§ 1

KIERUNKI REGULACJI PRAWNYCH NA ŚWIECIE

Kwestie związane z jakością usług podpisów elektronicznych, a co za tym idzie, bezpieczeństwa obrotu za pośrednictwem Internetu, są na tyle ważkie, iż stały się przedmiotem prac legislacyjnych. Mają one na celu zrównanie prawne podpisu elektronicznego z podpisem własnoręcznym oraz wytyczają normy regulujące działalność urzędów certyfikacji. Prawne regulacje podpisu elektronicznego istnieją już w wielu krajach, m. in. USA, Czechach, Wielkiej Brytanii, Niemczech, Hiszpanii, Irlandii... Lista jest długa ponieważ kraje Unii Europejskiej były zobligowane unormować swoje prawo odnośnie podpisu elektronicznego już do połowy lipca 2001 roku. W światowych regulacjach główny nacisk kładzie się na otwarty katalog technologii podpisów, w wiarygodne procedury autoryzacji i weryfikacji składania oświadczeń woli w drodze elektronicznej, ochronę konsumenta, ochronę danych, bezpieczeństwo prawne obrotu, regulacje rynku poświadczania autentyczności podpisów elektronicznych oraz możliwie najwyższy poziom tych usług.

Również Polska jako kandydat do Unii Europejskiej musi dostosować odpowiednio swoje normy prawne w tym zakresie. Prace nad polską ustawą o podpisie elektronicznym rozpoczęto już w 2001 roku. Początkowo istniały dwa projekty, różniące się zasadniczo w wielu punktach, z których powstała finalna wersja ustawy przyjęta przez Sejm 31 sierpnia 2001 roku. Wskutek wniesienia poprawek senackich ustawa wróciła pod obrady Sejmu, gdzie 18 września 2001 roku na ostatnim posiedzeniu w kadencji ostatecznie uchwalono obowiązujący tekst ustawy. Po podpisaniu przez Prezydenta RP, została ogłoszona 15 listopada 2001r. w Dzienniku Ustaw. Vacatio legis dla ustawy wynosi dziewięć miesięcy. Wprowadzenie rozwiązań dotyczących tej kwestii wymaga pośpiechu, gdyż tylko te kraje, które szybko dostosują się do wyzwań społeczeństwa informacyjnego mogą liczyć na największe korzyści. Uchwalona przez Sejm ustawa jest zgodna z Dyrektywą Unii Europejskiej w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego.

Najważniejszym zadaniem ustawy jest usankcjonowanie prawne ważności podpisu elektronicznego oraz uznanie go za wiążący dowód zawarcia umowy. Od chwili, gdy podpis elektroniczny wejdzie do polskiego systemu prawnego, będzie możliwe przeprowadzanie transakcji od początku do końca w Internecie. Wyobraźmy sobie sprzedaż polisy

ubezpieczeniowej on-line. Oto jak może ona wyglądać w nieodległej przyszłości. Klient wypełnia na stronie WWW formularz i otrzymuje ofertę z wysokościami składek. Następnie wybiera polisę, składa podpis elektroniczny i otrzymuje podpisaną umowę, oczywiście również w postaci elektronicznej. Wówczas płaci pierwszą składkę, używając ponownie podpisu elektronicznego. Dziś w Internecie można jedynie uzyskać informację o ofercie towarzystw ubezpieczeniowych i wypełnić formularz, dzięki któremu agent ma szansę wcześniej przygotować umowę. Papierowe dokumenty wciąż dublują techniki komputerowe.

Obecnie niezadowolenie właścicieli firm sprzedających produkty lub usługi za pośrednictwem Sieci jest w pełni uzasadnione. Internetowi dowcipnisie nie próżnują, często podają fałszywe dane i znaczna część transakcji nie jest finalizowana. W przyszłości nie będzie miejsca na takie żarty. Kupującemu, który złoży zamówienie potwierdzone elektronicznym podpisem, trudno będzie wyprzeć się zawarcia umowy. Zagrożone będzie to sankcją karną.

Bardzo istotny jest fakt, że ustawy o podpisie elektronicznym są całkowicie "wolne" technologicznie i nie ograniczają w żaden sposób rozwiązań, które będą wspierać zastosowanie podpisu elektronicznego. W wyniku zastosowania takich rozwiązań nie trzeba będzie zmieniać norm prawnych w razie dalszego rozwoju technologicznego.

---

§ 2
ZAUFANIE ZWYKŁE I KWALIFIKOWANE

Wiarygodność prawna obrotu na stronach WWW zakłada wiele jego poziomów, takich jak konstrukcja instytucji prawa materialnego, dostosowanie procedur odpowiednio do przyjmowanej wartości oświadczeń woli składanych drogą elektroniczną, ochrona prawna komunikowania się w cyberprzestrzeni oraz wyznaczenie poziomu zaufania do osób świadczących usługi dla kontrahentów w Internecie.

Uważa się, że między kontrahentami w sieci najważniejsza rola przypadnie tzw. zaufanej trzeciej stronie (ang. trusted third party), czyli osobom, firmom lub urzędom dostawcom usług poświadczania autentyczności podpisu (ang. certification service providers). Przy podpisie odręcznym taką rolę pełnią notariusze, a w pewnych sytuacjach

adwokaci i radcy prawni oraz urzędnicy. Poziom zaufania publicznego, podobnie jak w stosunku do wyżej wymienionych, zakłada instytucjonalna forma akredytacji przy specjalnym urzędzie nadzorującym podmioty świadczące usługi certyfikacyjne. Przy tym nie neguje się istnienia innej kategorii takich podmiotów, gdyż zgodnie z kierunkiem wytycznych Unii Europejskiej nie ma obowiązku akredytacji. Zaufanie trzeciej strony działa w obrocie niejako na dwóch poziomach zaufania: "bez akredytacji" oraz "z akredytacją". Obie kategorie można określić jako:

- zaufanie zwykłe ("bez akredytacji") czyli nie wykraczające poza ogólne ramy gwarancji i rękojmi powszechnego obrotu cywilno-prawnego;
- zaufanie kwalifikowane ("z akredytacją") odnoszące się do szczególnego poziomu weryfikacji oferowanych usług i związane z tym odpowiednio najwyższe zaufanie do jakości usług poświadczania i certyfikacji. Przypada więc ono podmiotom akredytowanym przy kompetentnym urzędzie nadzorującym i monitorującym usługi wydawania certyfikatów.

Warto zauważyć, że znany i używany na całym świecie system oprogramowania zapewniający "całkiem niezłą prywatność" PGP (ang. pretty good privacy) wymaga tylko znalezienia i zaakceptowania przez strony nawiązujące kontakt dwóch osób, firm lub instytucji, które już mają poświadczenia swoich podpisów. Te dwa podmioty swoim podpisem i autorytetem certyfikują podpisy i klucze innych. Wynika z tego wniosek, iż system poświadczania autentyczności może się obejść bez kontroli urzędów i centralnego monitorowania.

---

§ 3
STRUKTURA KLUCZA PUBLICZNEGO

Światowe rozwiązania prawne wprowadzają pojęcia dwóch rodzajów certyfikatów: zwykłego i kwalifikowanego. Certyfikat kwalifikowany wydawany jest przez podmiot posiadający akredytację Krajowego Centrum Certyfikacji. Wprowadzenie zasady akredytacji, ma na celu zapewnienie użytkowników, że organizacje ubiegające się o pełnienie funkcji zaufanej trzeciej strony są do tego odpowiednio przygotowane i spełniają założenia właściwej im ustawy. Jednakże akredytacja jest całkowicie dobrowolna a organy, które nie będą jej podlegały mogą

wystawiać tzw. certyfikaty zwykłe. W ten sposób powstaje hierarchia centrów certyfikacji oparta o strukturę klucza publicznego (PKI). Infrastruktura Klucza Publicznego (PKI) służy do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów. Większość najważniejszych standardów w dziedzinie bezpieczeństwa teleinformatycznego jest zaprojektowana tak, aby umożliwić współpracę z PKI. Do podstawowych usług PKI należą:

- uwierzytelnianie podmiotów partnerskich, które oznacza pełną identyfikację uczestników transakcji
- uwierzytelnianie danych pozwalające stwierdzić, że informacja była podpisana przez użytkownika
- zapewnienie integralności danych czyli pewności, że informacja podpisana cyfrowo nie została zmieniona
- poręczenie niezaprzeczalności, uniemożliwiające uczestnikom transakcji późniejsze zaprzeczenie podpisu
- zapewnienie odpowiedniego stopnia poufności, umożliwiającej użytkownikom właściwą ochronę danych przed nieuprawnionym ujawnieniem
- zapewnienie prywatności, pozwalającej użytkownikom na nakazanie specjalnej obsługi informacji podczas transmisji.

Idea PKI oparta jest na cyfrowych certyfikatach potwierdzających związek między konkretnymi uczestnikami transakcji a kluczami kryptograficznymi, stosowanymi podczas realizowania bezpiecznych transakcji.

Certyfikat cyfrowy jest wydawany przez Urząd Certyfikacji (Certification Authority - CA), który w momencie wydania dokumentu potwierdza podpisem cyfrowym związek pomiędzy użytkownikiem a kluczem, którego używa. Ponieważ tak wystawiony certyfikat ma zawsze pewien okres ważności (np. jeden rok), należy przewidzieć następujące sytuacje związane z zarządzaniem certyfikatami: rejestracja użytkowników, generowanie certyfikatów, dystrybucja, aktualizacja i unieważnianie.

Struktura PKI składa się z trzech głównych elementów :

- Urzędów Rejestracji (ang. Registration Authority - RA), dokonujących weryfikacji danych użytkownika a następnie jego rejestracji.
- Urzędów Certyfikacji (ang. Certification Authority - CA), wydających certyfikaty cyfrowe. Jest to poprzedzone procesem identyfikacji

zgłaszającego się o wydanie certyfikatu. Pozytywne rozpatrzenie zgłoszenia kończy się wydaniem certyfikatu wraz z datą jego rozpatrywania.

- Repozytoriów kluczy, certyfikatów i list unieważnionych certyfikatów (ang. Certificate Revocation Lists - CRLs). Dostęp do CRLs jest możliwy dzięki protokołom HTTP, FTP, X.500, LDAP i poczcie elektronicznej. Certyfikat może stać się nieważny przed datą jego wygaśnięcia. Przyczyną tego może być np. zmiana nazwiska lub adresu poczty elektronicznej użytkownika czy ujawnienie klucza prywatnego. W takich przypadkach CA odwołuje certyfikat i umieszcza jego numer seryjny na ogólnodostępnej liście CRL.

Struktura PKI jest tworzona w oparciu o Główny Urząd Certyfikacji, przy czym dla każdego z obszarów zastosowań (np. handel elektroniczny, sektor bankowo-finansowy, administracja publiczna), które będą korzystać z PKI, można tworzyć odrębne CA podległe Głównemu Urzędowi. Główny CA określa ogólną politykę certyfikacji, natomiast CA obsługujące dany obszar zastosowań odpowiadając za politykę w tym obszarze. W strukturze podległej danemu CA dla konkretnych zastosowań może istnieć dowolna liczba podległych CA oraz użytkowników. Taka struktura tworzy hierarchię uwierzytelniania, która z kolei określa łańcuch certyfikatów, wiodący od użytkowników aż do cieszącego się ich zaufaniem Głównego CA. Krajowa struktura PKI musi współdziałać ze strukturami PKI innych krajów, aby zapewnić usługi o podobnym do opisanych charakterze w kontaktach międzypaństwowych.

Podstawowe funkcje, które musi realizować każde PKI, aby zapewnić właściwy poziom usług to :

- rejestracja (ang. registration)

Użytkownik końcowy składa wniosek do Organu Rejestracji o wydanie certyfikatu. Jest to związane z dostarczeniem szeregu informacji, wymaganych przez Kodeks Postępowania Certyfikacyjnego (Certification Practices Statement - CPS) wybranego CA. Dane te to np. nazwa własna, nazwa domenowa czy adres IP. Zanim CA wystawi certyfikat sprawdza (korzystając z wytycznych zapisanych w CPS), czy podane przez użytkownika dane są zgodne z prawdą. Jeżeli o certyfikat ubiega się osoba fizyczna, CA weryfikuje także autentyczność własnoręcznego podpisu na wniosku o wydanie certyfikatu.

- certyfikacja (ang. certification)

Jeżeli dane podane przez ubiegającego się o certyfikat we wniosku zostaną potwierdzone, CA wystawia nowy certyfikat (zawierający m.in. klucz publiczny posiadacza) i dostarcza go użytkownikowi. Jednocześnie certyfikat zostaje udostępniony wszystkim zainteresowanym poprzez złożenie go we właściwym repozytorium publicznym.

- generacja kluczy (ang. key generation)

Para kluczy (prywatny i publiczny) może zostać wygenerowana samodzielnie przez użytkownika końcowego lub może on tę operację powierzyć CA. W pierwszym przypadku użytkownik przesyła do CA jedynie swój klucz publiczny w celu poddania go procesowi certyfikacji. Klucz prywatny pozostaje przez cały czas w rękach właściciela, dlatego też metodę tę uważa się za najbardziej bezpieczną. Jeżeli natomiast klucze generuje CA, to są one dostarczane do użytkownika końcowego w sposób gwarantujący ich poufność. Najchętniej wykorzystuje się do tego celu karty mikroprocesorowe (ang. smartcard) czy karty PCMCIA, obie zabezpieczone dodatkowym kodem PIN.

- odnawianie kluczy (ang. key update)

Wszystkie pary kluczy oraz skojarzone z nimi certyfikaty wymagają okresowego odnawiania. Jest to kolejne zabezpieczenie na wypadek ujawnienia klucza prywatnego skojarzonego z kluczem publicznym umieszczonym na certyfikacie. Istnieją dwa przypadki, kiedy wymiana kluczy jest konieczna :

a) upłynął okres ważności certyfikatu

Jest to sytuacja normalna, występująca regularnie co pewien czas (np. raz do roku). Wymiana kluczy odbywa się wtedy w możliwie krótkim czasie, bez dodatkowych formalności.

b) klucz prywatny skojarzony z kluczem publicznym umieszczonym na certyfikacie został skompromitowany

Jest to sytuacja wyjątkowa, a więc wymiana kluczy nie będzie już tak płynna jak poprzednio. W takich przypadkach CA odwołuje certyfikat poprzez umieszczenie jego numeru seryjnego na ogólnodostępnej liście CRL. Od tego momentu stary certyfikat traci ważność i rozpoczyna się procedura wystawiania nowego certyfikatu. Najgorszy przypadek dla każdego CA to kompromitacja klucza prywatnego jego Głównego CA (Root CA). W takim przypadku cała infrastruktura PKI podległa temu

pechowemu CA zostaje uznana za skompromitowaną i musi być tworzona od nowa.

- certyfikacja wzajemna (ang. cross-cerification)

Ponieważ społeczność międzynarodowa nie stworzyła dotąd Globalnego Organu Certyfikacji (Global Root CA), powstało wiele Głównych Organów Certyfikacji (Root CA), początkowo nie powiązanych wzajemnie relacjami zaufania. Certyfikacja wzajemna rozwiązuje ten problem i pozwala użytkownikom z jednej struktury PKI ufać certyfikatom wystawianym przez CA z innej struktury. Główne CA z różnych struktur certyfikują się wzajemnie - może być to certyfikacja jednokierunkowa albo dwukierunkowa.

- odwołanie certyfikatu (ang. revocation)

Istnieją sytuacje, w których zachodzi potrzeba wcześniejszego odwołania certyfikatu. Powodem może być kompromitacja klucza prywatnego, zmiana nazwy przez użytkownika końcowego czy też odejście pracownika z firmy, która wystawiła mu certyfikat. Zdefiniowana w standardzie X.509 metoda odwoływania certyfikatów wykorzystuje wspomniane już Listy Unieważnionych Certyfikatów (Certificate Revocation Lists - CRLs), okresowo publikowane przez CA w tym samym repozytorium, w którym są przechowywane certyfikaty. Każdy certyfikat posiada swój unikalny numer seryjny przypisany przez CA w momencie jego wystawiania. Lista CRL zawiera spis identyfikatorów odwołanych certyfikatów i jest opatrzona znacznikiem czasu wystawionym przez CA.

- odzyskiwanie klucza (ang. key recovery)

Jest to dodatkowe zabezpieczenie na wypadek sytuacji, gdy użytkownik utraci swoje klucze. Jeżeli wszystkie klucze do szyfrowania albo negocjacji kluczy były przechowywane w bezpiecznym archiwum, to będzie można je odzyskać i umożliwić dostęp do zaszyfrowanych danych. Najważniejszym zagadnieniem przy realizacji tej funkcji jest zagwarantowanie, że klucze będzie mógł odzyskać tylko ich właściciel a nie osoba trzecia.

---

§ 4
ROZWIĄZANIA PRAWNE W STANACH ZJEDNOCZONYCH

Pierwszym krajem, który przyjął ustawę o podpisie elektronicznym były Stany Zjednoczone. Prezydent Bill Clinton podpisał 30 czerwca 2000 roku ustawę o podpisach elektronicznych w obrocie krajowym i globalnym (Electronic Signatures in Global and National Commerce Act), która weszła w życie trzy miesiące później. Ustawa amerykańska przyznaje podpisowi elektronicznemu identyczną moc prawną jaką ma podpis złożony na papierze, jednak nie nakłada obowiązku posługiwania się nim. Przewiduje, że w każdej okoliczności należy zagwarantować obywatelom możliwość posługiwania się wyłącznie podpisem odręcznym. Zgodnie z ustawą, podpis elektroniczny jest ciągiem zakodowanych znaków, które jednoznacznie identyfikują użytkownika. Aby uniknąć oszustw w USA każdy podpis będzie weryfikowany dodatkowo poprzez np. wpisanie numeru ubezpieczenia społecznego. Ustawa nie przesądza jaka technologia podpisu elektronicznego może być stosowana, nie ogranicza też rynku usług certyfikacyjnych.

Federalna ustawa amerykańska (tzw. e-sign) weszła w życie 1 października 2000 roku. Przyjętą praktyką w USA jest, iż ustawy federalne mają charakter ramowy, pozostawiając szczegółowe rozwiązania regulacjom stanowym. Ustawa federalna nie jest więc prawem zupełnym, jakie można odnieść do materii podpisu elektronicznego, problematyka ta bowiem jest objęta jeszcze ustawami stanowymi. Dwadzieścia dwa stany wprowadziły, po poprawkach, tzw. Uniform Electronics Transaction Act. Kilka stanów np. Utah, Kalifornia i Washington wprowadziło dodatkowo przepisy dotyczące rejestracji oraz licencjonowania organów certyfikacyjnych.

Amerykańscy analitycy podkreślają, że choć przyjęcie tego aktu prawnego jest niezmiernie istotne dla tworzenia podstaw funkcjonowania elektronicznego obrotu gospodarczego, upłynie jednak sporo czasu zanim elektroniczne podpisy i certyfikaty zyskają powszechną aprobatę i zaufanie. Chociaż Amerykanie mogą już nie wychodząc z domu kupić samochód lub podpisać umowę o kredyt hipoteczny a wszelkie formalności, łącznie z zawarciem umowy mogą być dokonywane elektronicznie to konsumenci na razie wykazują się pewną wstrzemięźliwością w tego rodzaju zakupach on-line. Nie ma obecnie powszechnej świadomości, że podpis elektroniczny to coś naprawdę niezbędnego. Pewną barierą są też wysokie koszty funkcjonowania systemu. Samo wydanie klucza prywatnego to wydatek rzędu 5-10 USD za użytkownika.Do tego należy doliczyć koszty oprogramowania

wahające się między 10 a 100 USD od osoby. Zatem nowa technologia wcale nie musi przynieść firmom znacznych oszczędności w związku z eliminacją wytwarzania i przechowywania papierowych dokumentów.

---

§ 5
ROZWIĄZANIA PRAWNE W UNII EUROPEJSKIEJ

Regulacja prawna podpisu elektronicznego na poziomie Unii Europejskiej była koniecznością, aby zharmonizować, w zakresie wynikającym z kompetencji Komisji Europejskiej, minimalne ramy prawne dla podpisu elektronicznego tak, aby różnice uregulowań pomiędzy krajami członkowskimi nie naruszały zasad swobody przepływu towarów i usług w rynku wewnętrznym.

Działając na podstawie art. 47 § 2 oraz art. 55 i 95 Traktatu powołującego Wspólnotę Europejską, 13 grudnia 1999 r. Parlament Europejski i Rada przyjęły Dyrektywę nr 1999/93/WE w sprawie ram wspólnotowych dla podpisu elektronicznego. Stanowi ona pierwszy przykład dyrektywy o tak zwanym Light and flexible approach. Oznacza to, w rozumieniu Komisji Europejskiej, że rynek zachowuje się rozsądnie i poza minimalnymi uregulowaniami prawnymi, niezbędnymi dla zapewnienia swobody przepływu towarów i usług, nie ma konieczności regulacji wszystkich elementów funkcjonowania podpisu elektronicznego.

Pierwotnym źródłem inspiracji dla projektu były wstępne prace nad jednolitymi regułami międzynarodowymi dotyczącymi podpisu elektronicznego, jakie zostały podjęte przez Komisję ds. Międzynarodowego Prawa Handlowego Organizacji Narodów Zjednoczonych w 1996 r.. W 1997 r. Komisja Europejska opublikowała komunikat zatytułowany: "Zapewnić bezpieczeństwo i zaufanie w komunikacji elektronicznej. W stronę europejskich ram dla podpisu cyfrowego i szyfrowania", a następnie przedstawiła projekt dyrektywy. Przyjęty tekst jest rezultatem kompromisu politycznego państw członkowskich. Członkowie Unii Europejskiej byli zobowiązani przenieść do swojego porządku prawnego postanowienia tej dyrektywy do 19 lipca 2001r.

Celem tej dyrektywy jest stworzenie jednolitych podstaw prawnych dla podpisu elektronicznego, które zapewnią sprawne funkcjonowanie rynku wewnętrznego Wspólnot Europejskich w tej materii. W zamyśle Komisji nowe ramy prawne obejmując zespół kryteriów prawnego uznania podpisu elektronicznego ułatwią działanie handlu elektronicznego i pozwolą konsumentom i podmiotom gospodarczym w Europie na lepsze włączenie się i korzystanie z globalnej sieci.

Dyrektywa ta stanowi warunek bezpieczeństwa prawnego transakcji elektronicznych i z tego względu warunkuje rozwój handlu elektronicznego. Jak wskazano w preambule do dyrektywy, te nowe formy podpisu będą stosowane w sektorze publicznym w kontaktach z administracją krajową i wspólnotową oraz w kontaktach pomiędzy tymi administracjami, jak również z obywatelami i podmiotami gospodarczymi, na przykład: przy okazji przetargów publicznych, w regulowaniu należności fiskalnych, przekazywaniu składek na ubezpieczenie społeczne lub zdrowotne itp. Stosowanie podpisu elektronicznego będzie się coraz bardziej rozwijać mnożąc okoliczności i warunki, w jakich stosowanie tej formy czynności prawnych, zrównane w skutkach prawnych z dotychczas stosowanymi, będzie stanowić równoprawną formę w obrocie gospodarczym.

Cel i zasięg dyrektywy

Dyrektywa europejska na temat ram wspólnotowych dla podpisu elektronicznego ma na celu ułatwienie korzystania oraz prawne uznanie podpisu elektronicznego (art. 1). Przyjęte zostało podejście funkcjonalne do podpisu elektronicznego, które można odnaleźć w ustawach wzorcowych w sprawie handlu elektronicznego przyjętego przez Komisję ds. Międzynarodowego Prawa Handlowego Organizacji Narodów Zjednoczonych (CNUDCI). Dyrektywa ma na celu ustanowienie ram prawnych dla podpisu elektronicznego oraz usług certyfikacji. Paragraf 2 tego artykułu wyklucza z zakresu dyrektywy "aspekty związane z zawieraniem oraz ważnością umów oraz innymi wymaganiami prawnymi, jeżeli ustawodawstwo krajowe lub wspólnotowe zawiera wymagania formalne w tym zakresie". Dyrektywa nie odnosi się również do zasad oraz ograniczeń używania dokumentów, które przewidują ustawodawstwa krajowe i wspólnotowe.

W preambule dyrektywy odnajdujemy również zapis o wykluczeniu z jej zasięgu sieci zamkniętych, których funkcjonowanie w wymianie gospodarczej może być regulowane zgodnie z zasadami swobody

kontraktowania. Jednakże podpis elektroniczny stosowany w obrębie takich sieci winien korzystać z takich samych gwarancji dopuszczalności jako dowód przed sądami powszechnymi, jak podpis elektroniczny regulowany dyrektywą, stosowany w sieciach otwartych.

Postanowienia dyrektywy, nie wykraczają poza kompetencje Komisji i pozostawiają państwom członkowskim pole manewru co do ewentualnego rozszerzenia zasięgu uregulowań prawnych dotyczących podpisu elektronicznego.

Niektórzy ustawodawcy europejscy wprowadzili uregulowania nowatorskie, a czasem nawet rewolucyjne w tej dziedzinie. Na przykład we Francji przy okazji dyskusji w Senacie nad ustawą nr 2000-230 z 13 marca 2000 r. w sprawie dostosowania przepisów o dowodzie do technologii informacyjnych oraz w sprawie podpisu elektronicznego, wprowadzono przepisy pozwalające na tworzenie i przechowywanie na nośnikach elektronicznych "aktów autentycznych" (akty prawne, do których sporządzenia potrzebna jest interwencja notariusza lub urzędnika państwowego) w warunkach określonych przez dekret Rady Państwa. Należy jednakże wskazać, że przyjęcie tego dekretu nie nastąpi szybko, praktyczne wprowadzenie w życie tego zapisu wymaga bowiem jeszcze długich prac i konsultacji eksperckich oraz przygotowania notariuszy do realizacji tego zadania.

Istotnym zapisem dyrektywy jest artykuł 3.7, który przewiduje, że stosowanie podpisu elektronicznego w sektorze publicznym może być poddane dodatkowym wymaganiom. Wymagania te muszą jednak spełniać kryteria obiektywności, przejrzystości, proporcjonalności oraz niedyskryminacji i nie powinny stanowić przeszkody do świadczenia usług ponadgranicznych dla obywateli. Można je stosować jedynie w szczególnych celach, takich jak specyficzne potrzeby związane z administracją fiskalną lub socjalną.

Definicje wg Dyrektywy UE

Artykuł 2.3 dyrektywy definiuje podpisującego jako "każdą osobę, która dysponuje urządzeniem do tworzenia podpisu na swój własny użytek lub użytek instytucji, lub osoby fizycznej, lub prawnej, którą reprezentuje". Definicja ta jest interpretowana bardzo szeroko, mowa jest bowiem tutaj o "każdej osobie", co pozwala przypuszczać, że obejmuje ona osoby fizyczne i prawne. Zresztą w komunikacie z 8 października 1997 r. Komisja zaproponowała, aby "klucze mogły być

przyznawane osobom prywatnym lub prawnym (na przykład spółkom z ograniczoną odpowiedzialnością)". Niektóre ustawodawstwa europejskie dokonały takiej właśnie interpretacji. Podpis osób prawnych jest dopuszczalny w prawie brytyjskim i włoskim, możliwość taką przewiduje również projekt ustawy belgijskiej. W ustawie wzorcowej CNUDCI na temat handlu elektronicznego termin "osoba" obejmuje zarówno osoby fizyczne, jak i prawne.Oznacza to, że osoba prawna może dysponować podpisem elektronicznym oraz odpowiadającym mu certyfikatem, który będzie wskazywał nazwę osoby prawnej bez wskazania reprezentującej ją osoby fizycznej.

Dyrektywa definiuje podpis elektroniczny jako "dane w formie elektronicznej załączone lub logicznie połączone z innymi danymi elektronicznymi i które służą jako metoda autoidentyfikacji" (art. 2.1). Definicja ta obejmuje całość technik pozwalających na realizację drogą elektroniczną funkcji podpisu klasycznego, to jest: identyfikację podpisującego oraz wyrażenie przez niego woli przystąpienia do zawartości podpisywanej wiadomości. Definicja ta odzwierciedla wolę Komisji zdefiniowania podpisu elektronicznego w sposób, który pozwala na objęcie wszelkich szczególnych technik podpisu elektronicznego, jeżeli pozwalają one samodzielnie lub w kombinacji na spełnienie funkcji podpisu.

Dyrektywa zawiera rozróżnienie pomiędzy terminami "podpis elektroniczny" oraz szczególną techniką podpisu elektronicznego "zaawansowanym podpisem elektronicznym" (art. 2.2.). W zakres tej definicji wchodzi podpis, który spełnia następujące wymagania:

a) należy wyłącznie do sygnatariusza,
b) pozwala na identyfikację sygnatariusza,
c) jest stworzony przy użyciu środków, które pozostają pod wyłączną kontrolą sygnatariusza,
d) jest połączony z danymi, do których się odnosi w taki sposób, że wszelka późniejsza modyfikacja tych danych jest możliwa do wykrycia.

Wybór terminu "zaawansowany podpis elektroniczny" jest wyborem neutralności technicznej, co pozwoli na uniknięcie jego szybkiego zdezaktualizowania oraz otwiera drogę do poszukiwań nowych technik podpisu.

Nie ulega jednak wątpliwości, że obecnie jedynie metoda podpisu cyfrowego opartego na kryptografii asymetrycznej odpowiada definicji

zaawansowanego podpisu elektronicznego w rozumieniu dyrektywy. Prace normalizacyjne prowadzone na forum międzynarodowym wskazują, że określenie poziomu bezpieczeństwa podpisu elektronicznego mającego spełniać wymagania zaawansowanego podpisu elektronicznego może faworyzować karty z mikroprocesorami jako metodę bezpieczniejszą.

Skutki prawne podpisu elektronicznego wg. Dyrektywy UE

Dyrektywa reguluje również skutki prawne podpisu elektronicznego. Cel ten spełnia art. 5, który zawiera dwie klauzule: równouprawnienia oraz zakazu dyskryminacji.

- klauzula równouprawnienia (art. 5.1) zmierza do równouprawnienia zaawansowanego podpisu elektronicznego z podpisem odręcznym, jeśli spełnione są następujące warunki: podpis musi mieć oparcie w certyfikacie określonym w art. 2.10 dyrektywy oraz musi być stworzony za pomocą bezpiecznej metody, takiej, jaką przewiduje aneks nr 3 do dyrektywy. Oznacza to, że podpis elektroniczny powinien być uznany za dowód przed organami sądowymi i powinien mieć taką samą siłę dowodu jak podpis odręczny. Klauzula ta odnosi się wyłącznie do zaawansowanego podpisu elektronicznego.

- klauzulę niedyskryminacji (5.2) stosuje się, jeśli warunki, jakim podlega klauzula równouprawnienia, nie są spełnione. Państwa członkowskie są zobowiązane do czuwania, aby odmowa skuteczności prawnej i dopuszczalności jako dowodu w sądzie podpisu elektronicznego nie była umotywowana jedynie tym, że podpis jest w formie elektronicznej lub nie towarzyszy mu kwalifikowany certyfikat, nie towarzyszy mu certyfikat wydany przez dostawcę usług certyfikacji akredytowany zgodnie z dyrektywą lub nie jest stworzony przez bezpieczną metodę tworzenia podpisów.

Warunki dopuszczalności i ważności zaawansowanego podpisu elektronicznego

Dopuszczalność przedstawienia przed sądem dokumentu podpisanego elektronicznie oraz zakwalifikowanie podpisu jako zaawansowanego zależy od spełnienia warunków związanych z: certyfikatem, dostawcą usług certyfikacji i procesem tworzenia podpisu elektronicznego.

W załączniku nr I do dyrektywy zostały określone wymagania co do niezbędnych informacji, które muszą się znaleźć w certyfikatach "kwalifikowanych". Załącznik nr II zawiera wymagania, jakie muszą

spełniać dostawcy usług certyfikacji wydający certyfikaty "kwalifikowane". Natomiast w załączniku nr III znalazły się wymagania minimalne dotyczące gwarancji, jakie muszą być zapewnione przez bezpieczną metodę tworzenia podpisu elektronicznego.

Proces akredytacji instytucji certyfikujących

Tworzenie zaawansowanych podpisów elektronicznych będzie się opierało na dobrowolnym systemie akredytacji instytucji świadczących usługi certyfikacji.

---

§ 6
DYREKTYWA UE A ROZWIĄZANIA PRAWNE PAŃSTW EUROPEJSKICH

Państwa europejskie, które w pełnym lub niepełnym zakresie wprowadziły przepisy dotyczące podpisów elektronicznych, to m.in. : RFN, Hiszpania, Irlandia oraz Czechy, a także Austria, Belgia, Francja, Finlandia, Słowacja i Słowenia.

Na uwagę zasługuje w tej grupie RFN, której gospodarka systematycznie i intensywnie przygotowuje się do wdrażania technologii informatycznych na szeroką skale. Niemieckie ustawy: z 1 sierpnia 1997 r. (jest to szerszy akt prawny odnoszący się do usług multimedialnych pod tytułem Informations-und Kommunikationsdienste-GesetzIuKDG, Art. 3 Signaturgesetz - SigG) oraz z 22 lipca 1997 r. (Signaturgesetz uzupełniona przez SignaturVerordnung) odróżnia to, iż posługują się kategoria podpisu cyfrowego, a nie elektronicznego. Definiują one podpis cyfrowy jako oparty na zasadzie dwóch kluczy (do kodowania oraz dekodowania), prywatnego i publicznego, ale otwarte są i na inne procedury podpisu. SigG nie zakłada mocy prawnej podpisu cyfrowego na równi z podpisem własnoręcznym na zasadzie powszechnej. To ograniczenie skuteczności prawnej podpisu cyfrowego zostało już poprawione.

Regulacje niemieckie ustanawiają nadzór oraz kontrole nad usługami certyfikacyjnymi, w tym na szczeblu federalnym, i postulują przymus akredytacyjny, co zostało wszakże zmienione ze względu na przepisy dyrektywy UE 99/93, zakładające jedynie dobrowolna akredytacje.

W Republice Czeskiej oraz Irlandii przyjęto rozwiązania oparte na dyrektywie unijnej z 13 grudnia 1999 r. Dla przykładu, w ustawie irlandzkiej (The Electronic Commerce Act 2000) definicje podpisów elektronicznych sformułowano dokładnie tak, jak czyni to dyrektywa UE (1999/93/EEC). W Hiszpanii regulacje dotyczące podpisu cyfrowego uchwalono jeszcze przed dyrektywa unijna (dekret królewski 14/99 z 17 września 1999 r. - ustawa o podpisie cyfrowym). Według regulacji hiszpańskiej zaawansowany podpis elektroniczny, w istocie określony jako podpis cyfrowy, ma tę sama moc prawna, co podpis odręczny.

Na tle porównawczym zwraca uwagę, ze regulacje dotyczące podpisów elektronicznych sprzed uchwalenia dyrektywy UE 99/93 nawiązują do kategorii podpisu cyfrowego, podczas gdy ustawy późniejsze posługują się pojęciem "podpis elektroniczny".

---

§ 7
POLSKA USTAWA O PODPISIE ELEKTRONICZNYM

Przyjęta 27.07.2001 ustawa o podpisie elektronicznym powstała w wyniku blisko 9 miesięcznych prac nad projektami wniesionymi przez grupę posłów oraz projektem rządowym. Prace w Sejmowej Podkomisji Nadzwyczajnej toczyły się z licznym udziałem ekspertów ze środowisk informatycznych (Polskie Towarzystwo Informatyczne; Polska Izba Informatyki i Telekomunikacji), bankowych (Narodowy Bank Polski, Związek Banków Polskich). Zasadniczymi celami w trakcie prac nad kształtem ustawy było dostosowanie polskiego prawa do wymagań społeczeństwa informatycznego i zachowanie zgodności ze standardami europejskimi zawartymi w Dyrektywie Unii Europejskiej.

W dniu 11 października 2001 Prezydent RP podpisał ustawę o podpisie elektronicznym sposobem tradycyjnym oraz elektronicznie.

15 listopada br. opublikowano (Dz. U 130 poz. 1450) ustawę o podpisie elektronicznym. Z mocy art. 59 ust. 1 Ustawa wchodzi w życie 9 miesięcy po opublikowaniu, czyli 16 sierpnia 2002. W tym dniu, dzięki zmianie przepisu art. 60 kc, podpis elektroniczny zaistnieje w sposób pełny jako środek wyrażania oświadczenia woli ponieważ, zgodnie z nowym brzmieniem art. 78 ust 2:
"Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy

ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej."

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym staje na stanowisku, że w obrocie prawnym będzie mógł być stosowany każdy rodzaj podpisów elektronicznych. Jedynie jednak kwalifikowana postać bezpiecznego podpisu elektronicznego będzie mieć charakter równorzędny z podpisem własnoręcznym. Stosowne zmiany w kodeksie cywilnym przewidują, że elektroniczne oświadczenia woli opatrzone bezpiecznym podpisem elektronicznym weryfikowanym z pomocą kwalifikowanego certyfikatu są równoważne zachowaniu formy pisemnej z podpisem własnoręcznym. Skutki prawne wywoła jednak wyłącznie podpis złożony w okresie ważności certyfikatu. Dlatego też każdy z uczestników obrotu może i powinien sprawdzić ważność certyfikatu drugiej strony (co nie wyłącza ryzyka związanego z ewentualnym unieważnieniem certyfikatu). Ustawa dopuszcza również zwykły podpis elektroniczny, który nie jest równoważny własnoręcznemu, lecz będzie stanowił dowód podległy swobodnej ocenie sądu. W ślad za Dyrektywą 1999/93/EC ustawa stanowi, że zwykłemu podpisowi elektronicznemu nie będzie można odmówić ważności i skuteczności wyłącznie ze względu na jego elektroniczną formę. Jako osobną kategorię wprowadzono znakowanie czasem zrównane z formą tzw. daty pewnej. Ten rodzaj podpisu będzie miał duże znaczenie dowodowe, gdyż bezpieczny podpis elektroniczny jest ważny tylko, jeśli został złożony w okresie ważności certyfikatu.

Bezpieczny podpis elektroniczny musi być przyporządkowany wyłącznie do (jednej) osoby fizycznej składającej podpis. Powinien być sporządzany za pomocą podlegających wyłącznej kontroli tej osoby bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu. Musi być powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych będzie rozpoznawalna. Podpisy elektroniczne będą mogły posiadać zarówno osoby fizyczne, jak i prawne. W tym ostatnim przypadku posługiwać się nimi będzie mogła wyłącznie oznaczona osoba fizyczna. Ustawa nie daje innej możliwości elektronicznego podpisu osób prawnych a także wyłącza podpis grupy osób. Jak się wydaje możliwe technologicznie i prawnie będzie wielokrotne podpisanie dokumentu elektronicznego przez poszczególne osoby fizyczne. Osoba fizyczna może złożyć podpis elektroniczny w imieniu osoby prawnej, innej osoby

fizycznej lub jednostki organizacyjnej nie posiadającej osobowości prawnej. Zmiana po stronie osoby reprezentującej firmę powodować będzie konieczność unieważnienia poprzedniego i wydania nowego podpisu. Ponieważ podobnie jak w przypadku kart płatniczych trudno całkowicie wykluczyć pozyskanie karty z kluczem prywatnym oraz wyłudzenia PIN-ów pamiętać należy, że ryzyko dokonywanych czynności obciążać będzie właściciela. Zasadniczo odpowiedzialność wystawcy certyfikatu ograniczona będzie do sytuacji, gdy dane w certyfikacie będą niezgodne z prawdą.

Nowa ustawa o podpisie elektronicznym zawiera szereg przepisów o charakterze administracyjnym dotyczących infrastruktury certyfikacyjnej. Wyłącznie działalność w charakterze kwalifikowanego podmiotu certyfikującego podlegać będzie wpisowi do rejestru podmiotów kwalifikowanych i przed rozpoczęciem działalności wymagać będzie przeprowadzenia obligatoryjnej kontroli. Ustawa nie przewiduje dobrowolnej akredytacji dla podmiotów z poza kręgu podmiotów kwalifikowanych. Certyfikat wydany przez podmiot świadczący usługi certyfikacyjne, nie mający siedziby na terytorium Rzeczypospolitej Polskiej i nie świadczący usług na jej terytorium, może zostać zrównany pod względem prawnym z kwalifikowanymi certyfikatami wydanymi przez podmiot certyfikujący, mający siedzibę lub świadczący usługi w Polsce pod warunkiem uzyskania akredytacji. Dopuszczalne będzie gwarantowanie przyjęcia odpowiedzialności przez podmiot polski za działalność certyfikacyjną podmiotu zagranicznego. Uznanie polskiego podpisu elektronicznego w innych jurysdykcjach zależeć będzie z zasady od podpisania stosownych umów.

Przepisy ustawy zostały sformułowane w sposób neutralny technologicznie. Stąd istotne znaczenie będą miały szczegółowe rozwiązania przepisów rozporządzeń wykonawczych do ustawy, które określą m.in. wymogi jakie muszą spełniać bezpieczne urządzenia służące złożeniu lub weryfikacji podpisów elektronicznych. W praktyce od treści rozporządzeń zależeć będzie dostosowanie starych czy opracowanie nowych aplikacji. Od rozporządzeń zależeć będzie czy nośnikiem bezpiecznego podpisu będzie karta procesorowa czy również plik lub dyskietka oraz jakie warunki będą musiały być zachowane dla złożenia podpisu z pomocą komputera lub komórki. Dopuszczalne będą rozwiązania inne niż najpopularniejszy obecnie i gotowy do stosowania podpis cyfrowy. Oprócz podpisów opartych na asymetrycznej kryptografii

obecna ustawa umożliwi wykorzystanie rozwiązań biometrycznych lub innych wypracowanych później. Wydanie rozporządzeń wykonujących przepisy ustawy o podpisie elektronicznym może, ale nie musi nastąpić przed wejściem w życie nowego prawa.

W ciągu roku Minister Finansów dostosuje przepisy o opłatach skarbowych za czynności administracyjne (znaczki skarbowe). Banki i organy władzy publicznej mają dwa lata na dostosowanie swojej działalność w zakresie świadczenia usług związanych z podpisem elektronicznym oraz wykorzystania systemów teleinformatycznych związanych ze świadczeniem usług. Jednakże organy władzy publicznej mają cztery lata od wejścia w życie ustawy na udostępnienie odbiorcom usług certyfikacyjnych wnoszenia podań i wniosków oraz innych czynności w postaci elektronicznej, w przypadkach gdy przepisy wymagają składania ich w określonej formie lub według określonego wzoru. Możliwość zdalnego wnoszenia podań, składania deklaracji podatkowych nie nastąpi natychmiast wraz z początkiem obowiązywania nowej ustawy i wymagać będzie stopniowego dostosowania prawa. Nie należy oczekiwać ułatwień w dostępie do urzędów oraz zmian w formie obrotu nieruchomościami, prawie rodzinnym oraz w zakresie weksli oraz czeków.

Podpisem elektronicznym będą mogły być podpisane jedyne dokumenty sporządzone w formie elektronicznej, bez względu na to, na jakim nośniku będą przenoszone (za pomocą sieci, CD-Romu, czy dyskietki). Nie będzie możliwe podpisanie dokumentu papierowego podpisem elektronicznym. W projektach ustawy nie przewiduje się, aby umowy zawarte z użyciem podpisu elektronicznego mogły zastąpić umowy zawierane w formie aktu notarialnego. Nie będzie więc dopuszczalne zawarcie umowy kupna sprzedaży nieruchomości za pośrednictwem Internetu. Niektóre czynności, takie jak sporządzenie testamentu czy zawarcie małżeństwa, również będą wymagać odręcznego podpisu.

Istotnym mankamentem nowej ustawy jest brak zmian w przepisach kodeksu postępowania cywilnego. W szczególności nie zmieni się sposób wprowadzania dokumentów elektronicznych jako dowodu do procesu cywilnego. Jak się wydaje w przypadku sporu dokument podpisany elektronicznie nadal będzie przedkładany sądowi w formie wydruku, będącego jedynie początkiem dowodu na piśmie. Braki zmian w kodeksie postępowania administracyjnego będą w znacznej mierze do usunięcia w

drodze nowej wykładni istniejącego prawa. Ustawa stanowi konieczny warunek i ważny krok naprzód w zakresie elektronicznego obrotu prawnego w naszym kraju. Wczesne wykorzystanie korzyści elektronicznej administracji i gospodarki zależeć będzie jednak od zmiany świadomości oraz zdecydowanej woli politycznej i nakładów przeznaczanych na te cele.

FF & LL

FOURTH SECTION

CASE OF LAWYER PARTNERS, A.S. v. SLOVAKIA

(Applications nos. 54252/07, 3274/08, 3377/08, 3505/08, 3526/08, 3741/08, 3786/08, 3807/08, 3824/08, 15055/08, 29548/08, 29551/08, 29552/08, 29555/08, 29557/08)

JUDGMENT

STRASBOURG

16 June 2009

FINAL

06/11/2009

This judgment may be subject to editorial revision.

In the case of Lawyer Partners, a.s. v. Slovakia,

The European Court of Human Rights (Fourth Section) sitting as a Chamber composed of:

Nicolas Bratza, ***President,***
Lech Garlicki,
Giovanni Bonello,
Ljiljana Mijović,
Ján Šikuta,
Päivi Hirvelä,
Mihai Poalelungi, ***judges,***
and Lawrence Early, ***Section Registrar*****,**

Having deliberated in private on 26 May 2009,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in fifteen applications (nos. 54252/07, 3274/08, 3377/08, 3505/08, 3526/08, 3741/08, 3786/08, 3807/08, 3824/08, 15055/08, 29548/08, 29551/08, 29552/08, 29555/08, 29557/08) against the Slovak Republic lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a private limited company, Lawyer Partners a.s. ("the applicant company"). The dates on which the applications were lodged are set out in Appendix I.

2. The applicant company was represented by Mr J. Fridrich, a lawyer practising in Bratislava. The Slovak Government ("the Government") were represented by their Agent, Mrs M. Pirošíková.

3. The applicant company alleged that its right of access to a court had been violated as a result of the ordinary courts' refusal to register actions submitted by it in electronic form.

4. On 3 July 2008, after having decided to give priority to the above applications (Rule 41 of the Rules of Court), the President of the Fourth Section decided to give notice of the applications to the Government. It was also decided to examine the merits of the applications at the same time as their admissibility (Article 29 § 3).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

5. The applicant is a private limited company with its registered office in Bratislava. The applications on its behalf were lodged by Mr D. Paľko and Mr M. Morong, the chairman and vice-chairman of its managing board.

A. Background to the case

6. On 15 July 2005 the applicant company concluded a contract with Slovak Radio, a public-law institution. Under that contract, taken together with two additional ones concluded on 20 September 2005 and 27 January 2006, the applicant company acquired the right, in exchange for compensation paid to Slovak Radio, to recover unpaid broadcast receiver licences in 355,917 cases, plus additional sums for default in those payments.

7. On 20 October 2008 the Bratislava I District Court confirmed the validity of the above contracts. The decision became final on 5 November 2008.

B. The applicant company's attempts to institute civil proceedings

8. The applicant company was obliged to sue those persons who had refused to pay the debt which it had acquired the right to recover. The applicant company prepared individual actions with a request for payment orders to be issued against the debtors. Given the number of persons concerned, the actions were generated by means of computer software and recorded on Digital Versatile Discs (DVD). The DVDs were sent to the district courts concerned, accompanied by an explanatory letter.

9. Thus the applicant company, on 31 March 2006 and 24 July 2006, filed actions, in electronic form, with several district courts. On 19 October 2006, after officials of the Ministry of Justice had stated that courts were in a position to register such actions, the applicant resubmitted the first group of actions to the courts concerned on DVDs. The courts refused to register the actions, indicating that they lacked the equipment to receive and process submissions made and signed electronically. Further relevant details of the applications under examination are set out in Appendix I.

10. In one case the applicant company submitted, on 14 December 2006, with the agreement of the Svidník District Court, a printed version of the 379 actions it had filed on a DVD on 31 March 2006. The documents in support of the claims remained available on the DVD exclusively. The file numbers indicate that the District Court registered those actions as having been filed in 2007.

11. On 15 December 2008 the applicant company informed the Court that its claims relating to the actions which the courts had refused to register had become statute-barred.

C. Constitutional proceedings

12. In 2006, following the district courts' refusal to register the actions it had submitted on DVDs, the applicant company lodged a complaint with the Constitutional Court in respect of each individual refusal. Referring to Article 6 § 1 of the Convention and its constitutional equivalent, it alleged a violation of its right of access to a court.

13. The Constitutional Court rejected the complaints in the cases under consideration as having been lodged outside the statutory time-limit of two months. The decisions stated that the applicant company had earlier learned, in

the context of its previous attempts to file actions electronically, that district courts lacked the necessary equipment for processing such actions and had failed to file a complaint with the Constitutional Court at that time. The Constitutional Court considered it irrelevant that the above-mentioned time-limit had been complied with in respect of the district courts' refusal to register actions in those cases which underlay the constitutional complaints under consideration (further details of the individual proceedings are set out in Appendix I).

D. Action taken by the Ministry of Justice

14. On 31 March 2006 several courts asked the Ministry of Justice for instructions as to how they should process the applicant company's submissions filed in electronic form. The Ministry advised the courts to wait until the position had been analysed.

15. In a letter of 3 April 2006 the Ministry stated that as ordinary courts did not have an electronic registration facility, the conditions for receiving submissions in electronic form as laid down in Act 215/2002 Coll. were not met.

16. At meetings with presidents of district and regional courts held on 24 November 2006 and 1 to 2 February 2007 the Ministry of Justice concluded that ordinary courts were duly equipped for receiving submissions bearing a secured electronic signature.

17. A press release issued by the Ministry of Justice on 16 October 2008 indicates that the Ministry had published on its website the electronic addresses of individual courts and information about the filing of submissions signed electronically.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The Code of Civil Procedure and Regulation no. 543/2005

18. Article 42 § 1 of the Code of Civil Procedure, as amended with effect from 1 May 2002, reads:

> **"Submissions to a court can be made in written form, orally into the record, by means of electronic devices subject to the submission bearing a secured electronic signature in accordance with a special law, by telegraph or by fax."**

19. Regulation no. 543/2005 governs, *inter alia*, the organisation of work within district courts and regional courts, including their registries. The relevant provisions read:

"Section 129

> **Submissions received by the registry which contain a petition for proceedings to be brought shall be registered by means of technical and**

software devices approved by the Ministry of Justice and designed for processing courts' agenda.

Section 132

Receipt of submissions made by electronic means and bearing a secured electronic signature

Submissions received by means of electronic devices and having a secured electronic signature shall be dealt with in accordance with special law[1]. Such submissions are to be transmitted to the court's central office for proceeding in accordance with section 129."

B. The Electronic Signature Act (Act no. 215/2002 Coll.) and Regulation no. 542/2002

20. The Act on Electronic Signature 2002 governs the establishment and use of electronic signature, the rights and obligations of persons in that context and protection of documents signed electronically (section 1).

21. At the relevant time Regulation no. 542/2002 governed the use of electronic signature in, *inter alia*, administrative relations. It was issued by the National Security Authority and entered into force on 1 October 2002. Sections 6-12 set out details on establishment and functioning of an electronic registry within public authorities which use secured electronic signature, the filing, processing and handling of electronic documents as well as their format and transfer between the dispatcher and the addressee.[2]

C. The Constitutional Court Act 1993 (Act no. 38/1993 Coll., as amended)

22. Section 53(3) provides that a complaint to the Constitutional Court can be lodged within a period of two months from the date on which the decision in question has become final and binding or on which a measure has been notified or on which notice of other interference has been given. As regards measures and other interferences, this period commences when the plaintiff could have become aware of them.

D. The Constitutional Court's practice

23. In the majority of the cases examined in the course of 2007 the Constitutional Court took the same approach as indicated in paragraph 13 above, namely that the period of two months under section 53(3) of the Constitutional Court Act 1993 had started running not later than in April 2006, when the applicant company had learned for the first time that ordinary courts were not in a position to register submissions in electronic form.

24. In a different decision, delivered on 4 January 2007, the Constitutional Court declared admissible a complaint in respect of the refusal, by the Čadca District Court, to register actions lodged electronically on 24 July 2006

(proceedings no. III. ÚS 7/07). In its judgment on the merits of 20 December 2007 the Constitutional Court found a violation of Article 6 § 1 of the Convention. It held that the relevant law entitled parties to file submissions to courts in electronic form. Public authorities were obliged to establish facilities for receiving and processing such submissions. In the above case the Constitutional Court ordered the Čadca District Court to proceed with the actions lodged on DVDs by the applicant company on 24 July 2006. Prior to that, the applicant company had informed the Constitutional Court of the Čadca District Court's earlier refusal to accept a different set of actions which had been filed on DVDs on 31 March 2006.

25. Since 2008 all chambers of the Constitutional Court have systematically approached cases of this type in the manner described in the preceding paragraph. Thus, in twenty-four other cases concerning similar complaints lodged in 2006 the Constitutional Court counted the period of two months from the moment when the applicant company had been informed about the refusal to register each specific submission filed electronically. This approach has been applied even in cases which concerned a second refusal to register an identical submission.

26. In those cases the Constitutional Court found a violation of the applicant company's right of access to a court under Article 6 § 1, holding that the relevant law obliged courts to accept actions submitted by electronic means and that there existed no justification for their refusal to do so. It ordered the district courts concerned to accept those actions as having been filed on the date when they had initially received them and to process any submissions signed electronically.

THE LAW

I. JOINDER OF THE APPLICATIONS

27. The Court notes that the fifteen applications under examination concern the same issue. It is therefore appropriate to join them, in application of Rule 42 § 1 of the Rules of Court.

II. ALLEGED VIOLATION OF ARTICLE 6 § 1 OF THE CONVENTION

28. The applicant company complained that its right of access to a court had been violated in that the district courts concerned had refused to register its actions submitted in electronic form. It relied on Article 6 § 1 of the Convention, which in its relevant part reads as follows:

> **“In the determination of his civil rights and obligations ... or everyone is entitled to a ... hearing ... by [a] ... tribunal...”**

A. Admissibility

1. The arguments of the parties

(a) The Government

29. The Government first objected that it was not clear from the documents submitted whether the applicant company had complied with the six-month time-limit laid down in Article 35 § 1 of the Convention.

30. Secondly, the Government argued that the applicant company had not exhausted domestic remedies as required by Article 35 § 1 of the Convention as it had failed to lodge its complaints under Article 127 of the Constitution in accordance with the formal requirements, as interpreted and applied by the Constitutional Court at the relevant time.

31. In particular, the applicant company had not complied with the time-limit of two months laid down in section 53(3) of the Constitutional Court Act 1993. That period had started running in April 2006, when the applicant company had received replies from several district courts that they were unable to process the submissions it had filed in electronic form on 31 March 2006. The Government relied on the Constitutional Court's argument that the applicant company's subsequent attempts to file actions electronically were irrelevant as it had already learned about the situation complained of in April 2006.

32. The above approach corresponded to the Constitutional Court's established practice at the relevant time. Admittedly, decision no. III. ÚS 7/07 of January 2007 ran counter to that practice. However, that decision was a mere exception and it could not affect the position as it had been delivered after the applications in the present case had been lodged. For similar reasons, the change in the practice of the Constitutional Court, from 2008 onwards (see paragraph 25 above), was irrelevant for the determination of the point in issue.

33. As to the applicant company's allegation that its civil claims had lapsed, the Government submitted that it was open to it to claim damages under Act no. 514/2003 Coll. on liability for damage resulting from the exercise of public authority.

(b) The applicant company

34. The applicant company maintained that it had lodged its applications with the Court within six months as required by Article 35 § 1 of the Convention. That period had started running on the date of delivery to its representative of the Constitutional Court's decisions in the proceedings complained of.

35. The Constitutional Court's decisions to dismiss the complaints in the proceedings complained of as having been submitted out of time were erroneous. In particular, both the Constitution and the Convention guaranteed the right to have one's civil rights or obligations determined by a court. The applicant company's complaints to the Constitutional Court concerned specific actions

against a number of persons which the ordinary courts concerned had refused to register and process. Those complaints had been submitted within the statutory time-limit of two months following the notification by ordinary courts that they would not accept those actions. The fact that in twenty-four other cases with similar factual and legal background the Constitutional Court had admitted the applicant's complaints as complying with formal requirements confirmed that position.

36. There existed no justification for a different approach by the Constitutional Court to the applicant company's complaints, all of which had been submitted in 2006. Such a contradictory approach was incompatible with the principle of legal certainty as interpreted by the Constitutional Court itself. The applicant company pointed out that one of the constitutional judges who had rejected its complaints in the proceedings in issue was registered among the debtors who had failed to pay the broadcast licence.

37. Finally, the applicant company was unable to claim compensation under Act no. 514/2003 Coll. as indicated by the Government. In particular, such a claim could be successful only if the Constitutional Court's decisions in issue had been quashed as being unlawful. However, the decisions relevant to the present case could not be reviewed or quashed.

2. The Court's assessment

38. On the basis of the documents before it, the Court is satisfied that the present applications were lodged within the period of six months from the service on the applicant company's representative of the corresponding decisions of the Constitutional Court (see Appendix I). The relevant requirement laid down in Article 35 § 1 of the Convention has therefore been met.

39. As regards the objection relating to non-exhaustion of domestic remedies, the Court reiterates that in order to exhaust domestic remedies as required by Article 35 § 1 of the Convention, applicants should use the remedies available in compliance with the formal requirements and time-limits laid down in domestic law, as interpreted and applied by domestic courts (see *Akdivar and Others v. Turkey*, 16 September 1996, § 65, *Reports of Judgments and Decisions* 1996-IV). The rules on time-limits are undoubtedly designed to ensure the proper administration of justice and legal certainty. Those concerned must expect those rules to be applied. However, as the Court has held in a different context, the rules in question, or the application of them, should not prevent litigants from making use of an available remedy. Since the issue concerns the principle of legal certainty, it raises not only a problem of the interpretation of a legal provision in the usual way, but also that of an unreasonable construction of a procedural requirement which may prevent a claim from being examined on the merits (see, *mutatis mutandis, Melnyk v. Ukraine*, no. 23436/03, § 23, 28 March 2006, with further references).

40. In the present case the applicant company lodged some 40 complaints with the Constitutional Court, all in 2006, concerning the same issue, namely the ordinary courts' refusal to register actions filed by electronic means. When

considering the applicant's compliance with the two-month time-limit laid down in section 53(3) of the Constitutional Court Act 1993, the Constitutional Court applied that provision in two different manners (see paragraphs 23-25 above).

41. Before the Constitutional Court the applicant company was not entitled to, and did not, complain of an infringement of its rights *in abstracto* on the ground that domestic courts lacked the equipment for processing electronic submissions. It actually complained that the refusal by individual district courts to register and process its specific actions was in breach of its right of access to a court. The Court therefore finds relevant the applicant's argument that it could reasonably be expected that the time-limit laid down in section 53(3) of the Constitutional Court Act 1993 would be counted from the date of notification of the district courts' refusal to register its specific submissions.

42. The Constitutional Court itself took such an approach in the majority of cases brought by the applicant company. The Court has been provided with no explanation as to the difference in the application of the relevant statutory requirement in cases with a similar factual and legal background which were all brought within a relatively short time span.

43. It is also relevant that the applicant company, on 19 October 2006, resubmitted to several courts its actions which had been originally lodged on 31 March 2006. It did so on the ground that officials of the Ministry of Justice had stated in the meantime that the courts were in a position to register such actions. However, the ordinary courts again refused to register the actions, indicating that they lacked the equipment to receive and process submissions made and signed electronically. The applicant company then lodged a complaint with the Constitutional Court within the statutory time-limit of two months.

44. In these circumstances, the Court cannot accept the Government's objection that the applicant company had lodged its constitutional complaints belatedly and had thus failed to exhaust domestic remedies.

45. As regards the Government's objection that it was open to the applicant company to claim damages under Act no. 514/2003 Coll. on liability for damage resulting from the exercise of public authority, the Court reiterates that where there is a choice of remedies, the exhaustion requirement must be applied to reflect the practical realities of the applicant's position, so as to ensure the effective protection of the rights and freedoms guaranteed by the Convention. Moreover, an applicant who has used a remedy which is apparently effective and sufficient cannot be required also to have tried others that were also available but probably no more likely to be successful (see *Adamski v. Poland* (dec.), no. 6973/04, 27 January 2009, with further references).

46. The Court considers that the applicant company's choice to seek redress before the Constitutional Court was reasonable. The Constitutional Court, as the supreme authority charged with the protection of human rights and fundamental freedoms in Slovakia, had jurisdiction to examine the alleged breach of the right forming the subject of the applicant company's complaints before the Court and to provide redress to the company if appropriate (see also paragraph 26 above). Its judgments on the merits of 25 other cases brought by

the applicant company concerning the same issue are in line with this conclusion (see paragraphs 24-25 above). Accordingly, the applicant company was not required to have recourse to the other remedy referred to by the Government.

47. For the above reasons, the Government's objections to the admissibility of the applications must be rejected.

48. The Court further considers, in the light of the parties' submissions, that the complaint raises serious issues of fact and law under the Convention, the determination of which requires an examination of the merits. The Court concludes therefore that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. No other ground for declaring it inadmissible has been established. It must therefore be declared admissible.

B. Merits

49. The applicant argued that the Code of Civil Procedure entitled parties to proceedings to freely choose any of the means mentioned in Article 42 § 1 for making a submission to a court. Given the extremely high number of individual proceedings which it intended to institute, namely more than 70,000, filing the actions in electronic form was the only practical possibility of doing so. Each action was accompanied by a number of annexes and supporting documents. If printed, the documents recorded on the DVDs would fill 43,800,000 pages.

50. With reference to several findings of the Constitutional Court concluding that the applicant company's right of access to a court had been violated the Government admitted that the applicant company's complaint in the cases under consideration raised serious questions of facts and law and was not manifestly ill-founded. It was relevant, however, that the domestic law permitted the filing of actions by other means than electronically. For example, the applicant company had submitted its actions on paper to the Svidník District Court on 14 December 2006.

51. The Court reiterates that the Convention is intended to guarantee rights that are not theoretical or illusory, but practical and effective. This is particularly relevant with regard to Article 6 § 1, in view of the prominent place held in a democratic society by the right to a fair trial. It must also be borne in mind that hindrance can contravene the Convention just like a legal impediment (see *Andrejeva v. Latvia* [GC], no. 55707/00, § 98, ECHR 2009-..., with further references).

52. The right of access to a court is an inherent aspect of the safeguards enshrined in Article 6. It secures to everyone the right to have a claim relating to his civil rights and obligations brought before a court. Where the individual's access is limited either by operation of law or in fact, the Court will examine whether the limitation imposed impaired the essence of the right and, in particular, whether it pursued a legitimate aim and there was a reasonable relationship of proportionality between the means employed and the aim sought to be achieved (for recapitulation of the relevant case-law see, for

example, *Ashingdane v. the United Kingdom*, 28 May 1985, § 57, Series A no. 93 and *Markovic and Others v. Italy* [GC], no. 1398/03, §§ 98-99, ECHR 2006-XIV).

53. In the present case the applicant company lodged or intended to lodge a large number of actions. They concerned several tens of thousands of persons. If printed, the actions together with documents supporting them would fill more than 40 million pages. In these circumstances, the applicant company's choice as to the means of filing the documents cannot be considered an abuse of process or otherwise inappropriate.

54. The ordinary courts, in 2006, refused to register the applicant's actions recorded on DVDs. However, the Code of Civil Procedure had plainly provided for electronic filing. The applicant company cannot be reproached for having availed itself of that facility. Indeed, that mode of lodging its actions was entirely in keeping with the volume of cases which it wished to pursue through the courts. Although the domestic courts pleaded their lack of technical equipment to process the applicant's actions, the Court would recall that the possibility of electronic filing had been incorporated in domestic law since 2002 (see paragraphs 18-21 above).

55. It is true that domestic law has provided for other means of filing documents with courts. The Court finds, however, that in the above circumstances the refusal complained of imposed a disproportionate limitation on the applicant's right to present its cases to a court in an effective manner. In more than 20 other cases the Constitutional Court reached the same conclusion and the Government have not contested this. Furthermore, no relevant reason has been cited by the Government or established by the Court which could serve as justification for such hindrance.

56. The foregoing considerations are sufficient to enable the Court to conclude that in the present cases the applicant company's right of access to a court has not been respected.

There has accordingly been a violation of Article 6 § 1 of the Convention.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

57. Article 41 of the Convention provides:

> **"If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."**

A. Damage

58. The applicant company claimed 506,928,253.43 euros (EUR) in respect of pecuniary damage. It also claimed EUR 4,681,069.49 in respect of non-pecuniary damage, that is, approximately EUR 332 in respect of each individual action submitted to the domestic courts (for further details see Appendix II).

59. The Government argued that there was no causal link between the alleged breach of the Convention and the pecuniary damage claimed. They considered the claim in respect of non-pecuniary damage to be excessive.

60. The Court notes that in the present case an award of just satisfaction can only be based on the fact that the applicant company did not have the benefit of its right of access to a court as guaranteed by Article 6 § 1 of the Convention. Whilst the Court cannot speculate as to the outcome of the proceedings had the position been otherwise, it does not find it unreasonable to regard the applicant company as having suffered a loss of real opportunities (see also *Yanakiev v. Bulgaria*, no. 40476/98, § 88, 10 August 2006, with further references). Ruling on an equitable basis, the Court awards the applicant company EUR 10,000, plus any tax that may be chargeable, for all heads of damage taken together.

61. The Court further reiterates that a judgment in which it finds a violation of the Convention or its Protocols imposes on the respondent State a legal obligation not just to pay those concerned the sums awarded by way of just satisfaction, but also to choose, subject to supervision by the Committee of Ministers, the general and/or, if appropriate, individual measures to be adopted in its domestic legal order to put an end to the violation found by the Court and make all feasible reparation for its consequences in such a way as to restore as far as possible the situation existing before the breach (see *Lungoci v. Romania*, no. 62710/00, § 55, 26 January 2006, with further references).

62. In the case of a violation of Article 6 of the Convention, the applicant should as far as possible be put in the position he or she would have been in had the requirements of this provision not been disregarded. The most appropriate form of redress in cases like the present ones, where an applicant has not had access to a tribunal because of an unjustified refusal to register its actions, would be to register the original submissions as if they had been filed on the date when the applicant company had submitted them to the courts concerned for the first time and to deal with them in keeping with all the requirements of a fair trial (see, *mutatis mutandis*, *Yanakiev v. Bulgaria* cited above, §§ 89 and 90). The Court has noted in this connection that the same approach was taken by the Constitutional Court in the cases in which it found a violation of the applicant company's right of access to a court and that the Slovak courts now have at their disposal the necessary equipment for processing submissions filed by means of electronic devices.

B. Costs and expenses

63. The applicant company also claimed EUR 924,685.94 for the costs and expenses incurred before the domestic courts and EUR 96,047.20 for those incurred before the Court (for further details see Appendix II).

64. The Government contested the claim in respect of the domestic proceedings. In their view the sum claimed in respect of the Convention proceedings was overstated.

65. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that

these have been actually and necessarily incurred and were reasonable as to quantum. In the present case, regard being had to the information in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 8,000 covering costs under all heads.

C. Default interest

66. The Court considers it appropriate that the default interest should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. ***Decides*** **to join the applications;**

2. ***Declares*** **the applications admissible;**

3. ***Holds*** **that there has been a violation of Article 6 § 1 of the Convention;**

4. ***Holds***
   (a) that the respondent State is to pay the applicant company, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts:
      (i) EUR 10,000 (ten thousand euros), plus any tax that may be chargeable, in respect of pecuniary and non-pecuniary damage, and
      (ii) EUR 8,000 (eight thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. ***Dismisses*** **the remainder of the applicant company's claim for just satisfaction.**

Done in English, and notified in writing on 16 June 2009, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Lawrence Early Nicolas Bratza
Registrar President

Appendix I

Application No.	Date lodged	District Court	Date of the action	District Court's reply	Constitution decis	
					No.	Date adop n
54252/07	05/12/2007	Veľký Krtíš	19/10/2006	31/10/2006	III. ÚS 142 /07	17/05 07
		Rimavská Sobota	19/10/2006	28/11/2006	III. ÚS 143/07	17/05 07
3274/08	17/01/2008	Dolný Kubín	19/10/2006	10/11/2006	III. ÚS 130/07	15/05 07
3377/08	17/01/2008	Humenné	19/10/2006	24/10/2006	II. ÚS 139/07	06/06 07
3505/08	17/01/2008	Levice	19/10/2006	24/10/2006	II. ÚS 138/07	06/06 07
3526/08	17/01/2008	Trenčín	19/10/2006	23/10/2006	III. ÚS 129/07	15/05 07
3741/08	17/01/2008	Nové Zámky	19/10/2006	30/10/2006	III. ÚS 131/07	15/05 07
3786/08	17/01/2008	Nové Zámky	24/07/2006	30/10/2006	III. ÚS 253/07	27/09 07
3807/08	17/01/2008	Bardejov	19/10/2006	13/11/2006	II. ÚS 132/07	06/06 07
3824/08	17/01/2008	Lučenec	19/10/2006	23/10/2006	II. ÚS 133/07	06/06 07
15055/08	25/02/2008	Kežmarok	24/07/2006	08/09/2006	III. ÚS 252/07	27/09 07
29548/08	10/06/2008	Rimavská Sobota	24/07/2006	01/08/2006	III. ÚS 320/07	03/12 07
29551/08	10/06/2008	Trnava	19/10/2006	20/10/2006	I. ÚS 39/08	07/02 08
29552/08	10/06/2008	Humenné	24/07/2006	12/10/2006	III. ÚS 323/07	03/12 07
29555/08	10/06/2008	Považ. Bystrica	19/10/2006	27/10/2006	III. ÚS 322/07	03/12 07
29557/08	10/06/2008	Svidník	24/07/2006	22/09/2006	III. ÚS 321/07	03/12 07

Appendix II

Claims for just satisfaction (Article 41 of the Convention)

Application No.	Pecuniary damage (EUR)	Non-pecuniary damage (EUR)	Costs and expenses (EUR)	
			Domestic proceedings	Convention proceedings
54252/07 (DC V. Krtíš)	19,255,405.30	155,015.60	30,778.06	6,002.95
54252/07 (DC Rim. Sobota)	78,030,943.04	659,895.11	129,936.39	6,002.95
3274/08	20,936,573.72	220,739.56	43,686.24	6,002.95
3377/08	32,613,332.67	289,782.91	57,246.36	6,002.95
3505/08	43,794,235.54	355,838.81	70,219.73	6,002.95
3526/08	54,701,275.97	513,177.99	101,121.15	6,002.95
3741/08	49,770,796.99	398,658.97	78,629.61	6,002.95
3786/08	18,811,070.84	236,672.64	46,815.50	6,002.95
3807/08	17,989,964.91	160,057.73	31,764.36	6,002.95
3824/08	60,172,870.94	474,009.16	93,428.39	6,002.95
15055/08	6,465,958.97	79,001.53	15,848.89	6,002.95
29548/08	23,034,356.70	300,073.03	59,267.33	6,002.95
29551/08	45,424,787.56	447,454.03	88,212.96	6,002.95
29552/08	12,461,352.65	129,788.22	25,823.40	6,002.95
29555/08	19,632,796.26	206,798.11	40,948.14	6,002.95
29557/08	3,832,531.37	54,106.09	10,959.43	6,002.95
Total	506,928,253.43	4,681,069.49	924,685.94	96,047.20

[1] Act no. 215/2002 on Electronic Signature, as amended and Regulation No. 542/2002 of the National Security Office on Use of Electronic Signature in Administrative and Business Relations

[2] A complete overview of the legislation concerning electronic signature is available at the website of the National Security Authority (http://www.nbusr.sk/en/electronic-signature/legislation/index.html)

LAWYER PARTNERS, A.S. v. SLOVAKIA JUDGMENT

LAWYER PARTNERS, A.S. v. SLOVAKIA JUDGMENT

LAWYER PARTNERS, A.S. v. SLOVAKIA JUDGMENT