Umowy elektroniczne i podpis elektroniczny w systemie prawa Republiki Czeskiej

Adam Kubiczek[1]

Przedmiotem niniejszego artykułu jest przedstawienie systemu prawa umów elektronicznych oraz podpisów elektronicznych w Republice Czeskiej. Autor omawia w nim kolejno zagadnienia dotyczące rodzajów umów elektronicznych w czeskim systemie prawnym, kwestię umowy elektronicznej jako dowodu w sądzie, zawieranie umów w czasie pandemii COVID-19 oraz rodzaje podpisów elektronicznych. Ponadto Autor w końcowej części artykułu opisuje specyfikę akredytowanych, publicznych oraz prywatnych urzędów certyfikacji, które niewątpliwie mają ścisły związek zarówno z zawieranymi umowami elektronicznymi, jak i podpisami elektronicznymi.

Uwagi wstępne

Coraz większa rola świata cyfrowego oraz niedawna sytuacja związana z pandemią COVID-19 przyspieszyła postęp nowych technologii i cyfryzacji. Pokazała, gdzie i w jaki sposób można usprawnić biznes, a gdzie jest miejsce na uefektywnienie i przyspieszenie pewnych procesów, jak chociażby zawieranie umów elektronicznych. Stąd też zwiększyła się rola umów elektronicznych, a podpis elektroniczny stał się bardzo przydatnym narzędziem dla wielu podmiotów gospodarczych i osób prawnych.

System umów elektronicznych w Republice Czeskiej

Z punktu widzenia prawa, przez umowę strony wyrażają wolę ustanowienia między sobą zobowiązania i związania się nim. Jest więc porozumieniem, z którego jej uczestnicy wywodzą różne prawa i obowiązki[2]. Za moment zawarcia umowy uważa się chwilę uzgodnienia przez strony jej treści lub też w wypadku już konkretnie umów elektronicznych moment, w którym druga strona mogła się zapoznać z treścią danej umowy.

W przypadku umowy zawieranej poprzez e-mail należy stwierdzić, że taka umowa opatrzona jest tzw. prostym podpisem elektronicznym, który przybiera postać wpisania imienia i nazwiska na końcu wiadomości i potwierdza on wyrażenie woli z takim samym skutkiem, jakby dokument podpisano własnoręcznie. Zawieranie umów za pomocą samego tekstu w wiadomości e-mail ma jednak wiele słabych stron. W praktyce bardzo trudne może być udowodnienie, że nadawcą wiadomości była rzeczywiście osoba w nim podpisana, a nie ktoś inny. Ponadto prawo wymaga formy pisemnej dla niektórych rodzajów umów (np. najmu mieszkania czy umowy agencyjnej). Zgodnie z § 562 ust. 1 czeskiego kodeksu cywilnego[3] forma pisemna jest zachowana nawet w postępowaniu sądowym prowadzonym drogą elektroniczną lub za pomocą innych środków technicznych umożliwiających ustalenie jego treści, a także osoby działającej. Wynika z tego więc, że jest to możliwe również przez e-mail. Jednak orzecznictwo sądowe, a zwłaszcza sądy wyższej instancji, są w niektórych przypadkach surowsze od prawa. Zwykły podpis elektroniczny w wiadomości e-mail często więc nie wystarcza, aby zachować formę pisemną. Sądy nie uznają takiego e-maila za dokument w formie pisemnej.

Bardzo popularnym sposobem zawierania umów na odległość jest praktyka polegająca na tym, że jedna ze stron drukuje umowę, podpisuje ją, a następnie przesyła drogą e-mailową do drugiej strony, która w ten sam sposób dołącza swój podpis. Takie podejście stwarza większe poczucie bezpieczeństwa niż sam tekst w treści e-maila. Z punktu widzenia klasyfikacji prawnej podpisów elektronicznych jest to również prosty podpis elektroniczny. Obie procedury są właściwie równoważne. Zaletą skanowania odręcznego podpisu może być nieco lepsza sytuacja dowodowa w przypadku sporu. Jednak nawet w tym przypadku poziom bezpieczeństwa nie jest zbyt wysoki[4].

Innym sposobem zawierania umów jest opatrywanie ich podpisami elektronicznymi gwarantowanymi i uznawanymi, które zawsze są potwierdzone certyfikatem, czyli określonym zbiorem danych służących do składania podpisów elektronicznych, których podpisujący może używać z dużym zaufaniem. Podpisy gwarantowane są oparte na certyfikacie komercyjnym (rozwiązanie z podpisem technicznym jest więc gwarantowane przez konkretnego dostawcę komercyjnego) i ich użycie jest zwykle prostsze. Certyfikaty kwalifikowane mogą być wydawane wyłącznie przez zatwierdzone

[1] Autor jest absolwentem Stacjonarnych Studiów Prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. ORCID: 0009-0009-1408-6339.

[2] Zob. https://www.602.cz/blog/elektronicke-uzavirani-smluv (dostęp z 20.3.2023 r.).

[3] Zákon č. 89/2012 Sb. –Občanský zákoník.

[4] Zob. https://www.602.cz/blog/elektronicke-uzavirani-smluv (dostęp z 20.3.2023 r.).

przez państwo urzędy certyfikacji i żeby je uzyskać, zazwyczaj na początku trzeba fizycznie udowodnić swoją tożsamość (w Czechach zwykle jest to CzechPoint)[5].

Również w wypadku umów elektronicznych zawieranych w Internecie w ustawodawstwie czeskim można wyróżnić kilka rodzajów umów o charakterze elektronicznym. Umowy zawierane w Internecie nie mają podpisu bezpośrednio na umowie i nie są zawierane w bezpośrednim kontakcie pomiędzy klientem a sprzedawcą, są one bowiem zawierane na odległość. Ze względu na sposób zawierania umów dzielimy je na: *click-wrap*, *click-through* oraz *browser-wrap*. To oznaczenie kontraktów opiera się na orzeczeniach sądów amerykańskich, głównie z tego powodu, że Stany Zjednoczone zdominowały handel internetowy. Ustawodawstwo czeskie akceptuje ten podział[6].

W przypadku umów *click-wrap* porozumienia takie są zawierane w celu korzystania z oprogramowania drogą elektroniczną. Klikając przycisk „zgadzam się", użytkownik akceptuje regulamin i umowa zostaje zawarta. Zgodnie z § 35 czeskiego kodeksu cywilnego, taka czynność musi spełniać wszystkie wymogi stawiane przez prawo. Problemem w przypadku tego rodzaju umów może okazać się sytuacja, gdy kupujący może omyłkowo kliknąć przycisk i uznać umowę za nieważną.

W przypadku umów *click-through*, podobnie jak w przypadku umowy *click-wrap*, kupujący musi wyrazić zgodę na zaakceptowanie umowy, klikając przycisk „zgadzam się" lub „akceptuję". Ponadto kupujący musi potwierdzić ostateczną umowę poprzez dodatkowy przycisk. W związku z tym niemożliwe jest, żeby kupujący omyłkowo kliknął w przycisk, jak w poprzednim przypadku. Najczęściej umowy te są wykorzystywane przy dokonywaniu klasycznych zakupów w sklepie internetowym[7].

Umowy *browse-wrap* różnią się wyraźnie od umów wcześniej omówionych. Zawarcie takiej umowy następuje poprzez przeglądanie odwiedzanej strony internetowej. Podczas gdy odwiedzający korzysta ze strony internetowej, zawierana jest umowa i nie ma wymogu dotyczącego kliknięcia ani zgody. W takim wypadku wystarczy odwiedzić stronę internetową i spędzić na niej trochę czasu. W przypadku tego typu umów problematyczne wydaje się wykazanie, że użytkownik rzeczywiście wiedział o jej zawarciu i zapoznał się z warunkami, jakie ta umowa przewiduje.

Zawieranie umów elektronicznych a dowód w sądzie

Przepisy prawa czeskiego nie definiują jednoznacznie, co należy rozumieć przez formę pisemną. Generalnie jednak dokument może mieć formę papierową, a także elektroniczną. Jednak w przypadku formy pisemnej czeski kodeks cywilny przewiduje, że dla ważności czynności prawnej (np. zawarcia umowy) dokonanej w formie pisemnej wymagany jest podpis osoby działającej. Podpis ten można złożyć własnoręcznie w formie papierowej lub też dokument może zostać podpisany elektronicznie. Przepisy prawa wyraźnie zezwalają na zawieranie pisemnych umów drogą elektroniczną. W przypadku gdy dodatkowo dołączymy do dokumentu choćby prosty podpis elektroniczny, nikomu nie powinno się udać podważenie ważności zawartej w ten sposób umowy z punktu widzenia jej formy elektronicznej.

Problem może pojawić się jednak w momencie udowodnienia, czy umowa faktycznie została zawarta. Podczas korzystania z podpisów elektronicznych ryzyko to występuje przede wszystkim w przypadku podpisów prostych. W przypadku tych podpisów tożsamość podpisujących nie jest w żaden sposób weryfikowana, jak to następuje w przypadku podpisów gwarantowanych czy też podpisów uznanych lub kwalifikowanych[8]. W razie zawarcia umowy w postaci elektronicznej z dołączeniem podpisu elektronicznego w dowolnej formie umowa jest ważna z punktu widzenia wymogu zachowania formy pisemnej. Jeżeli jednak umowa została podpisana podpisem elektronicznym dającym mniejsze gwarancje identyfikacji sygnatariusza, zwłaszcza podpisem prostym, w praktyce mogą pojawić się problemy z udowodnieniem autentyczności podpisu. Zgodnie z przepisami czeskiego kodeksu cywilnego każdy, kto powołuje się na dokument prawa prywatnego, ma obowiązek wykazać jego autentyczność i prawidłowość[9].

W przypadku prostego podpisu elektronicznego udowodnienie, że dokument został podpisany przez właściwą osobę, zazwyczaj jest problematyczne z powodu samego charakteru podpisu. Zwykły podpis elektroniczny nie daje możliwości wykrycia późniejszych zmian w podpisanym dokumencie, jak to jest w przypadku podpisów o większej wiarygodności. Nie oznacza to jednak, że podpis elektroniczny jest całkowicie niewiarygodny lub bezużyteczny. Jego zaletami są przede wszystkim prostota i niskie koszty transakcyjne. Nawet proste podpisy mogą być zatem stosowane np. w mniej ważnych transakcjach lub umowach opartych na długotrwałych relacjach biznesowych. W przypadku sporu zawsze jednak konieczne jest przedstawienie sądowi innych istotnych argumentów potwierdzających ważność dołączonego prostego podpisu elektronicznego. Bardzo ważną rolę odgrywa również praktyka stron. Jeżeli zawarcie umowy jest wynikiem

[5] *Ibidem*.

[6] Zob. https://www.altaxo.cz/zacatek-podnikani/pravo/elektronicke-smlouvy-na-internetu (dostęp z 22.3.2023 r.).

[7] *Ibidem*.

[8] Zob. https://www.602.cz/blog/elektronicke-uzavirani-smluv-a-soudni-dokazovani (dostęp z 22.3.2023 r.).

[9] *Ibidem*.

długotrwałej, powtarzającej się komunikacji ze stałym partnerem biznesowym, to nagłe zakwestionowanie tej komunikacji wydaje się dosyć skomplikowane. Jeżeli jednak umowa została zawarta niezgodnie z dotychczasową praktyką, z wykorzystaniem nieznanej skrzynki e-mail, sytuacja dowodowa będzie znacznie bardziej skomplikowana[10]. W przypadku przeprowadzania dowodu w sporze o ważność umowy porządek prawny nie stawia żadnych ograniczeń. Co do zasady będzie to dotyczyć komunikacji stron umowy przed zawarciem umowy, dokumentów potwierdzających jej spełnienie przez strony umowy (wyciągi bankowe, dowody dostawy), wyraźnego potwierdzenia zawarcia umowy w komunikacji e-mail i tym podobne. Sądy dość rutynowo wykorzystują e-maile jako dowody. Jeśli jednak druga strona zakwestionuje, że e-mail faktycznie został wysłany, mogą zostać wykonane złożone ekspertyzy lub np. weryfikacja adresów IP.

Wykorzystanie systemów elektronicznych może być również użyte jako dowód autentyczności podpisu, jeżeli dokonują one tzw. zapisów systematycznych i sekwencyjnych oraz jeżeli są zabezpieczone przed zmianami. Jednak takie systemy z pewnością nie są standardem, zwłaszcza dla mniejszych przedsiębiorców lub osób fizycznych. Dla tych potrzeb można skorzystać z wyspecjalizowanych usług podmiotów trzecich (m.in. Software602), które pośredniczą w zawarciu umowy, a na potrzeby sprawy sądowej obie strony umowy są dostatecznie zidentyfikowane za pomocą swoich aplikacj[11].

Zawieranie umów elektronicznych w czasie stanu wyjątkowego

W związku z pandemią COVID-19 w marcu 2020 r. w Republice Czeskiej wprowadzono tzw. *nouzový stav* (stan zagrożenia). Działania kryzysowe zasadniczo zmieniły tradycyjny sposób pracy, do którego większość z nas była przyzwyczajona. Spotkania zostały zastąpione wideokonferencjami, mocno ograniczone zostały osobiste spotkania czy też załatwianie spraw w urzędach. W związku z tym pojawiły się takie kwestie, jak w praktyce radzić sobie z kontaktami z partnerami biznesowymi i władzami bez fizycznego spotkania. Prawo czeskie od dawna umożliwia zawieranie umów i prowadzenie postępowań sądowych drogą elektroniczną, czyli wtedy, gdy obie strony nie mogą osobiście się spotkać[12].

W przypadkach dotyczących prywatnego obrotu prawnego w formie elektronicznej praktycznie brak jest ograniczeń. Przy podpisywaniu dokumentu elektronicznego w stosunkach prywatnoprawnych można posługiwać się każdym rodzajem podpisu elektronicznego, w tym także tzw. prostym podpisem elektronicznym. Dlatego w większości przypadków możliwe jest „podpisanie" umowy pomiędzy dwoma podmiotami prawa prywatnego, np. poprzez wysłanie prostego e-maila z nagłówkiem, stopką lub nazwą, z odręcznym podpisem na odpowiednim dokumencie i jego późniejszym przesłaniem e-mailem w formie skanu, o wyższym poziomie wiarygodności dowodowej niż za pośrednictwem odpowiednich platform kontraktacyjnych (np. platformy DocuSign, jednak są też rozwiązania czeskie), a także poprzez łączenie wyższych form (gwarantowanego lub kwalifikowanego) podpisu elektronicznego[13]. Chociaż każda umowa podpisana elektronicznie powinna być ważna, doktryna zaleca ustanowienie jasnych wewnętrznych zasad dotyczących podpisów elektronicznych. Pomimo pojawiających się jeszcze sporadycznie orzeczeń SN kwestionujących równoważność prawną formy elektronicznej i formy papierowej, podejście sądów, zwłaszcza niższych instancji, jest w tym zakresie pozytywne na korzyść formy elektronicznej.

Inaczej jest jednak w przypadku kontaktów z podmiotami publicznymi (np. gminą lub jakimkolwiek organem państwowym). W takim przypadku można używać wyłącznie uznanego podpisu elektronicznego. Dotyczy to wszelkich czynności prawnych, w tym zawierania umów. Pisma do organów władzy publicznej nie muszą być jednak opatrzone podpisem elektronicznym, jeżeli są przesłane za pomocą tzw. skrzynek danych (*datová schránka*). Przesłanie dokumentu za pomocą skrzynek danych, nawet bez opatrzenia go podpisem, ma takie same skutki jak akt podpisany elektronicznie czy też własnoręcznie.

Podpis elektroniczny w systemie prawa Unii Europejskiej

Bardzo duże znaczenie dla regulacji prawnej podpisów elektronicznych ma rozporządzenie UE Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w transakcjach elektronicznych na europejskim rynku wewnętrznym oraz uchylające dyrektywę Nr 1999/93/WE, które w skrócie nazywane jest eIDAS[14]. Zgodnie z treścią art. 3 pkt 10 tego rozporządzenia podpis elektroniczny oznacza „dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis".

[10] *Ibidem*.
[11] *Ibidem*.
[12] Zob. https://www.havelpartners.cz/jak-uzavrit-smlouvu-ci-podepsat-dokument-na-dalku-nejen-v-nouzovem-stavu/ (dostęp z 23.3.2023 r.).
[13] *Ibidem*.
[14] Dz.Urz. UE L Nr 275, s. 73; dalej jako: eIDAS. Rozporządzenie to uchyliło dyrektywę UE 1999/93/WE. Aktualna i obowiązująca wersja eIDAS została opublikowana przez Parlament Europejski i Radę Europejską 23.7.2014 r. Bliżej także: *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [online]. The European Parliament and the Council of the European Union.*

Zgodnie z tym aktem prawnym podpisy elektroniczne mogą być w pełni wykorzystywane do zawierania negocjacji prawnych. Rozporządzenie to ponadto nadzoruje identyfikację elektroniczną i usługi zaufania dla transakcji elektronicznych na rynku wewnętrznym UE[15]. Reguluje podpisy elektroniczne, transakcje elektroniczne, definiuje także zaangażowane podmioty i procesy zapewniające bezpieczeństwo użytkownikom prowadzącym działalność w Internecie, na przykład podczas elektronicznego przesyłania środków lub komunikacji z usługami publicznymi. Umożliwia ono bezpieczne i wygodne dokonywanie transakcji transgranicznych bez korzystania z tradycyjnych metod papierowych, takich jak chociażby poczta czy faks. Rozporządzenie to stworzyło standardy podpisów elektronicznych, kwalifikowanych certyfikatów cyfrowych, pieczęci elektronicznych, znaczników czasu i innych sposobów weryfikacji mechanizmów uwierzytelniania. Dzięki nim transakcja elektroniczna ma taki sam status prawny jak transakcja dokonywana na papierze.

Rozporządzenie weszło w życie w lipcu 2014 r.[16] jako sposób na umożliwienie bezpiecznych i płynnych transakcji elektronicznych na terenie UE. Państwa członkowskie UE są zobowiązane do uznawania podpisów elektronicznych spełniających standardy eIDAS. Warto dodać, że eIDAS towarzyszą rozporządzenia wykonawcze Komisji (UE) Nr 2015/1501 i Nr 2015/1502, oba z 8.9.2015 r.

Rozporządzenie kieruje podmioty do stosowania wyższego poziomu bezpieczeństwa informacji i zgodności z wymaganiami technologicznymi. Ponadto koncentruje się na interoperacyjności, tzn. państwa członkowskie UE są zobowiązane do stworzenia wspólnych ram, które uznają eID z innych państw członkowskich i jednocześnie zapewniają ich autentyczność i bezpieczeństwo. Pozwala to użytkownikom na łatwe prowadzenie interesów ponad granicami państwowymi. Kolejnym elementem jest przejrzystość, eIDAS[17] udostępnia bowiem publicznie dostępną listę zaufanych usług, z których można korzystać w ramach scentralizowanego podpisu. Pozwala to interesariuszom na podjęcie dialogu na temat wyboru najlepszych technologii i narzędzi do zabezpieczania podpisów cyfrowych.

W elDAS uregulowano kilka kategorii podpisów elektronicznych[18]. Także tzw. gwarantowany podpis elektroniczny, który częściowo zastępuje podpis rzeczywisty, ma moc prawną. Podpis elektroniczny wywołuje skutki prawne i nie może być odrzucony jako dowód w postępowaniu sądowym i administracyjnym tylko dlatego, że ma formę elektroniczną lub z powodu niespełnienia wymogów koniecznych dla kwalifikowanego podpisu elektronicznego. Podpisy elektroniczne są regulowane przez rozporządzenie eIDAS oraz krajowe przepisy dostosowawcze. W rezultacie wyróżniamy:

- kwalifikowany podpis elektroniczny (wykorzystuje on środek do składania podpisów elektronicznych – np. kartę chipową lub token USB z certyfikacją);
- gwarantowany podpis elektroniczny oparty na certyfikacie kwalifikowanym (certyfikat kwalifikowany, ale bez karty/tokena);
- gwarantowany podpis elektroniczny (certyfikat nie jest stawiany żadnym wymaganiom);
- prosty podpis elektroniczny (wszystko, co ma formę elektroniczną i czego ktoś używa jako podpisu, choćby tylko podpisu w treści e-maila)[19].

Uregulowania prawne oraz rodzaje podpisów elektronicznych w Republice Czeskiej

Zgodnie z przepisami czeskiego kodeksu cywilnego dla ważności czynności prawnej dokonanej w formie pisemnej wymagany jest podpis osoby działającej. W związku z tym, że forma pisemna oprócz formy papierowej może przybrać również formę elektroniczną, konieczne jest określenie sposobu prawidłowego posługiwania się podpisem elektronicznym, aby zamierzona czynność prawna przyniosła zamierzone skutki[20]. Regulacja prawna dotycząca podpisów

[15] Rozporządzenie eIDAS wyewoluowało z dyrektywy 1999/93/WE, której celem było połączenie państw członkowskich UE systemem podpisu elektronicznego. Dyrektywa zobowiązała europejskie państwa członkowskie do stworzenia prawa, które umożliwiłoby im stworzenie systemu podpisu elektronicznego w ramach UE. Wszystkie państwa członkowskie są zobowiązane do przestrzegania wymagań wymienionych w eIDAS od 1.7.2016 r., kiedy to rozporządzenie weszło w życie.

[16] Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Bliżej także: decyzja wykonawcza Komisji (UE) 2015/1505 z 8.9.2015 r. ustanawiająca specyfikacje techniczne i formaty zaufanych list.

[17] W krajach członkowskich UE obowiązuje eIDAS, które jest bezpośrednio skuteczne, tzn. żadne ustawodawstwo krajowe nie może być z nim bezpośrednio sprzeczne. Przyjęcie eIDAS w UE skutecznie harmonizuje ustawodawstwo krajowe na poziomie tzw. usług budowy zaufania, w tym podpisów elektronicznych, pieczęci elektronicznych, weryfikacji podpisów i pieczęci elektronicznych oraz długoterminowego przechowywania podpisów i pieczęci elektronicznych oraz identyfikacja elektroniczna.

[18] Podpis elektroniczny jest tworzony w następujący sposób: obliczany jest hash (odcisk palca) dokumentu, który jest szyfrowany za pomocą klucza prywatnego. Tworzy to podpis elektroniczny, który jest następnie dołączany do dokumentu. Odbiorcy zostanie przesłany oryginał dokumentu (nie jest on zaszyfrowany ani w inny sposób zabezpieczony przed wzrokiem osób nieupoważnionych), podpis elektroniczny oraz certyfikat. Odbiorca przechodzi następnie przez ponowne obliczenie skrótu dokumentu i użycie klucza publicznego do odszyfrowania podpisu elektronicznego, uzyskując w ten sposób oryginalny odcisk palca – porównując je, może następnie dowiedzieć się, czy dokument został zmieniony, tj. naprawdę dokument, który napisał i podpisał nadawca.

[19] Zob. https://azlegal.cz/uzavirani-smluv-online-a-elektronicke-podpisy/ (dostęp z 23.3.2023 r.).

[20] Zob. https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html (dostęp z 25.3.2023 r.).

elektronicznych w Republice Czeskiej regulowana jest przede wszystkim przez przepisy unijnego eIDAS. Ponadto przepisy rozporządzenia unijnego uzupełnia Ustawa Nr 297/2016 Sb. o usługach zaufania w zakresie transakcji elektronicznych[21]. Zgodnie bowiem z eIDAS niektóre regulacje tego aktu należy dostosować na poziomie krajowym. Ponadto innymi istotnymi aktami prawnymi w tej tematyce są: Ustawa Nr 227/2000 Sb. o podpisie elektronicznym[22], Ustawa Nr 298/2016 Sb.[23], nowelizująca niektóre przepisy ustawy o usługach zaufania w zakresie transakcji elektronicznych i zmianie niektórych innych ustaw, a także Ustawa Nr 250/2017 Sb. o identyfikacji elektronicznej[24].

W ustawodawstwie Republiki Czeskiej można wyróżnić cztery rodzaje podpisu elektronicznego[25]:
- prosty podpis elektroniczny (*Prostý elektronický podpis*);
- gwarantowany podpis elektroniczny (*Zaručený elektronický podpis*);
- uznawany podpis elektroniczny, inaczej też nazywany gwarantowanym podpisem elektronicznym na bazie kwalifikowanego certyfikatu podpisu elektronicznego (*Uznávaný elektronický podpis*);
- kwalifikowany podpis elektroniczny (*Kvalifikovaný elektronický podpis*).

Prosty podpis elektroniczny to podstawowy i prawdopodobnie również najczęściej spotykany rodzaj podpisu elektronicznego w Republice Czeskiej. Do tej kategorii można zaliczyć wiele metod technicznego wykonania podpisu elektronicznego. Metody te obejmują w szczególności wpisanie imienia i nazwiska (na końcu dokumentu lub w wiadomości e-mail), zaznaczenie pola „zgadzam się" na stronie internetowej (np. „zgadzam się z regulaminem"), wstawianie obrazu z zeskanowanym odręcznym podpisem (np. na końcu jakiegoś dokumentu) czy złożeniem wzoru podpisu utworzonym ołówkiem elektronicznym itp. Ten rodzaj podpisu elektronicznego jest stosowany zwłaszcza pomiędzy dwoma podmiotami prawa prywatnego, gdzie wymagany jest podpis własnoręczny (np. przy zawieraniu umowy). Jednak to zawsze od samych stron zależy, jakie warunki postawią przed podpisem elektronicznym[26].

Gwarantowany podpis elektroniczny natomiast jest podpisem elektronicznym tworzonym na podstawie klucza prywatnego i odpowiedniego certyfikatu. Stosowany certyfikat nie musi spełniać żadnych specjalnych wymagań i dlatego może być wydany przez dowolny urząd certyfikacji lub może być tzw. *self-signed*. Gwarantowany podpis elektroniczny można rozumieć jako rodzaj nadrzędnej formy podpisu elektronicznego. Wprawdzie podpis ten gwarantuje możliwość wykrycia każdej późniejszej zmiany danych, a także umożliwia identyfikację osoby podpisującej, jednak nie gwarantuje tego, co najważniejsze, czyli tego, kto jest jego autorem. Osoba podpisująca może złożyć gwarantowany podpis elektroniczny właściwie dowolnej osoby. Dlatego w nauce przyjmuje się, że stosowanie tego typu podpisu elektronicznego jest obecnie niepraktyczne, a nawet niebezpieczne[27]. Wymogi gwarantowanego podpisu elektronicznego regulowane są w art. 26 eIDAS, a w ramach krajowego prawa Republiki Czeskiej także w Ustawie w sprawie podpisu elektronicznego. Zgodnie więc z przepisami powyżej wskazanych aktów prawnych gwarantowany podpis elektroniczny powinien spełniać następujące wymagania:
- jest unikalnie przyporządkowany podpisującemu;
- umożliwia ustalenie tożsamości podpisującego;
- jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz
- jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna[28].

Uznany podpis elektroniczny jest gwarantowanym podpisem elektronicznym, a dodatkowo do jego stworzenia wykorzystano tzw. certyfikat kwalifikowany. Certyfikat taki jest wydawany odpłatnie przez kwalifikowane urzędy certyfikacji[29]. Ten rodzaj podpisu nie wynika z eIDAS, ale z Ustawy Nr 297/2016 Sb. i jest rodzajem podpisu elektronicznego specyficznym dla prawa czeskiego. W odróżnieniu jednak od wyżej wymienionych rodzajów podpisów ten rodzaj podpisu musi zostać „potwierdzony" przez urząd certyfikacji. Daje to pewność, że zastosowany uznany podpis elektroniczny jest rzeczywiście powiązany z osobą, której został wydany. Ten rodzaj podpisu elektronicznego jest wymagany przykładowo

[21] Zákon č. 297/2016 Sb. – Zákon o službách vytvářejících důvěru pro elektronické transakce.

[22] Zákon č. 227/2000 Sb. – Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

[23] Zákon č. 298/2016 Sb. – Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

[24] Zákon č. 250/2017 Sb. – Zákon o elektronické identifikaci.

[25] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Warto wspomnieć, że w 2000 r. w Republice Czeskiej przyjęto ustawę Nr 227/2000 Sb. o podpisach elektronicznych, dzięki czemu Republika Czeska stała się krajem trzecim, w którym weszła w życie ustawa regulująca stosowanie podpisów elektronicznych. To praktycznie zapoczątkowało erę stosowania i legalizacji gwarantowanego podpisu elektronicznego w Czechach. Ustawa została oparta na dyrektywie Nr 1999/93/WE Parlamentu Europejskiego i Rady. W 2016 r. przyjęto Ustawę Nr 297/2016 o usługach budowania zaufania dla transakcji elektronicznych (zákon o službách vytvářejících důvěru pro elektronické transakce), uzupełniającą europejskie eIDAS. Ustawą Nr 297/2016 Sb. uchylona została pierwotna ustawa o podpisie elektronicznym.

[26] Zob. https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html (dostęp z 26.3.2023 r.).

[27] *Ibidem*.

[28] *Ibidem*.

[29] *Ibidem*.

do podpisania dokumentu elektronicznego z podmiotem publicznoprawnym.

Ostatnim z rodzajów podpisów elektronicznych jest kwalifikowany podpis elektroniczny. Pochodzi on z eIDAS. Umożliwia on długoterminową weryfikację autorstwa oświadczeń podczas elektronicznej wymiany danych. Kwalifikowany podpis elektroniczny można uznać za cyfrowy odpowiednik podpisu odręcznego. Definicja podpisu kwalifikowanego znajduje się w art. 3 pkt 12 eIDAS, który stanowi, że „kwalifikowanym podpisem elektronicznym jest zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego”[30].

Podpis kwalifikowany dzięki oparciu na certyfikacie kwalifikowanym w sposób niezaprzeczalny wskazuje podpisującego, którego tożsamość została zweryfikowana i potwierdzona w certyfikacie przez kwalifikowanego dostawcę usługi zaufania. Wymaganie kwalifikowanego urządzenia zapewnia, że dane do składania podpisu elektronicznego nie mogą zostać skopiowane – występują tylko jednokrotnie w tym urządzeniu i nigdy go nie opuszczą. Z tego powodu kwalifikowanego podpisu elektronicznego nie można podrobić[31]. Kwalifikowany podpis elektroniczny niesie za sobą domniemanie prawne pewności złożenia podpisu elektronicznego przez osobę ujawnioną w kwalifikowanym certyfikacie, dzięki temu nie trzeba udowadniać jego jakości w postępowaniach sądowych. Wynika to z tego, że podpis kwalifikowany ma skutek prawny równoważny podpisowi własnoręcznemu. Dodatkowo wszystkie podpisane nim dokumenty są tak samo ważne we wszystkich państwach członkowskich UE[32]. Osoba podpisująca musi posiadać kwalifikowany certyfikat, a także musi posiadać odpowiednie urządzenie umożliwiające złożenie podpisu elektronicznego, na którym jest przechowywany prywatny klucz osoby podpisującej.

Administracja państwowa jest zobowiązana do stosowania w swojej działalności kwalifikowanych podpisów elektronicznych z wstawionymi kwalifikowanymi znacznikami czasu. Zatem, jak już zostało wyjaśnione powyżej, osoby fizyczne i prawne komunikujące się z administracją państwową za pomocą podpisu elektronicznego są zobowiązane do posługiwania się co najmniej uznanym podpisem elektronicznym. Korzystanie z podpisu elektronicznego między osobami prawnymi a osobami fizycznymi nie jest dalej regulowane i dlatego mogą one używać wszystkiego, co wspólnie uzgodnią.

Ponadto Ministerstwo Spraw Wewnętrznych Republiki Czeskiej stworzyło aplikację CertIQ[33] do weryfikacji certyfikatów na listach zaufanych wg eIDAS, a podległa jej Administracja Rejestrów Podstawowych stworzyła system informatyczny administracji publicznej pod nazwą Krajowy Punkt Identyfikacji i Uwierzytelnienia (*Národní bod pro identifikaci a autentizaci*)[34]. Krajowy punkt służy jako narzędzie do bezpiecznej i gwarantowanej weryfikacji tożsamości użytkowników usług online administracji publicznej. Dostawcy usług online potrzebują gwarantowanych informacji o tym, kto rejestruje się jako klient usług, które świadczą. Do potwierdzania tożsamości online są wykorzystywane różne środki identyfikacji, których dostawcy uzyskali akredytację i są podłączeni do Krajowego Punktu Identyfikacji i Uwierzytelnienia. Należą do nich np. nowy dowód osobisty z chipem, który wydawany jest od 1.7.2018 r., czy logowanie przy użyciu konta użytkownika krajowego organu tożsamości (*uživatelský účet národní identitní autority*).

Urzędy certyfikacji w Republice Czeskiej

Urząd certyfikacji (w skrócie CA, czyli *certifikační autorita*) to podmiot, który wydaje certyfikaty cyfrowe (podpisane elektronicznie publiczne klucze szyfrujące), ułatwiając w ten sposób korzystanie z PKI (Public Key Infrastructure) poprzez potwierdzanie prawdziwości danych zawartych w ogólnodostępnym kluczu publicznym ze swoim autorytetem. Zgodnie z zasadą transferu zaufania możemy ufać danym zawartym w certyfikacie cyfrowym, pod warunkiem że ufamy samemu urzędowi certyfikacji.

W Internecie działa wiele komercyjnych urzędów certyfikacji, które zwykle swoje klucze publiczne umieszczają bezpośrednio w przeglądarkach internetowych i innych programach, co może ułatwić użytkownikom decydowanie o poziomie zaufania serwerów WWW, z którymi się łączą (ale także e-maili podpisanych cyfrowo i innych danych). Istnieją również bezpłatne urzędy certyfikacji lub te, które podlegają prawu danego kraju, regulaminom wewnętrznym organizacji itp.[35].

Pierwszym z rodzajów urzędów certyfikacji są akredytowane urzędy certyfikacji. W komunikacji z administracją państwową jest wymagany kwalifikowany certyfikat wydany przez akredytowanego dostawcę usług certyfikacyjnych. Certyfikaty te, które mogą być oczywiście wydawane tylko przez akredytowane podmioty, mają bardzo szerokie zastosowanie.

[30] Zob. art. 3 pkt 12 eIDAS.

[31] Zob. https://obserwatorium.biz/jaki-podpis-elektroniczny-wybrac-kwalifikowany-zaawansowany-czy-zwykly.html (dostęp z 27.3.2023 r.).

[32] *Ibidem*.

[33] Aplikacja CertIQ sprawdza, czy przedstawiony certyfikat jest kwalifikowany w rozumieniu eIDAS lub jest wykorzystywany do wydawania kwalifikowanych elektronicznych znaczników czasu przez kwalifikowanego dostawcę usług budowy zaufania mającego siedzibę w państwie członkowskim UE lub EOG.

[34] Zob. https://www.identitaobcana.cz/Home (dostęp z 27.3.2023 r.).

[35] Zo. https://cs.wikipedia.org/wiki/Certifika%C4%8Dn%C3%AD_autorita (dostęp z 27.3.2023 r.).

Proces akredytacji, który jest dokonywany odrębnie, gwarantuje nie tylko bardzo dobrą pewność, zwłaszcza w zakresie bezpieczeństwa takich certyfikatów, ale także zapewnia, że dostawca posiada wystarczające środki na pokrycie ewentualnych szkód. Można stwierdzić, że najbardziej wiarygodne są certyfikaty od akredytowanych dostawców. Akredytowany dostawca musi spełniać dodatkowo określone w przepisach warunki, które nie dotyczą innych dostawców. W Czechach kwalifikowanymi dostawcami usług certyfikacyjnych są: Pierwszy Urząd Certyfikacji (*První certifikační autorita*), PostSignum QCA[36] – usługi Poczty Czeskiej (*Česká pošta*)[37] oraz eIdentity[38].

Kolejną grupę stanowią publiczne urzędy certyfikacji, które jednak nie posiadają akredytacji, ale oferują publicznie swoje usługi certyfikacyjne. Takich firm na rynku jest więcej niż w przypadku pierwszej grupy urzędów certyfikacji. Do 2011 r. ciekawym urzędem certyfikacji była firma CA Czechia, która miała stosunkowo szerokie portfolio usług[39].

W Czechach działają dziesiątki, a nawet setki prywatnych urzędów certyfikacji. W zasadzie każdy, kto posiada niezbędne *know-how*, może być takim urzędem certyfikacyjnym (*Certifikační autorita*, CA). Dla dużych i znanych organizacji ta droga jest tańsza od uzyskania certyfikatów wydanych przez zewnętrzne urzędy certyfikacji. Organizacja gwarantuje certyfikaty we własnym imieniu. Zazwyczaj organy te nie wydają zaświadczeń dla ogółu społeczeństwa. Nie funkcjonują one na rynku jako podmioty komercyjne. Certyfikaty wydawane są na potrzeby organizacji lub jej partnerów-klientów itp. Prywatne urzędy certyfikacji są najczęściej prowadzone przez uczelnie wyższe, operatorów usług hostingowych lub podobnych oraz duże firmy[40].

Urzędy certyfikacji spełniają dwie podstawowe funkcje, którymi są certyfikacja oraz walidacja. Funkcja certyfikacyjna gwarantuje, że zadeklarowany klucz publiczny należy do danej osoby. Celem certyfikacji jest wydawanie użytkownikom certyfikatów, gdzie certyfikat jest dokumentem potwierdzającym, że klucz publiczny (wskazany w certyfikacie) jednoznacznie należy do danej osoby. Certyfikat zawiera jednocześnie dodatkowe informacje dotyczące użytkownika, okresu ważności klucza, informacje o wykorzystaniu klucza oraz informacje o urzędzie certyfikacji. Certyfikat podpisany jest podpisem elektronicznym urzędu certyfikacji. W przypadku komunikacji pomiędzy dwoma użytkownikami użytkownicy najpierw weryfikują podpis swojego partnera za pomocą swojego klucza publicznego, a następnie weryfikują autentyczność klucza publicznego partnera poprzez weryfikację podpisu certyfikatu za pomocą klucza publicznego urzędu certyfikacji. W takim przypadku wymóg zaufania dotyczy tylko urzędu certyfikacji.

Z kolei funkcja walidacyjna polega na tym, że użytkownik zwraca się do urzędu certyfikacji z zapytaniem o ważność certyfikatu swojego partnera. System zapytań można rozwiązać online lub korzystając z listy certyfikatów nieważnych, czyli listy certyfikatów, których ważność wygasła przed upływem określonego terminu ważności.

Podsumowanie

Jak można zauważyć, umowy elektroniczne, podpisy elektroniczne czy też urzędy certyfikacji mają duże znaczenie w systemie prawnym Republiki Czeskiej. Umowy elektroniczne w obecnych czasach zdają się zyskiwać coraz większą popularność jak w systemie prawnym, gdzie zostały one zrównane z umowami zawieranymi w formie tradycyjnej, tak i w praktyce, gdzie umowy te zdają się być formą coraz częstszego zawierania w ramach stosunków publicznoprawnych, jak też prywatnoprawnych. Elektroniczne zawieranie umów oferuje szybki i skuteczny sposób komunikowania się na odległość, jednak w naszych warunkach nie jest jeszcze zbyt popularny ze względu na to, że nie cieszy się na razie powszechnym zaufaniem. Przyczyną może być nowość i związany z nią pewien brak regulacji prawnych, zwłaszcza w odniesieniu do braku praktyki orzekania w sądownictwie.

Osobista wizyta sygnatariusza czy już na poczcie, u notariusza, adwokata, radcy prawnego lub w innym miejscu w celu stwierdzenia autentyczności podpisu, a następnie klasyczna „fizyczna" weryfikacja podpisu przez inną osobę, nadal stanowi najwyższą formę gwarancji, że czynność prawna została faktycznie podjęta przez sygnatariusza i z jego własnej woli. Ja osobiście jestem jednak przekonany, że system prawny Republiki Czeskiej jest już dostosowany do coraz większej informatyzacji zawierania umów i biorąc pod uwagę zalety zawierania takich umów, wydaje się kwestią czasu, zanim ustąpią obawy społeczeństwa co do ich stosowania.

[36] Zob. https://www.postsignum.cz/popis_sluzeb_postsignum.html (dostęp z 27.3.2023 r.).

[37] Česká pošta, s.p. jest przedsiębiorstwem państwowym świadczącym usługi pocztowe na terenie Republiki Czeskiej.

[38] Zob. https://www.eidentity.cz/ (dostęp 27.03.2023 r.).

[39] Zob. https://cs.wikipedia.org/wiki/Certifika%C4%8Dn%C3%AD_autorita (dostęp z 28.3.2023 r.).

[40] Zob. https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis (dostęp z 28.3.2023 r.).

Słowa kluczowe: umowy elektroniczne, Republika Czeska, podpis elektroniczny, prawo, urzędy certyfikacji.

Electronic contracts and electronic signature in the legal system of the Czech Republic

The object of the article is to present the legal system of electronic contracts and electronic signatures in the Czech Republic. Consecutively, the author presents issues regarding the types of electronic contracts in the Czech legal system, the issue of an electronic contract as evidence in court, concluding contracts during the COVID-19 pandemic and the types of electronic signatures. In addition, in the final part of the article, the author describes the specificity of accredited, public and private certification authorities, which undoubtedly have a close relationship with both electronic contracts and electronic signatures.

Keywords: electronic contracts, the Czech Republic, electronic signature, law, certification authorities.