Rejent * rok 13 * nr 4(144)
kwiecień 2003 r.

Dariusz Szostek

Czeska ustawa o podpisie elektronicznym i zmianie niektórych dalszych ustaw[1]

I. Wprowadzenie

Aktualnie w polskiej literaturze, w związku z uchwaleniem ustawy o podpisie elektronicznym[2], coraz częściej podejmowana jest problematyka zawierania umów z użyciem elektronicznych nośników informacji. Rozwiązania polskiej ustawy są porównywane do dyrektywy Parlamentu Europejskiego i Rady w sprawie wspólnotowych warunków ramowych dotyczących podpisu elektronicznego i ewentualnie do wybranych rozwiązań ustaw krajowych niektórych państw członkowskich, a także USA[3].

---

[1] Zákon o elektronickém podpisu a o změně některych dalších zákonu. Zákon č. 227/2000 Sb z dnia 29 czerwca 2000 r.; patrz Sbirka Zákonu Česka Republika Častka 68, a także http://www.mvcr.cz/sbirka/2000/zakony 3g.html, zwana w niniejszym artykule ustawą.

[2] Dz.U. z 2001 r. Nr 130, poz. 1450; zm.: Dz.U. z 2002 r. Nr 153, poz. 1271.

[3] Patrz min. A. A m b r o z i e w i c z, *Podpis elektroniczny – pojecie i funkcje w obrocie*, Przegląd Sądowy 2001, nr 1, s. 99 i nast.; K. B o r o w i c z, *Ustawa o podpisie elektronicznym*, Bielsko-Biała 2002, s. 9 i nast.; J. J a c y s z y n, S. Z a k r z e w s k i, *Podpis elektroniczny jako element systemu zabezpieczenia danych w sieci*, Rejent 2001, nr 10, s. 45 i nast., a także Rejent 2001, nr 11, s. 60 i nast.; J. J a c y s z y n, J. P r z e t o c k i, A. W i t t l i n, S. Z a k r z e w s k i, *Podpis elektroniczny. Komentarz do ustawy z 18 września 2001 r.*, Warszawa 2002, s. 7 i nast.; M. M a r u t a, *Podpis elektroniczny – zarys przyszłych regulacji prawnych*, Radca Prawny 2001, nr 2, s. 52 i nast.; D. K o t, *Zawarcie umowy za pomocą elektronicznych środków porozumiewania się na odległość,* [w]: *Prace z wynalazczości i ochrony własności intelektualnej. Prace ku czci S. Grzybowskiego*, Kraków

Celem niniejszego artykułu jest przedstawienie kompleksowych rozwiązań w zakresie podpisu elektronicznego, ustanowionych przez Republikę Czeską. Wybór ten nie jest przypadkowy. Republika Czeska, podobnie jak Polska, aspiruje do członkostwa we Wspólnocie Europejskiej i podobnie jak nasz kraj ujednolica swoje prawo zgodnie z wymogami unijnymi. Polska gospodarka jest bardziej zbliżona do gospodarki czeskiej niż wspólnotowej. Najprawdopodobniej oba kraje równocześnie wejdą do Unii Europejskiej. Ponadto bardzo często polskie dokonania są przedstawiane na tle rozwiązań naszego południowego sąsiada. Między innymi z tych powodów wydaje się właściwym przybliżenie rozwiązań czeskiej ustawy o podpisie elektronicznym.

II. Czeska ustawa o podpisie elektronicznym

Rząd czeski dosyć szybko dostrzegł szansę rozwoju gospodarczego poprzez rozwój i promocję handlu elektronicznego i 31 maja 1999 r. przyjął dokument strategiczny „Państwowa polityka informacyjna", w którym rozwój *e-commerce* został określony jako jeden z priorytetów działań rządu. Z tekstu dokumentu wynika, że „handel elektroniczny jest dla Republiki Czeskiej szansą na zwiększenie konkurencyjności w ekonomii, sposobem na wspieranie eksportu, a małym i średnim przedsiębiorstwom daje możliwość szerszego zaistnienia na arenie międzynarodowej. Głównym zadaniem państwa w tej dziedzinie jest zapewnienie podmiotom, które chcą wykorzystywać elektroniczne nośniki informacji do zawierania umów oraz do kontaktów z kontrahentami, podstaw prawnych i odpowiednich środków bezpieczeństwa". Rząd czeski uznał, że dla rozwoju *e-commerce* najważniejsze jest uchwalenie ustawy o podpisie elektronicznym oraz przyznanie dokumentom elektronicznym takiej samej mocy prawnej jak dokumentom sporządzonym w sposób tradycyjny.

2002, s. 57 i nast.; W. K o c o t, *Charakter prawny podpisu elektronicznego*, PPH 2002, nr 4, s. 36; Z. R a d w a ń s k i, *Elektroniczna forma czynności prawnych*, MoP 2001, nr 22, s. 1107 i nast.; Z. N e u m a n, M. Ś w i e r c z y ń s k i, *Podpis elektroniczny – prawne i techniczne objaśnienia pojęć,* MoP 2001, nr 11, s. 591 i nast.; A. S t o s i o, *Umowy zawierane przez internet*, Warszawa 2002, s. 13 i nast.; M. Ś w i e r c z y ń s k i, *Podpis elektroniczny w praktyce handlowej*, dodatek *Gospodarka elektroniczna* do MoP 2002, nr 24; F. W e j m a n, *Wprowadzenie do cywilistycznej problematyki ustawy o podpisie elektronicznym*, Prawo Bankowe 2002, nr 2, s. 37 i nast.

Należy w tym miejscu zwrócić uwagę, że w czeskim kodeksie cywilnym[4] dosyć liberalnie podchodzi się do zasady zachowania formy pisemnej. Zgodnie z § 110, „oświadczenie woli złożone w innej formie niż wymaga tego ustawa lub porozumienie (umowa) stron jest nieważne. Porozumienie (umowa) zawarte w formie pisemnej może zostać skutecznie zmienione lub unieważnione wyłącznie w formie pisemnej. Forma pisemna oświadczenia woli jest zachowana, jeżeli została podpisana przez odpowiednią osobę[5], a w przypadku gdy dla ważności oświadczenia woli wymagane jest złożenie oświadczenia przez większą ilość osób, podpisy tychże osób nie muszą znajdować się na tym samym dokumencie, chyba że przepis prawa stanowi inaczej. Podpis może być nałożony środkami mechanicznymi, jeżeli w danych przypadkach jest to zwyczajowo przyjęte. Forma pisemna jest zachowana, jeżeli oświadczenie woli zostało wysłane telegraficznie, dalekopisem lub środkami elektronicznymi, jeżeli środki te umożliwiają ewidencjonowanie (zachowanie) treści oświadczenia woli i określenie tożsamości osoby, która oświadczenie wysłała[6]".

W czeskim systemie prawnym, odmiennie niż w polskim, uznaje się że forma pisemna jest zachowana, jeżeli oświadczenie woli zostało przesłane przez telegraf, dalekopis lub środki elektroniczne. Jedyne wymogi, jakie muszą zostać spełnione, to możliwość zachowania (zaewidencjonowania) treści oświadczenia woli, a także możliwość określenia tożsamości osoby składającej oświadczenie. W czeskim kodeksie cywilnym nie jest wymagane dla zachowania formy pisemnej złożenie własnoręcznego podpisu. Ponadto, zgodnie § 125 czeskiego kodeksu postępowania cywilnego[7] (rodzaje dowodów), jako dowód mogą służyć wszystkie środki, na podstawie których można stwierdzić stan rzeczy, a w szczególności takie, jak przesłuchanie świadków, opinia biegłych, raporty, materiały pisemne, rekonstrukcja oraz przesłuchanie stron. Jeśli sposób przeprowadzenia dowodów nie jest określony przepisem, zostanie on określony

---

[4] Občanski zákonik Zákon č.40/1964 Sb.

[5] Odpowiednią osobą jest osoba fizyczna, która działa we własnym imieniu, w imieniu innej osoby fizycznej lub w imieniu osoby prawnej bądź jednostki nie posiadającej osobowości prawnej.

[6] Brzmienie art. 110 przed uchwaleniem ustawy o podpisie elektronicznym (tłum. autora).

[7] Zákon č. 99/1963 Sb. občansky soudni řád.

przez sąd. Powyższe wyliczenie ma charakter przykładowy, sąd może bowiem dopuścić inne niż wymienione dowody (np. zapis na elektronicznym nośniku informacji), jeżeli tylko na ich podstawie można stwierdzić rzeczywisty stan rzeczy.

Liberalne podejście czeskiego ustawodawcy do zasad zachowania formy pisemnej spowodowało, że nie było potrzeby, ze względu na *e-commerce*, przeprowadzenia gruntownej zmiany przepisów kodeksu cywilnego w zakresie formy czynności prawnych. Forma pisemna jest bowiem zachowana, jeżeli oświadczenie zostaje przesłane przez elektroniczne środki komunikacji, a treść oświadczenia woli zostanie zachowana (zapisana) oraz gdy istnieje możliwość określenia tożsamości składającego oświadczenie. Dla spełnienia pierwszego wymogu wystarczający jest odpowiedni zapis treści oświadczenia woli na elektronicznym nośniku informacji, np. na twardym dysku, dyskietce, CD-romie, w pamięci telefonu komórkowego itp. Trudności sprawia natomiast określenie tożsamości składającego oświadczenie woli. Każdy bowiem może, wykorzystując pocztę elektroniczną, podszywać się i podpisywać cudzym nazwiskiem. Otrzymanie oświadczenia woli podpisanego np. Vaclav Havel nie oznacza, że wiadomość pochodzi od byłego prezydenta Czech, tylko od kogoś, kto użył takiego imienia i nazwiska[8]. Z tego też powodu 29 czerwca 2000 r. (15 miesięcy[9] wcześniej niż Polska!) uchwalono ustawę o podpisie elektronicznym i zmianie niektórych dalszych ustaw, której głównym celem było wprowadzenie odpowiedniej procedury identyfikacji tożsamości składającego oświadczenie woli.

III. Cel i zakres ustawy

Czeska ustawa w dużej mierze opiera się na dokumentach międzynarodowych i ustawach wzorcowych, a w szczególności na modelowej ustawie UNCITRAL dotyczącej zagadnień prawnych związanych z elek-

[8] Na kwestię tę zwracają uwagę J. B a r t a i R. M a r k i e w i c z, *Internet a prawo*, Kraków 1998, s. 53, 70 i nast. Autorzy wprawdzie przedstawiają ten problem przede wszystkim na gruncie prawa polskiego, jednakże jest on aktualny także w ramach innych systemów prawnych.

[9] Czeska ustawa o podpisie elektronicznym weszła w życie prawie 20 miesięcy wcześniej niż jej polski odpowiednik.

tronicznym przekazem danych i pokrewnych środków komunikacji[10], materiałach UNCITRAL dotyczących technologicznych aspektów podpisu elektronicznego[11] oraz dyrektywie Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych warunków ramowych dotyczących podpisu elektronicznego (1999/93/WE).

Jednym z głównych celów ustawodawcy w trakcie tworzenia ustawy było zachowanie neutralności technologicznej, tj. na tyle ogólne zdefiniowanie pojęć, aby w przypadku zmiany technologii wykorzystywanej do tworzenia podpisu elektronicznego nie było konieczne nowelizowanie ustawy (podobna zasada została przyjęta przez polskiego ustawodawcę w trakcie prac nad polską ustawą o podpisie elektronicznym). Zasada ta wynika z rozwiązań wzorcowej ustawy UNCITRAL oraz dyrektywy.

Podstawowym jednak powodem uchwalenia ustawy było umożliwienie, a także ułatwienie dokonywania czynności prawnych z użyciem elektronicznych nośników informacji oraz zapewnienie równego traktowania dokumentów tradycyjnych i elektronicznych[12]. W ustawie określono zasady używania podpisu elektronicznego, świadczenia usług certyfikacyjnych, działalności organów kontroli oraz sankcje związane z naruszeniem przepisów ustawy o podpisie elektronicznym (§ 1 ustawy).

Określenie niektórych pojęć – definicje (§ 2 ustawy)

Czeski ustawodawca przy definiowaniu pojęć ustawy w dużej mierze oparł się na definicjach określonych w artykule 2 dyrektywy Parlamentu Europejskiego i Rady w sprawie wspólnotowych warunków ramowych dotyczących podpisu elektronicznego. Przyjęcie rozwiązań dyrektywy, a właściwie jej implementacja do prawa krajowego, jest zgodne z umową stowarzyszeniową pomiędzy Republiką Czeską oraz państwami-członkami Wspólnoty Europejskiej. Przyjęcie innych zasad lub definicji mogłoby spowodować pozostawienie czeskiego rynku *e-commerce* poza global-

---

[10] Na temat modelowej ustawy UNCITRAL w polskiej literaturze W. K o c o t, *Zawieranie umów sprzedaży według Konwencji Wiedeńskiej*, Warszawa 1998; t e n ż e, *Zawarcie umowy w drodze elektronicznej wymiany informacji,* PPH 1998, nr 4.

[11] Dokumenty: A/CN.9/WG.IV/WP.73; A/CN.9/WG.IV/WP.80; A/CN.9/WG.IV/WP.81; A/CN.9/WG.IV/WP.82.

[12] Z uzasadnienia projektu ustawy.

nym, a także europejskim rynkiem elektronicznym[13]. Ponadto w momencie wejścia Republiki Czeskiej do Unii Europejskiej musiałoby nastąpić przystosowanie prawa czeskiego w zakresie handlu elektronicznego do prawa unijnego[14].

Definicje podpisu elektronicznego, kwalifikowanego podpisu elektronicznego, certyfikatu, danych służących do generowania podpisu elektronicznego, danych służących do weryfikacji podpisu, urządzenia do generowania podpisu, urządzenia do weryfikacji podpisu, produktu dla podpisów elektronicznych, zaświadczenia o akredytacji[15] są zgodne, a często identyczne z definicjami określonymi w dyrektywie[16]. Pozostałe definicje nieco się różnią lub w ogóle nie istnieją w dyrektywie, i tak:

– **danymi elektronicznymi** (wiadomościami) są dane, które można przenosić za pomocą środków komunikacji elektronicznej i przechowywać na elektronicznych mediach (a właściwie na ich nośnikach), służące do zapisu, używania lub obróbki i transmisji danych drogą elektroniczną[17],

– **podmiotem świadczącym usługi certyfikacyjne** jest podmiot wydający certyfikaty i prowadzący ich ewidencję, a także świadczący inne usługi związane z podpisem elektronicznym. W związku z brakiem ustawowych ograniczeń dotyczących możliwości podejmowania działalności jako podmiotu świadczącego usługi certyfikacyjne, należy uznać, że może nim zostać każdy, a więc zarówno osoba fizyczna, osoba prawna,

[13] Pierwotny projekt ustawy w znacznym stopniu różnił się od brzmienia ustawy. Początkowo czeski ustawodawca podjął próbę samodzielnego zdefiniowania pojęć związanych z podpisem elektronicznym, przez co były one zasadniczo odmienne od definicji zawartych w dyrektywie. W ostatecznej wersji przyjęto jednak rozwiązania Unii Europejskiej.

[14] Nie wszystkie zasady dyrektywy mogły zostać przyjęte bezpośrednio, dotyczy to przede wszystkim zasad związanych z członkostwem we Wspólnocie, np.: zasada jednolitego rynku, swoboda zakładania działalności przez dostawców usług certyfikacyjnych itp.

[15] W dyrektywie posłużono się pojęciem „dobrowolna akredytacja", jednakże zakres obu pojęć jest identyczny.

[16] Szerzej na temat definicji zawartych w dyrektywie D. S z o s t e k, *Dyrektywa Parlamentu Europejskiego i Rady w sprawie podpisu elektronicznego*, Rejent 2001, nr 11, s. 92 i nast.

[17] Początkowo w projekcie ustawy czeski ustawodawca przy określaniu danych elektronicznych oparł się na definicji wzorcowej ustawy UNCITRAL, określając je jako „informacje wytworzone, przesyłane bądź przyjęte poprzez elektroniczne, optyczne lub inne podobne środki umożliwiające dalszą przesyłkę informacji". Ostatecznie przyjęto definicję jak wyżej.

podmioty prywatne, jak i publiczne, jeżeli tylko spełniają wymogi określone w ustawie. Jednakże podmioty świadczące usługi certyfikacyjne nie mogą świadczyć innych usług niż określone w ustawie ani prowadzić innej działalności; wyjątkiem jest działalność adwokatów, notariuszy lub rzeczoznawców (§ 10 pkt 6 ustawy)[18],

– **akredytowanym podmiotem świadczącym usługi certyfikacyjne** jest podmiot świadczący usługi certyfikacyjne, któremu zostało wydane zaświadczenie o akredytacji,

– **kwalifikowanym certyfikatem** jest certyfikat zgodny z wymogami ustawy, wydany przez podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w ustawie[19],

– **środkiem** (urządzeniem) **do wytworzenia bezpiecznego podpisu** jest środek do wytwarzania podpisu elektronicznego, spełniający wymogi ustawy (§ 17 ustawy),

– **zaświadczeniem o akredytacji** jest zaświadczenie (świadectwo) stwierdzające, że podmiot świadczący usługi certyfikacyjne spełnia wymogi ustawy dotyczące wykonywania działalności jako akredytowany podmiot świadczący usługi certyfikacyjne.

Zgodnie z przepisami ustawy uznaje się, że dane elektroniczne są podpisane, jeżeli dokument elektroniczny został opatrzony podpisem elektronicznym. Jednakże opatrzenie danych elektronicznych „zwykłym" podpisem elektronicznym nie spełnia wymogów formy pisemnej. Dla jej zachowania wymagane jest bowiem stwierdzenie tożsamości składającego oświadczenie, co może zagwarantować wyłącznie kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie i sporządzony za pomocą bezpiecznego środka (urządzenia) do składania podpisów. Zastosowanie kwalifikowanego podpisu elektronicznego umożliwia sprawdze-

---

[18] Co ciekawe, polski ustawodawca w ogóle wyłączył możliwość świadczenia usług certyfikacyjnych przez notariuszy. Zgodnie bowiem z art. 3 pkt 14, podmiotem świadczącym usługi certyfikacyjne może być wyłącznie podmiot prowadzący działalność gospodarczą w znaczeniu ustawy z dnia 19 listopada 1999 r. o działalności gospodarczej, NBP lub organ władzy publicznej. Notariusz nie jest podmiotem prowadzącym działalność gospodarczą ani organem władzy publicznej, nie może wobec tego świadczyć usług certyfikacyjnych; patrz J. Jacyszyn, J. Przetocki, A. Wittlin, S. Zakrzewski, *Podpis elektroniczny...*, s. 54; K. Borowicz, *Ustawa...*, s. 106.

[19] Wymogi te określa § 12 ustawy i są one całkowicie zgodne z wymaganiami załącznika I dyrektywy.

nie, że dane elektroniczne zostały podpisane przez osobę wymienioną w kwalifikowanym certyfikacie oraz zapewnia, iż w sytuacji naruszenia podpisanych danych elektronicznych takie naruszenie zostanie niezwłocznie stwierdzone (§ 4).

V. Obowiązki i zasady odpowiedzialności składającego podpis oraz podmiotu świadczącego usługi certyfikacyjne wydającego kwalifikowany certyfikat

Zgodnie z ustawą, na składającym podpis spoczywa szereg obowiązków. Jest on zobowiązany między innymi do przechowywania z należytą starannością wszelkich środków (urządzeń) koniecznych do wytworzenia kwalifikowanego podpisu elektronicznego, tak aby nie doszło do ich jakiegokolwiek bezprawnego wykorzystania oraz do niezwłocznego powiadomienia dostawcy usług certyfikacyjnych w przypadku zaistnienia prawdopodobieństwa wadliwego (sprzecznego z prawem) wykorzystania kwalifikowanego podpisu elektronicznego i zapewnienia, że wszelkie informacje złożone podmiotowi świadczącemu usługi certyfikacyjne lub też innym podmiotom w związku z użyciem kwalifikowanego podpisu elektronicznego są ścisłe, prawdziwe i pełne.

W przypadku zaistnienia szkody wynikającej z niedopełnienia powyższych obowiązków, podmiot składający podpis elektroniczny odpowiada za wyrządzoną szkodę zgodnie z obowiązującymi przepisami (tj. zgodnie z § 420 czeskiego kodeksu cywilnego[20]). Odpowiedzialność ta zostaje wyłączona, jeżeli składający podpis wykaże, że poszkodowany nie dokonał wszelkich czynności koniecznych do sprawdzenia (uwierzytelnienia) ważności kwalifikowanego (bezpiecznego) podpisu elektronicznego oraz kwalifikowanego certyfikatu, np. nie sprawdził tożsamości składającego oświadczenie woli. Ciężar przeprowadzenia dowodu spoczywa na składającym podpis.

Podmiot świadczący usługi certyfikacyjne ma natomiast obowiązek (§ 6 ustawy):

– zapewnić, aby certyfikaty przez niego wydane jako certyfikaty kwalifikowane miały wszystkie przewidziane w ustawie właściwości certyfikatu kwalifikowanego,

[20] Zákon č. 40/1968 Sb.

– zapewnić, aby wszystkie dane w kwalifikowanym certyfikacie były dokładne, prawdziwe i pełne,

– przed wydaniem kwalifikowanego certyfikatu sprawdzić tożsamość oraz ewentualne inne istotne z punktu widzenia prawa przymioty[21] osoby wnioskującej o wydanie certyfikatu,

– sprawdzić, czy w momencie wydania kwalifikowanego certyfikatu osoba podpisująca była w posiadaniu danych do tworzenia podpisu elektronicznego, którym odpowiadają dane weryfikujące podpis, określone w kwalifikowanym certyfikacie,

– stworzyć, w postaci elektronicznej, bezpieczną i publicznie dostępną listę wszystkich wydanych kwalifikowanych certyfikatów, a także wszystkich certyfikatów, które zostały unieważnione,

– udostępnić osobom trzecim informacji dotyczących kwalifikowanego certyfikatu z dokładnym określeniem daty oraz godziny, minuty i sekundy, w której kwalifikowany certyfikat został wydany lub unieważniony,

– zatrudnić osoby mające fachową wiedzę, doświadczenie i kwalifikacje niezbędne do świadczenia oferowanych usług. Osoby te powinny posiadać znajomość technologii i procedur bezpieczeństwa wymaganych w ustawie,

– stosować bezpieczne urządzenia oraz systemy do wytwarzania i weryfikacji podpisu elektronicznego. Urządzenia do wytwarzania i weryfikacji podpisu elektronicznego są uznawane za bezpieczne, jeżeli spełniają wymogi określone w ustawie oraz są sprawdzone przez Urząd do Spraw Ochrony Danych Osobowych[22],

– podjęcia stosownych kroków zapobiegających nadużyciu oraz fałszowaniu kwalifikowanego certyfikatu oraz zapewnia utajenia danych potrzebnych do tworzenia kwalifikowanego podpisu elektronicznego,

– posiadać wystarczające środki finansowe konieczne do spełnienia wymogów określonych w ustawie i innych aktach wykonawczych, z uwzględnieniem ewentualnej odpowiedzialności odszkodowawczej,

---

[21] Przykładem innych, z punktu widzenia prawa, przymiotów osoby wnioskującej o wydanie certyfikatu jest prawo do reprezentacji osoby prawnej. Przed wpisaniem takich danych do certyfikatu podmiot świadczący usługi certyfikacyjne zobowiązany jest do sprawdzenia odpowiednich wypisów z rejestru itp.

[22] W dalszej części artykułu Urząd do Spraw Ochrony Danych Osobowych zwany jest Urzędem.

– wszelkie informacje oraz dokumentację o wydanych kwalifikowanych certyfikatach przechowywać przez okres co najmniej 10 lat[23] od momentu zakończenia ważności kwalifikowanego certyfikatu. Informację i dokumentację można przechowywać w postacie elektronicznej,

– przed zawarciem umowy poinformować na piśmie podmiot wnioskujący o wydanie certyfikatu o zasadach dotyczących używania elektronicznego podpisu opartego na kwalifikowanym certyfikacie, ograniczeniach w jego stosowaniu, warunkach reklamacji oraz o fakcie uzyskania bądź też nieuzyskania akredytacji. Informacje te można przekazać także w postaci elektronicznej,

– stosować takie systemy wytwarzania podpisu elektronicznego, aby nie było możliwe przechowywanie bądź kopiowanie danych koniecznych do utworzenia kwalifikowanego podpisu elektronicznego osób, którym certyfikat został wydany,

– w przypadku cofnięcia przez Urząd do Spraw Ochrony Danych Osobowych akredytacji powiadomić o tym fakcie podmioty, dla których świadczy usługi certyfikacyjne oraz zamieścić stosowną informację w prowadzonych przez siebie listach wydanych lub cofniętych certyfikatów,

– na wniosek osoby podpisującej lub w przypadku wydania certyfikatu na podstawie nieprawdziwych danych, certyfikat unieważnić,

– unieważnić certyfikat w sytuacji, gdy dowiedział się, na podstawie dowodów pewnych, że osoba podpisująca zmarła bądź sąd pozbawił ją lub ograniczył jej zdolność do czynności prawnych albo dane, (np. rejestr) na podstawie których certyfikat został wydany, przestały obowiązywać,

– w przypadku ograniczenia stosowania kwalifikowanego certyfikatu do niektórych czynności lub do pewnej wartości transakcji, informacje o tychże ograniczeniach udostępnić w sposób umożliwiający zapoznanie się z nimi przez osoby trzecie[24].

---

[23] W Polsce tego typu dokumentację należy przechowywać co najmniej przez 20 lat.

[24] Przepis określający obowiązki podmiotu świadczącego usługi certyfikacyjne został w porównaniu z projektem ustawy znacznie rozszerzony (widoczne jest uwzględnienie przepisów dyrektywy). Według pierwotnego projektu ustawy obowiązki podmiotu świadczącego usługi certyfikacyjne ograniczały się do:

a) przedsięwzięcia wszelkich czynności wymaganych do uwierzytelnienia tożsamości sygnatariusza,

Podmiot świadczący usługi certyfikacyjne może wydać wnioskującemu certyfikat dopiero po zawarciu odpowiedniej umowy. Umowa ta musi zostać zawarta na piśmie pod rygorem nieważności. Należy przy tym pamiętać o liberalnym podejściu czeskiego ustawodawcy do wymogów formy pisemnej. Ponadto podmiot świadczący usługi certyfikacyjne zobowiązany jest prowadzić odpowiednią dokumentację zawierającą następujące dane: umowę zawartą z osobą wnioskującą o wydanie kwalifikowanego certyfikatu, wydany kwalifikowany certyfikat, kopie przedstawionych dokumentów osoby wnioskującej o wydanie kwalifikowanego certyfikatu, potwierdzenie odebrania kwalifikowanego certyfikatu, dokładne określenie okresu ważności wydanego kwalifikowanego certyfikatu.

Za szkodę spowodowaną naruszeniem ustawy podmiot świadczący usługi certyfikacyjne odpowiada na podstawie przepisów czeskiego kodeksu cywilnego[25]. Jednakże nie ponosi odpowiedzialności za szkodę wynikającą z naruszenia ograniczeń dotyczących wykorzystywania certyfikatu kwalifikowanego. W przypadku gdy naruszenie dotyczy zastrzeżonej w certyfikacie czynności prawnej, świadczący usługi certyfikacyjne nie odpowiada za szkodę wynikającą z dokonania tejże czynności, natomiast w sytuacji, kiedy naruszenie polegało na dokonaniu transakcji przekraczającej maksymalną dopuszczalną wartość, odpowiedzialność podmiotu świadczącego usługi certyfikacyjne zostaje ograniczona do maksymalnej dopuszczalnej wartości transakcji określonej w certyfikacie.

---

b) zapewnienia informacji o:

– tożsamości dostawcy usług certyfikowanych,

– metodzie używanej do określenia (uwierzytelnienia) tożsamości sygnatariusza,

– sytuacjach (przypadkach), w których skuteczne używanie bezpiecznych kluczy elektronicznych jest wyłączone,

– o tym, że certyfikat jest ważny, a kwalifikowany podpis elektroniczny nie został wykorzystany sprzecznie z obowiązującymi zasadami,

c) poinstruowania sygnatariusza o sposobie informowania dostawcy usług certyfikowanych w przypadku zaistnienia niebezpieczeństwa naruszenia bezpieczeństwa (wykorzystania przez osobę trzecią) kwalifikowanego podpisu elektronicznego,

d) zapewnienia prawdziwości, dokładności i pełności danych przekazywanych innym podmiotom w związku z kwalifikowanym podpisem elektronicznym.

[25] Patrz § 10 czeskiego kodeksu cywilnego.

VI. Akredytacja i nadzór nad działalnością podmiotów świadczących usługi certyfikacyjne

Czeski ustawodawca przekazał prawo do przyznawania akredytacji, jak również nadzór nad przestrzeganiem ustawy przez podmioty świadczące usługi certyfikacyjne Urzędowi do Spraw Ochrony Danych Osobowych[26].

Urząd ten został wyposażony w szereg kompetencji, do których należy między innymi: udzielanie i odbieranie akredytacji podmiotom działającym w Republice Czech[27], nadzór nad działalnością akredytowanych dostawców usług certyfikowanych oraz dostawców usług certyfikowanych wydających kwalifikowany certyfikat, określanie, jakie działania należy podjąć w celu poprawy działalności, nakładanie kar na podmioty świadczące usługi certyfikacyjne za naruszenie obowiązków określonych w ustawie, prowadzenie ewidencji przyznanych akredytacji oraz ich zmiany, prowadzenie ewidencji podmiotów świadczących usługi certyfikacyjne, którzy poinformowali Urząd o wydawaniu kwalifikowanych certyfikatów, publikowanie listy przyznanych akredytacji oraz listy podmiotów świadczących usługi certyfikacyjne, wydających kwalifikowany certyfikat; publikacja ta powinna umożliwiać zdalny dostęp do wszystkich informacji[28]. Ponadto Urząd kontroluje zgodność środków do wytwarzania lub sprawdzania podpisów elektronicznych z wymaganiami ustawy (§ 9 ustawy). Aby Urząd miał możliwość dokonywania czynności nadzoru, akredytowani dostawcy usług certyfikowanych, a także dostawcy wydający kwalifikowane certyfikaty, mają obowiązek:

1) umożliwić upoważnionym pracownikom Urzędu wstęp w niezbędnym i koniecznym zakresie do pomieszczeń handlowych i eksploatacyjnych;

---

[26] W projekcie ustawy Urząd nosił nazwę Urzędu do Spraw Podpisu Elektronicznego i podlegał Ministerstwu Transportu i Łączności.

[27] W projekcie ustawy Urząd zobowiązany był wydawać i odbierać zezwolenia na działalność podmiotów świadczących usługi certyfikacyjne. Ostatecznie Urząd zobligowany jest do przyznawania i cofania wyłącznie akredytacji, gdyż działalność podmiotów świadczących usługi certyfikacyjne nie wymaga uprzedniej zgody, co całkowicie odpowiada zasadom określonym w dyrektywie.

[28] Przez „zdalny dostęp" należy uznać dostęp umożliwiający osobom trzecim samodzielne uzyskanie informacji, np. przez internet. Ustawodawca z rozmysłem użył ogólnego, technologicznie neutralnego sformułowania, co ma w przyszłości umożliwić wykorzystanie innych, obecnie nieznanych technologii „zdalnego dostępu".

2) na żądanie tychże osób przedłożyć wszelką dokumentację, pisma, zapisy (np. na elektronicznych nośnikach informacji) i inne dowody związane z prowadzoną działalnością;

3) umożliwić dostęp do informatycznego systemu dostawcy usług certyfikowanych;

4) udzielić wszelkich informacji oraz podjąć wszelką potrzebną współpracę.

Ustawodawca nie określił trybu, w jakim Urząd zobligowany jest przeprowadzić nadzór, należy zatem stosować przepisy ustawy o kontroli państwowej[29].

Urząd poprzez wydanie zarządzenia tymczasowego może nakazać podmiotowi świadczącemu usługi certyfikacyjne[30] unieważnienie kwalifikowanego certyfikatu osoby składającej podpis elektroniczny. Zarządzenie to może zostać wydane, jeżeli istnieje uzasadnione podejrzenie, że kwalifikowany certyfikat został podrobiony, przerobiony lub wydany na podstawie nieprawdziwych danych. Urząd może także nakazać unieważnienie kwalifikowanego certyfikatu w przypadku, kiedy środek służący do składania kwalifikowanego podpisu elektronicznego posiada wady umożliwiające podrabianie podpisu lub zmianę podpisywanych danych. Podmiot świadczący usługi certyfikacyjne zobowiązany jest prowadzić listę unieważnionych certyfikatów z podaniem godziny, minuty i sekundy unieważnienia certyfikatu. Ponowne uruchamianie (odnawianie) unieważnionych certyfikatów jest niedopuszczalne (§ 15 ustawy). Należy zwrócić uwagę, że czeski ustawodawca nie przewiduje instytucji zawieszenia ważności certyfikatów[31].

Każdy podmiot świadczący usługi certyfikacyjne może zwrócić się do Urzędu o przyznanie akredytacji[32]. Należy jednak zauważyć, że od-

---

[29] Patrz ustawa o kontroli państwowej, Zákon č. 552/1991 Sb.

[30] Przepis ten dotyczy wszystkich podmiotów świadczących usługi certyfikacyjne, a nie tylko podmiotów akredytowanych.

[31] Instytucję taką przewiduje natomiast ustawodawca polski; patrz art. 21 ust. 4 polskiej ustawy o podpisie elektronicznym.

[32] Złożenie wniosku o akredytację podlega opłacie administracyjnej zgodnie z ustawą o opłatach administracyjnych, Zákon č. 368/1992 Sb. Aktualnie powyższa opłata wynosi 100 000 Kč, tj. ok. 12 500 zł. W Polsce opłata za rozpatrzenie wniosku o wpisanie do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne wynosi równowartość 10.000 euro, tj. ok. 40.000 zł.

miennie niż w Polsce, gdzie wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne jest wymagany dla wydawania kwalifikowanych certyfikatów, uzyskanie akredytacji nie jest konieczną przesłanką dla wydawania kwalifikowanych certyfikatów. Aby wydawać kwalifikowane certyfikaty należy co najmniej na 30 dni przed wydaniem pierwszego certyfikatu powiadomić o tym Urząd. Nie jest przy tym wymagana zgoda Urzędu na prowadzenie tego typu działalności. Akredytacja jest całkowicie dobrowolna. We wniosku wnioskodawca musi przedstawić szereg informacji i danych, np. nazwę handlową, siedzibę, REGON, dokument poświadczający prowadzenie działalności gospodarczej, w przypadku podmiotu wpisanego do rejestru handlowego wypis z tego rejestru nie starszy niż 3 miesiące, wypis o niekaralności przedsiębiorcy[33] nie starszy niż 3 miesiące, dokumenty udowadniające posiadanie merytorycznych, personalnych, organizacyjnych i finansowych możliwości działania jako akredytowany podmiot świadczący usługi certyfikacyjne, dane o wydawaniu lub zamiarze wydawania kwalifikowanego certyfikatu, potwierdzenie uiszczenia opłaty administracyjnej.

Dla uzyskania akredytacji podmiot świadczący usługi certyfikacyjne musi spełnić wszystkie wymogi określone w ustawie i mieć siedzibę na terytorium Republiki Czeskiej. Ograniczenie to związane jest z zapewnieniem bezpieczeństwa i kontroli systemów podpisów elektronicznych przez władze czeskie. Należy spodziewać się, że po wejściu Republiki Czeskiej do Unii Europejskiej przepis ten zostanie zmieniony na „terytorium Wspólnoty"[34]. Podmiot świadczący usługi certyfikacyjne, wydający kwalifikowane certyfikaty, nie może, oprócz usług przewidzianych w ustawie, prowadzić innej działalności; wyjątkiem od tej zasady jest działalność adwokata, notariusza lub biegłego[35]. Przyczyną takiego ograniczenia jest potencjalna możliwość konfliktów interesów lub możliwość nadużycia

[33] Dotyczy to osób fizycznych prowadzących działalność gospodarczą, natomiast w stosunku do osób prawnych należy przedstawić wypis o niekaralności osób działających jako organ osoby prawnej.

[34] Z uzasadnienia projektu ustawy.

[35] W tym miejscu należy zwrócić uwagę, że zgodnie z ustawami o adwokaturze (Zákon č. 85/1992 Sb.), o notariacie (Zákon č. 358/1992) oraz biegłych i tłumaczach (Zákon č. 36/1967 Sb. z późn. zm.) osoby prowadzące działalność określoną w wymienionych ustawach są podmiotami prowadzącymi działalność gospodarczą.

systemu składania podpisów elektronicznych w przypadku prowadzenia innej niż określona w ustawie działalność. W związku z powyższym, nie mają możliwości prowadzenie działalności jako akredytowane podmioty świadczące usługi certyfikacyjne banki i inne instytucje, np. finansowe. Z drugiej strony, nie ma żadnych ograniczeń w tworzeniu przez te instytucje odrębnych podmiotów (osób prawnych), działających wyłącznie jako akredytowane podmioty świadczące usługi certyfikacyjne.

W ramach procedury wydawania akredytacji Urząd może przeprowadzić kontrolę i badać zgodność przedstawionych dokumentów i informacji we wniosku z rzeczywistością.

VII. Obowiązki akredytowanego podmiotu świadczącego usługi certyfikacyjne po zakończeniu działalności

Czeski ustawodawca przyjął dosyć ciekawe rozwiązanie dotyczące sytuacji, kiedy akredytowany podmiot świadczący usługi certyfikacyjne zamierza zakończyć swoją działalność. Zamiar taki musi zgłosić do Urzędu co najmniej trzy miesiące przed planowaną datą zakończenia działalności i powiadomić o swym zamiarze, w sposób dający się udowodnić, każdą osobę, która uzyskała od niego certyfikat[36]. Ponadto podmiot taki zobowiązany jest dołożyć wszelkich starań, aby ważne kwalifikowane certyfikaty zostały przejęte przez inny akredytowany podmiot świadczący usługi certyfikacyjne[37]. W przypadku, kiedy akredytowany podmiot świadczący usługi certyfikacyjne, zamierzający zakończyć swoją działalność, nie jest w stanie zapewnić kontynuacji wydanych przez siebie kwalifikowanych certyfikatów, jest zobowiązany powiadomić o tym fakcie Urząd, który przejmuje ewidencję wydanych kwalifikowanych certyfikatów i oznajmia to zainteresowanym podmiotom[38].

---

[36] Osoby podpisujące muszą zostać powiadomione o zamiarze zaprzestania działalności co najmniej na dwa miesiące przed jej zakończeniem.

[37] Powyższe rozwiązanie należy uznać za bardzo dobre. Umożliwia ono kontynuację wydanych kwalifikowanych certyfikatów bez szkody dla ich posiadaczy.

[38] W projekcie ustawy proponowano przepis, wedle którego w przypadku, kiedy akredytowany dostawca usług certyfikacyjnych zamierzający zakończyć swoją działalność nie znalazł innego akredytowanego dostawcy usług certyfikacyjnych, który dobrowolnie przejąłby jego kwalifikowane certyfikaty, Urząd wyznaczałby sam taki podmiot lub podmioty. Wyznaczony podmiot musiałby przejąć wskazane kwalifikowane certyfikaty bez

Zasady określone powyżej mają także zastosowanie w przypadku, kiedy akredytowany podmiot świadczący usługi certyfikacyjne zaginie, umrze (dotyczy to oczywiście tylko osób fizycznych) lub zaprzestanie wykonywania swej działalności bez dopełnienia obowiązku zgłoszenia.

VIII. Uznawalność zagranicznych certyfikatów

Działalność jako podmiotu świadczącego usługi certyfikacyjne albo jako akredytowanego podmiotu świadczącego usługi certyfikacyjne dopuszczalna jest wyłącznie dla podmiotów posiadających swoją siedzibę na terytorium Republiki Czeskiej (§ 10 pkt 5), jednakże certyfikat wydany przez zagraniczny podmiot świadczący usługi certyfikacyjne jako certyfikat kwalifikowany może być stosowany na terytorium Republiki Czeskiej, jeżeli zostanie uznany i potwierdzony przez czeski podmiot świadczący usługi certyfikacyjne, który wydaje kwalifikowane certyfikaty. Podmiot ten musi zagwarantować zgodność i ważność kwalifikowanych certyfikatów wydawanych za granicą z wymogami czeskiej ustawy. W powyższym zakresie przejmuje odpowiedzialność za szkody wynikające z uznania zagranicznego certyfikatu.

Ponadto zagraniczny kwalifikowany certyfikat może zostać uznany jako spełniający wymogi ustawy, jeżeli zostanie uznany jako certyfikat kwalifikowany decyzją Urzędu lub na podstawie umowy międzynarodowej. Urząd może także uznawać kwalifikowane certyfikaty w związku z zawarciem z odpowiednim organem zagranicznym umowy o wzajemnym uznawaniu certyfikatów.

IX. Kary

Zgodnie z ustawą przewidziane są następujące kary:

1. Karę do wysokości 10.000.000 (dziesięć milionów) koron[39] zapłaci akredytowany podmiot świadczący usługi certyfikacyjne lub podmiot świadczący usługi certyfikacyjne wydający kwalifikowany certyfikat za naruszenie obowiązków wynikających z ustawy.

---

możliwości jakiegokolwiek protestu. Wydaje się, że słusznie ustawodawca zrezygnował z powyższego przepisu, który w proponowanej wersji ograniczałby swobodę w prowadzeniu działalności gospodarczej.

[39] Ok. 1,25 mln zł.

2. W przypadku ponownego naruszenia obowiązków wynikających z niniejszej ustawy w przeciągu roku od dnia nałożenia pierwszej kary, może zostać na akredytowany podmiot lub podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty nałożona kara do wysokości 20.000.000 (dwudziestu milionów) koron[40].

3. Akredytowany podmiot lub podmiot świadczący usługi certyfikacyjne, wydający kwalifikowane certyfikaty, który uniemożliwia lub utrudnia Urzędowi przeprowadzenie kontroli, może otrzymać karę porządkową do wysokości 1.000.000 (miliona) koron. Kara ta może być nakładana wielokrotnie.

4. Na osobę lekceważącą i nie wykonującą poleceń Urzędu w trakcie kontroli, można nałożyć karę do wysokości 25.000 koron. Karę te można nałożyć powtórnie.

5. Przy określaniu wysokości powyższych kar bierze się pod uwagę stopień i czas trwania zawinienia, zakres, czas trwania i konsekwencje bezprawnego postępowania. Karę można nałożyć w przeciągu roku od dnia wykrycia przewinienia, nie dłużej jednak niż trzy lata, licząc od chwili przewinienia. Środki wynikające z kary wpływają do Urzędu. Karę pobiera odpowiedni terytorialny organ finansowy[41]. Kwoty wynikające z kar zasilają budżet państwa (§ 18).

X. Podsumowanie

Analiza czeskiej ustawy o podpisie elektronicznym pozwala stwierdzić, że w głównym zarysie jest ona zbliżona do polskich rozwiązań. Należy jednak zauważyć, że jest o wiele mniej skomplikowana, bardziej przejrzysta i liberalna niż jej polski odpowiednik. Wprowadzono też wiele ułatwień i udogodnień, jak chociażby możliwość świadczenia usług certyfikacyjnych przez notariuszy, możliwość przejęcia certyfikatów przez Urząd w związku z likwidacją podmiotu świadczącego usługi certyfikacyjne, o wiele mniej skomplikowaną procedurę akredytacji, „mniej państwa" w procedurze świadczenia usług certyfikacyjnych, mniej rygorystyczne kary

[40] Należy zauważyć, że zgodnie z polską ustawą o podpisie elektronicznym za naruszenie niektórych przepisów ustawy może grozić nawet kara do 5 lat pozbawienia wolności; patrz art. 45-53 ustawy o podpisie elektronicznym.

[41] Patrz ustawa o pobieraniu kar i podatków, Zákon č. 337/1992 Sb.

za naruszenie ustawy itp. I co najistotniejsze, nie jest wymagane uzyskanie zezwolenia oraz wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, aby móc wydawać kwalifikowane certyfikaty. Wystarczające jest powiadomienie Urzędu do Spraw Ochrony Danych Osobowych o zamiarze wydawania tego typu certyfikatów. Akredytacja jest dobrowolna. W Polsce, aby wydawać kwalifikowane certyfikaty należy uzyskać wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, co *de facto* jest związane z uzyskaniem akredytacji[42]. Jak jest to trudne wskazuje fakt, że dopiero pół roku po wejściu w życie ustawy wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne uzyskał pierwszy polski podmiot świadczący usługi certyfikacyjne[43].

Można tylko pozazdrościć czeskiemu ustawodawcy przenikliwości i dbałości przy tworzeniu i uchwalaniu ustawy, która umożliwiła wydawanie kwalifikowanych podpisów elektronicznych, weryfikowanych przy pomocy ważnego kwalifikowanego certyfikatu, niezwłocznie po upływie *vacatio legis* ustawy.

[42] Tak też M. D r o z d o w i c z, *(Nie)bezpieczny podpis elektroniczny,* PPH 2003, nr 1, s. 31.

[43] Ustawa weszła w życie 16 sierpnia 2002 r., natomiast pierwszy kwalifikowany podmiot świadczący usługi certyfikacyjne uzyskał wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne 31 grudnia 2002 r.