechowywanego na karcie kryptograficznej, ze względu na fakt, iż przedmiotowy numer łatwiej jest odgadnąć lub bezprawnie wejść w jego posiadanie w porównaniu z uzyskaniem dostępu do cech biometrycznych (np. odcisku palca lub dłoni) osoby fizycznej[23].

Posługiwanie się podpisem biometrycznym ma wiele zalet, lecz również wad. W szczególności zdarza się, iż system oparty na urządzeniach badających cechy biometryczne daje błędne rezultaty, mylnie identyfikując podmiot jako oznaczoną osobę, mimo że nią nie jest, albo nie przypisując podmiotowi określ-

[20] *J. Janowski*, Podpis elektroniczny, s. 39.

[21] *L. Brazell*, Electronic Signatures Law and Regulation, London 2004, s. 39.

[22] Tamże, s. 40; *P. Polański*, Podpisy elektroniczne, s. 90.

[23] *L. Brazell*, Electronic Signatures, s. 40; *P. Polański*, Podpisy elektroniczne, s. 90; *R. Podpłoński*, *P. Popis*, Podpis elektroniczny, Komentarz, Warszawa 2004, s. 44.

lonej tożsamości, chociaż ją posiada. Nadto, istnieje ryzyko bezprawnego ujawnienia lub kradzieży danych dotyczących cech biometrycznych człowieka z baz danych, w których są one przechowywane, i wykorzystania ich w różnych celach przez podmioty nieuprawnione, co może mieć dla osoby fizycznej poważne, negatywne konsekwencje w wielu sferach życia. Wydaje się więc, że niektóre osoby nie będą chciały posługiwać się wskazaną technologią z uwagi na obawę naruszenia ich prawa do prywatności lub inne względy.

IV. Biometryczny podpis własnoręczny.

Biometryczny podpis własnoręczny (*Biodynamic version of manuscript signature*) to szczególny rodzaj podpisu biometrycznego charakteryzujący się badaniem dynamiki pisma manualnego[24]. Sygnatariusz składa podpis za pomocą bezprzewodowego pióra elektronicznego na specjalnej podkładce (*pad*, *tablet*) połączonej z komputerem lub wbudowanej w niego. Podpis jest odtwarzany na monitorze komputera. W czasie jego składania urządzenie mierzy i zapisuje cechy biometryczne pisma, takie jak: prędkość, miarowość, forma, kolejność pociągnięć, dynamika, które są charakterystyczne dla podpisującego. Plik obejmujący wskazane dane może zostać dołączony do dokumentu elektronicznego jako podpis elektroniczny sygnatariusza[25].

Mając na względzie kryterium sposobu składania podpisu, należy uznać, że biometryczny podpis własnoręczny jest najbardziej zbliżony do tradycyjnego podpisu odręcznego, różnica zaś polega jedynie na tym, że w miejsce długopisu i papieru używa się pióra elektronicznego i podkładki połączonej z komputerem. Za wadę wskazanego rozwiązania można jednak uznać to, iż plik obejmujący przedmiotowy podpis może zostać skopiowany przez nieuprawnioną osobę trzecią i bezprawnie przez nią wykorzystany. Obecnie stworzono już metody zapewniające za pomocą algorytmu skrótu i znakowania czasem integralność dokumentu sygnowanego biometrycznym podpisem własnoręcznym[26], lecz nie są one rozpowszechnione.

Nieco podobnym, jednak niemającym charakteru biometrycznego, gdyż niemierzącym i niezapisującym cech dynamiki pisma, jest podpis elektroniczny napisany piórem cyfrowym, które zapisuje pismo ręczne w formie elektronicznej

[24] *S. Mason*, The International Implications Of Using Electronic Signatures, Computer and Telecommunications Law Review, Vol. 11, No. 5, 2005, s. 160; *P. Polański*, Podpisy elektroniczne, s. 90.

[25] *S. Mason*, The International, s. 160.

[26] *P. Polański*, Podpisy elektroniczne, s. 91.

i odtwarza je na monitorze urządzenia elektronicznego, w szczególności komputera.

V. Podpis hasłowy

Podpis hasłowy to hasło, w szczególności numer PIN[27], które w połączeniu z nazwą użytkownika jest szeroko wykorzystywany do identyfikacji podmiotu i uwierzytelniania transakcji w obrocie elektronicznym[28]. Może on zostać stworzony i dostarczony osobie fizycznej przez podmiot profesjonalnie się tym trudniący, w tym bank lub organ administracji publicznej albo osoba zainteresowana posługiwaniem się nim może samodzielnie go wygenerować, chcąc np. dokonywać zakupów na aukcji internetowej[29]. Hasło może zostać podejrzane lub wykradzione przez nieuprawnioną osobę trzecią, dlatego też stosuje się rozmaite zabezpieczenia mające na celu zapobieżenie bezprawnemu ujawnieniu podpisu hasłowego.

Podpis hasłowy sprawdza się w systemach zamkniętych, w szczególności w bankowości, gdyż w połączeniu z szyfrowaniem danych pozwala on na identyfikację osoby i uwierzytelnienie transakcji[30]. Jak już wyżej wskazano, stosuje się go również do zabezpieczenia dostępu do klucza prywatnego przechowywanego na karcie kryptograficznej służącego do składania podpisu cyfrowego.

VI. Skanowany podpis własnoręczny

Skanowany podpis własnoręczny (*scanned manuscript signature*), nazywany również krócej podpisem skanowanym, stanowi cyfrową postać tradycyjnego podpisu własnoręcznego napisanego na papierze, po czym zeskanowanego, tak by stworzył elektroniczny obraz podpisu odręcznego na monitorze, który można zamieścić pod treścią oświadczenia ujętego w dokumencie elektronicznym. Wskazany podpis służy wprawdzie do identyfikacji sygnatariusza, lecz nie zapewnia integralności danych nim opatrzonych, nadto łatwo może zostać zeskanowany z dokumentu sporządzonego na papierze, w tym listu, albo skopiowany z dokumentu elektronicznego i użyty bezprawnie przez osobę trzecią.

---

[27] *J. Janowski* uznaje podpis PIN-owy, czyli składany za pomocą osobistego numeru identyfikacyjnego, razem z numerem karty płatniczej, w celu np. potwierdzenia dyspozycji, za odrębny rodzaj podpisu elektronicznego. *J. Janowski*, Podpis elektroniczny, s. 39.

[28] *P. Polański*, Podpisy elektroniczne, s. 91; *L. Brazell*, Electronic Signatures, s. 37.

[29] *P. Polański*, Podpisy elektroniczne, s. 91.

[30] Tamże, s. 92.

VII. Podpis klawiaturowy

Podpis klawiaturowy to imię i nazwisko lub samo nazwisko bądź pseudonim napisany przez sygnatariusza pod treścią oświadczenia zawartego w dokumencie elektronicznym. Wskazany podpis służy do identyfikacji podpisującego, lecz nie pozwala na pewne ustalenie jego tożsamości i nie gwarantuje też integralności danych nim opatrzonych. Jednak, mimo że nie zapewnia on wysokiego stopnia wiarygodności i autentyczności sygnowanego nim dokumentu, jest wszakże powszechnie stosowany przy składaniu oświadczeń w treści e-maila wysyłanego za pomocą poczty elektronicznej.

W przypadku posługiwania się podpisem klawiaturowym jego pochodzenie od określonego nadawcy może zostać dodatkowo uwierzytelnione wysłaniem wiadomości elektronicznej z oznaczonego adresu mailowego lub łącznie z tekstem uprzedniej korespondencji prowadzonej z adresatem bądź przez posłużenie się w nagłówku albo innej części dokumentu znakiem firmowym osoby prawnej lub logiem przedsiębiorstwa, jak również przez potwierdzenie za pomocą innego środka komunikacji, w tym telefonu, faktu złożenia i przesłania oświadczenia e-mailem[31]. Wskazane dodatkowe zabezpieczenia, w szczególności wysłanie e-maila z określonego adresu poczty elektronicznej bądź posłużenie się znakiem firmowym podmiotu, są jednak łatwe do podrobienia przez nieuprawnioną osobę trzecią.

Mimo braku zapewnienia wysokiego stopnia bezpieczeństwa transakcji przez podpis klawiaturowy samodzielnie lub łącznie z innymi metodami jest on w pewnych stosunkach wystarczająco wiarygodny i stosowany do sygnowania składanych oświadczeń, w tym również oświadczeń woli (np. do złożenia oraz przyjęcia ofert i zamówień między przedsiębiorcami).

VIII. Kliknięcie na ikony „Akceptuję", „Zgadzam się" lub „Tak" na stronie internetowej

Kliknięcie na ikony „Akceptuję", „Zgadzam się", „Tak" lub „OK" bądź inną podobną (*clicking the „I accept" or „I agree" icon*), umieszczone na stronie internetowej, również może stanowić złożenie podpisu elektronicznego[32]. Wskazany podpis elektroniczny jest składany m.in. przez użytkowników stron sklepów internetowych w celu zaaprobowania ogólnych warunków umów stosowanych przez przedsiębiorcę oraz wyrażenia woli zawarcia umowy sprzedaży określo-

[31] Tamże, s. 92–93.

[32] *L. Brazell*, Electronic Signatures, s. 39; *S. Mason*, Electronic Signatures in Law, London 2003, s. 81.

nych towarów i usług. Kliknięcie na ikonę generuje dane elektroniczne (bity), które są logicznie powiązane z innymi danymi elektronicznymi stanowiącymi np. zamówienie określonej rzeczy z listy towarów i usług dostępnych u przedsiębiorcy[33]. Ustalenie tożsamości podmiotu następuje m.in. przez zarejestrowanie się użytkownika w systemie za pomocą loginu i hasła przed dokonaniem przez niego czynności lub na podstawie danych osobowych zawartych w formularzu wypełnionym przez kupującego, a w przypadku płatności kartą kredytową – również w oparciu o dane dotyczące jej właściciela. Kliknięcie na przedmiotową ikonę może wyrażać wolę dokonania czynności prawnej również w systemach aukcyjnych (np. umowa sprzedaży rzeczy) i bankowych (np. umowa lokaty terminowej), po uprzedniej rejestracji do systemu odpowiednio użytkownika serwisu i klienta banku.

Podsumowując, pojęcie podpisu elektronicznego jest obecnie rozumiane bardzo szeroko i w sposób technologicznie neutralny, zatem można go złożyć za pomocą rozmaitych technik. W praktyce podmioty prawa posługują się licznymi rodzajami podpisów elektronicznych, które zapewniają różny stopień wiarygodności pochodzenia podpisu od oznaczonego sygnatariusza oraz autentyczności opatrzonego nim dokumentu.

Pewną identyfikację podpisującego i integralność danych elektronicznych gwarantuje stosowanie podpisu cyfrowego lub jego szczególnego rodzaju, tj. podpisu mobilnego. Natomiast podpis biometryczny, w tym własnoręczny podpis biometryczny, zapewnia ustalenie tożsamości sygnatariusza, lecz nie pozwala na wykrycie zmian dokonanych w dokumencie po jego sygnowaniu i wysłaniu. Wskazaną funkcję mógłby on pełnić jedynie w połączeniu z inną technologią umożliwiającą jej realizację. W literaturze wyrażono wszakże pogląd, że podpis biometryczny należy uznać za bezpieczny[34].

Podpis hasłowy stosowany w systemach zamkniętych, zwłaszcza w połączeniu z szyfrowaniem danych, pozwala na wiarygodną identyfikację sygnatariusza i uwierzytelnienie dokonanej czynności. Natomiast w porównaniu z wyżej wskazanymi podpisami skanowany podpis własnoręczny i podpis klawiaturowy gwarantują zdecydowanie mniejszy stopień pewności co do integralności dokumentu i jego pochodzenia od oznaczonego nadawcy. Jednak wiele podmiotów prawa w różnych stosunkach i sytuacjach uznaje podpis klawiaturowy złożony

[33] *L. Brazell*, Electronic Signatures, s. 39.

[34] Tak *P. Polański*, Podpisy elektroniczne, s. 109; *L. Brazell*, Electronic Signatures, s. 49. Odmienny pogląd wyraził *S. Mason*, uzasadniając swoją opinię możliwością łatwego ujawnienia cech biometrycznych osoby fizycznej i ewentualnymi poważnymi negatywnymi skutkami ich bezprawnego wykorzystania. *S. Mason*, Electronic Signatures, s. 96–99.

pod oświadczeniem wysłanym e-mailem za wystarczająco wiarygodny, co w sumie zdecydowało o jego powszechnym stosowaniu.

§ 2. Podstawowe modele regulacji prawnej podpisu elektronicznego

Mając na względzie sposób i zakres normowania oraz podejście do technologii tworzenia podpisu elektronicznego, można wyróżnić trzy podstawowe modele regulacji prawnej podpisu elektronicznego: podpisu cyfrowego, minimalistyczny i dwutorowy[35].

I. Model podpisu cyfrowego

Model podpisu cyfrowego (*digital signature approach*, *prescriptive approach*, *mandatory approach*), określany również mianem rygorystycznego, charakteryzuje się tym, że normuje tylko jedną technologię tworzenia podpisu elektronicznego, tj. technikę podpisu cyfrowego. Wskazane podejście jest technologicznie zależne. W akcie w sposób szczegółowy reguluje się przede wszystkim problematykę podpisu cyfrowego, nadto często obszernie normuje się również zagadnienia dotyczące urzędów certyfikacji i Infrastruktury Klucza Publicznego[36]. Ustawa może przy tym wyznaczać technologię podpisu cyfrowego jako standard techniczny, zapewniający bezpieczne uwierzytelnianie danych, jednocześnie nie wskazując skutków prawnych wywoływanych przez podpis cyfrowy, ani nie normując jego statusu prawnego i dowodowego. Stanowi to wówczas wariant techniczny modelu, przykładowo zastosowany w Niemczech w 1997 r.

Prawodawcy najczęściej jednak sięgają po wariant prawny charakteryzujący się uznaniem na gruncie prawa podpisu cyfrowego opartego na kwalifikowanym certyfikacie wystawionym przez autoryzowany urząd certyfikacji za równoważny pod względem skutków prawnych podpisowi własnoręcznemu. Nadto, w przywołanych regulacjach wprowadza się niekiedy domniemania prawne dotyczące podpisu cyfrowego czyniącego zadość przytoczonym wyżej przesłankom. W ustawach opierających się na przedmiotowym podejściu pomija się przy tym kwestię spełnienia przez zapis elektroniczny prawnego wymo-

[35] Wskazany podział zaproponowali *B. Aalberts* i *S. van der Hof* w publikacji poświęconej analizie modeli regulacji prawnej podpisu elektronicznego. *B. Aalberts*, *S. van der Hof*, Digital Signature Blindness Analysis of Legislative Approaches to Electronic Authentication, The EDI Law Review, No. 7, 2000, s. 16.

[36] Tamże, s. 17.

gu pisma, przez co nie normują one problematyki formy czynności prawnych w sposób całościowy. Warto jednak zaznaczyć, że wariant prawny modelu zastosowano przykładowo w pierwszym na świecie akcie prawnym dotyczącym instytucji podpisu elektronicznego uchwalonym w stanie Utah w 1995 r. czy też we Włoszech w 1997 r.

Model podpisu cyfrowego wykorzystano wprawdzie w ustawodawstwie krajowym, natomiast nigdy nie posłużono się nim w regulacjach międzynarodowych i wspólnotowych. Wskazane podejście było często stosowane w pierwszych aktach normatywnych dotyczących instytucji podpisu elektronicznego, lecz w niedługim czasie zaczęto od niego odchodzić. W sumie model podpisu cyfrowego wykorzystano zarówno w porządkach prawnych opartych na systemie *common law* (stan Utah), jak i *ius civile* (Niemcy, Włochy)[37].

Zaletą podejścia rygorystycznego jest pewność prawa uzyskiwana przez wprowadzenie aktu szczegółowo normującego podpis cyfrowy i PKI oraz wskazującego w wariancie prawnym status i skutki prawne takiego podpisu. Za atut modelu należy także uznać, iż prawodawca, znając właściwości, możliwości i wady technologii podpisu cyfrowego, może przewidzieć rozwiązania prawne, które zapewnią bezpieczeństwo obrotu prawnego i gospodarczego[38].

Natomiast minusem modelu rygorystycznego jest brak uznania prawnego i uwzględnienia innych znanych lub mogących powstać w przyszłości technologii tworzenia podpisu elektronicznego. Z uwagi na dynamiczny rozwój techniczny w niedługim czasie może bowiem okazać się, że inna technologia niż preferowana przez ustawodawcę służy osiągnięciu stawianych przez niego celów lub znajdzie w praktyce większe zastosowanie, a wówczas racjonalny prawodawca powinien zmienić akt tak, by je uwzględnić. Zatem przyjęcie modelu technologicznie zależnego potencjalnie wiąże się z częstą modyfikacją ustawodawstwa, co należy uznać za wadę podejścia. Wprowadzenie modelu podpisu cyfrowego nie sprzyja lub wręcz może hamować rozwój innych technik generowania podpisu elektronicznego oraz korzystanie z nich przez uczestników obrotu elektronicznego[39]. Nadto, wskazane podejście może okazać się nieadekwatne do rzeczywistości w przypadku, gdy preferowana technologia będzie miała znikome zastosowanie. Model podpisu cyfrowego może też zakłócić naturalny rozwój rynku[40].

---

[37] *B. Aalberts*, *S. van der Hof*, Digital Signature, s. 19.

[38] Tamże, s. 8.

[39] *S. Fischer*, Saving Rosencrantz And Guildenstern In A Virtual World? A Comparative Look At Recent Global Electronic Signature Legislation, 7 Boston University Journal of Science and Technology Law 229, Summer 2001, s. 236.

[40] *B. Aalberts*, *S. van der Hof*, Digital Signature, s. 9.