Rejent * rok 11 * nr 12(128)
grudzień 2001 r.

Dariusz Szostek

Dyrektywa Parlamentu Europejskiego i Rady Europy w sprawie podpisu elektronicznego

Wprowadzenie

Współcześnie wiele państw i organizacji (w tym także Polska) podejmuje działania mające na celu wprowadzenie do światowego obrotu gospodarczego możliwości zawierania umów z wykorzystaniem podpisu elektronicznego[1].

Problematyka związana z elektroniczną wymianą i przesyłaniem danych znalazła się w kręgu zainteresowania Komisji Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego (UNCITRAL), która doprowadziła do uchwalenia przez Zgromadzenie Ogólne Narodów Zjednoczonych na 29 sesji w czerwcu 1996 r. modelowej ustawy Jednolitego Prawa Elektronicznego Przesyłania Danych (zwanej EDI od angielskiego określenia *Electronic Data Interchange*[2]). Uchwalenie ustawy modelowej

---

[1] Pierwszym na świecie aktem, w którym *expressis verbis* został dopuszczony do obrotu prawnego podpis elektroniczny, była ustawa o podpisach cyfrowych stanu Utah (USA), uchwalona w 1995 r. Patrz J. J a c y s z y n, *Elektroniczne czynności prawne*, Przegląd Prawa Handlowego 1999, nr 7, s. 30 w przypisie.

[2] Tekst ustawy Model Law on Electronic Commerce of United Nations Commission on International Trade Law został opublikowany w języku angielskim i francuskim w Raportach UNCITRAL Dokumenty Oficjalne Zgromadzenia Ogólnego ONZ, Suplement nr 17 (A/50/17) oraz Suplement nr 17 (A/51/17) New York 1996. Patrz także http://www.un.or.at/uncitral/. Tłumaczenie ustawy w języku polskim dostępne w: W. K o c o t, *Zawieranie umów sprzedaży według Konwencji Wiedeńskiej*, Warszawa 1998, s. 269-277.

miało olbrzymie znaczenie – stała się ona wzorcem, na którym oparło się wiele państw w trakcie tworzenia ustaw krajowych, regulujących kwestie podpisu elektronicznego. Jednym z celów ustawy było ustanowienie wzorca, który poprzez wprowadzenie do wewnętrznych systemów prawnych państw członków ONZ miał spowodować ujednolicenie i stypizowanie rozwiązań prawnych, a przez to umożliwić i nadać skuteczność kontraktom zawieranym poprzez elektroniczne nośniki informacji[3]. I tak już jesienią 1997 r. Amerykański Kongres uwzględnił szereg rozwiązań wzorcowej ustawy UNCITRAL przy uchwalaniu zmian II rozdziału Jednolitego Kodeksu Handlowego[4].

Nie tylko Organizacja Narodów Zjednoczonych dostrzegła potrzebę ujednolicenia prawa w zakresie handlu i podpisu elektronicznego. Dosyć szybko taką potrzebę dostrzegła także Unia Europejska: „Handel elektroniczny ma szansę stać się głównym stymulatorem światowej gospodarki w następnym stuleciu, ale dla wykorzystania tej szansy w Europie niezwykle istotne jest bezpieczeństwo transakcji"[5]. Już w 1994 r. w tzw. Raporcie Bangemanna[6] rozwój informatyki oraz usług Społeczeństwa Informatycznego[7]

[3] Patrz W. K o c o t, *Zawarcie umowy w drodze elektronicznej wymiany informacji*, Przegląd Prawa Handlowego 1998, nr 4, s. 6. Ramy niniejszego artykułu nie pozwalają na przeprowadzenie dokładniejszej analizy pojęcia „elektroniczne nośniki informacji".

[4] Tamże s. 14 w przypisie. Projekt tego aktu został opublikowany przez National Conference of Commissioners on Uniform State Laws 1995 by The American Law Institute and NCCUSL.

[5] Z materiałów prasowych Rady Sekretariatu Generalnego Unii Europejskiej z 2140 posiedzenia Rady – Telekomunikacja, Bruksela 27 listopada 1998 r.

[6] Raport Bangemanna został przygotowany przez międzynarodowy zespół w składzie: Martin Bangemann, Enrico Cabral da Fonseca, Peter Davis, Carlo de Benedetti, Pehr Gyllenhammar, Lothar Hunsel, Pierre Lescure, Pascual Maragall, Gaston Thorn, Candido Velazquez-Gastelu, Peter Bonfield, Etienne Davignon, Jean-Marie Descarpentries, Brian Ennis, Hans-Olaf Henkel, Anders Knutsen, Constantin Makropoulos, Romano Prodi, Jan Timmer, Heinrich von Pierer. Patrz: Europe and the global information society Recommendations to the European Council, Bruksela 26 maja 1994. Patrz także na temat raportu M. K o n d r a t, *Regulacje wspólnotowe dotyczące internetu*, Prawo Unii Europejskiej 2000, nr 1, s. 23 oraz Evolution of the Internet and the www in Europe, Final Raport for European Commission DG XII Oct. 1997.

[7] Po raz pierwszy definicja Społeczeństwa Informatycznego pojawiła się w Dyrektywie 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustalającej procedurę dostarczania informacji w dziedzinie standardów technicznych i regulacji zmienionej Dyrektywą 98/48/WE Parlamentu Europejskiego i Rady z dnia 20 listopada 1998 r. w sprawie ochrony prawnej usług opartych lub polegających na dostępie warunkowym. Definicja za-

został potraktowany jako środek do uzyskania wzrostu gospodarczego i zmniejszenia bezrobocia[8].

W latach 1997-1999 na starym kontynencie odpowiednie uregulowania przyjęły między innymi Niemcy (1997)[9] Włochy (1997), natomiast inne kraje podjęły działania w celu uchwalenia odpowiednich aktów prawnych

---

warta w tej Dyrektywie określa, iż usługami Społeczeństwa Informatycznego (w polskiej literaturze używane jest także sformułowanie „usługa informacyjna") są usługi zwykle świadczone za lub w zamian za wynagrodzenie, na odległość poprzez sieć, przy pomocy wyposażenia elektronicznego dla przetwarzania (w tym kompresji cyfrowej) i przechowywania danych i na indywidualne zamówienie otrzymującego usługę. Podobna definicja została zaproponowana w artykule 2 pierwszej wersji propozycji Dyrektywy Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych handlu elektronicznego na jednolitym rynku (propozycja Dyrektywy w tłumaczeniu na język polski http://www.mg.gov.pl/structur/hand-usl/dyrektyw.htm), zgodnie z którą „usługami Społeczeństwa Informatycznego są wszelkie usługi normalnie świadczone w zamian za wynagrodzenie, na odległość, przy pomocy środków elektronicznych i na indywidualne zapotrzebowanie usługobiorcy" – gdzie „na odległość" oznacza, że usługa jest świadczona bez jednoczesnej obecności stron; „przy pomocy środków elektronicznych" oznacza, że usługa jest wysłana i odebrana w miejscu przeznaczenia przy pomocy wyposażenia elektronicznego służącego do przetwarzania i przechowywania danych oraz w całości transmitowana, przeniesiona i otrzymana przez kabel, drogą radiową, przez środki optyczne lub inne środki elektromagnetyczne. Ostatecznie w uchwalonej Dyrektywie 2000/31/EC Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych handlu elektronicznego na jednolitym rynku przyjęto definicję określoną w Dyrektywie 98/34/WE (w art. 2 pkt a następuje bezpośrednie odesłanie do Dyrektywy 98/34/WE zmienionej przez Dyrektywę 98/48/WE). Problematyka pojęcia „usługi informacyjnej" została omówiona w: D. K o t, *Dyrektywa o handlu elektronicznym i jej implikacje dla prawa cywilnego*; Kwartalnik Prawa Prywatnego 2001, nr 1, s. 47-50. Patrz także: *Zmieniona propozycja Parlamentu Europejskiego i Rady na temat niektórych aspektów handlu elektronicznego na Jednolitym Rynku*; http://www.mg.gov.pl/structur/hand-usl/dyrektyw.htm.; A.M. W i l k, [w]: *Internet fenomen społeczeństwa informacyjnego*, red. T. Zasępa, Częstochowa 2001, s. 146.

[8] Należy zwrócić uwagę, iż Wspólnota Europejska jest zaangażowana w działania mające na celu regulacje handlu elektronicznego od ponad dekady. Fundamenty pod działalność Wspólnoty w tym zakresie zostały położone w 1987 roku wraz z uruchomieniem programu TEDIS Electronic Data Interchange, którego głównym celem było zachęcanie przedsiębiorców do wykorzystywania w handlu elektronicznych nośników informacji. Patrz J. D i c k i e, *Internet and Electronic Commerce Law in the European Union*, Oregon 1999, s. 3; a także: Dziennik Urzędowy OJ 1987 L 285/1.

[9] Niemcy były pierwszym europejskim krajem, który uchwalił ustawę o podpisie elektronicznym, a mianowicie ustawę o regulacji warunków ramowych dla usług informacyjnych i komunikacyjnych z dnia 22 lipca 1997 r. (Gesetz über die Nutzung von Telediensten – w skrócie TDG); regulacja dotycząca podpisu elektronicznego została zawarta w pkt 3 § 16

(aktualnie większość państw europejskich uchwaliła odpowiednie regulacje dotyczące kwestii podpisu elektronicznego)[10]. Wprowadzanie przez poszczególne państwa własnych uregulowań dotyczących handlu elektronicznego i podpisu elektronicznego stworzyło niebezpieczeństwo powstania szeregu odmiennych od siebie rozwiązań (systemów) dotyczących *electronic commerce*[11], co w znacznym stopniu mogło ograniczyć rozwój handlu elektronicznego w stosunkach międzynarodowych. Brak ujednoliconych zasad dotyczących handlu elektronicznego w Unii Europejskiej poważnie zwiększał koszt działania operatorów elektronicznych nośników informacji, pragnących rozwijać działalność poza granicami swego państwa. Szczególnie wysokim kosztem okazała się obsługa prawna w związku z wprowadzeniem usług Społeczeństwa Informatycznego na zagraniczne rynki[12].

---

tegoż aktu (Signaturgesetz – SigG w: Federalny Dziennik Ustaw BGBL 1997, cz. I, nr 52 z dnia 28 lipca 1997 r., a także http//www.bmbf.de; http//www.iid.de) oraz w rozporządzeniu dotyczącym podpisu elektronicznego (Verordnung zur digitalen Signatur – Signatur-verordnung – SigV) z dnia 8 października 1997 r., wydanego przez Rząd Federalny na podstawie § 16 ustawy o podpisie elektronicznym. W 2001 r. ustawa to została uchylona (jako sprzeczna z Dyrektywą Unii Europejskiej), a w jej miejsce została uchwalona nowa ustawa Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (ustawa z dnia 16 maja 2001 r., BGBL 2001, cz. I, nr 22 z dnia 21 maja 2001 r., poz. 876). Obok ustawy dotyczącej podpisu elektronicznego z dnia 13 lipca 2001 r. uchwalono ustawę dotyczącą nowej elektronicznej formy Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (BGBL 2001, cz. I, nr 35 z dnia 18 lipca 2001 r., poz. 1542).

[10] Szerzej na ten temat D. S z o s t e k, *Przegląd ustawodawstwa w zakresie podpisów elektronicznych*; [w:] *Ekonomiczne, społeczne i ekologiczne problemy procesu transformacji*, red. J. Siemianowicz, Katowice 2001, s. 459-464.

[11] Definicja *electronic-commerce* (*e-commerce*) odnosi się do handlu elektronicznego. Według Światowej Organizacji Handlu (WTO) *e-commerce* to produkcja, reklama, sprzedaż i dystrybucja towarów poprzez sieci teleinformatyczne. Za instrumenty gospodarki elektronicznej są uznawane telefon, telefax, telewizja, elektroniczna wymiana danych (EDI) oraz internet, w tym poczta elektroniczna. Patrz: *Secrets of Electronic Commerce A Guide for Small – and Medium – Sized Exporters*, wyd. International Trade Centre UNCTAD/WTO Genewa 2000, Doc.No. ITC290/1B/00-VII-TP, s. 2. Patrz także J. D i c k i e, *Internet...,* s. 1-7; a także dokument OECD *Electronic Commerce Opportunities and Challenges for Government* (The „Sacher Report"), wyd. OECD Paryż 1997, s. 11; E. A t h a n a s e k o u, *UK Report on Information Technology,* [w:] *Internet European Compared Law*, red. G. Chatillon, Bruksela 2000, s. 83-85.

[12] Unia Europejska przeprowadziła ankietę wśród przedsiębiorców oferujących usługi związane z elektronicznymi nośnikami informacji (w skrócie ENI) w różnych krajach Wspól-

Operatorzy, aby prowadzić działalność na różnych rynkach, planowali swoje usługi w taki sposób, by były one kompatybilne oraz zgodne z uregulowaniami prawnymi wszystkich krajów członkowskich. Wysokość kosztów takiej działalności powodowała, iż usługi *e-commerce* poza granicami kraju mogły podejmować tylko duże i bogate firmy.

Mając powyższe na uwadze, Parlament Europejski wraz z Radą uchwalił[13] 13 XII 1999 r. Dyrektywę w sprawie wspólnotowych warunków ramowych dotyczących podpisu elektronicznego[14] (zwaną dalej Dyrektywą lub Dyrektywą dotyczącą podpisu elektronicznego)[15].

---

noty, która została rozprowadzona jako wkładka do Commercial Communications. W ankiecie tej przedsiębiorcy określili koszty związane z analizą systemu prawnego w zakresie *e-commerce* w krajach, w których zamierzali uruchomić swe usługi. Przykładowo jeden z operatorów stwierdził, iż korzysta z zewnętrznych porad prawnych w skali 50 godzin miesięcznie, co wynosi 70 000 DM rocznie; inny określił, iż do uruchomienia usługi w innym państwie potrzebuje ok. 50 dni własnych i zewnętrznych porad prawnych. Jeden z kluczowych operatorów na rynku handlu elektronicznego stwierdził, iż w swojej działalności musi opierać się na ośmiu własnych prawnikach, przeznaczających na analizę 45 godzin tygodniowo i 18 prawnikach zewnętrznych, świadczących średnio 175 godzin porad w tygodniu. Przegląd ram prawnych dla usługi tylko na rynku Zjednoczonego Królestwa kosztował go 60 000 ECU. Główne zagadnienia prawne podlegające analizie to prawa autorskie, ogólne wymagania w zakresie reklamy, kontraktów, oferty promocyjnej, nieuczciwej konkurencji, ochrony konsumenta, odpowiedzialności itp. Patrz uzasadnienie propozycji Dyrektywy Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych handlu elektronicznego na jednolitym rynku COM (1998) 586 final 98/0325 (COD) – tzw. pierwsza propozycja Dyrektywy.

[13] Dyrektywa ta w dużej mierze opiera się na wzorcowej ustawie UNCITRAL. Tak F. M o o s, [w:] *Handbuch zum Internet-Recht. Electronic Commerce, Informations, Kommunikations- und Mediendienste;* Berlin-Heidelberg-New York 2000*,* s. 23.

[14] Obok państw członkowskich Unii Europejskiej zasady Dyrektywy przyjęły także Islandia, Norwegia oraz Lichtenstein, dzięki czemu europejski rynek *e-commerce* stał się największym rynkiem, w ramach którego zostały ujednolicone zasady dotyczące podpisu elektronicznego (obejmuje on 370 milionów konsumentów). Należy przy tym zwrócić uwagę, iż kraje pretendujące do wejścia do UE, takie jak Polska, Czechy, Węgry, Estonia i Litwa, w ramach ujednolicania swojego prawa z prawem UE są zobowiązane do przyjęcia rozwiązań opartych na Dyrektywie, co jeszcze zwiększy wielkość tegoż rynku. Drugim co do wielkości rynkiem, w którym zostały ujednolicone zasady podpisu elektronicznego, jest USA (obejmuje on 260 milionów konsumentów). Wprawdzie rynek The North American Free Trade Association, w skład którego wchodzi m.in. USA, jest większy od rynku europejskiego, jednakże w jego ramach nie zostały do dnia dzisiejszego ujednolicone zasady podpisu elektronicznego. Patrz J. D i c k i e, *Internet...*, s. 1.

[15] Dyrektywa w tłumaczeniu na język polski: F. W e j m a n, *Przekład dyrektywy o wspól-*

1. Cel i zakres stosowania Dyrektywy[16]

Dyrektywa w sprawie wspólnotowych warunków dotyczących podpisu elektronicznego została uchwalona w celu ułatwienia stosowania podpisów elektronicznych i ma przyczynić się do ich prawnego uznania[17]. Ustala ona ramowe zasady prawne dla podpisów elektronicznych i określonych usług certyfikacyjnych w celu zapewnienia sprawnego funkcjonowania rynku wewnętrznego. Komunikacja elektroniczna oraz elektroniczny obrót handlowy wymagają stosowania podpisów elektronicznych, a także odpowiednich instrumentów potwierdzających autentyczność danych. Dotychczasowa różnorodność reguł prawnych państw członkowskich w powyższym zakresie (tj. uznawania podpisów elektronicznych oraz akredytacji podmiotów dokonujących certyfikacji) stanowiła istotną przeszkodę dla rozwoju elektronicznego obrotu handlowego. Uchwalenie Dyrektywy, a przez to uznanie podpisów elektronicznych, ma na celu ułatwienie rozwoju *electronic-commerce* oraz wzmocnienie zaufania do nowych technologii, a także przyczynienie się do ich powszechnej akceptacji[18].

Jednym z ważniejszych celów Dyrektywy jest stworzenie podstawowych zasad dotyczących podpisu elektronicznego dla zapewnienia swobodnego obrotu i przepływu towarów na rynku wewnętrznym[19], który jest zagwarantowany przez Traktat Wspólnoty Europejskiej (art. 14). Należy zwrócić uwagę, iż Traktat zapewnia pełną swobodę przepływu osób w ramach Wspólnoty, co powoduje, iż obywatele UE w coraz większym stopniu zostają „zmuszeni" do kontaktowania się (w tym do zawierania kontraktów) z podmiotami w innych państwach niż te, na których terytorium mają swoje miejsce zamieszkania. Ustalenie jednakowych reguł dotyczących

---

notowej infrastrukturze podpisów elektronicznych, Transformacje Prawa Prywatnego 2000, nr 1-2, s. 187 i nast.

[16] Niniejsza część artykułu oparta jest na materiałach uzyskanych od Ministerstwa Gospodarki.

[17] Jak sugeruje już sama nazwa Dyrektywy, nie jest jej celem wprowadzenie jednorodnego prawa, lecz prawnych ram dla państw członkowskich. Takie podejście wynika z wprowadzenia zasady neutralności technologicznej oraz faktu, iż w różnych krajach wykorzystuje się do generowania podpisów elektronicznych różne systemy i technologie. Patrz J. D i c k i e, *Internet...*, s. 37.

[18] Patrz uzasadnienie Dyrektywy.

[19] A. R o s s n a g e l, [w:] *Recht der Multimedia Dienste. Kommentar*, red. A. Rossnagel, München 2000, s. 99-100.

e-commerce oraz podpisu elektronicznego znacznie ułatwia i obniża koszty związane z komunikowaniem się, a także z dokonywaniem czynności na odległość[20].

Dyrektywa nie obejmuje aspektów związanych z zawieraniem i ważnością umów, w szczególności wymogów dotyczących formy, nie narusza też reguł ani ograniczeń prawa krajowego lub wspólnotowego, dotyczących wykorzystywania dokumentów (art. 1). Celem Dyrektywy jest określenie ram prawnych podpisu elektronicznego, a nie harmonizacja prawa krajowego w państwach członkowskich w zakresie zawierania i wykonywania umów.

W Dyrektywie nie zostały określone zasady i warunki ramowe dla podpisów elektronicznych, które są wykorzystywane wyłącznie w systemach opierających się na dobrowolnych, prywatnoprawnych porozumieniach zawieranych pomiędzy określoną liczbą osób (podmiotów)[21] – tak zwane „systemy zamknięte". W ramach takich systemów pierwszeństwo ma zasada swobody umów, dzięki której strony mogą same określić warunki i zasady, zgodnie z którymi akceptują oraz uznają podpisy elektroniczne. Strony mogą same stworzyć odpowiedni system zabezpieczeń, sposób i zasady składania podpisu elektronicznego, a nawet przyjąć pewne stosowane tylko w określonym kręgu (po zawarciu stosownych umów) nowatorskie systemy techniczne lub szczególnego rodzaju oprogramowanie. Zgodnie z Dyrektywą, państwa członkowskie nie mogą pozbawić podpisów, stosowanych w systemach zamkniętych, prawnej skuteczności i dopuszczalności jako środka dowodowego w postępowaniach prawnych. Jedyną przesłanką, jaka musi zostać spełniona, jest zgodność umowy tworzącej oraz określającej zasady, jakie muszą spełnić podpisy elektroniczne w systemie zamkniętym, z prawem krajowym, a przez to z przepisami Unii Europejskiej.

Przepisów Dyrektywy nie należy stosować do usług świadczonych w zakresie poufności informacji, jeżeli w odniesieniu do takich usług zasto-

[20] Dyrektywa nie wyłącza przepisów Dyrektywy 97/7/WE z dnia 20 maja 1997 r. Parlamentu Europejskiego i Rady o ochronie konsumentów w umowach zawieranych na odległość, Dziennik Urzędowy L. 144/19 z dnia 4 czerwca 1997 r. Dyrektywa ta w tłumaczeniu na język polski jest dostępna w: E. Ł ę t o w s k a, *Komentarz do ustawy o ochronie niektórych praw konsumentów,* Warszawa 2000, oraz E. Ł ę t o w s k a, *Prawo umów konsumenckich*; Warszawa 1999, s. 559, a także s. 224 i nast.

[21] Patrz uzasadnienie Dyrektywy.

sowanie mają przepisy krajowe dotyczące porządku publicznego lub bezpieczeństwa[22]. Powyższe wyłączenie jest związane z istniejącymi w państwach Unii Europejskiej różnicami systemów i przepisów prawnych w zakresie poufności informacji. Każde z państw członkowskich może samodzielnie określać sytuacje, w których osoby trzecie (np. policja, prokuratura, wywiad, służby specjalne itd.) mogą zapoznawać się z informacjami, dokumentami, umowami itp. przesyłanymi w formie elektronicznej z użyciem elektronicznych nośników informacji.

Ponadto przepisy Dyrektywy nie naruszają Dyrektyw dotyczących ochrony praw konsumenta, ochrony danych osobowych, a także rozporządzenia Rady 3381/94 z dnia 19 grudnia 1994 r., w sprawie wspólnotowych zasad kontroli wywozu towarów o podwójnym znaczeniu[23], decyzji Rady 94/942/GASP z 19 XII 94 r. dotyczącej wspólnego działania podjętego przez Radę w celu kontroli wywozu towarów o podwójnym znaczeniu[24], oraz międzynarodowych praw i obowiązków Wspólnoty[25].

2. Definicje

Rozwój handlu elektronicznego uzależniony jest od ujednolicenia ram prawnych dotyczących *e-commerce*, a w szczególności od wprowadzenia jednolitego nazewnictwa i definicji. Dlatego też ustawodawca bardzo szczegółowo zdefiniował w Dyrektywie podstawowe pojęcia dotyczące podpisu elektronicznego, przy czym definicje zostały sformułowane w taki sposób, aby podpisy elektroniczne mogły być wykorzystywane nie tylko do „podpisywania" dokumentów podpisem elektronicznym, ale także do świadczenia innych usług i produktów elektronicznych, takich jak rejestracja, datowniki, indeksowanie, obliczenia i inne pozostające w związku z podpisem elektronicznym.

Zgodnie z Dyrektywą, przez **„podpis elektroniczny"** rozumie się dane w formie elektronicznej, które są dołączone do innych danych albo z nimi logicznie związane i służą stwierdzeniu autentyczności. Dosyć szeroka

[22] Patrz uzasadnienie Dyrektywy.

[23] Dziennik Urzędowy L.367 z dnia 31 XII 1994 r., s. 1 – rozporządzenie zmienione przez rozporządzenie Rady (WE) 837/95, Dziennik Urzędowy L.90 z 21 IV 1995 r., s. 1.

[24] Dziennik Urzędowy L.367 z dnia 31 XII 1994 r., s. 8 – zm. przez decyzję 1999/93/GASP, Dziennik Urzędowy L.73 z 19 III 1999 r., s. 1.

[25] Patrz uzasadnienie Dyrektywy.

definicja powoduje, iż podpisem elektronicznym będzie każde dołączenie lub logiczne związanie danych w formie elektronicznej do innych danych, służące do stwierdzenia autentyczności[26]. Na ważność podpisu elektronicznego nie wpływa fakt jego nieodporności na sfałszowanie, możliwość zmiany danych po ich opatrzeniu podpisem elektronicznym itp. Podpis elektroniczny można stworzyć samodzielnie. Dla jego wytworzenia wystarczające jest odpowiednie oprogramowanie, dostępne między innymi w internecie, np. programy tworzenia kluczy prywatnych i publicznych PGP[27].

Dla bezpieczeństwa obrotu wymogi, jakie spełnia podpis elektroniczny, są niewystarczające. Dlatego obok określenia „podpis elektroniczny" wpro-

---

[26] Tak też F. W e j m a n, *Przekład...*, s. 190.

[27] Pomysł stosowania klucza prywatnego do podpisywania dokumentów i klucza publicznego do ich odczytywania jest autorstwem Amerykanina Phila Zimmermanna (System PGP – Pretty Good Privacy – całkiem niezła prywatność). Jest on oparty o algorytm matematyczny RSA (Rivest – Shamir – Adelman), nazwany tak od pierwszych liter nazwisk jego twórców. System PGP pozwala szyfrować dokumenty, sygnować (podpisywać) dokumenty w sposób umożliwiający adresatowi stwierdzenie, od kogo pochodzi dokument oraz czy jego treść nie została po podpisaniu modyfikowana przez osoby trzecie. Klucz deszyfrowania musi pozostać tylko do wiadomości jego właściciela, dlatego zwany jest kluczem prywatnym, natomiast klucz szyfrowania powinien zostać udostępniony ogółowi – klucz publiczny. System wykorzystuje odpowiednią konstrukcję algorytmu szyfrowania/deszyfrowania. Klucz deszyfrowania bazuje na parze dużych liczb pierwszych, klucz szyfrowania bazuje natomiast na iloczynie tychże liczb. Dla odpowiednio dużych liczb rzędu 10 do potęgi 100 operacja znalezienia liczb odpowiadających kluczowi prywatnemu i publicznemu może zająć całe lata. Przykładem może być eksperyment dokonany w latach 1993-1995, gdzie 600 wolontariuszy – użytkowników internetu dokonało rozkładu liczby 129 cyfrowej na ok. 1600 komputerach w cztery miesiące. Aktualnie wykorzystuje się przy algorytmie liczby nie mniejsze niż 300-cyfrowe. Program do tworzenia kluczy można znaleźć pod adresem ftp://pipeta.chemia.pk.edu.pl/pub/pgp/; http://agh.edu.pl/pub/security/pgp. Szerzej na ten temat W. B i e s e r, *Digitale Signatur. Vom Papierdokument zum beweissicheren Digitalem Dokument,* [w:] *Rechtaspekte des elektronischen Geschäftverkehrs*, red. I. Geis, Eschborn 1999, s. 49-53; T. S c h w e p p e, *Die digitale Signatur- Verfahren und systematische Einordnung,* [w:] *Rechtsfragen der Informationsgesellschaft*, red. T. Hoeren, R. Queck, Berlin 1999, s. 122; B. K l e i n e - V o s s b e c k, *Electronic mail und Verfassungsrecht*, Marburg 2000, s. 195; S. E n g e l - F l e c h s i g, A. R o s s n a g e l, [w:] Multimedia Recht 1998, s. 500-505; B. H ö r l, *Aufklärung und Beratung beim Computer Kauf*, München 1999, s. 8-11; D. S z o s t e k, *Przegląd...*, s. 465 i nast.; J. S t o k ł o s a, *Techniczne i prawne aspekty stosowania podpisu cyfrowego w internecie,*[w:] *Internet – problemy prawne,* red. R. Skubisz, Lublin 1999, s. 120-124; K. M ł y n a r s k i, *Kryptografia a bezpieczeństwo danych,* http://www.cyber.com.pl/archiwum/12/25/shtml. Zasady działania podpisu elektronicznego opisali także. J. B a r t a i R. M a r k i e w i c z, *Internet a Prawo*, Kraków 1998, s. 70-81.

wadzono określenie, **„kwalifikowany podpis elektroniczny"**. Jest nim podpis elektroniczny, który spełnia dodatkowo następujące przesłanki:

– jest przyporządkowany wyłącznie składającemu podpis;

– umożliwia identyfikację składającego podpis;

– jest sporządzany za pomocą środków, które składający podpis może mieć pod swoją wyłączną kontrolą;

– jest związany z danymi, do których się odnosi, w taki sposób, że wtórna zmiana danych może być rozpoznana[28].

„**Składającym podpis"** jest osoba, która posiada urządzenie służące do generowania podpisów i działa we własnym imieniu albo w imieniu osoby fizycznej lub prawnej, którą reprezentuje, albo jako organ osoby prawnej.

Zgodnie z przepisami Dyrektywy, **„danymi służącymi do generowania podpisu elektronicznego"** są oryginalne dane, takie jak kody lub osobiste klucze kryptograficzne, wykorzystywane przez składającego podpis do generowania podpisu. Dyrektywa przyjmuje zasadę technicznej neutralności w stosunku do technologii używanej do generowania podpisu elektronicznego. Wprawdzie w Dyrektywie wymienia się jako dane służące do generowania podpisu elektronicznego kody lub osobiste klucze kryptograficzne, co może sugerować nakaz stosowania tychże technologii, należy jednak uznać, iż powyższe wyliczenie ma charakter wyłącznie przykładowy, na co wskazuje sformułowanie „takie jak...". Ponadto została ustalona procedura mająca na celu dopuszczenie nowatorskich technologii, innych niż określone w Dyrektywie (art. 3 pkt 4).

„Urządzeniem do generowania podpisów" jest skonfigurowany *software* i *hardware*[29] stosowany do implementacji danych służących do

---

[28] Tak też R. S c h l e c h t e r, *Ein europäischer Rahmen für elektronische Signaturen*, [w:] *Rechtsaspekte des elektronischen Geschäftsverkehrs*, red. I. Geis, Eschborn 1999, s. 114.

[29] *Hardware*, czyli dodatkowy nowy sprzęt doinstalowany do komputera, np. karta muzyczna, drukarka itp.; natomiast przez *software* należy rozumieć odpowiednie oprogramowanie. Patrz J. S c h m i d t, *Der Computersystemvertrag. Rechtsnauter und Vertragsgestaltung einer komplexen Leistungsbeziehung*, Illertissen 1995, s. 37-42; G.F. von G r a v e n r e u t h, *Computerrecht von A-Z*; München 1992, s. 131 i 218; A. J u n k e r, *Computerrecht*, Baden-Baden 1988, s. 38-45; M. C z a j k o w s k i, *Leksykon internetu*, Warszawa 1999, s. 285; a także *Easy PC*, t. II, część *Windows,* wydawnictwo Vogel International GmbH, s. 69-71.

generowania podpisu. Tradycyjnie określenie *software* i *hardware* ogranicza się do komputerów, co w dosłownym znaczeniu Dyrektywy oznaczałoby, iż tylko poprzez urządzenia i oprogramowanie komputerowe można wygenerować podpis elektroniczny. Biorąc pod uwagę cel Dyrektywy, należy znaczenie „urządzenia do generowania podpisów" rozszerzyć także na inne urządzenia, nie będące komputerowymi w ścisłym tego słowa znaczeniu. Wystarczający jest fakt wykorzystywania do swego działania procesora lub podobnego urządzenia, a także dysponowanie odpowiednią pamięcią do tworzenia, przetwarzania, przechowywania lub wysyłania danych np. telefon komórkowy, pager itp. Zgodnie z Dyrektywą, skonfigurowany *software* i *hardware* wykorzystywany do implementacji danych służących do generowania podpisów jest urządzeniem do generowania tychże podpisów, niezależnie od metody, techniki, sposobu i osoby generującej podpis. Jest nim każde urządzenie i oprogramowanie, byleby służyło generowaniu podpisów.

W Dyrektywie obok „urządzeń do generowania podpisów" zostało wprowadzone dodatkowe określenie **„bezpieczne urządzenie do generowania podpisów"** – czyli urządzenie spełniające wymogi określone w załączniku III Dyrektywy, a więc takie urządzenia do składania podpisów, które poprzez odpowiednie środki techniczne i proceduralne zapewniają co najmniej, iż:

– dane kreujące podpis elektroniczny, używane do wywołania podpisu elektronicznego, mogą w praktyce wystąpić tylko raz, a ich poufność jest dostatecznie zagwarantowana;

– dane kreujące podpis elektroniczny, używane do wywołania podpisu, nie mogą być pozyskane, a podpis przy zastosowaniu dostępnej technologii jest chroniony przed fałszerstwem;

– istnieje możliwość rzetelnej ochrony przed użyciem bezpiecznych urządzeń do generowania podpisu przez osoby trzecie.

Ponadto „bezpieczne urządzenia do składania podpisów" nie mogą zmienić danych, które mają być opatrzone podpisem. Nie chodzi tu o zmiany, przekształcenia techniczne konwertujące dane (np. konwersja danych wyświetlonych na monitorze na sygnał, który zostaje przesłany poprzez internet do innego użytkownika sieci), lecz o zmiany, które powodowałyby sytuację, kiedy dane otrzymywane od adresata, po przeprowadzeniu odpowiednich

konwersji, różniłyby się w momencie ich odczytywania od wysłanego przez nadawcę oryginału. Dodatkowo „bezpieczne urządzenia do składania podpisów elektronicznych" muszą umożliwiać odczytywanie danych, które mają zostać opatrzone podpisem elektronicznym, tj. muszą zawierać system umożliwiający zapoznanie się z podpisywanymi danymi przed ich podpisaniem. Składający podpis musi mieć możliwość zapoznania się z treścią pliku, zanim ten zostanie podpisany i wysłany. Ma to na celu ograniczenie możliwości zaistnienia pomyłki.

„Danymi służącymi do weryfikacji podpisu" są dane i kody albo publiczne klucze kryptograficzne stosowane do weryfikacji podpisów elektronicznych. Podobnie jak przy definicji „danych służących do generowania podpisów", zgodnie z zasadą technicznej neutralności, nie określono w Dyrektywie technicznych komponentów, jakie powinny być stosowane do weryfikacji podpisów, pozostawiając całkowitą swobodę podmiotom oferującym lub korzystającym z usług związanych z elektronicznym podpisem.

„Urządzeniem do weryfikacji podpisu" jest skonfigurowany *software* i *hardware* służący do implementacji danych służących do weryfikacji podpisów. Uwagi dotyczące „urządzeń do generowania podpisu" są w tym miejscu jak najbardziej aktualne.

Gwarancję, iż wiadomość elektroniczna, w tym oświadczenie woli, które zostało opatrzone podpisem elektronicznym, pochodzi od osoby podającej się za nadawcę zapewnia wprowadzony system certyfikatów. **„Certyfikatem"** jest elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu są przyporządkowane do określonej osoby i potwierdzają jej tożsamość[30]. Nie ma przy tym znaczenia, kto, czy też jaki podmiot wystawił certyfikat, ani też jaki jest jego termin ważności. Certyfikat nie musi nawet zawierać danych o wystawcy certyfikatu, a więc w powyższym znaczeniu może go wystawić każdy, nawet nadawca wiadomości.

Dlatego też w Dyrektywie obok zwykłego certyfikatu wyróżniono **„kwalifikowany certyfikat"**, tj. certyfikat zawierający co najmniej następujące dane:

– wskazanie, że certyfikat został wydany jako kwalifikowany, co ma odróżnić go od zwykłego certyfikatu: opatrzenie dokumentu podpisem

[30] R. Schlechter, *Ein europäischer...*, s. 114.

elektronicznym opartym na kwalifikowanym certyfikacie spełnia w odniesieniu do danych istniejących w formie elektronicznej wymóg prawny podpisu w taki sam sposób, jak podpis własnoręczny spełnia ten wymóg w odniesieniu do danych istniejących na papierze (art. 5 Dyrektywy)[31]. Opatrzenie dokumentu podpisem elektronicznym opartym czy też potwierdzonym zwykłym certyfikatem nie zawsze spełnia ten warunek;

– określenie podmiotu świadczącego usługę certyfikacji i państwa, w którym ma on siedzibę;

– nazwisko składającego podpis albo pseudonim, dający się zidentyfikować. Podmioty mogą dokonywać czynności prawnych pod pseudonimem tylko wtedy, kiedy taką możliwość przewiduje prawo krajowe. Dyrektywa nie harmonizuje prawa państw członkowskich w zakresie dopuszczalności działalności pod pseudonimem;

– szczególny przymiot składającego podpis, jeżeli jest on relewantny stosownie do celu, dla którego certyfikat został przewidziany, np. dane określające, iż osoba składająca podpis dokonuje czynności prawnych jako organ osoby prawnej;

– dane pozwalające na weryfikację podpisu, które odpowiadają danym niezbędnym przy składaniu podpisu pozostającym pod kontrolą składającego podpis, np. klucz publiczny umożliwiający weryfikację podpisu elektronicznego złożonego przy użyciu klucza prywatnego;

– dane o początku i końcu okresu ważności certyfikatu. Dzięki tym informacjom adresat podpisanej elektronicznie wiadomości posiada możliwość sprawdzenia ważności podpisu elektronicznego. W Dyrektywie nie został określony minimalny okres ważności certyfikatu, pozostawiając tę kwestię do określenia przez państwa członkowskie lub przez podmioty wydające kwalifikowane certyfikaty (w praktyce certyfikaty wydawane są na dwa – trzy lata, co jest związane z szybko rozwijającą się techniką);

– kod identyfikacji certyfikatu;

– kwalifikowany podpis elektroniczny podmiotu świadczącego usługi certyfikacyjne wydającego dany certyfikat. Umieszczenie kwalifikowane-

[31] Państwa członkowskie mają prawo do określenia sytuacji, w ramach których oświadczenie woli złożone w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym opartym na kwalifikowanym certyfikacie, nie jest zrównane i nie wywołuje skutków prawnych tak, jak oświadczenie woli złożone w „tradycyjnej" formie pisemnej.

go podpisu elektronicznego na certyfikacie gwarantuje, iż dane w nim zawarte nie zostały zmienione w trakcie ich przesyłania do adresata;

– ograniczenia zakresu ważności certyfikatu, jeżeli mają zastosowanie, przykładowo poprzez określenie rodzajów czynności prawnych bądź działań nie gwarantowanych przez wystawcę certyfikatu. Ograniczenia mogą dotyczyć określenia obszaru, terytorium bądź państw, w których wystawca certyfikatu gwarantuje prawdziwość podpisu elektronicznego[32];

– ograniczenia wartości transakcji, jeżeli ograniczenia takie mają zastosowanie. Ze względu na zapewnienie bezpieczeństwa obrotu, państwa członkowskie lub podmioty świadczące usługi certyfikacyjne mogą określić maksymalną wartość transakcji, jaka może zostać dokonana w formie elektronicznej poprzez złożenie podpisu elektronicznego opartego na kwalifikowanym certyfikacie[33].

Nie każdy podmiot świadczący usługi certyfikacyjne może wydawać certyfikaty kwalifikowane. Dla uzyskania takiego uprawnienia podmiot powinien spełnić następujące wymagania:

– powinien wykazać, iż jest rzetelny i godny zaufania wymaganego dla świadczenia usług certyfikacyjnych;

– w ramach swojej działalności musi zapewnić funkcjonowanie szybkiej i niezawodnej usługi zapisu oraz niezawodnej i bezzwłocznej usługi odwołania, tj. usługi bezzwłocznego odwołania certyfikatu na wniosek składającego podpis (np. w sytuacji ujawnienia osobom trzecim kodów lub prywatnego klucza kryptograficznego składającego podpis);

– powinien zapewnić, iż dane i moment wystawienia albo odwołania certyfikatu zostaną dokładnie określone (w przypadku odwołania certyfikatu kwalifikowanego umieszcza się w nim najczęściej godzinę, minutę i sekundę odwołania);

– przed wydaniem certyfikatu zobligowany jest sprawdzić, przy pomocy właściwych środków i w zgodzie z prawem wewnętrznym, tożsamość oraz szczególne przymioty osoby (jeżeli takie istnieją), dla której ma zostać wydany kwalifikowany certyfikat (np. jeżeli podpis elektroniczny jest wystawiany osobie fizycznej w związku z pełnieniem przez nią jakiejś funkcji – należy sprawdzić, czy osoba ta w rzeczywistości taką funkcję

[32] Patrz niniejszy artykuł punkt 6 „odpowiedzialność cywilna".

[33] Patrz R. S c h l e c h t e r, *Ein europäischer...*, s. 117-118.

pełni). Kontrola tożsamości ma zasadnicze znaczenie dla całego systemu certyfikacji. Certyfikat jest bowiem gwarancją na prawdziwość danych, na które powołuje się podmiot składający podpis elektroniczny;

– w związku z działalnością dotyczącą wydawana certyfikatów, danych do generowania podpisów elektronicznych oraz inną działalnością określoną w Dyrektywie, powinien zatrudniać personel, który posiada wymaganą dla świadczonych usług wiedzę fachową, doświadczenie i kwalifikacje, do których należą między innymi umiejętności w zakresie zarządzania, znajomości technologii podpisów elektronicznych i obeznanie z właściwymi procedurami zabezpieczającymi;

– przyjąć i stosować stosowne procedury administracyjne i zarządzania, które odpowiadają uznanym normom;

– dla świadczonych usług musi używać wiarygodnych systemów i produktów, które są chronione przed zmianami i zapewniają techniczne oraz kryptograficzne zabezpieczenia procesu, w którym są używane;

– zobowiązany jest podejmować wszelkie działania i stosować środki przeciwdziałające fałszerstwom certyfikatów, a w przypadku gdy podmiot świadczący usługi certyfikacyjne sam tworzy dane składające się na podpis elektroniczny, musi zapewnić poufność procesu tworzenia tych danych;

– powinien dysponować wystarczającymi środkami finansowymi, aby móc prowadzić działalność spełniającą wymagania Dyrektywy. W szczególności musi być w stanie ponosić ryzyko odpowiedzialności odszkodowawczej, na przykład poprzez zawarcie odpowiedniego ubezpieczenia;

– rejestrować na odpowiednio długi okres czasu wszystkie istotne informacje dotyczące kwalifikowanego certyfikatu, w szczególności dla celów udowodnienia faktu certyfikacji w postępowaniu sądowym. Rejestracja może być dokonana w formie elektronicznej;

– nie może przechowywać ani kopiować danych kreujących podpis elektroniczny osób, którym świadczone są usługi zarządzania kluczem;

– przed zawarciem umowy z osobą, która występuje o certyfikat kwalifikowany, musi poinformować ją za pomocą trwałych środków przekazu o dokładnych warunkach użycia certyfikatu, w tym o wszelkich ograniczeniach jego użycia, istnieniu systemu dobrowolnej akredytacji oraz procedurach dotyczących składania skarg i rozwiązywania sporów. Dane te muszą być przedstawione na piśmie, ewentualnie w formie elektronicznej, w łatwo zrozumiałym języku. Istotne elementy tych informacji muszą być na wnio-

sek udostępniane osobom trzecim, opierającym się na wystawionym certyfikacie kwalifikowanym. Sposób udowodnienia faktu poinformowania o warunkach użycia certyfikatu należy do dostawcy usług certyfikacyjnych. W praktyce jest to odpowiednio podpisane oświadczenie osoby występującej o certyfikat;

– zobowiązany jest do używania godnych zaufania systemów przechowywania certyfikatów w formie umożliwiającej ich weryfikację, tak aby:

• tylko upoważnione osoby mogły dokonywać wprowadzania i zamiany danych,

• informacje mogły być sprawdzane co do ich autentyczności,

• certyfikaty były publicznie dostępne tylko w wypadkach, w których uzyskano zgodę posiadacza certyfikatu,

• zmiany techniczne, które wpływają na zachowanie wymagań w zakresie bezpieczeństwa były przejrzyste dla operatora.

Uzyskanie prawa do wydawania certyfikatów kwalifikowanych jest możliwe wyłącznie wtedy, gdy powyższe wymogi zostaną spełnione łącznie.

„Podmiotem świadczącym usługi certyfikacyjne" jest jednostka organizacyjna, osoba fizyczna lub prawna, która wystawia certyfikaty lub świadczy inne usługi w związku z podpisami elektronicznymi. Ustawodawca zezwala na oferowanie usług certyfikacyjnych zarówno podmiotom publicznym, prywatnym, osobom fizycznym, prawnym, jak i jednostkom organizacyjnym nie posiadającym osobowości prawnej, o ile działają one w zgodności z prawem krajowym. Państwa członkowskie Wspólnoty nie mogą odmawiać zgody podmiotom świadczącym usługi certyfikacyjne na prowadzenie takiej działalności, wyłącznie z powodu niepoddania się dobrowolnej akredytacji. Niepoddanie się dobrowolnej akredytacji nie stanowi przeszkody dla świadczenia usług certyfikacyjnych. Jednakże takie podmioty mogą wydawać co najwyżej certyfikaty zwykłe, nie mogą natomiast wydawać certyfikatów kwalifikowanych. W związku z czym, świadczone usługi podpisu elektronicznego nie będą zrównane w skutkach prawnych z podpisami własnoręcznymi.

„Dobrowolną akredytacją" jest zezwolenie, na mocy którego stwierdzane są prawa i obowiązki związane ze świadczeniem usług certyfikacyjnych, wydawane na wniosek określonego podmiotu świadczącego usługi

certyfikacyjne przez organ publiczny lub prywatny, właściwy do ustalenia tych praw i obowiązków oraz do nadzorowania ich przestrzegania.

„Produktem dla podpisów elektronicznych" jest *hardware* lub *software* względnie ich odpowiednie komponenty, które mają być wykorzystywane przez podmiot świadczący usługi certyfikacyjne do świadczenia usług w zakresie podpisów elektronicznych albo które mają mieć zastosowanie do generowania i weryfikacji podpisów elektronicznych. Podobnie jak przy definicji urządzeń do generowania oraz weryfikacji podpisu elektronicznego, ustawodawca przy określaniu produktu dla podpisów elektronicznych stosuje zasadę neutralności technologicznej.

3. Dostęp do rynku

Jedną z podstawowych zasad Dyrektywy jest zasada całkowitej swobody świadczenia usług certyfikacyjnych. Państwo członkowskie nie może uzależniać świadczenia usług certyfikacyjnych od jakiejkolwiek uprzedniej zgody[34]. Każdy z podmiotów, takich jak jednostki organizacyjne, osoby fizyczne, prawne, niezależnie, czy są podmiotami publicznymi, czy też prywatnymi, jeśli tylko mają siedzibę w kraju Unii Europejskiej, mogą świadczyć usługi certyfikacyjne. Nie oznacza to jednak, iż państwa członkowskie nie mogą sprawować żadnej kontroli nad tymi podmiotami. Każde z państw Wspólnoty może wprowadzić system dobrowolnej akredytacji względnie utrzymać (wprowadzić) systemy mające na celu podniesienie poziomu świadczonych usług certyfikacyjnych. Fakt wprowadzenia dobrowolności akredytacji nie oznacza, iż podmioty świadczące usługi certyfikacyjne muszą się im poddać. W praktyce, dla uzyskania prawa do wydawania certyfikatów kwalifikowanych podmiot świadczący usługi certyfikacyjne musi uzyskać akredytację i wykazać swoją rzetelność i godność zaufania wymaganą dla świadczenia usług. Wszystkie wymogi związane z systemem akredytacji muszą być obiektywne, przejrzyste, proporcjonalne i nie dyskryminujące. Państwa członkowskie nie mogą ograniczać liczby pod-

[34] Ciekawe rozwiązanie zostało wprowadzone w austriackiej ustawie o podpisie elektronicznym (BGBL I nr 190/1999 Nr GP XX RV 1999 AB 2065 s. 180 BR: AB 6065, s. 657). Austriacki ustawodawca nie wymaga uzyskania uprzedniej zgody dla podjęcia działalności jako podmiotu świadczącego usługi certyfikacyjne, jednakże fakt rozpoczęcia działalności podlega zgłoszeniu odpowiedniemu organowi najpóźniej z chwilą jej podjęcia.

miotów świadczących usługi certyfikacyjne z przyczyn wchodzących do zakresu regulacji Dyrektywy, co nie oznacza, iż takie ograniczenie nie jest możliwe (np. ze względu na bezpieczeństwo narodowe), jednakże podstawą takich ograniczeń nie może być omawiana Dyrektywa.

Państwa członkowskie mają obowiązek dołożenia wszelkich starań, aby został stworzony odpowiedni system nadzoru podmiotów świadczących usługi certyfikacyjne, wystawiających kwalifikowane certyfikaty, mających siedzibę na ich terytorium. Obowiązek nadzoru nie obejmuje podmiotów świadczących usługi certyfikacyjne wystawiających zwykłe certyfikaty. Określenie sposobu i zasady nadzoru należy do poszczególnych państw członkowskich. W Dyrektywie nie przesądzono, czy nadzór powinien opierać się na systemie nadzoru publicznego, czy też prywatnego. Należy z tego wnioskować, iż obydwa systemy są dopuszczalne, natomiast wybór systemu należy do państwa członkowskiego.

Podmiot świadczący usługi certyfikacyjne, aby mógł wystawiać w ramach swojej działalności certyfikaty kwalifikowane musi wyposażyć podmioty składające podpis elektroniczny w bezpieczne urządzenia do generowana podpisów. Dla stwierdzenia zgodności oferowanych urządzeń z wymogami określonymi w Dyrektywie, państwa członkowskie mają obowiązek powołania odpowiednich organów publicznych lub prywatnych, które będą tę zgodność potwierdzały. Kryteria wyboru i sposób działania tychże organów zostaną określone przez Komisję wspieraną przez Komitet do Spraw Podpisów Elektronicznych[35]. Ujednolicenie kryteriów wyboru i działania tychże organów jest związane z wzajemnym uznawaniem przez wszystkie państwa członkowskie decyzji stwierdzających zgodność urządzeń do generowania podpisów z wymogami Dyrektywy. Pozostawienie państwom członkowskim swobody w określaniu kryteriów i sposobu działania tychże organów spowodowałoby utrudnienia, a niekiedy i niemożność uznawania decyzji organów działających w innym państwie Unii Europejskiej. Komisja wspierana przez Komitet do Spraw Podpisów Elektronicznych może określić ogólne parametry i wskazać numery referencyjne ogólnie uznanych produktów dla podpisów elektronicznych i opublikować je w Dzienniku Urzędowym Wspólnoty Europejskiej. Uznaje się, iż produkt spełniający normy opublikowane w Dzienniku Urzędowym spełnia warunki wymagane

[35] O Komitecie do Spraw Podpisów Elektronicznych patrz pkt 10.

dla bezpiecznego urządzenia generującego podpis elektroniczny oraz jest systemem, który skutecznie chroni przed zmianami i zapewnia techniczne oraz kryptograficzne zabezpieczenie procesu, w którym jest używany. W ten sposób z jednej strony Unia Europejska określa ogólne zasady, warunki, a przez to rodzaj urządzeń spełniających wymogi bezpiecznych urządzeń generujących kwalifikowany podpis elektroniczny, z drugiej dopuszcza, poprzez wprowadzenie systemu weryfikacji, możliwość wprowadzenia nowych rozwiązań technologicznych i systemowych zachowując zasadę neutralności technologicznej[36]. Państwa członkowskie mają obowiązek współpracy z Komisją oraz Komitetem do Spraw Podpisów Elektronicznych w zakresie określonym Dyrektywą, ze szczególnym uwzględnieniem interesów konsumenta.

Państwa wchodzące w skład UE mogą w swoich systemach prawnych uzależnić stosowanie podpisów elektronicznych w sferze publicznej od spełnienia określonych dodatkowych warunków. Państwa same określą i sprecyzują powyższe warunki, muszą one jednak być obiektywne, przejrzyste, proporcjonalne oraz nie dyskryminujące i mogą odnosić się jedynie do specyficznych cech określonego zastosowania, np. wpisy do rejestrów, zmiana adresu zamieszkania itp. Warunki te nie mogą stanowić dla obywateli przeszkody w dostępie do usług transgranicznych.

4. Zasady rynku wewnętrznego

Dyrektywa dotycząca podpisu elektronicznego stanowi ogólne warunki, jakie powinny zostać spełnione przez podmioty świadczące usługi certyfikacyjne. Państwa członkowskie Unii Europejskiej były zobowiązane w terminie do 19 lipca 2001 r. wydać odpowiednie przepisy krajowe, zgodne z omawianą Dyrektywą. Przepisy te mają zastosowanie dla podmiotów świadczących usługi certyfikacyjne, których siedziba znajduje się na terytorium danego państwa. Cechą implementacji Dyrektyw wspólnotowych jest brak wymogu dosłownego ich wprowadzania do prawa krajowego, konieczna jest natomiast realizacja celu Dyrektywy. Jednakże ze względów praktycznych uzasadnione jest wierne odwzorowanie w prawie krajowym przepisów Dyrektywy[37], szczególnie w zakresie definicji i nazewnictwa.

---

[36] A. R o s s n a g e l, U. P o r d e s c h, [w:] *Recht der Multimedia*...., s. 11, pkt 1.

[37] Patrz E. Ł ę t o w s k a, *Ustawa o ochronie*..., s. 22.

Państwa Unii Europejskiej nie mogą ograniczyć świadczenia usług certyfikacyjnych pochodzących z innych państw członkowskich w dziedzinach objętych Dyrektywą, zapewniając im możliwość swobodnego działania na swoim terytorium. Państwa członkowskie mają obowiązek dołożenia wszelkich starań, aby produkty dla podpisów elektronicznych, spełniające wymogi Dyrektywy, mogły być przedmiotem swobodnego obrotu na obszarze rynku wewnętrznego. Ma to na celu zwiększenie rozwoju i dostępności tychże produktów na całym obszarze UE. Swobodny obrót nie obejmuje zastrzeżonych przepisami krajowymi systemów kryptograficznych szyfrowania i deszyfrowania, wykorzystywanych przez państwo w związku z zapewnieniem bezpieczeństwa narodowego.

5. Skutki prawne zastosowania podpisu elektronicznego

Państwa członkowskie mają obowiązek dołożenia wszelkich starań, aby kwalifikowane podpisy elektroniczne, które opierają się na kwalifikowanym certyfikacie i które zostały wygenerowane przez bezpieczne urządzenie do generowania podpisów, spełniały w odniesieniu do danych istniejących w formie elektronicznej wymóg prawny podpisu w taki sam sposób, jak podpisy własnoręczne spełniają ten wymóg w odniesieniu do danych istniejących na tradycyjnym dokumencie, np. na papierze, oraz by były dopuszczalne w postępowaniach prawnych jako środki dowodowe. Ustawodawca nakłada na państwa członkowskie obowiązek zrównania dokumentów podpisanych własnoręcznie z dokumentami elektronicznymi. Nie jest natomiast wymagane uznawanie na równi z dokumentami (danymi) podpisanymi własnoręcznie dokumentów elektronicznych opatrzonych zwykłym podpisem elektronicznym, dokumentów elektronicznych opartych na zwykłym certyfikacie czy też dokumentów elektronicznych, które zostały opatrzone podpisem elektronicznym wygenerowanym przez urządzenie nie spełniające wymogów Dyrektywy lub które nie zostało uznane przez odpowiednie organy za bezpieczne urządzenie do generowania podpisów elektronicznych.

Ustawodawca nie ingeruje ani nie zamierza harmonizować prawa krajowego państw członkowskich w zakresie formy czynności prawnej. Państwa same określają zasady dotyczące formy czynności prawnych. Jednakże w przypadku, gdy prawo krajowe dla danej czynności prawnej wymaga zwykłej formy pisemnej, opatrzenie dokumentu elektronicznego (danych)

kwalifikowanym podpisem elektronicznym zgodnie z powyższą procedurą, zostaje uznane jako zachowanie formy pisemnej.

Państwa członkowskie są zobligowane do dołożenia wszelkich starań, aby podpisy elektroniczne nie traciły prawnej skuteczności i dopuszczalności jako środek dowodowy w postępowaniach prawnych z powodu:

– istnienia w formie elektronicznej albo

– nieopierania się na kwalifikowanym certyfikacie, albo

– nieopierania się na kwalifikowanym certyfikacie wystawionym przez akredytowany podmiot świadczący usługi certyfikacyjne, albo

– niewytworzenia przez bezpieczne urządzenie do generowania podpisów.

W prawie krajowym powinno być dopuszczalne przeprowadzenie dowodu z każdego dokumentu elektronicznego, jednakże należy pamiętać, iż nie każdy dokument elektroniczny będzie traktowany na równi z dowodem z dokumentu tradycyjnego, podpisanego własnoręcznie. Teoretycznie państwa członkowskie mają prawo do zrównania każdego dokumentu z dokumentem podpisanym własnoręcznie, w tym z dokumentem elektronicznym, nie spełniającym wymogów Dyrektywy. Wydaje się jednak, iż w praktyce państwa nie będą z tego prawa korzystać.

Państwa członkowskie poprzez odpowiednie regulacje w prawie krajowym mają prawo do wskazania obszarów prawa, w których dokumenty elektroniczne i podpisy elektroniczne nie mogą być stosowane.

Dyrektywa nie narusza uprawnień sądów krajowych do rozstrzygania w przedmiocie zgodności prawa krajowego z wymogami prawa Unii Europejskiej, nie narusza także przepisów krajowych dotyczących sądowej oceny dowodów.

6. Odpowiedzialność cywilna

Zgodnie z Dyrektywą, państwa członkowskie zapewniają co najmniej, iż podmiot świadczący usługi certyfikacyjne, który publicznie wystawia certyfikat jako certyfikat kwalifikowany albo za taki certyfikat publiczny poręcza, w przypadku wyrządzenia szkody jednostkom organizacyjnym albo osobom prawnym lub fizycznym, które w rozsądnych granicach opierały się na certyfikacie, odpowiada za to, że:

– wszelkie informacje zawarte w certyfikacie kwalifikowanym w czasie jego wystawienia są prawdziwe, a certyfikat zawiera wszelkie dane wy-

magane dla kwalifikowanego certyfikatu. Dlatego w interesie dostawcy usług certyfikacyjnych jest dokładne sprawdzenie tożsamości i wszelkich innych danych podawanych przez podmiot starający się o certyfikat[38];

– składający podpis wskazany w kwalifikowanym certyfikacie w czasie wystawiania certyfikatu był w posiadaniu danych służących do wygenerowania podpisu, które odpowiadają danym służącym do weryfikacji podanym, względnie zidentyfikowanym w certyfikacie;

– w przypadkach gdy podmiot świadczący usługi certyfikacyjne wytwarza zarówno dane służące do generowania podpisów, jak również dane służące do weryfikacji podpisów, dostawca usług certyfikacyjnych odpowiada za zgodność i kompatybilność tychże danych.

Ustawodawca przyjął domniemanie winy dostawcy usług certyfikacyjnych za wyrządzone szkody. Jeżeli nie przedstawi on odpowiedniego przeciwdowodu, będzie ponosił odpowiedzialność niezależnie od rzeczywistego stanu rzeczy. Obowiązek udowodnienia braku niedbalstwa leży po jego stronie.

Podmiot świadczący usługi certyfikacyjne, który publicznie wystawił certyfikat w formie certyfikatu kwalifikowanego, w przypadku gdy odwołanie certyfikatu nie zostało zarejestrowane, odpowiada za szkody wyrządzone jednostkom organizacyjnym albo osobom fizycznym lub prawnym, które w rozsądnych granicach opierały się na certyfikacie, chyba że podmiot świadczący usługi certyfikacyjne wykaże, iż nie dopuścił się niedbalstwa.

W związku z powyższą odpowiedzialnością ustawodawca nałożył na państwa członkowskie obowiązek dopuszczenia w swoim prawie krajowym możliwości ograniczenia zastosowania certyfikatu kwalifikowanego przez podmiot świadczący usługi certyfikacyjne. Podmiot ten powinien posiadać możliwość określenia, w stosunku do jakich czynności prawnych certyfikat nie będzie miał zastosowania. Nie będzie on wówczas odpowiadał za szkody wynikające z zastosowania certyfikatu, jeżeli czynności prawne wykraczają poza określone ramy. W podobny sposób państwa członkow-

[38] Przykładowo, zgodnie z austriacką ustawą dotyczącą podpisu elektronicznego, dostawca usług certyfikacyjnych przed wydaniem certyfikatu kwalifikowanego ma obowiązek, na podstawie urzędowego dowodu ze zdjęciem, w sposób pewny sprawdzić tożsamość i ewentualnie specjalne, istotne z punktu widzenia prawa przymioty osoby, na którą ma zostać wydany certyfikat.

skie mają obowiązek zagwarantowania podmiotom świadczącym usługi certyfikacyjne możliwość określenia w certyfikacie kwalifikowanym wartości maksymalnej transakcji, co do której certyfikat może mieć zastosowanie. W przypadku dokonania przez podmioty transakcji przekraczającej wartość maksymalną określoną w certyfikacie, dostawca usług certyfikacyjnych nie odpowiada za szkody ponad określoną wartość maksymalną transakcji. Warunkiem ograniczenia odpowiedzialności do określonych czynności prawnych lub do określonej wartości maksymalnej transakcji jest zamieszczenie odpowiedniej informacji w certyfikacie, w sposób umożliwiający osobom trzecim rozpoznawanie, w stosunku do jakich czynności prawnych lub powyżej jakiej wartości transakcji odpowiedzialność dostawcy usług certyfikacyjnych zostaje ograniczona.

8. Aspekty międzynarodowe

Główną zaletą *e-commerce* jest jej globalny zasięg. Dzięki elektronicznym nośnikom informacji można w kilka sekund, przy bardzo niskich kosztach, porozumieć się z każdą osobą na świecie posiadającą swój adres *e-mailowy* i dostęp do internetu. Ze względu na globalny charakter handlu elektronicznego, państwa członkowskie Unii Europejskiej zobowiązane są dołożyć wszelkich starań, aby certyfikaty, które są wystawione przez podmiot świadczący usługi certyfikacyjne, pochodzący z państwa trzeciego, jako certyfikaty kwalifikowane, były pod względem prawnym zrównane z certyfikatami wystawionymi przez podmioty świadczące usługi certyfikacyjne, mające siedzibę na obszarze UE. Jednakże zrównanie tych certyfikatów jest uzależnione:

– od faktu spełnienia przez podmiot świadczący usługi certyfikacyjne, pochodzący z państwa trzeciego, wymogów Dyrektywy w sprawie wspólnotowych warunków dotyczących podpisu elektronicznego oraz uzyskania akredytacji w ramach systemu dobrowolnej akredytacji jednego z państw członkowskich. Obie przesłanki muszą zostać spełnione łącznie, nie wystarczy wypełnianie wymogów Dyrektywy. Dopiero uzyskanie akredytacji powoduje zrównanie pod względem certyfikatów kwalifikowanych, wydawanych przez dostawcę z kraju trzeciego, z certyfikatami kwalifikowanymi wydawanymi przez dostawców mających siedzibę na terenie UE. Podmiot może sam wybrać państwo i system dobrowolnej akredytacji, któremu chce

się poddać. Uzyskanie akredytacji w jednym z krajów członkowskich umożliwia prowadzenie działalności na terenie całej UE;

– od faktu poręczenia za certyfikat kwalifikowany przez podmiot świadczący usługi certyfikacyjne na obszarze Unii. W przypadku gdy podmiot świadczący usługi certyfikacyjne, mający siedzibę na obszarze Wspólnoty, poręczy certyfikat kwalifikowany wydawany przez podmiot pochodzący z państwa trzeciego, certyfikat taki zostaje zrównany prawnie z certyfikatem kwalifikowanym wydawanym przez dostawców z terenu UE. Dostawca pochodzący z kraju trzeciego (spoza UE) nie musi wówczas uzyskiwać akredytacji w ramach systemu dobrowolnej akredytacji państwa członkowskiego. Wystarczy odpowiednie potwierdzenie, poręczenie certyfikatu. Podmiot poręczający przyjmuje odpowiedzialność za szkody wyrządzone przez dostawcę usług certyfikacyjnych, za którego poręczył, zgodnie z zasadami odpowiedzialności określonymi w Dyrektywie. Certyfikat poręczyć może wyłącznie podmiot świadczący usługi certyfikacyjne, mający siedzibę na terenie UE. Nie jest wystarczająca działalność na terenie Wspólnoty, poręczający musi mieć na terenie UE swoją siedzibę. Nie będzie więc ważne poręczenie złożone przez podmiot pochodzący z kraju trzeciego, który działa na terenie Unii, ale nie ma na jej terenie swojej siedziby;

– od faktu uznania certyfikatu lub podmiotu świadczącego usługi certyfikacyjne pochodzącego z kraju trzeciego w ramach dwustronnych lub wielostronnych umów pomiędzy Wspólnotą a państwami trzecimi lub organizacjami międzynarodowymi.

Wydaje się, iż w praktyce najczęściej będziemy mieli do czynienia z drugą sytuacją, tj. poręczaniem certyfikatów przez dostawców usług certyfikacyjnych, mających siedzibę na terenie Unii Europejskiej. Najprawdopodobniej dostawcy usług certyfikacyjnych będą zawierać umowy o współpracy i wzajemnie poręczać swoje certyfikaty[39].

W drugiej kolejności zastosowanie będą miały dwustronne lub wielostronne umowy zawierane pomiędzy Wspólnotą i państwami trzecimi lub organizacjami międzynarodowymi. Umowy te będą negocjowane przez Radę po przedstawieniu przez Komisję odpowiednich propozycji, mających na celu efektywne wdrożenie norm i umów międzynarodowych dotyczących usług certyfikacyjnych.

---

[39] Patrz R. S c h l e c h t e r, *Ein europäischer...*, s. 122.

9. Ochrona danych

Państwa członkowskie zobowiązane są do dokonania wszelkich działań, aby podmioty świadczące usługi certyfikacyjne oraz krajowe organy odpowiedzialne za akredytację i nadzór nie naruszały Dyrektywy 95/46/WE Parlamentu Europy i Rady z dnia 24 X 1995 r. w sprawie ochrony osób fizycznych w procesie przetwarzania danych osób i swobody przepływu takich danych[40]. Zgodnie z przepisami Dyrektywy, podmioty świadczące usługi certyfikacyjne mogą zbierać dane osobowe wyłącznie bezpośrednio od osób, których one dotyczą, lub po wyraźnej zgodzie tychże osób i tylko w takim zakresie, jaki jest niezbędny dla wydania i zachowania certyfikatu. Dane te nie mogą być wykorzystywane do innych celów bez wyraźnej zgody osoby, której dotyczą.

Jeżeli krajowe systemy prawne dopuszczają działanie osób pod pseudonimem w miejsce imienia i nazwiska, dopuszczalne jest wydanie takiej osobie certyfikatu i zamieszczenie w miejsce danych osobowych tegoż pseudonimu[41].

10. Komitet do spraw podpisu elektronicznego

Na mocy Dyrektywy został powołany Komitet do Spraw Podpisów Elektronicznych, którego celem jest wspieranie Komisji. Komitet działa na podstawie przyjętego przez siebie regulaminu i precyzuje dane określające wymagania stawiane kwalifikowanym certyfikatom; wymagania dotyczące podmiotów świadczących usługi certyfikacyjne, które wystawiają kwalifikowane certyfikaty; wymagania dotyczące bezpiecznych urządzeń do generowania podpisów; zalecenia dla bezpiecznej weryfikacji podpisu; kryteria określające, jakie muszą zostać spełnione warunki, aby dany organ mógł skutecznie dokonywać weryfikacji urządzeń do generowania podpisów. Ponadto Komitet powinien określić numery referencyjne ogólnie uznanych norm produktów dla podpisów elektronicznych, zgodnie z przepisami Dyrektywy (art. 3 ust. 5).

---

[40] O.JL.1995.281.31 (Dir) Protection of individuals with regard to the processing of personel data and on the free movement of such data. (95/46/EC).

[41] Patrz R. S c h l e c h t e r, *Ein europäischer...*, s. 123.

Państwa członkowskie mają obowiązek notyfikować Komisji oraz pozostałym państwom członkowskim:

– informacje o krajowych systemach dobrowolnej akredytacji; jest to związane zasadą, iż uzyskanie akredytacji w jednym z państw członkowskich umożliwia działalność podmiotu świadczącego usługi certyfikacyjne oraz skuteczność wydawanego przez niego kwalifikowanego certyfikatu, bez wymogu dodatkowych akredytacji, na terenie całej Unii Europejskiej;

– nazwy i adresy krajowych organów właściwych do akredytacji i nadzoru;

– nazwy i adresy wszystkich akredytowanych krajowych podmiotów świadczących usługi certyfikacyjne.

Państwa członkowskie zobowiązane są do notyfikacji dostarczonej zgodnie z powyższą procedurą informacji, a także każdej jej zmiany tak szybko, jak to jest możliwe.

Zgodnie z przepisami Dyrektywy, państwa członkowskie miały obowiązek ustanowienia lub zmiany swojego prawa tak, aby przepisy prawa krajowego były zgodne z przepisami Dyrektywy do dnia 19 lipca 2001 r.