

WOJCIECH WYTRĄŻEK

PROBLEMY INFORMATYZACJI ADMINISTRACJI PUBLICZNEJ

Ogromny rozwój mediów, takich jak internet, łączność satelitarna umożliwia natychmiastowe przekazywanie informacji pomiędzy dowolnymi miejscami na świecie. Rewolucja informatyczna jest dla administracji publicznej dużym wyzwaniem. Koszty uzyskania nowych technologii są często wysokie, co sprawia, że administracja nie może sobie pozwolić na dostateczne wyposażenie techniczne, tak jak ma to miejsce w organizacjach komercyjnych. Z drugiej strony, wysoka informatyzacja umożliwia bardzo szybkie zarządzanie i przekazywanie informacji, ułatwia kontakt z organami administracji i oszczędza czas.

Celem niniejszego artykułu jest wskazanie kilku najważniejszych problemów dotyczących przeobrażeń polskiej administracji, mających na celu dostosowanie jej do coraz bardziej z informatyzowanego otoczenia.

1. BUDOWA SYSTEMU INFORMACYJNEGO

Procesy administracyjne są coraz bardziej rozbudowane i wymagają sprawnego działania urzędów. Takie działanie jest możliwe do realizowania tylko przy zastosowaniu odpowiednich technik przepływu informacji i komunikacji.

Dr WOJCIECH WYTRĄŻEK – asystent Katedry Administracyjnego Prawa Gospodarczego WPPKiA; adres do korespondencji: Al. Raclawickie 14, 20-950 Lublin; e-mail: wwojtek@kul.lublin.pl

Z tego powodu rośnie znaczenie systemów informacyjnych w urzędach administracji jako konkretnych organizacji. System informacyjny to „formalny zespół środków ludzkich i kapitałowych oraz programów, których funkcjonowanie przejawia się w zbieraniu, kodowaniu, magazynowaniu, przetwarzaniu, odnajdywaniu, komunikowaniu, dekodowaniu i użytkowaniu danych dla podejmowania decyzji i zarządzania”¹.

System informacyjny należy traktować jako podsystem, ale ze względu na jego ważną rolę można go nazwać systemem, ponieważ decyduje on o poprawnym funkcjonowaniu organizacji jako całości, a jego elementy znajdują się w podsystemach zarządzania i wykonawczym. Pozwala on kierownictwu szybko reagować na szanse i zagrożenia pojawiające się w otoczeniu poprzez szybkie i efektywne podejmowanie decyzji, a następnie ich wdrażanie².

Głównym zadaniem systemu informacyjnego urzędu jest zapewnienie efektywnego przepływu informacji w urzędzie i sprawnej wymiany informacji z otoczeniem, czyli zewnętrznym środowiskiem informacyjnym. Należy też pamiętać o tym, że taki system musi gwarantować bezpieczeństwo chronionych przez prawo informacji przetwarzanych w urzędzie (chodzi tu w szczególności o dane osobowe, informacje objęte tajemnicą skarbową, informacje niejawnne), ich wiarygodność, kompletność, poufność oraz dostępność dla określonych podmiotów³. Przykładowo, za prawidłowe funkcjonowanie korpusu służby cywilnej jest w szczególności odpowiedzialny dyrektor generalny, który zapewnia funkcjonowanie i ciągłość pracy urzędu – nadzór nad tworzeniem i działaniem wynika z obowiązków określonych w art. 20 ustawy o służbie cywilnej. W praktyce zadania związane ze sprawnym przepływem informacji wykonują komórki do spraw informatyki, komórki organizacyjne do spraw ogólnych oraz pion ochrony. Budowa systemu informacyjnego urzędu opiera się również na regulaminie organizacyjnym urzędu, instrukcji kancelaryjnej oraz wymaganiach dotyczących ochrony informacji niejawnnych oznaczonych jako „zastrzeżone”.

Najważniejsze wymagania dotyczące systemów informacyjnych w urzędach administracji publicznej znajdują się w ustawie z 29 sierpnia 1997 r.

¹ Definicja H. Kriebla, R. L. Van Horna; M. Z m y ś l o n y, *O systemie informacyjnym urzędu administracji publicznej*, [w:] *Internet – fenomen społeczeństwa informacyjnego*, red. T. Zasępa, Częstochowa: Edycja św. Pawła 2001, s. 270.

² Por. Z. Ś c i b o r e k, *Podejmowanie decyzji*, Warszawa: Agencja Wydawnicza ULMAK 2003, s. 90-91.

³ Por. J. P a r t y k a - P o j ę t a, *Zarządzanie w organach administracji publicznej*, Chorzów: Wydawnictwo „Marka” 2004, s. 12 n.

o ochronie danych osobowych⁴ i w ustawie z 22 stycznia 1999 r. o ochronie informacji niejawnych⁵ oraz w aktach wykonawczych do wymienionych ustaw. Nie ulega wątpliwości, że każdy organ administracji publicznej dysponuje mniejszym lub większym zasobem danych osobowych. Dane te przetwarzane są w systemach informatycznych, które muszą zapewniać ich bezpieczeństwo i integralność. Należy zwrócić uwagę na różnice i zbieżności w rozumieniu pojęć „system informatyczny” i „system informacyjny”. Zasadniczo system informatyczny jest częścią systemu informacyjnego. System informatyczny to „system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje”⁶.

M. Zmyślony zaproponował opis systemu informacyjnego urzędu, opierając go na modelu trzywarstwowym⁷:

1. Warstwa fizyczna – systemy łączności i zarządzanie nimi, aspekty techniczne i technologiczne funkcjonowania systemów cywilnych, infrastruktura sieciowa, problematyka harmonizacji systemów teleinformatycznych administracji legalnym krajowym wzorcem czasu, karty chipowej na potrzeby identyfikacji i autoryzacji użytkowników w obrębie administracji, standaryzacja oprogramowania wspomagającego zarządzanie systemami teleinformatycznymi.

2. Warstwa proceduralno-administracyjna – procedury administracyjne przygotowane i wdrażane na potrzeby organizacji współdziałania rządowych systemów teleinformatycznych, tworzenie i wdrażanie dokumentów normatywnych określających politykę bezpieczeństwa, procedury certyfikacyjne w zakresie zabezpieczeń i ochrony danych, procedury identyfikacji i autoryzacji użytkowników.

⁴ Dz.U. 1997, nr 133, poz. 883, tekst jednolity: Dz.U. z 2002 r., nr 101, poz. 926.

⁵ Dz.U. z 1999 r., nr 11, poz. 95

⁶ § 1, p. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – Dz.U. 1998, nr 80, poz. 521. Rozporządzenie to obecnie nie obowiązuje, ale zostało przytoczone ze względu na określenie pojęcia systemu informatycznego.

⁷ M. Z m y ś l o n y, *Ochrona danych i systemów teleinformatycznych w administracji rządowej*, „Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne” 1998, nr 10; t e n - ż e, *O ochronie danych i systemów teleinformatycznych w administracji rządowej*, [w:] *Internet 2000 – prawo – ekonomia – kultura*, red. R. Skubisz, Lublin 2000, s. 7-14; t e n - ż e, *O systemie informacyjnym urzędu administracji publicznej*, s. 272-273.

3. Warstwa legislacyjna – ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia, akty wykonawcze, akty prawa miejscowego, polskie normy. Zadania organów administracji w zakresie współdziałania systemów; dokumenty elektroniczne, podpis elektroniczny wraz ze wszystkimi aspektami prawnymi.

Znaczenie zagadnień związanych z problematyką systemów informacyjnych wzrasta wraz z rozwojem komputeryzacji i zmianami organizacji pracy. Z roku na rok urzędy przetwarzają i przechowują coraz większe ilości danych. Zapewnienie harmonijnej wymiany informacji w urzędach i między nimi jest uzależnione nie tylko od wyposażenia w sprzęt komputerowy i umiejętności technicznych urzędników, ale również od prawnych ram działania.

2. ZASTOSOWANIE PODPISU ELEKTRONICZNEGO

Komunikacja za pomocą poczty elektronicznej jest niezwykle wygodna i szybka, jednak ze względu na specyfikę internetu niezbyt bezpieczna. Najprostszym przykładem jest wysłanie z kawiarenki internetowej listu i podanie się za inną osobę. Założenie skrzynki oparzonej dowolnym opisem zajmuje zaledwie kilka minut, w polu nadawcy wiadomości również można wpisać dowolne dane, zatem wysłanie oświadczenia woli sygnowanego nazwiskiem innej osoby nie jest żadnym problemem. Złożenie oświadczenia woli przez internet jest podobne do jego złożenia za pomocą telefonu czy faksu, z tym że w przypadku faksu pozostaje przynajmniej materialny ślad w postaci kopii dokumentu. Zwykłemu oświadczeniu woli złożonemu na nośniku informatycznym trudno przypisać cechy materialne. Składanie oświadczeń woli za pomocą internetu ma szczególny charakter także ze względu na uzależnienie od strony technicznej (komputerów, serwerów, łącz).

Aby zachować bezpieczeństwo przesyłanych danych przy obsłudze poczty elektronicznej, należy korzystać z szyfrowania i podpisu elektronicznego, które są uregulowane w ustawie z 18 września 2001 r. o podpisie elektronicznym⁸. Ustawa weszła w życie 9 miesięcy od jej ogłoszenia, czyli latem

⁸ Dz.U. z 2001 r., nr 130, poz. 1450; zgodnie z definicją ustawową, podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny (art. 3, pkt 1). Używanie podpisu elektronicznego regulują także ustawy dotyczące handlu elektronicznego: ustawa z 29.08.1997 r. Prawo bankowe (Dz.U. 1997 r., nr 140, poz. 939); ustawa z 02.03.2000 r. o ochronie niektórych praw konsumentów oraz o odpowie-

2004 r. Zastosowań kryptografii i podpisu elektronicznego jest bardzo wiele, jako najważniejsze przykłady można wskazać zawieranie umów cywilnoprawnych przez internet czy dysponowanie zasobami pieniężnymi w coraz popularniejszych systemach wirtualnych banków. W literaturze istnieją różne sposoby rozumienia podpisu elektronicznego. Bywa on rozumiany szeroko, a więc nie tylko jako podpis cyfrowy oparty na systemie kryptografii asymetrycznej z użyciem klucza prywatnego i klucza publicznego, ale również jako inne sposoby identyfikacji związane z cechami biometrycznymi, takimi jak odcisk linii papilarnych, obraz tęczówki oka, kształt twarzy. Za podpis elektroniczny uważa się również podpis skanowany, podpis tworzony przy użyciu pióra cyfrowego czy też dostosowaną do obrotu elektronicznego technologię kodu PIN, a nawet wpisane w komputer imię i nazwisko konkretnej osoby⁹.

Wykorzystanie podpisu elektronicznego w rozumieniu przepisów ustawy o podpisie elektronicznym w administracji publicznej umożliwia wiarygodne przesyłanie dokumentów, a taki obieg informacji ma wpływ na sprawniejsze i bardziej efektywne działanie administracji, choćby tylko w kwestii składania podań do organów administracji. Zgodnie z art. 63 § 1 Kodeksu postępowania administracyjnego¹⁰, podania (żądania, wyjaśnienia, odwołania, zażalenia) mogą być wnoszone pisemnie, telegraficznie lub za pomocą dalekopisu, telefaksu, poczty elektronicznej, a także ustnie do protokołu. Każda z wymienionych form ma takie samo znaczenie prawne i nie można ustalać między nimi żadnej gradacji, zatem wnosząc podanie petent może wybrać dowolnie jedną z wymienionych form, chyba że przepis szczególny stanowi inaczej. Niestety, w praktyce przyjmowanie podań w postaci elektronicznej stwarza urzędowi jeszcze sporo trudności, należy jednak mieć nadzieję, że ta sytuacja szybko

działności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. 2000 r., nr 22, poz. 271); ustawa z 16.07.2004 r. Prawo telekomunikacyjne (Dz.U. 2004 r., nr 171, poz. 1800); ustawa z 05.07.2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. 2002 r., nr 126, poz. 1068); ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 r., nr 144, poz. 1204); ustawa z 12.09.2002 r. o elektronicznych instrumentach płatniczych (Dz.U. 2002 r., nr 169, poz. 1385).

⁹ M. M a r u c h a - J a w o r s k a, *Podpis elektroniczny*, Warszawa: Wydawnictwo Prawo i Praktyka Gospodarcza 2002, s. 21.

¹⁰ Ustawa z 14.06.1960 r. Kodeks postępowania administracyjnego – tekst jednolity: Dz.U. 2000 r., nr 98, poz. 1071. W regulacjach międzynarodowych wyodrębnia się kilka rodzajów podpisu elektronicznego: podpis „sensu largo” – wszelkie środki i techniki mogące zastąpić podpis tradycyjny w obrocie elektronicznym, oraz podpis „sensu stricto” – oparty na kryptografii asymetrycznej albo innych technikach uwierzytelniania.

się zmieni, a urzędnicy przyzwyczajają się do komunikacji za pomocą sieci i doceniają jej zalety. Jedną z barier jest oczywiście niedostateczna infrastruktura techniczna, czyli zwykły brak komputerów i sprawnej sieci. Ustawodawca wziął ten problem pod uwagę i w art. 58 ust. 2 ustawy o podpisie elektronicznym przewidział obowiązek stworzenia przez organy władzy publicznej w ciągu czterech lat od uchwalenia ustawy o podpisie elektronicznym możliwości wnoszenia podań, wniosków oraz dokonywania innych czynności w formie elektronicznej. W tej kwestii obserwuje się jednak swoisty opór organów administracji wobec szerokiego stosowania podpisu elektronicznego. Przykładem może być zachowanie organów podatkowych, które nie godzą się na elektroniczną formę faktury, mimo że nie ma przepisu, który stwierdzałby, iż faktura musi mieć postać papierową, a stosowanie faktury elektronicznej usprawniłoby działanie przedsiębiorców, nie powodując żadnych obciążeń budżetu państwa¹¹.

Główne aspekty bezpieczeństwa związane z zastosowaniem podpisu elektronicznego to:

(1) *uwierzytelnienie* – strony wymieniające komunikaty są faktycznie tymi, za kogo się podają, ważność i prawdziwość podpisu zależą jedynie od danych służących do weryfikacji i zawartych w certyfikacie¹², co oznacza, że osoba, która utworzyła podpis, może być zidentyfikowana automatycznie w sposób bezpośredni i obiektywny¹³;

(2) *integralność* – podpis nie gwarantuje tego, że wiadomość podczas przesyłania nie zostanie zmieniona przez osobą niepowołaną, ale dzięki niemu wiadomo, czy taka zmiana nastąpiła czy nie („Bezpieczny podpis elektroniczny [...] jest powiązany z danymi, do których został dołączony, w taki

¹¹ R. P o d p ł o ń s k i, P. P o p i s, *Podpis elektroniczny – Komentarz*, Warszawa: Difin 2004, s. 537.

¹² „Certyfikat – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby” (art. 3, ust. 8). Pierwsze z funkcjonujących w Polsce publicznych centrów certyfikacji to PolCert (obsługujące komunikację między bankami), SigNet (związane z TP SA) oraz Unizeto (obsługuje ZUS). Na temat prawnych aspektów działania podmiotów świadczących usługi certyfikacyjne zob. K. K i c z k a, *Podpis elektroniczny na tle wybranych zagadnień administracyjnoprawnych*, [w:] *Prawo do dobrej administracji*, Warszawa: UKSW 2003, s. 407-418.

¹³ J. M u s z y ń s k i, *Podpis elektroniczny w praktyce*; <http://www.networld.pl/artykuly/23340.html> (22.06.2007).

sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna” – art. 3 pkt 2 lit. c ustawy o podpisie elektronicznym)¹⁴;

(3) niezaprzeczalność – nadawca wiadomości nie może się wyprzeć faktu jej wysłania, dzięki podpisowi można udowodnić pochodzenie, a przynajmniej fakt dostarczenia określonych danych; rolę świadka pełni organizacja certyfikująca, świadcząca kwalifikowane usługi certyfikacyjne – taki podmiot ma prawo znakowania usług elektronicznych czasem, co daje takie skutki prawne jak data pewna w rozumieniu przepisów kodeksu cywilnego (art. 7 ust. 2 ustawy o podpisie elektronicznym).

Podrobienie podpisu cyfrowego zasadniczo nie jest niemożliwe, ale bardzo trudne, przynajmniej wtedy, gdy usiłuje się uzyskać klucz metodami matematycznymi. Należy jednak zwrócić szczególną uwagę na kwestie bezpieczeństwa danych służących do generowania podpisu; chodzi zwłaszcza o ochronę tajnego klucza nadawcy wiadomości, którym szyfruje się podpis¹⁵. Zakłada się, że certyfikaty służące do tworzenia podpisów są bezpieczne, ponieważ wydają je ośrodki poręczone i podpisane prywatnym kluczem wydawcy. Dzięki certyfikatом podpis elektroniczny jest prosty do weryfikacji przez niezależne osoby. Większość użytkowników przechowuje certyfikaty w konwencjonalnych systemach komputerowych lub na kartach chipowych – oba sposoby są w dużym stopniu podatne na zewnętrzne zagrożenia. Pamięć komputera jest narażona na atak wirusów i włamania z użyciem oprogramowania szpiegowskiego. Nie należy też lekceważyć możliwości fizycznego ataku, mającego na celu przechwycenie nośnika danych (twardego dysku czy pamięci przenośnej, jak np. *pen-drive* czy karta chipowa).

Pod względem skutków prawnych dokumenty podpisane cyfrowo przy pomocy ważnego kwalifikowanego certyfikatu wywołują takie same skutki prawne, jak dokumenty podpisane własnoręcznie¹⁶. Należy jednak pamiętać

¹⁴ Tamże. Zmiana podpisanych danych pociąga za sobą zmianę danych tworzących podpis elektroniczny. Nie jest on więc dokładnym odpowiednikiem podpisu złożonego na papierze, ponieważ podpis na papierze nie jest w sensie zapisu związany z treścią dokumentu, a jedynie jest to zapis imienia i nazwiska.

¹⁵ Szerzej na temat kryptografii i podpisu elektronicznego zob. J. S t o ł o s a, *Kryptografia w sieci internet*, [w:] *Internet – fenomen społeczeństwa informacyjnego*, s. 497-513; por. M. G a n c z a r, *Elektroniczne sygnowanie – analiza ustawy o podpisie elektronicznym*, „Prawo–Administracja–Kościoł” (Lublin: Wydawnictwo KUL) 2004, nr 1-2, s. 29-44.

¹⁶ Art. 5 ust. 2; wymieniony oraz inne skutki prawne określono w rozdziale II cytowanej ustawy. Szerzej na temat zasady równoważności zob. K. K o r u s, *Oświadczenie woli w postaci elektronicznej i podpis elektroniczny*, [w:] *Prawo handlu elektronicznego*, red. F. Zoll, Bydgoszcz: Branta 2005, s. 28-31.

o tym, że aby podpis elektroniczny był ekwiwalentem podpisu własnoręcznego, musi nie tylko gwarantować potwierdzenie treści złożonego podania w sposób bezpieczny i pewny, ale też pozwalać na identyfikację osoby składającej podpis elektroniczny – spełnienie tego wymogu gwarantuje bezpieczny podpis elektroniczny (art. 3 ust. 2 u.p.e.).

Zastosowanie bezpiecznego podpisu elektronicznego nie rozwiązuje wszystkich problemów związanych z wnoszeniem podań drogą elektroniczną, ponieważ „podanie [art. 63 § 1 k.p.a.] o załatwienie sprawy to nie tylko pismo zawierające wniosek, ale i stosowne dokumenty na odpowiednim formularzu”¹⁷. Wniesienie podania na formularzu i dołączenie załączników stwarza problem wyboru formy ich wniesienia. Formularze w obrocie elektronicznym funkcjonują z powodzeniem, więc wymóg ich stosowania nie jest barierą nie do przewyciężenia. Inna sytuacja ma miejsce w przypadku załączników, ponieważ mogą zaistnieć takie sytuacje, że przepisy szczególne będą wymagać załączników, których nie można wnieść w formie elektronicznej; wtedy wniesienie podania opatrzonego bezpiecznym podpisem elektronicznym nie będzie możliwe¹⁸. Problemy mogą pojawić się również wtedy, gdy wniesienie podania uzależnione jest od uiszczenia opłat, w szczególności opłaty skarbowej, ponieważ sposoby ich uiszczania nie są jeszcze wystarczająco dostosowane do obrotu elektronicznego, jednak art. 58 ust. 4 u.p.e. nakłada na ministra właściwego do spraw finansów publicznych obowiązek dostosowania przepisów regulujących sposób wnoszenia opłat za czynności administracyjne do wymogów obrotu prawnego z wykorzystaniem podpisu elektronicznego w ciągu roku od wejścia w życie ustawy.

Regulacje prawne dotyczące podpisu elektronicznego rozkładają ryzyko związane z transakcjami zawieranymi przez internet między sprzedawcę, nabywcę, wystawcę karty kredytowej i podmiot certyfikujący. Dobra ustawa o podpisie elektronicznym w możliwie minimalnym stopniu reguluje zagadnienia związane ze strukturą rynku i technologią, ze względu na bardzo duże tempo zmian w obszarze sieci, rynku usług elektronicznych i dziedzinie techniki komputerowej. Zbyt szczegółowe regulacje mogłyby być nieaktualne krótko po wejściu ustawy w życie albo nawet przed jej wejściem w życie. Ustawa powinna umożliwiać wprowadzanie szybkich zmian i dostosowanie

¹⁷ Wyrok NSA z 09.06.1987, SAB/Wr 1/87, niepublikowany.

¹⁸ A. S k ó r a, *Zastosowanie podpisu elektronicznego w postępowaniu administracyjnym w świetle prawa obywatela do dobrej administracji*, [w:] *Prawo do dobrej administracji*, s. 117; inne problemy związane z wnoszeniem podań drogą elektroniczną zob. s. 118.

do nowych warunków, należy też brać pod uwagę konieczność spójności prawa krajowego z prawem wspólnotowym i międzynarodowym. R. Warner sugeruje utworzenie międzynarodowej organizacji branżowej, która nie byłaby nastawiona na zysk, a wypracowywała jednolite rozwiązania prawne, na wzór systemu administracji nazw domenowych¹⁹.

Rozwój cywilizacyjny umożliwił swego rodzaju oddzielenie podpisu elektronicznego od osoby fizycznej i przypisania go do osoby prawnej. Problematyczna może się okazać jednak identyfikacja takiej osoby. Trudniejsze niż w normalnych warunkach byłoby stwierdzenie, kto jako organ dokonał określonej czynności prawnej, a zastosowanie wielu przepisów, dotyczących na przykład wad oświadczeń woli czy zdolności do czynności prawnych, byłoby niemożliwe. Kolejnym niebezpieczeństwem jest użycie podpisu elektronicznego przez osoby nieuprawnione; mógłby istnieć podpis, którego skuteczne użycie byłoby niemożliwe²⁰.

Optymistyczne jest to, że media cyfrowe stają się coraz szerzej dostępne, także dla biedniejszych jednostek administracji publicznej. Działania w dziedzinie informatyki są obecnie lepiej skoordynowane, niż miało to miejsce jeszcze kilka lat temu na przełomie XX i XXI w., kiedy upadały kolejne projekty informatyzacji administracji, często występowały problemy z tzw. polskimi literami, czyli właściwymi dla polskiego języka znakami spoza amerykańskiego standardu, a strony internetowe instytucji administracyjnych były mało atrakcyjne i rzadko aktualizowane²¹.

Obecnie dyskutuje się nad możliwościami wprowadzenia alternatywnych metod doręczeń, jak choćby decyzja administracyjna w formie cyfrowej dostępna dla adresata po zalogowaniu się do systemu, w którym potwierdzenie jej otrzymania będzie możliwe do uzyskania w momencie otwarcia strony z tą decyzją. Oczywiście z zachowaniem wymogów bezpieczeństwa, takich jak chociażby połączenie szyfrowane.

¹⁹ R. Warner, *Digital Signature Statutes: Why Have Them, and How To Write Them*, [w:] *Internet – problemy prawne*, red. R. Skubisz, Lublin: Wydawnictwo Polihymnia 1999, s. 149-150.

²⁰ D. Szostek, *Czynność prawna a środki komunikacji elektronicznej*, Kraków: Zakamycze 2004, s. 240.

²¹ A. M. Wilk, *Polska wobec wyzwań społeczeństwa informacyjnego*, [w:] *Internet – fenomen społeczeństwa informacyjnego*, s. 158.

3. KOMPLEKSOWA INFORMATYZACJA ADMINISTRACJI

Systemy informatyczne tworzone w ramach systemów informacyjnych administracji publicznej były do niedawna nieprawidłowo wdrażane i nie tworzyły jednego spójnego narzędzia wymiany informacji w ramach systemu administracji. Z wdrażaniem tych systemów związane były często nadmierne straty finansowe, ponieważ każda zmiana w istniejącym czy dopiero wdrażanym systemie kosztuje. Wadliwe systemy zagrażają również bezpieczeństwu danych – pojawia się zagrożenie skasowania lub wycieku danych. Innym problemem jest kwestia kompatybilności i możliwości wymiany danych między różnymi podmiotami administracji. W związku z powyższym ustawodawca dostrzegł potrzebę jednolitego unormowania procesów informatyzacji administracji. Głównym założeniem tworzenia nowej ustawy było wyznaczenie minimalnych standardów budowy systemów teleinformatycznych. Systemy takie muszą spełniać wymóg interoperacyjności, czyli zapewniać możliwości wzajemnej współpracy różnych systemów teleinformatycznych i rejestrów publicznych przez techniczną zgodność sprzętu i programów²².

Ujęte w projekcie wymagania sprzętowe i programowe dotyczą przede wszystkim bezpieczeństwa wymiany informacji, niezawodności i wydajności systemów informatycznych oraz jednolitości (kodowanie znaków, szyfrowanie dokumentów, zgodność formatów plików, strukturalizacja dokumentów elektronicznych). Należy również zwrócić uwagę na jawność i neutralność technologiczną interfejsów w systemach teleinformatycznych wykorzystywanych do realizacji zadań publicznych.

Sejm RP przyjął w trzecim czytaniu rządowy projekt ustawy o informatyzacji – ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne została uchwalona 17 lutego 2005 r. o godzinie 17:15²³. Uderzająca jest prawie stuprocentowa zgodność parlamentarzystów – „za” głosowało 381 z 388 głosujących posłów, co może świadczyć o tym, że wszystkie ugrupowania polityczne zgadzają się co do konieczności wprowadzenia podstawowych standardów informatyzacji. Prezydent RP podpisał ustawę 7 kwietnia 2005 r., weszła ona w życie po upływie trzech miesięcy

²² Można wyróżnić cztery płaszczyzny wymiany informacji: między administracją publiczną i obywatelami; między administracją publiczną a podmiotami gospodarczymi; między różnymi jednostkami administracji polskiej; między polską administracją a administracjami innych państw.

²³ Dz.U. 2005 r., nr 64, poz. 565.

od dnia ogłoszenia, z wyjątkiem kilku przepisów mających wydłużone *vacatio legis*.

Z samego tytułu ustawy wynika jasno, że zawarte w niej uregulowania dotyczą nie tylko podmiotów administracji, lecz także wszystkich podmiotów publicznych, którym powierzono realizowanie zadań publicznych. Jej zakres podmiotowy obejmuje: organy administracji rządowej, organy kontroli państwowej i ochrony prawa, sądy, jednostki organizacyjne prokuratury, jednostki i organy samorządu terytorialnego, jednostki budżetowe, zakłady budżetowe i ich gospodarstwa pomocnicze, fundusze celowe, samodzielne publiczne zakłady opieki zdrowotnej, Zakład Ubezpieczeń Społecznych, Kasy Regionalnego Ubezpieczenia Społecznego, Narodowy Fundusz Zdrowia oraz inne szeroko pojęte podmioty publiczne (państwowe i samorządowe osoby prawne utworzone na podstawie ustaw i realizujące zadania publiczne). Ustawy nie stosuje się do przedsiębiorstw państwowych, spółek handlowych, jednostek badawczo-rozwojowych, państwowych szkół wyższych (także zawodowych), Polskiej Akademii Nauk, Kancelarii Sejmu, Senatu, Prezydenta, Trybunału Konstytucyjnego, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Instytutu Pamięci Narodowej oraz Narodowego Banku Polskiego (z wyjątkiem określonych przypadków).

Ustawa wprowadza Plan Informatyzacji Państwa. Zgodnie z art. 5, plan jest instrumentem planowania i koordynowania informatyzacji działalności podmiotów publicznych w zakresie realizowanych przez te podmioty zadań publicznych. Ma on na celu określenie organizacyjnych i technologicznych instrumentów rozwoju społeczeństwa informacyjnego, koordynację projektów informatycznych realizowanych przez podmioty publiczne, modernizację oraz łączenie systemów teleinformatycznych służących do realizacji zadań publicznych, zapewnienie warunków bezpieczeństwa i zgodności działania systemów oraz tworzenie warunków do rozwoju międzynarodowej współpracy w dziedzinie informatyzacji. Z punktu widzenia spójności działania administracji publicznej jest to w polskich warunkach rozwiązanie dotychczas nie stosowane i przełomowe ze względu na doniosłość, rozmiary tego przedsięwzięcia i jego ramy czasowe (plan ustanawia się na okres do 5 lat). Wejście w życie ustawy nie spowoduje natychmiastowej poprawy spójności systemów informacyjnych, ale daje możliwości jej poprawy i stworzenia jednolitego, bezpiecznego i prawidłowo działającego systemu komunikacji podmiotów wykonujących zadania publiczne. Ustawa wydaje się tworzyć warunki do ożywienia martwych – jak dotąd – przepisów dotyczących kwalifikowanego podpisu elektronicznego i jego zastosowania w kontaktach z administracją publiczną.

Plan ma być ustanowiony w drodze rozporządzenia Rady Ministrów na wniosek ministra właściwego do spraw informatyzacji i dostosowany do potrzeb i możliwości finansowych państwa, stąd dużą rolę będą odgrywać informacje o aktualnym stanie systemów teleinformatycznych i działaniach służących rozwojowi społeczeństwa informacyjnego, podejmowanych przez podmioty publiczne.

W celu wykonania planu ustanawia się projekty informatyczne:

– ponadsektorowy projekt informatyczny w drodze rozporządzenia Rady Ministrów na wniosek ministra właściwego do spraw informatyzacji, który może być ustanowiony jako projekt wieloletni w rozumieniu ustawy o finansach publicznych;

– sektorowe projekty informatyczne w drodze rozporządzenia ministrów odpowiedzialnych za poszczególne działy administracji rządowej, których dotyczą projekty, które również mogą być realizowane jako projekty wieloletnie w rozumieniu ustawy o finansach publicznych.

Ustawa wprowadza Radę Informatyzacji jako organ opiniodawczo-doradczy ministra właściwego do spraw informatyzacji. Jej zadaniem jest opiniowanie projektu plan informatyzacji oraz projektów rozporządzeń dotyczących minimalnych wymagań systemów teleinformatycznych i rejestrów publicznych. Rada ma również za zadanie przygotowywać propozycje rozwiązań dotyczących minimalnych wymagań systemów teleinformatycznych, rejestrów publicznych, wymiany informacji, tłumaczenia na język polski norm i dokumentów normalizacyjnych. Może również wydawać opinie w sprawach istotnych dla rozwoju standardów i technologii informatycznych (art. 17). Na mocy ustawy została utworzona Krajowa Ewidencja Systemów Teleinformatycznych i Rejestrów Publicznych, którą prowadzi minister właściwy do spraw informatyzacji.

Zapewnieniu spójnego działania systemów teleinformatycznych używanych do realizacji zadań publicznych ma służyć wymóg badania poprawności wdrożenia rozwiązań technicznych przy wykorzystaniu testów akceptacyjnych (art. 21). Badanie przeprowadza na swój koszt twórca oprogramowania, które ma być wykorzystywane do realizacji zadań publicznych.

Przestrzeganie przepisów ustawy będzie sprawdzane przez imiennie upoważnionych kontrolerów, wyznaczonych przez organy kontroli, którymi w zależności od jej szczebla są: Prezes Rady Ministrów, minister właściwy do spraw informatyzacji, minister kierujący działem administracji, wojewoda, organ administracji rządowej nadzorujący podmiot publiczny.

Ustawa nie jest pozbawiona pewnych niedociągnięć czy nawet wad. Ujęcie w jej słowniku pojęcia „system teleinformatyczny” wydaje się chybione, lepszym rozwiązaniem byłoby chyba określenie: system informacyjny realizowany za pomocą systemu informatycznego. Samo wytłumaczenie pojęcia utrudnia jej zrozumienie, ponieważ ustawodawca odsyła w tym zakresie do definicji zawartej w art. 2 pkt 3 ustawy z 18.07.2003 r. o świadczeniu usług drogą elektroniczną, który z kolei odsyła do ustawy Prawo telekomunikacyjne z 21.07.2000 r. Dociekliwa osoba, usiłująca zrozumieć, co to jest system teleinformatyczny, może złożyć razem trzy przytoczone wyżej zapisy, jednak sens otrzymanej definicji wciąż pozostanie trudny do zrozumienia²⁴.

Jakie znaczenie dla funkcjonowania administracji publicznej ma uchwalenie ustawy o informatyzacji? Biorąc pod uwagę dyskusję towarzyszącą jej tworzeniu, wypowiedzi przedstawicieli Ministerstwa Nauki i Informatyzacji, komentarze prasowe oraz jej krótką analizę, można powiedzieć, że jest ona przełomowym aktem prawnym, który wyznacza kierunek rozwoju społeczeństwa informacyjnego w Polsce przez określenie standardów, jakie muszą spełniać systemy teleinformatyczne, aby zapewnić spójność działania administracji publicznej i innych podmiotów wykonujących zadania publiczne. Na tle sąsiednich krajów Polska, mająca obecnie ustawę o informatyzacji wprowadzającą Plan Informatyzacji Państwa, jawi się jako swego rodzaju pionier. Ustawa cieszy się zainteresowaniem sąsiadów, którzy prosili o jej przetłumaczenie na język angielski, aby mogła służyć jako wzór do tworzenia podobnych aktów prawnych.

Pojawiają się również głosy, iż ustawa powinna była powstać dziesięć lat temu. Z pewnością byłby to jeszcze bardziej spektakularny przełom w tworzeniu społeczeństwa informacyjnego i poprawianiu spójności administracji publicznej. Fakt, iż ustawa powstała i została jednogłośnie przyjęta przez parlament, jest niewątpliwie optymistyczny, jednak jakość jej regulacji będzie można dokładnie ocenić po dłuższym czasie. Z punktu widzenia teorii organizacji i zarządzania ustalanie celów i formułowanie planów jest niezbędnym elementem sprawnego zarządzania organizacją. Administracja publiczna, którą można porównać do systemu nerwowego w organizmie, musi działać sprawnie, a powszechna i przemyślana informatyzacja wydaje się jednym z najważ-

²⁴ Problem jakości ustawy został podniesiony przez W. Iszkowskiego na konferencji „W mocy prawa”, poświęconej zgodności systemów informatycznych z wymogami prawa oraz zasadami ładu korporacyjnego, która odbyła się 14.09.2005 r. w Warszawie, zob. <http://www.computerworld.pl/konferencje/prawo2005/index.html> (22.06.2007).

niejszych czynników wpływających na poprawę jej funkcjonowania. W związku z tym samą ideę wprowadzenia planów informatyzacji należy ocenić pozytywnie, krytycznie analizując realność ich realizacji, ograniczanej wciąż zbyt małymi zasobami rzeczowymi, finansowymi, małą liczbą dobrze wykwalifikowanych (szczególnie pod względem pracy w systemie informatycznym) urzędników. Liczba dobrze przygotowanych do pracy administratywistów z każdym rokiem rośnie, jednak czy administracja publiczna jest odpowiednio otwarta i atrakcyjna dla młodej kadry?

THE PROBLEMS OF INFORMATIZATION OF PUBLIC ADMINISTRATION

S u m m a r y

The tremendous development of the media, such as the Internet or satellite communication, allows instantaneous transfer of information between two chosen locations around the globe. IT revolution is a big challenge for public administration. The cost of obtaining new technologies are often high – too expensive for the administration to buy, unlike in other commercial establishments. However, a high degree of computerization allows quick management and distribution of information, facilitates contacts with administrative boards and saves time.

The goal of this article is to show some of the key problems related to the transformation of Polish public administration, the objective of which is to adjust it to the increasingly computerized environment. Public administration, which can be likened to a nervous system, has to run efficiently, therefore a general and thoughtful computerization seems to be one of the crucial factors that enhance its functioning. However, apart from technical changes, such as restructuring of back-office information systems and making them mutually compatible, accelerating the exchange of information by means of electronic mail, or general computerization of the whole apparatus of public administration, the mindsets and habits of officials and co-workers have to change.

*Translated by Tomasz Pałkowski
and shaped by Wojciech Wytrążek*

Słowa kluczowe: informatyzacja, podpis elektroniczny, system informacyjny, sprawność, administracja.

Key words: computerization, electronic signature, information system, efficiency, administration.