Czas informacji
Prawo nowych technologii • Informacja w administracji i gospodarce
ISSN 2081-6189 kwartalnik 1(6)/2011

Informatyzacja służby zdrowia

Przeciw e-wykluczeniu
Wacław Iszkowski

Debata nad kompleksową reformą ochrony danych osobowych
Michał Czerniawski

Ściśle tajne czy zastrzeżone – nowe regulacje dotyczące informacji niejawnych
Anita Jackiewicz

Podpis urzędniczy 2.0
Michał Tabor

Informatyzacja służby zdrowia – czy się wreszcie powiedzie?
Piotr Kociński

Jak generować klucze dla podpisu osobistego
Przemysław Kubiak

cpi
centrum promocji informatyki
www.cpi.com.pl

centrum promocji informatyki
www.cpi.com.pl

poleca

Praca zbiorowa pod redakcja Henryka Hollendra

- Wstęp: Intencje i inicjatywy - Henryk Hollender

Cz. 1: ASPEKTY

- Polskie biblioteki cyfrowe A.D. 2010: kształtowanie paradygmatu - *Aleksander Trembowiecki*
- Do czego jest potrzebna informatyka w digitalizacji? - *Marcin Werla*
- Digitalizacja, cyfryzacja czy dyskretyzacja i jaka? - *Kazimierz Schmidt*
- Aspekty prawne digitalizacji - Rafał Golat
- Krajowa strategia cyfryzacji dziedzictwa narodowego - *Tomasz Makowski, Katarzyna Ślaska*
- Preliminaria do polskiego programu digitalizacji muzealiów - *Agnieszka Jaskanis*
- W kierunku uczelnianego repozytorium cyfrowego - *Emilia Karwasińska, Małgorzata Rychlik*

Cz. 2: REALIZACJE

- Digitalizacja dokumentów piśmienniczych – strategie Rozwoju - *Jerzy Franke*
- Jak posługiwać się biblioteką cyfrową? - *Lidia Derfert-Wolf*
- Pozyskiwanie finansowania na budowanie cyfrowych zasobów - *Bożena Bednarek-Michalska*
- Podsumowanie: Przemiany i perspektywy - *Henryk Hollender*

Wydawca:

Centrum Promocji Informatyki Sp. z o.o., 04-041 Warszawa, ul. Międzyborska 50 Tel. (022) 870 69 10 (78), fax (022) 870 69 95, e-mail:cpi@cpi.com.pl

ZAMÓWIENIA

www.cpi.com.pl

4 **Przeciw e-wykluczeniu**
Wacław Iszkowski

NAUKA

8 **Debata nad kompleksową reformą ochrony danych osobowych**
Michał Czerniawski

14 **Ochrona materiałów nieobjętych prawem autorskim**
Bohdan Widła

19 **Dokumentacja medyczna a bezpieczeństwo danych**
Marcin Kędzierski

25 **Skuteczne doręczenie elektronicznych dokumentów i oferty w postaci elektronicznej zamawiającemu będącemu podmiotem publicznym**
Kinga Telecka

30 **Zasada powszechności prawa do informacji publicznej**
Dorota Fleszer

40 **Program komputerowy jako próbka w świetle przepisów dotyczących zamówień publicznych**
Wojciech Kaliński

47 **Jak generować klucze dla podpisu osobistego**
Przemysław Kubiak

PUBLICYSTYKA

55 **Ściśle tajne czy zastrzeżone – nowe regulacje dotyczące informacji niejawnych**
Anita Jackiewicz

61 **Jaka będzie przyszłość elektronicznej administracji? Część I - trendy**
Dariusz Bogucki

67 **Podpis urzędniczy 2.0**
Michał Tabor

75 **Informatyzacja służby zdrowia – czy się wreszcie powiedzie?**
Piotr Kociński

83 **Informacja w transgranicznej opiece zdrowotnej. Polska na tle przepisów wspólnotowych oraz USA**
Bartłomiej Michalak

88 **ICT w inicjatywach przewodnich UE „Mobilna Młodzież" oraz „Program na rzecz nowych umiejętności i zatrudnienia"**
Dariusz Bogucki

91 **Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne – część V**
Wojciech Kaliński

95 **Artykuł 27 czy paragraf 22?**
Robert Podpłoński

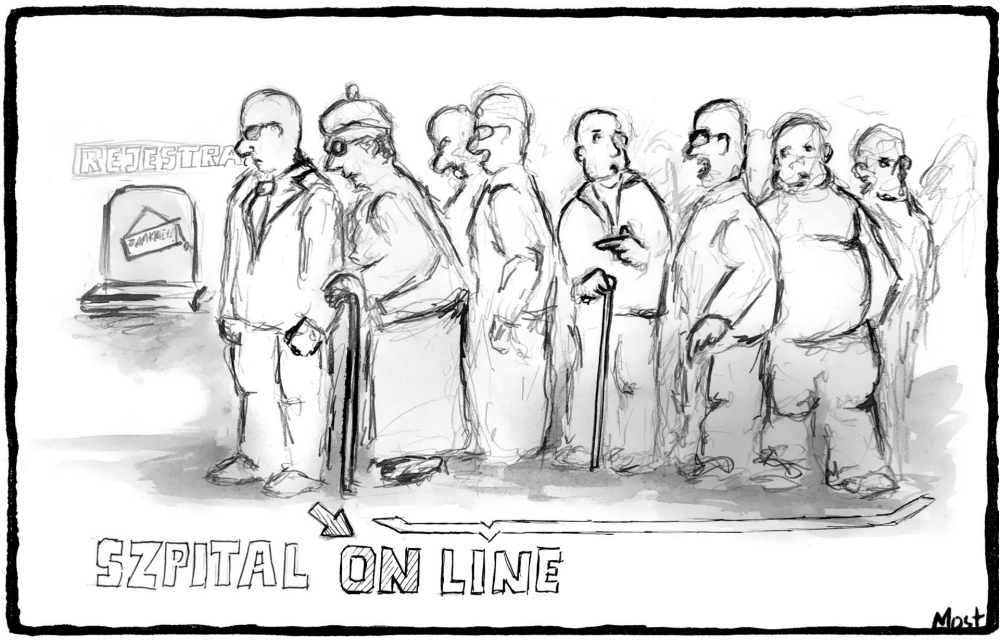
STAŁE RUBRYKI

108 **Ochrona danych osobowych: Nowelizacja ustawy o ochronie danych osobowych – konsekwencje i nowe wyzwania**
Monika Krasińska

112 **Przegląd orzecznictwa w zakresie zamówień publicznych: Postanowienie Krajowej Izby Odwoławczej z 22 kwietnia 2010 r., KIO/UZP 600/10**
Wojciech Kaliński

114 **Cyfrowe społeczeństwo otwarte i jego wrogowie**
Edwin Bendyk

116 **Bibliografia zagadnień prawno-informatycznych 2010**
Wojciech R. Wiewiórowski



W kolejnym numerze:

W najbliższym numerze m.in.:

- Jaka będzie przyszłość elektronicznej administracji? Część II - scenariusze rozwoju - Dariusz Bogucki
- Nowa instrukcja kancelaryjna - Kazimierz Schmidt
- Prawo do zapomnienia - Arwid Mednis
- Prawna ochrona abonenta w świetle zmian prawa wspólnotowego w zakresie tajemnicy telekomunikacyjnej - Andrzej Krasuski
- Przepisy grupowe i ich zastosowanie - Przemysław Kubiak
- Potwierdzenie tożsamości w elektronicznym obrocie gospodarczym a elektroniczna administracja - część II - Izabela Adamska
- E-faktura, od legalnej do normalnej - Robert Podpłoński
- Monitoring BIP sądów woj. śląskiego - Grzegorz Wójkowski

Wiesław Paluszyński redaktor naczelny
wieslaw.paluszynski@czasinformacji.pl

Nowy rok nie rozpieszcza nas tempem publikowanych inicjatyw legislacyjnych, a zaległe, jeszcze z ubiegłego roku, rozporządzenia ślimaczą się okrutnie. Ich jakość też pozostawia wiele do życzenia, szczególnie dołączana do nich ocena skutków wprowadzanych regulacji. W lutym zostało poddane społecznym uzgodnieniom (z 7-dniowym terminem wyrażenia opinii) jedno z najważniejszych rozporządzeń dotyczące wymagań technicznych dla warstwy elektronicznej dowodu osobistego, stanowiące wykonanie delegacji do art. 15 Ustawy o dowodach osobistych. Wiele proponowanych w tym rozporządzeniu rozwiązań wzbudziło wątpliwości ekspertów, a nam udało się zdobyć opinię dra Przemysława Kubiaka o jednym z najważniejszych jego aspektów, czyli jak generować klucze dla podpisu osobistego, aby były one dla nas bezpieczne. W tematyce podpisu elektronicznego kolejny raz gościmy Michała Tabora z ciekawą koncepcją „podpisu urzędniczego". Z nowości prawnych polecam publikację Anity Jackiewicz o właśnie wchodzącej w życie nowej ustawie o ochronie informacji niejawnych.

W drugiej połowie roku, w trakcie polskiej Prezydencji zaplanowana została odbywająca się co dwa lata Konferencja Ministerialna UE nt. administracji elektronicznej (eGovernment). Próbę oceny przyszłości e-administracji podejmuje Dariusz Bogucki w pierwszym z kilku artykułów, jakie planujemy opublikować w ramach przygotowań merytorycznych do tej konferencji. Także w ramach tych przygotowań zamieszczamy artykuł Piotra Kocińskiego, próbującego uporządkować naszą wiedzę o dotychczasowych wysiłkach, jakie podejmujemy w informatyzacji służby zdrowia. Podsumowanie jest wstrząsające. Zachęcam do wypowiedzi kontynuujących ten temat. W końcu niezależnie od tego czy jesteśmy zaangażowani w kwestie przetwarzania informacji, czy nie, dotyczą one każdego z nas.

Problem wykluczenia cyfrowego podejmuje na naszych łamach dr Wacław Iszkowski, Prezes Polskiej Izby Informatyki i Telekomunikacji. Warto ten artykuł przeczytać, a ja zachęcam do polemiki na naszych łamach.

Zupełnie nowy dział naszego czasopisma powstał z inicjatywy Generalnego Inspektora Ochrony Danych Osobowych, pana ministra dra Wojciecha Wiewiórowskiego. Będziemy w nim informować o najważniejszych problemach związanych z ochroną danych osobowych - zarówno o praktyce działania, jak i planowanych regulacjach prawnych. Ponieważ w grudniu rozpoczął się cykl bardzo ciekawych konferencji dotyczących ochrony danych osobowych, w tym numerze zamieszczamy omówienie problemu ochrony prywatności pióra Michała Czerniawskiego i kilka istotnych materiałów z tej tematyki. I jak zawsze - trochę analiz prawnych, dział o zamówieniach publicznych, bibliografia. Na deser zaś Edwin Bendyk, tym razem o wrogach cyfrowego społeczeństwa otwartego. Lecz aby zrozumieć, o co chodzi, trzeba przeczytać...

Zapraszam

Przeciw e-wykluczeniu

Wacław Iszkowski

Jestem przeciwko obrażaniu pokolenia 50+, mówiąc o nich, że są wykluczeni cyfrowo. Cokolwiek by to bowiem znaczyło i bez względu na to, jak to ci starsi mogą zrozumieć (bo wielu zrozumie to jakoś opacznie), jest to pojęcie negatywne. A przecież to pokolenie nie jest winne temu, że w czasie ich młodości, ich okresu nauki i chłonności poznawania nowych rzeczy tylko niewielka grupka osób zajmowała się i rozumiała, czym jest i jak działa elektroniczna maszyna cyfrowa. Tylko niewielka grupa osób w tym czasie zajmowała się rozwojem informatyki i telekomunikacji – i tylko oni dzisiaj w wieku 50+ mogą się jako tako odnaleźć w tym cyfrowym świecie.

Pozostali w wieku 50+, nawet używający komórki, bankomatu, gpsu czy laptopa, nie mają już szansy na zrozumienie istoty teleinformatyki (ICT) – ogólnie czym jest, jak działa i po co jest potrzebna oraz dlaczego jest tak fascynująca dla młodego pokolenia. Ta wiedza jest już poza możliwościami mojego pokolenia, tak jak pewnie dla was będzie kłopotem zrozumienie inżynierii genotypu lub czegoś podobnego. I dlatego jeszcze raz proszę, aby nie używać tego negatywnego pojęcia – wykluczenie cyfrowe. Zresztą UE dość szybko zmieniła to na e-inclusion, co niestety słabo się tłumaczy na język polski!

No dobrze, ale przecież Internet jest pożytecznym narzędziem, dającym szanse na rozwój oraz możliwość większej efektywności w nauczaniu oraz pracy itd. Tak, ale ci starsi już nie mają ochoty (poza nielicznymi) się rozwijać. Nie chcą się już uczyć nowych rzeczy, a tym bardziej pracować (we Francji, i nie tylko tam, strajkują o obniżenie wieku emerytalnego). Większość z nich u nas w Polsce, niestety, jest kompletnie podporządkowana Kościołowi i nawet na rozkaz biznesmena Rydzyka zakupili aparaty komórkowe (nawet specjalnie uproszczone w użytkowaniu) – tylko potem nie widzieli potrzeby korzystania z nich! Inni wolą, albo muszą, zajmować się wnukami, aby ich dzieci mogły robić karierę i spędzać więcej czasu w internecie. Pozostali wolą mieć święty spokój i trochę odpocząć przed telewizorem, który myśli za nich, co im pokazać.

Zadajmy sobie pytanie, po co temu starszemu pokoleniu Internet? Spróbuję na to odpowiedzieć na swoim przykładzie, chociaż akurat ja jestem bardzo tutaj nietypowy, gdyż:

- Nie jestem wykluczony cyfrowo, bo dość dobrze się znam na teleinformatyce (ostatnio w trzy godziny zainstalowałem sieć domową z drukarką sieciową i trzema komputerami - każdy z innym systemem).
- Jeszcze pracuję zawodowo (tutaj Internet mi się przydaje), ale spróbuję tę część wyłączyć z opisu, bo większość tych 50+ już nie pracuje.

Internetu można używać do:

- dokonywania elektronicznych płatności domowych, co bardzo upraszcza ten problem i oszczędza czas, ale zbyt wielu z tych 50+ nie ma kont bankowych i oszczędności, a więc ta funkcja może ich nie dotyczyć,

- zakupów w e-sklepie, ale większość z 50+ woli jednak dla oszczędności wydatków najpierw dobrze obejrzeć, co kupuje – nie mówiąc już o tym, że jest to pewna forma przyjemności, pamiętając jeszcze o pustych półkach,
- zamawiania produktów spożywczych lub pizzy, ale wielu jednak woli się przejść, czy podjechać do sklepu na osiedlu, bo jest szansa sobie trochę pogadać o lokalnych osiedlowych problemach i plotkach,
- elektronicznego wypełnienia PITu, ale na razie jest z tym więcej kłopotu niż pożytku (ten, co to wymyślił, potem 5 razy był wzywany do US), a za emerytów PIT wypełnia ZUS,
- załatwiania spraw urzędowych, ale wielu takich spraw zbyt często się nie załatwia, a więc może lepiej przespacerować się do urzędu, gdzie sprawny urzędnik szybko i bez potrzeby wysyłania po załączniki załatwi jego sprawę,
- poszukania miejsca na wyjazd na wakacje, ale samo zamówienie wielu woli zrobić w agencji, bo można się wtedy dowiedzieć więcej rzeczy i wybrać sobie lepszy pokój z widokiem na morze,
- do rezerwacji biletu lotniczego, przy czym pracującym 50+ służbowe loty załatwia sekretarka, a prywatne są charterami dołączonymi do wycieczki i z reguły załatwia to agencja,
- korzystania z Naszej Klasy, co jednak w wielu przypadkach prowadzi do awantur rodzinnych, albo też nie warto widzieć wszystkich byłych kolegów i koleżanek, jak się posunęli w czasie, a o tych kilku bliższych wie się, jak ich znaleźć,
- korzystania z Facebooka, Twittera i innych podobnych portali – owszem wpisałem się tam, ale już się wypisałem, bo zalew tych bzdurnych komentarzy od moich „znajomych" był irytujący (a już nawet Facebook sprzedał moje dane – co przemyślnie sprawdziłem!),
- czytania prasy i informacji, ale stwierdzam, że zbyt długie przesiadywanie przed komputerem jest ze szkodą dla zdrowia, bo lepiej iść na spacer niż się denerwować kolejnymi wybrykami polityków,
- korzystania ze Skype'a do kontaktu z dziećmi i wnukami przebywającymi w innych miastach i za granicą – ta funkcja jest bardzo pożyteczna i nawet moja 80+ ciocia też jej używa w swoim laptopie, ale tylko jej!,
- rozrywki – szczególnie tej z serii XXX, gdy już można tylko popatrzeć, ale nie wolno się do tego przyznawać ☺.

Oczywiście wielu z tych 50+ wskaże pożytki z korzystania Internetu i wykaże chęć poznania zasad jego użytkowania. Dlatego też oczywiście warto promować Internet wśród starszych i przekonywać ich, że nie jest to takie trudne i aż tak kosztowne.

Tym samym popieram determinację wielu organizacji i fundacji w opracowywaniu i wdrażaniu programu włączenia pokolenia 50+ do społeczności teleinformatycznej. Dobrze, że fundacje te są sponsorowane przez firmy teleinformatyczne dostarczające usługi dostępu do Internetu, widząc w tym również własny interes. Wszak trzeba jakoś przekonać starszych lokatorów do zaabonowania oprócz telewizji kablowej również dostępu do Internetu– bo przecież już cały budynek jest okablowany, a tych kilkanaście lokali nie chce z tego dobra skorzystać.

A teraz konstruktywnie, co można zrobić w tej materii:

1. Nie należy mówić o wykluczeniu cyfrowym, ale o możliwościach zastosowania Internetu dla potrzeb ludzi 50+.
2. Należy dążyć do tego, aby korzystanie z Internetu odbywało się również pośrednio dla potrzeb 50+, a jednak przynosiło bezpośrednie korzyści – np. zinformatyzowanie wizyt do lekarzy,

wspomaganie codziennej krzątaniny, przypominanie o ważnych sprawach, gps dla tych z demencją itp.

3. Należy dążyć do maksymalnego uproszczenia zasad korzystania z komputera i telefonu bez konieczności czytania i zrozumienia „niezrozumiałych" instrukcji oraz ergonomicznego ich przystosowania dla ludzi starszych – większych klawiszy, czytelnych ekranów, prostych funkcji itp.
4. Należy wyselekcjonować grupę jeszcze aktywnych zawodowo, starszych, ambitnych w poszukiwaniu wiedzy (są też tacy) i innych, którzy się sami zgłoszą – i tym warto zapewnić pomoc w poznawaniu najważniejszych funkcji i dobroci Internetu (wg mnie będzie to grupa ok. 1-2 mln osób).
5. I na koniec – koniecznie o realizacji internetowych potrzeb ludzi starszych powinni przede wszystkim decydować oni sami, żeby nie byli traktowani jak dzieci. Oczywiście młodsi są potrzebni do nauczenia ich korzystania z tych nowych technologii.

I na tym można by zakończyć ten temat, gdybym nie napotkał w ostatnim czasie kilku przykładów cyfryzacji życia codziennego z potencjalnym wykluczaniem wielu obywateli w każdym wieku:

- W Brukseli, gdzie przyjeżdżają tysiące osób ze sprawami do Komisji Europejskiej, w metrze bilet można kupić tylko za odliczoną wartość. Maszyny nie wydają reszty i nikt nie chce w kioskach wymieniać euro na bilon, a stacji z czynną kasą coraz mniej. Miejscowi mogą sobie kupić specjalną kartę z drobnymi wartościami. A co mają zrobić przyjezdni?
- W Wiedniu z lotniska(to jest ważne!) jest szybki pociąg CAT do Centrum. Bilety można kupić tylko w automatach. Najtańszy bilet kosztuje 10 euro, ale też nie można za niego zapłacić wyższym nominałem, licząc na wydanie reszty. Tylko papierowe 10 euro lub bilonem. Kart zresztą również te automaty nie przyjmują. A proszę zgadnąć w jakich nominałach wypłacają pobliskie bankomaty?
- Na lotniskach już od pewnego czasu są automaty do samodzielnego check-in. Wielu stara się z nich skorzystać przy wydatnej pomocy obsługi. Jest to ułatwienie i odciążenie w jakimś stopniu obsługi lotniskowej. Ostatnio zaczęto więc w niektórych liniach przymuszać pasażerów do korzystania z tych automatów. Do automatów tworzą się więc kolejki. Problem w tym, że bagaż trzeba potem i tak nadać w stanowisku obsługi, stojąc po raz drugi w kolejce. Nie zawsze też ten automat akceptuje posiadane przez pasażera informacje o rezerwacji – szczególnie, gdy bilet był kupowany przez Internet (sic!). I wreszcie każda z linii ma nieco inne typy tych automatów, a więc ciągle trzeba się na nowo uczyć ich obsługi lub też z przyzwyczajenia popełnia się błędy. I tak trwa to dla pasażera dłużej, niż gdyby postał w kolejce do obsługi stanowiskowej.
- Aha, te systemy teleinformatyczne rezerwacji miejsc w samolotach automatycznie przydzielają miejsca, co powoduje, że potem rodzina musi się szukać po samolocie. Co prawda, bardziej zaawansowanej w obsłudze tych systemów udaje się wymusić na systemie miejsca koło siebie, ale zawsze jest to loteria. W mniejszych samolotach chodziło zapewne o równomierne rozłożenie ciężaru, ale w dużych, przy ponad 90% obłożeniu, wydaje się to celowym utrudnianiem życia pasażerom.
- Wiele się mówi o cenach Internetu, a Regulator siłowo wymusza jego obniżkę. A może by tak Europejski Regulator spojrzał na ceny dostępu do Internetu w hotelach? Najlepiej to sprawdzić w Brukseli po drugiej stronie ulicy, gdzie w hotelu mamy słaby dostęp za 20 euro za dobę, a w Hiltonie w Wiedniu

(cena za pokój 200 euro+) za 60 minut do wykorzystania w 24 godziny za 256 kbs liczą sobie 10 euro. Mam nadzieję, że czytelnicy mogą dorzucić podobne informacje, ale też może i te pozytywne, gdzie dobry dostęp do Internetu jest już w cenie pokoju.

Takie przykłady można mnożyć (czekam na przykłady od Czytelników). Wystarczy tylko uważnie i krytycznie przyglądać się temu, co nam się oferuje w ramach powszechnej cyfryzacji społeczeństwa. Warto jest też zbierać i nagłaśniać takie przykłady wykluczania pewnych grup obywateli z możliwości skorzystania z danej usługi, aby wreszcie ci, co projektują te automaty, zaczęli myśleć logiczniej i w pełnym spektrum potrzeb klientów.

I dlatego jestem przeciw e-wykluczeniu.

Dr inż. Wacław Iszkowski
- Waclaw@Iszkowski.pl

Zapraszamy do udziału

XVI FORUM INFORMATYKI W ADMINISTRACJI

CZAS NA USŁUGI E-ADMINISTRACJI - ROZWIĄZANIA TECHNOLOGICZNE, PRAWNE, ORGANIZACYJNE

13-14 kwietnia 2011 r., Mszczonów

Każda edycja Forum Informatyki w Administracji ma swój temat przewodni - tym razem są to usługi e-administracji. Wstępem do rozważań na ten temat będzie wykład Wiesława Paluszyńskiego, wiceprezesa PTI o nowym dowodzie osobistym, stanowiącym elektroniczny klucz do nowoczesnych usług administracji w najbliższej perspektywie.
Pierwszy dzień obrad będzie zakończony prezentacją tematu budzącego ogromne zainteresowanie i ożywioną dyskusję, czyli omówieniem zarządzania elektroniczną dokumentacją i rolą nowej instrukcji kancelaryjnej. Zwieńczeniem dnia będzie recital Piotra Bałtroczyk, którego nie trzeba specjalnie reklamować.
Drugi dzień to przede wszystkim fundamentalny wykład prof. Grażyny Szpor, stanowiący w zasadzie vademecum dokumentu elektronicznego i jego różnorodnych uwarunkowań w e-administracji.
Ponadto program, jak zwykle, zawiera wystąpienia najbardziej znaczących postaci dla polskiej administracji: prof. Michała Kuleszy, dyrektora Departamentu Służby Cywilnej KPRM, Zastępcy Szefa Służby Cywilnej Dagmira Długosza, dyrektora CPI dra Zbigniewa Olejniczka i dra Włodzimierza Marcińskiego. Program w ciekawy sposób uzupełniają starannie dobrane prezentacje firmowe wiodących w tym obszarze firm teleinformatycznych.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Debata nad kompleksową reformą ochrony danych osobowych

Michał Czerniawski

Reforma ochrony prywatności była tematem ogólnopolskiej konferencji zorganizowanej w grudniu 2010 roku przez Uniwersytet Kardynała Stefana Wyszyńskiego, Generalnego Inspektora Ochrony Danych Osobowych i Naukowe Centrum Prawno-Informatyczne w Warszawie. W przededniu obrad plenarnych odbyła się ekspercka debata nad zmianami unijnych i polskich przepisów z zakresu ochrony danych osobowych. W panelowej dyskusji wzięło udział wielu wybitnych specjalistów w dziedzinie ochrony danych osobowych tak przedstawicieli nauki, jak i praktyków. Punktem wyjścia dla dyskusji był Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej" (KOM(2010) 609). W trakcie debaty skoncentrowano się na zagadnieniach zgody na przetwarzanie danych osobowych, roli administratorów bezpieczeństwa informacji, retencji danych telekomunikacyjnych, prawa do bycia zapomnianym i autonomii informacyjnej. Zasygnalizowano także wiele innych problemów. Owocem konferencji było przygotowanie uwag do strategii poprawy skuteczności unijnych przepisów dotyczących ochrony danych osobowych, przesłanych następnie przez Naukowe Centrum Prawno-Informatyczne do Komisji Europejskiej. Poniższy tekst prezentuje uporządkowane tematycznie stanowiska uczestników debaty.

Zgoda na przetwarzanie danych osobowych

Dr Wojciech Wiewiórowski

Niezwykle istotne jest, aby zgoda na przetwarzanie danych osobowych była udzielana – w sytuacjach, w których jest ona potrzebna – świadomie i dobrowolnie. Powoływanie się przez administratora danych na zgodę osoby, której dane dotyczą, powinno następować tylko wtedy, gdy zgoda jest w pełni dobrowolna, przy czym „dobrowolność" zgody może mieć miejsce tylko w przypadku istnienia rynku konkurencyjnego. W sytuacji, w której konkretna osoba nie ma realnego wyboru odnośnie udzielenia bądź nieudzielenia zgody na przetwarzanie danych osobowych, np. jest ona potrzebna do realizacji zadania publicznego, mamy *de facto* do czynienia z przymusem, a nie dobrowolną zgodą.

Innym zagadnieniem wartym zasygnalizowania jest kwestia zgody na przetwarzanie danych osobowych osoby małoletniej. Nie ma aktualnie w Unii Europejskiej regulacji ujednolicającej wiek, do którego jest się osobą małoletnią. Powyższy problem nabiera coraz większego znaczenia m.in. dlatego, iż aktualnie znaczącą grupę użytkowników Internetu, którzy wyrażają zgody na przetwarzanie swoich danych osobowych *online*, stanowią osoby małoletnie.

Dr hab. Paweł Fajgielski

Należy podkreślić, iż zgoda na przetwarzanie danych osobowych musi być zgodą osoby poinformowanej, posiadającej wiedzę o tym, co będzie się z jej danymi dziać. Często zdarza się, iż sposób przedstawienia

informacji dotyczących przetwarzania danych uniemożliwia odpowiednie zapoznanie się z nimi przez osobę, której dane dotyczą np. poprzez objętość dokumentu czy też konstrukcję strony internetowej. Wypracowanie wspólnych rozwiązań w tej materii może być aktualnie utrudnione, gdyż wymogi dotyczące zgody na przetwarzanie danych osobowych w poszczególnych państwach członkowskich Unii Europejskiej są bardzo zróżnicowane.

Mecenas Xawery Konarski

Z całą pewnością doprecyzowania w dyrektywie wymaga zagadnienie udzielania zgody na przetwarzanie danych osobowych przez kogoś innego niż podmiot danych osobowych. Jak wiadomo, zgodnie z obecnym stanem prawnym wspomniana zgoda może być udzielana nie tylko przez podmiot danych, ale także przez osobę trzecią. Taki sposób udzielania zgody nabiera coraz większego znaczenia: istnieją sytuacje, np. w sprawach pracowniczych, w których możliwość wyrażenia zgody na przetwarzanie danych przez osobę trzecią może mieć niezwykle istotne znaczenie.

Dyrektor Departamentu Orzecznictwa, Legislacji i Skarg w Biurze GIODO Monika Krasińska

Warto zauważyć, iż możliwość uzyskania przez osobę, której dane dotyczą, podstawowych informacji dotyczących przetwarzania jej danych osobowych jest istotna także dlatego, iż prawo złożenia sprzeciwu co do procesu przetwarzania jej danych osobowych, o którym nie ma ona pojęcia, jest *de facto* iluzją.

Prof. UKSW dr hab. Grażyna Szpor

Należy poświęcić uwagę także kwestii trudności z wycofaniem zgody na przetwarzanie danych osobowych. Formalności, które należy spełnić, aby zgodę wycofać, nie powinny być rażąco bardziej skomplikowane niż formalności niezbędne do tego, aby zgodę na przetwarzanie danych osobowych wyrazić.

Dr Arwid Mednis

Istotne jest, aby dyrektywa jednoznacznie przesądzała kwestię odwoływalności zgody na przetwarzanie danych osobowych, a także warunki (czas załatwienia sprawy, koszty) i skutki odwołania zgody (obowiązek zaprzestania przetwarzania danych dla celów objętych zgodą).

Administratorzy Bezpieczeństwa Informacji

Dr Paweł Litwiński

Dyrektywa powinna wzmocnić pozycję Administratora Bezpieczeństwa Informacji. ABI powinien być instytucją obowiązkową, a jego obecność mogłaby dawać administratorowi danych pewne specjalne uprawnienia, np. pozwalać na rezygnację z obowiązku rejestracji zbiorów danych zwykłych czy też dawać możliwości scedowania na ABI procedury uprzedniej kontroli przy rejestracji zbiorów danych drażliwych.

Dr Grzegorz Sibiga

Należy oddzielić urzędnika do spraw ochrony danych osobowych od procedury notyfikacji. Obecnie wspomniany urzędnik jest niejako „przypisany" do procedury notyfikacji i do procedury kontroli wstępnej. Wydaje się, iż należałoby stworzyć samodzielną regulację prawną dla ww. urzędnika. Regulacja tego typu doprowadziłaby do wzmocnienia efektywności kontroli przestrzegania przepisów o ochronie danych osobowych. Obecnie organy krajowe nie są w stanie skontrolować w całości tego, w jaki sposób przetwarzane są dane osobowe. Ponadto należy zagwarantować wspomnianemu urzędnikowi niezależność od administratora danych osobowych.

Dr Arwid Mednis

Pozycja urzędnika do spraw ochrony danych osobowych powinna zdecydowanie ulec wzmocnieniu. Dyrektywa powinna przewidywać obowiązek jego powołania, a także podstawowe kompetencje. Powołanie urzędnika mogłoby wiązać się z przejęciem przez niego niektórych kompetencji organu ochrony danych, a tym samym ograniczeniem niektórych obowiązków administratora wobec organu ochrony danych. Warto rozważyć rozwiązanie, zgodnie z którym urzędnik prowadziłby rejestr danych zwykłych, a notyfikacja do organu ochrony danych osobowych dotyczyłaby wyłącznie danych sensytywnych. Jednocześnie status urzędnika powinien mu gwarantować niezależność od administratora danych.

Retencja danych telekomunikacyjnych

Prof. dr hab. Andrzej Adamski

Traktat Lizboński przewiduje jednolity tryb legislacji w postaci dyrektyw, znosząc dotychczasowe ograniczenia, które wynikały z trójfilarowej struktury Unii Europejskiej. Należy podkreślić, iż poprawiona dyrektywa ramowa dotycząca retencji danych telekomunikacyjnych powinna być bardziej kompleksowa i regulować nie tylko zachowania operatorów telekomunikacyjnych, tj. dostawców usług świadczonych publicznie, ale także zachowania „konsumentów" tych danych: organów ścigania i wymiaru sprawiedliwości. Krokiem w dobrą stronę byłoby dodanie do grupy podmiotów, których zachowania są regulowane, także służb specjalnych.

Ponadto w znowelizowanej dyrektywie konieczne jest określenie pewnych zasad wynikających głównie z orzecznictwa Europejskiego Trybunału Praw Człowieka, dotyczących ochrony praw i wolności obywatelskich. Zasady te byłyby przeciwwagą dla naruszeń wyżej wymienionych praw i wolności koniecznych ze względu na interes państwa oraz wymiar sprawiedliwości, np. naruszeń związanych z udostępnianiem danych telekomunikacyjnych na potrzeby prowadzenia dochodzeń w sprawach dotyczących poważnych przestępstw. Niezwykle istotna jest także kwestia tzw. autonomii informacyjnej – obywatel w każdym wypadku powinien zostać poinformowany, iż jego dane były/są przetwarzanie.

Redaktor Piotr Waglowski

Należy podkreślić, iż retencja danych nie powinna być dokonywana na koszt przedsiębiorcy. Dobrym pomysłem wydaje się być wprowadzenie opłaty od rekordu dotyczącego konkretnej osoby, a udostępnianego przez przedsiębiorcę odpowiednim organom/służbom na podstawie przepisów prawa. Byłby to swoisty „filtr ekonomiczny", racjonalizujący korzystanie przez odpowiednie służby/organy z przechowywanych przez przedsiębiorców danych.

Katarzyna Szymielewicz

Konieczne jest poddanie działalności organów egzekwowania prawa i wymiaru sprawiedliwości tym samym zasadom ochrony danych osobowych i prywatności w ogóle. Na tym tle na szczególną uwagę zasługuje problem blankietowej retencji danych – instrumentu, który stanowi najbardziej inwazyjny środek inwigilacji społeczeństwa w prawie europejskim. Obecnie istniejące przepisy w zakresie retencji danych (Dyrektywa 2006/24/WE) nakładają na państwa obowiązek retencji danych telekomunikacyjnych, a jednocześnie nie określają granic, które gwarantowałyby poszanowanie podstawowych praw jednostki.

Dlatego niezbędne są daleko idące zmiany w Dyrektywie, przede wszystkim:

- skrócenie maksymalnego okresu zatrzymywania danych do przedziału między 3 a 6 miesięcy, w zależności od rodzaju danych,
- ograniczenie zakresu gromadzonych danych do informacji, które są standardowo zbierane przez operatorów telekomunikacyjnych na potrzeby komercyjne,
- określenie ścisłych reguł dostępu do zatrzymywanych danych, przy zapewnieniu kontroli sędziego lub prokuratora,
- ścisłe określenie celów, w których zatrzymywane dane mogą być wykorzystywane i ich ograniczenie do walki z najcięższymi przestępstwami (potrzebny jest przynajmniej ich zamknięty katalog).

Prawo do bycia zapomnianym

Prof. UKSW dr hab. Irena Lipowicz

Prawo osoby do spowodowania skutecznego i trwałego usunięcia jej danych osobowych nie jest obdarzane należytą uwagą. Brak mechanizmów kontrolowania daty „przydatności do spożycia" danych powoduje bezkarne wykorzystywanie danych od dawna niepotrzebnych do przetwarzania w zgodnych z prawem celach przez organy państwowe, pracodawców, podmioty gospodarcze.

Nawet w przypadku sprawców przestępstw dojrzałe systemy prawne przewidują zatarcie skazania, tymczasem nierozważny czyn lub wypowiedź młodej osoby mogą rzutować na jej życie zawodowe, prywatne czy np. karierę polityczną po 20-30 latach. Współczesna globalizacja przetwarzania i wielkie portale społecznościowe czynią niezbędnymi regulacje ponadnarodowe (w tym unijne) i są dowodem na internacjonalizację prawa administracyjnego.

Dr Arwid Mednis

Prawo do bycia zapomnianym, tj. prawo osoby do spowodowania usunięcia jej danych oraz zaprzestania ich przetwarzania, jeżeli przestały być potrzebne do zgodnych z prawem celów, powinno służyć osobom fizycznym w szczególności w przypadkach umieszczenia ich danych w sieci (np. na portalach społecznościowych).

W praktyce jednak regulacja prawna tego zagadnienia może okazać się trudna do sformułowania, jak również niemożliwa do wyegzekwowania. Być może należałoby rozważyć wprowadzenie przepisów zachęcających do poszukiwania rozwiązań technicznych pozwalających np. na określenie „daty ważności" informacji umieszczanych w sieci, a także zachęcających do edukacji o skutkach umieszczania danych w Internecie.

Prawo właściwe i jurysdykcja w zakresie ochrony danych osobowych. Przekazywanie danych osobowych

Dr Marek Świerczyński

W przypadku przetwarzania danych osobowych przez administratorów/procesorów z siedzibą w UE/EOG łącznikiem powinna być siedziba jednego z tych podmiotów. Powinna ona być rozumiana w sposób spójny z siedzibą usługodawcy w rozumieniu dyrektywy o handlu elektronicznym 2000/31/WE (zasada państwa pochodzenia). Powinno to zostać jednak (aby uniknąć „forum shopping") połączone z dalszą harmonizacją reguł dotyczących ochrony danych osobowych poprzez zastąpienie istniejącej dyrektywy rozporządzeniem. W przypadku przetwarzania danych osobowych poza UE/EOG kryterium lokalizacji danych nie powinno mieć znaczenia. Zasadne jest natomiast uwzględnienie kryterium nakierowania (również na podobieństwo propozycji dotyczących ochrony prywatności w kontekście reguł kolizyjnych ppm). Rozwiązaniem problemu ustalenia prawa właściwego dla administratorów/procesorów spoza UE/EOG byłby obowiązek (w przypadku powiązania działalności

obejmującej przetwarzanie danych osobowych z terenem UE/EOG) powołania przedstawiciela administratora na terenie UE/EOG (jako przykład takiej regulacji można podać tzw. przedstawiciela prawnego sponsora badań klinicznych pochodzącego spoza UE/EOG). W takim wypadku prawem właściwym dla ochrony danych osobowych byłoby prawo państwa, w którym znajduje się siedziba tego przedstawiciela. W przypadku, gdyby taki przedstawiciel nie został ustanowiony, konieczne jest przyjęcie innego „tymczasowego" łącznika. Łącznikiem takim musiałby być albo łącznik umiejscowienia środków technicznych (co nie jest najtrafniejszym rozwiązaniem), albo łącznik państwa, w związku z którym dane są przetwarzane (łącznik miejsca faktycznego prowadzenia działalności – np. prowadzenia sklepu internetowego nastawionego na sprzedaż na danym terytorium).

Dr Bogdan Fischer

Mimo wspólnych ram prawnych Unii Europejskiej można dostrzec brak dostatecznej harmonizacji przepisów o ochronie danych, obowiązujących w poszczególnych państwach członkowskich. Brakuje nadrzędnych instrumentów mających zastosowanie do wszystkich sektorów i wszystkich polityk UE, w szczególności nie wypracowano jednolitego standardu przechowywania danych. Jednocześnie coraz powszechniejsze staje się powierzanie przetwarzania danych podmiotom zewnętrznym, bardzo często spoza UE, m.in. w ramach *cloud computing*. Takie powierzanie rodzi pytania o prawo właściwe oraz o sposób rozwiązania problemów dotyczących ustalania związanej z przetwarzaniem odpowiedzialności. Powstaje także pytanie, czy w przypadku modelu *cloud computing* administrator rzeczywiście decyduje o celach i środkach przetwarzania, ponadto dyskusji wymaga kwestia, czy postęp techniczny nie zmusza nas do przedefiniowanie pojęcia administratora danych osobowych.

Dr Anna Sobaczewska

W komunikacie Komisji znaleźć można propozycje zmian regulacji zmierzających przede wszystkim w kierunku zwiększenia przejrzystości przetwarzania danych, wzmocnienia zasady minimalizacji danych, zwiększenia kontroli nad danymi oraz skuteczność sankcji – zwłaszcza kar kryminalnych. Kierunki te mogą wpłynąć na dalsze obciążanie administratorów obowiązkami administracyjnymi. Należy uwzględnić, że obciążanie obowiązkami administracyjnymi i ściślejszym nadzorem nad przetwarzaniem danych w warunkach rozwoju technik i metod pozyskiwania danych w celu prowadzenia działalności gospodarczej wydaje się chybionym pomysłem, gdyż może prowadzić między innymi do zmniejszenia konkurencyjności podmiotów z UE względem niezwiązanych omawianymi ograniczeniami konkurentów spoza Unii.

Mgr Michał Czerniawski

Aktualnie mamy do czynienia z szybko rosnącą skalą transgranicznego przekazywania danych osobowych. Mając na uwadze znaczącą liczbę państw niezapewniających odpowiednich gwarancji ochrony danych osobowych, znaczenia nabiera kwestia jak największego uproszczenia procedur legalizacji przekazywania danych. Z pomocą przychodzą tutaj narzędzia regulacji wewnętrznej (samoregulacji) podmiotów prywatnoprawnych działających na skalę międzynarodową, takie jak wiążące reguły korporacyjne (BCR) czy standardowe klauzule umowne, legalizujące wielokrotne przekazywanie danych osobowych. W celu spopularyzowania narzędzia samoregulacji, jakim jest BCR, konieczna jest unifikacja przepisów poszczególnych państw członkowskich pozwalająca na bezpośrednie stosowanie BCR w każdym państwie członkowskim Unii oraz rozszerzenie procedury wzajemnego uznawania na wszystkie państwa członkowskie UE.

Kompleksowa regulacja autonomii informacyjnej w sieci

Prof. UKSW dr hab. Grażyna Szpor

Podstawą dla wytyczania nowych celów kompleksowej ochrony danych osobowych w prawie europejskim powinna być pogłębiona refleksja nad nadchodzącą od wydania dyrektywy z 1995 roku ewolucją: wartości chronionych prawem europejskim, związanym z ochroną danych, celów regulacji ochrony danych i hierarchii tych celów, a także relacji między prawem do prywatności a prawem do ochrony danych osobowych. Istotą nowych zagrożeń jest ograniczenie autonomii informacyjnej jednostki związane z utratą kontroli nad przechowywanymi przez nią danymi, monitorowaniem jej zachowań, ich ujawnianiem oraz próbami sterowania tymi zachowaniami. Rozumienie informacji jako dobra zmniejszającego niepewność i autonomii informacyjnej jako samodecydowania o zmniejszaniu niepewności może być pomocne przy weryfikacji dotychczasowej siatki pojęciowej. Potrzebne jest kompleksowe ujęcie ograniczeń swobody przetwarzania danych osobowych przez różne kategorie podmiotów, w tym osoby fizyczne, a w szczególności spójna regulacja autonomii informacyjnej w Internecie.

Abstract

Privacy reform debate – report

The debate was held in Warsaw on December 15, 2010 and attracted many prominent lawyers. The discussion focused on the new challenges for personal data protection both in Poland and within the European Union. During the debate among other things the following issues were raised:

- consent of a data subject,
- data retention,
- right 'to be forgotten'.

As the conference's outcome a contribution to the EU consultation on the Commission's comprehensive approach on personal data protection was submitted. The report summarizes statements of the debate's participants.

Michał Czerniawski - LL.M. (Law & Technology), doktorant Wydziału Prawa i Administracji Uniwersytetu Warszawskiego.

Polecamy

SEMINARIUM

FUNKCJONALNOŚĆ I EFEKTYWNOŚĆ SYSTEMÓW BILINGOWYCH W ENERGETYCE, TELEFONII, CIEPŁOWNICTWIE, WODOCIĄGACH

24 maja 2011 r., Warszawa

W programie:

- Optymalizacja modeli funkcjonalnych systemów bilingowych.
- Biling a smart metering.
- Jak ograniczyć koszty działalności operatora?
- Czy można ufać bilingom?
- System bilingowy Sara - niezawodny partner w dobie liberalizacji rynku usług masowych.
- Aspekty prawne bilingu w branży Utilities.
- Ryzyka związane z funkcjonowaniem systemów bilingowych i funkcja Revenue Assurance.
- Innowacje teleinformatyczne w branżach sieciowych - nowe usługi dla odbiorców, producentów i operatorów (energii, gazu, wody, etc.).

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Ochrona materiałów nieobjętych prawem autorskim

Bohdan Widła

Stwierdzenie o wszechobecności prawa autorskiego i rosnącym jego znaczeniu we współczesnym społeczeństwie, gospodarce i kulturze stało się truizmem. Można jednak odnieść wrażenie, że rosnąca świadomość znaczenia prawa autorskiego i innych praw na dobrach niematerialnych niekoniecznie pociąga za sobą wiedzę o tym, co i w jakich przypadkach może podlegać ochronie. Z jednej strony często nie dostrzega się, że swobodne korzystanie, w tym kopiowanie, jakichś materiałów nie jest dozwolone z uwagi na ograniczenia wynikające z prawa autorskiego. Z drugiej strony nierzadko prezentowane są poglądy, w myśl których prawa autorskie przysługują do wytworów, które nie są lub z definicji nie mogą być nimi chronione. Tymczasem prawo autorskie nie jest jedynym instrumentem pozwalającym na ochronę tak zwanej własności intelektualnej. Niekiedy jednak fałszywe przekonanie, że dany materiał jest utworem w rozumieniu prawa autorskiego, utrudnia lub wręcz uniemożliwia sięgnięcie po „właściwe" dla niego instrumenty ochrony. Celem artykułu jest sygnalizacja problemów związanych z granicami ochrony prawnoautorskiej i potencjalnymi alternatywami dla tej konstrukcji.

Co nie podlega ochronie prawnoautorskiej?

Zagadnienia pojęcia utworu i granic ochrony prawnoautorskiej należą do najbardziej spornych w literaturze i orzecznictwie. Spory te są nieuniknione wobec ustawowej definicji utworu, zgodnie z którą jest to „każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia". Twierdzi się, że skoro może być to „każdy" przejaw i w „jakiejkolwiek" postaci, definicję utworu należy rozumieć szeroko, tak aby objąć nią jak najwięcej wytworów działalności człowieka. Mniejsze znaczenie przypisuje się najbardziej spornej przesłance istnienia utworu, czyli „twórczości". Podejście takie jest widoczne w orzecznictwie. Przypadki takie jak przyznanie ochrony prawnoautorskiej zapachowi perfum przez sąd w Holandii[1], uznanie przez Sąd Okręgowy w Tarnowie trasy biegu półmaratońskiego za utwór[2] albo stwierdzenie, że na ochronę zasługuje tytuł artykułu prasowego taki jak *Music makes school cool*[3], mogą skłaniać do uznania, że prawo autorskie rzeczywiście „jest wszędzie". Przeciwko takiemu wnioskowi przemawia jednak brzmienie kolejnego przepisu ustawy o prawie autorskim i prawach pokrewnych.

Art. 1 ust. 2[1] pr. aut. stwierdza, że „objęty może być wyłącznie sposób wyrażenia; nie są objęte ochroną odkrycia, idee, procedury, metody i zasady działania oraz koncepcje matematyczne". Przepis ten jednoznacznie wprowadza do polskiego prawa zasadę obowiązującą właściwie we wszystkich modelach prawa autorskiego, czyli rozróżnienie pomiędzy ideą a sposobem

1 Wyrok holenderskiego Sądu Najwyższego z 16 czerwca 2006 r., LJN AU 8940, C04/372HR.
2 M. Więcek, *Czy to oznacza, że w Bochni nie będzie już Biegu Niepodległości?*, „Polska Gazeta Krakowska" z 4 stycznia 2008 r.
3 Wyrok Sądu Pierwszej Instancji w Brukseli z 13 lutego 2007 r. w sprawie Copiepresse et al. v Google.

wyrażenia (ang. *idea-expression dichotomy*). Identyczna zasada obowiązuje w przypadku programów komputerowych. Zgodnie z art. 74 ust. 2 pr. aut. „idee i zasady będące podstawą jakiegokolwiek elementu programu komputerowego, w tym podstawą łączy, nie podlegają ochronie".

Co to oznacza w praktyce? Przede wszystkim, mimo że niejednokrotnie to pomysł jest wart miliony, a kartka papieru, na której został omówiony, jest bezwartościowa, prawa autorskie mogą przysługiwać jedynie do treści opisu[4]. W efekcie, powołując się na prawo autorskie, nie można zakazać innemu podmiotowi zarządzania projektem zgodnie z określoną metodyką. Można natomiast zakazać kopiowania podręcznika omawiającego procesy wchodzące w jej skład. Podobnie, o ile program komputerowy wykorzystujący pewien algorytm podlega ochronie, to sam algorytm nie podlega prawu autorskiemu. Powołując się na powyższą zasadę, można też wytoczyć poważne argumenty przeciwko poglądom, według których ochronie prawnoautorskiej podlega np. konfiguracja oprogramowania komputerowego (rozumiana jako zestaw procedur albo „klasyczny" plik konfiguracyjny). Wreszcie, prawa autorskie nie przysługują do koncepcji biznesowych. Przykładowo, sam fakt, że ktoś jako pierwszy wymyśli rewolucyjny portal społecznościowy, nie oznacza jeszcze, że jeśli inna osoba uruchomi taki portal i odniesie sukces, pomysłodawcy należy się z tego tytułu odszkodowanie[5].

Ochrona na podstawie innych praw własności intelektualnej

Tam, gdzie o twórczości nie ma mowy, w grę wchodzą inne prawa wyłączne, czyli tzw. prawa własności intelektualnej. W branży informatycznej do rzadkości będą należały przypadki ochrony z tytułu praw pokrewnych, takich jak prawa artystów wykonawców czy prawa producentów fonogramów i wideogramów. Częściej można spotkać się z przypadkami ochrony z tytułu praw do baz danych[6] lub praw własności przemysłowej[7].

Nie ulega wątpliwości, że ochronie prawnoautorskiej nie mogą podlegać fakty. Są one odkrywane i postrzegane, ale nie tworzone, więc nie może być spełniona podstawowa przesłanka uznania ich za utwór. Prawo autorskie dopuszcza ochronę twórczego zestawienia niechronionych faktów, jednak takie przypadki należą do mniejszości – zestawienia funkcjonalne najczęściej są przygotowywane według oczywistych kryteriów. Częstsze są zatem sytuacje, w których zestawienie danych w określony sposób jest z góry narzucone, ale wymaga znacznych nakładów (klasyczny przykład to książka telefoniczna z układem alfabetycznym, ale można wyobrazić sobie ochronę z tego tytułu np. bazy

4 Rozróżnienie to bywa niedoceniane. Przykładowo, w konkursie Urzędu Patentowego RP na plakat z dziedziny prawa własności intelektualnej, ogłoszonym w 2010 r., jedna z nagrodzonych prac zawierała hasło „Nie kradnij pomysłów!".

5 Nie przeszkodziło to w zawarciu wielomilionowej ugody w głośnej sprawie braci Winkelvoss przeciwko Markowi Zuckerbergowi, założycielowi portalu Facebook. Do ostrych krytyków tego zjawiska należy Lawrence Lessig, który stwierdził: „*...jakikolwiek system prawny, który pozwoliłby tym dzieciakom na wymuszenie 65 milionów dolarów z firmy, która odniosła największy sukces w tym stuleciu, powinien się wstydzić" (*L. Lessig, *Sorkin vs. Zuckerberg,* The New Republic, http://www.tnr.com/print/article/books-and-arts/78081/sorkin-zuckerberg-the-social-network).

6 Tzw. prawa *sui generis* wynikające z ustawy z 27 lipca 2001 r. o ochronie baz danych.

7 Wynikające z ustawy z 30 czerwca 2000 r. – Prawo własności przemysłowej i szeregu aktów prawa unijnego i międzynarodowego.

danych konfiguracyjnych urządzeń). Jeżeli podmiot finansujący takie działania wykaże, że poniósł istotne nakłady na przygotowanie bazy, może zakazać pobierania i wtórnego wykorzystywania zawartych w niej danych. W praktyce, ze względu na niejednoznaczność przepisów, częstym problemem jest ustalenie progu „istotności" nakładów.

Ciekawym zagadnieniem jest ochrona graficznego interfejsu użytkownika programu komputerowego (GUI). Przez kilkanaście ostatnich lat trwały zacięte spory, czy wobec daleko idącej standaryzacji można objąć je ochroną prawnoautorską[8]. Brak pewności skłonił niektórych do poszukiwania alternatywnej ścieżki, którą okazała się rejestracja elementów interfejsu jako wzorów przemysłowych. Prawo do wzoru przemysłowego, należące do tzw. praw własności przemysłowej, chroni dostrzegalną dla użytkownika postać produktu, jeżeli jest nowa (nie została wcześniej udostępniona publicznie) i ma indywidualny charakter (wywołuje na zorientowanym użytkowniku inne, ogólne wrażenie niż wcześniej upublicznione wzory). Tradycyjnie pojmowane prawo to dotyczy na przykład kształtu mebli, sztućców czy ubrań. Wśród zarejestrowanych wzorów można jednak znaleźć także nietwórcze w rozumieniu prawa autorskiego ikony będące elementami GUI. Uzyskanie prawa z rejestracji wzoru przemysłowego wymaga przejścia stosunkowo nieskomplikowanej procedury rejestracyjnej w Urzędzie Patentowym RP lub, dla wzorów wspólnotowych skutecznych na terytorium całej Unii Europejskiej, w Urzędzie ds. Harmonizacji Rynku Wewnętrznego. W przypadku wzorów przemysłowych uwidacznia się wspomniany na wstępie problem wynikający z błędnego uznania materiału za chroniony prawem autorskim. Jeżeli niebędący utworem produkt, który mógłby być chroniony jako wzór przemysłowy, zostanie udostępniony publicznie przed datą zgłoszenia do rejestracji, najprawdopodobniej uniemożliwi to skuteczną ochronę z powodu braku nowości.

Opisane wyżej prawa są o tyle podobne do praw autorskich, że opierają się na tym samym modelu, czyli przyznaniu konkretnemu podmiotowi wyłącznego prawa do eksploatacji ich przedmiotu w określonym zakresie. Prawo do baz danych ma jeszcze jedną wspólną cechę z prawem autorskim – jego powstanie nie wymaga wypełnienia dodatkowych formalności.

Ochrona na podstawie prawa konkurencji

W przypadkach, w których materiał, który ma być chroniony przed korzystaniem przez osoby trzecie, nie może być objęty prawem wyłącznym (nie jest utworem, chronioną bazą danych ani przedmiotem praw własności przemysłowej), ochrony można poszukiwać w przepisach ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Reguluje ona między innymi zasady ochrony tajemnicy przedsiębiorstwa, którą zgodnie z art. 11 ust. 4 u.z.n.k. są „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności".

8 Ostatnio wypowiedział się na ten temat Trybunał Sprawiedliwości UE w wyroku z 22 grudnia 2010 r., C-393/09, stwierdzając, że GUI może podlegać ochronie prawnoautorskiej, ale nie w ramach szczególnego reżimu przewidzianego dla programów komputerowych, lecz na ogólnych zasadach. Trudno stwierdzić, czy orzeczenie to zamknie spory, ponieważ w konkretnym przypadku i tak niezbędne będzie rozstrzygnięcie, czy elementy interfejsu są twórcze, czy zdeterminowane funkcją.

Warto tu podkreślić, że informacje objęte tajemnicą nie muszą być ani twórcze, ani nowe, ani niebanalne. Istotne jest po pierwsze, aby miały one wartość gospodarczą. Tym samym na gruncie prawa zwalczania nieuczciwej konkurencji można chronić zarówno wynalazki (możliwe lub niemożliwe do opatentowania), jak i informacje finansowe, strategię przedsiębiorstwa czy też metody i pomysły biznesowe. Po drugie konieczne jest podjęcie pozytywnych, rozsądnych działań ze strony przedsiębiorcy, zmierzających do zachowania poufności informacji. To, jakie działania powinny być podjęte w konkretnym przypadku, zależy od charakteru tajemnicy i od cech danej organizacji. W niektórych przypadkach wystarczy wyraźne oznaczenie poufnych dokumentów i ograniczenie dostępu do nich do zamkniętej grupy osób, związanych zasadami poufności. W innych konieczne może być stworzenie całego systemu zabezpieczeń, również o charakterze technicznym (np. szyfrowanie dysków). Po trzecie, co oczywiste, należy pamiętać, że publiczne ujawnienie informacji lub zaniechanie chronienia jej poufnego charakteru, także w mylnym przekonaniu, że jest ona chroniona prawem autorskim, może pociągać za sobą bezpowrotną utratę jej statusu jako tajemnicy przedsiębiorstwa[9].

Ochrona za pomocą zabezpieczeń technicznych

Tam, gdzie nie wchodzą w rachubę żadne prawa wyłączne ani ochrona tajemnicy przedsiębiorstwa, można skoncentrować się na zabezpieczeniach przed dostępem do chronionych informacji. Problematyka technicznych zabezpieczeń kojarzy się najczęściej ze zjawiskiem stosowania systemów Digital Rights Management i podobnych mechanizmów chroniących przed kopiowaniem, których zakaz przełamywania został uregulowany w prawie autorskim. Nie oznacza to jednak, że w przypadku zabezpieczenia dostępu do informacji nieobjętych prawem autorskim nie istnieją mechanizmy prawne zmierzające do ich zachowania. W przypadku systemów informatycznych w grę wchodzi zwłaszcza przepis art. 267 §2 kodeksu karnego, zgodnie z którym karze podlega ten, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Zgodnie z §4 tego przepisu karze podlega także ten, kto ujawnia informację uzyskaną po uzyskaniu dostępu do systemu bez uprawnienia. Sprawca ścigany jest na wniosek pokrzywdzonego. Odpowiedzialność karna wymaga oczywiście udowodnienia winy i umyślności działania. Warto jednak zwrócić uwagę na bardzo szerokie ujęcie czynu zabronionego[10]. Przede wszystkim odpowiedzialność nie jest uzależniona od przełamania jakichkolwiek zabezpieczeń.

Czy wszystko należy chronić?

Popularność prawa autorskiego jako środka zapewniającego wyłączność korzystania z różnego rodzaju materiałów nie powinna dziwić. Przyznaje ono szerokie prawa wyłączne, których powstanie nie jest uzależnione od dochowania żadnych formalności, a przesłanki uznania wytworu za twórczy są stosunkowo liberalne. Konstrukcje prawne, które mogłyby w konkretnych przypadkach bardziej przystawać do charakteru materiałów, wymagają natomiast dalej idących działań ze strony podmiotu poszukującego ochrony – przejścia procedury rejestracyjnej (prawa własności przemysłowej), podjęcia kroków dla utrzymania informacji w poufności (tajemnica przedsiębiorstwa), poniesienia

9 Zob. A. Michalak, *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne,* Kraków 2006, s. 132.

10 Wątpliwości może wywoływać także bardzo ogólne i niejasne sformułowanie przepisu. W praktyce ocena, czy „dostęp do systemu" był „uprawniony", jest trudna. Przepisy karne powinny być natomiast formułowane tak, aby nie było istotnych trudności w odróżnieniu zachowań karalnych od zachowań dozwolonych.

istotnych nakładów inwestycyjnych (prawa do baz danych) czy też kosztów uruchomienia zabezpieczeń technicznych.

Nie oznacza to jednak, że zawsze należy zmierzać do uzyskania jak najszerszej ochrony. Z jednej strony nie należy zapominać, że tzw. prawa własności intelektualnej funkcjonują nie tylko dla potrzeb ochrony partykularnych interesów, ale także w interesie publicznym[11]. Z drugiej strony czasami uzyskanie zbyt szerokiej ochrony byłoby szkodliwe dla samego uprawnionego. Przykładowo, gdyby zaakceptować pogląd, według którego utworem może być domena internetowa[12], oznaczałoby to paradoksalnie, że każda strona WWW zawierająca odsyłacz do tego adresu zwielokrotniałaby utwór bez zgody uprawnionego, co jest naruszeniem praw autorskich. Tymczasem „kreatywne" nazwy domen tworzone są nie po to, aby chować je przed publicznością, lecz aby jak najmocniej je rozpowszechniać.

Abstract

Protection of non-copyrightable materials

The vagueness of the definition of a copyrightable work has led to such court decisions as those which assume copyrightability of a short press headline. However, one should not forget about the fundamental principle of copyright law, which is the idea-expression dichotomy. This principle precludes the copyrightability of ideas. Non-copyrightable materials could be protected by other IP rights, such as database rights or design rights. The regulations regarding the protection of know-how could also be applicable. Last but not least, purely technological measures can be adopted.

Bohdan Widła - absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, prawnik w kancelarii Maruta i Wspólnicy sp. j., aplikant radcowski.

11 Najdobitniej zasada ta została wysłowiona w Konstytucji USA, zgodnie z którą Kongres może „popierać rozwój nauki i użytecznych umiejętności przez zapewnienie na określony czas autorom i wynalazcom wyłącznych praw do ich dzieł czy wynalazków".

12 Np. J. Błeszyński, *Domeny internetowe w świetle Prawa autorskiego*, w: A. Brzozowski, W. Kocot, K. Michałowska (red.), *W kierunku europeizacji prawa prywatnego. Księga pamiątkowa dedykowana Profesorowi Jerzemu Rajskiemu*, Warszawa 2007, s. 609-618.

Proponujemy

WARSZTATY
UMOWY NA USŁUGI I SYSTEMY IT - ASPEKTY PRAWNE I BIZNESOWE

Dowiedzą się Państwo:

- jak efektywnie przygotować specyfikację wymagań i kluczowe warunki umowy na wdrożenie systemu IT,
- jak prowadzić skuteczne negocjacje umowy na wdrożenie systemu IT,
- jak zapewnić sukces wdrożenia systemów IT,
- gdzie tkwią podstawowe zagrożenia biznesowe i prawne związane z wdrożeniem i eksploatacją systemów IT oraz poznają Państwo sposoby ich unikania.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Dokumentacja medyczna a bezpieczeństwo danych

Marcin Kędzierski

Inicjatywy legislacyjne Ministerstwa Zdrowia, jakie w 2010 r. zostały podjęte w obszarze szeroko rozumianej informatyzacji, wskazują, iż podjęto próbę uspójnienia stosowanych rozwiązań prawnych z możliwymi do zastosowania rozwiązaniami technicznymi. Po opublikowaniu nowego rozporządzenia o dokumentacji medycznej można oczekiwać, iż od tego roku nastąpi przełom w stosowaniu elektronicznej dokumentacji medycznej. **Nowe rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania** (Dz. U. 2010 nr 252 poz. 1697) wydane na podstawie art. 30 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417 i Nr 76, poz. 641 oraz z 2010 r. Nr 96, poz. 620) określa zasady prowadzenia dokumentacji medycznej, w tym również dokumentacji medycznej prowadzonej w postaci elektronicznej. Prowadzenie dokumentacji medycznej w postaci elektronicznej jest możliwe od kilku lat, a poprzez wyraźne korzyści jej stosowania zyskuje ona coraz szerszą rzeszę sympatyków. Dotychczasowe wymagania dotyczące konieczności stosowania bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu oraz konieczność stosowania znaczników czasu były główną przeszkodą szerszego stosowania i popularyzacji elektronicznej dokumentacji medycznej. Placówki udzielające świadczeń zdrowotnych zmuszone do prowadzenia dokumentacji medycznej sygnalizowały Ministerstwu Zdrowia, iż narzucone rozwiązania są często nie do przyjęcia, głównie ze względów finansowych. Wychodząc naprzeciw oczekiwaniom środowiska medycznego, w nowym rozporządzeniu o dokumentacji medycznej zastosowano zapisy mające na celu odejście od kwalifikowanych podpisów i przerzuceniu wymagań z zakresu bezpieczeństwa i niepodważalności wpisów na niezbędne funkcjonalności systemu używanego do prowadzenia i archiwizacji dokumentacji pacjenta. Nowa regulacja[1] doprecyzowuje minimalne wymagania funkcjonalne dla systemu teleinformatycznego stosowanego do prowadzenia dokumentacji medycznej, zgodnie z którym system powinien zapewniać:

- zabezpieczenie dokumentacji przed uszkodzeniem lub utratą;
- zachowanie integralności i wiarygodności dokumentacji;
- stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;
- identyfikację osoby udzielającej świadczeń zdrowotnych i rejestrowanych przez nią zmian, w szczególności dla odpowiednich rodzajów dokumentacji przyporządkowanie cech informacyjnych zgodnie z §10 ust. 1 pkt 3 lit. a-d;
- udostępnienie, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu, w formacie XML i PDF;

1 §80 ww. rozporządzenia

- eksport całości danych w formacie XML, w sposób zapewniający możliwość odtworzenia tej dokumentacji w innym systemie teleinformatycznym;
- wydrukowanie dokumentacji w formach określonych w rozporządzeniu.

Ważnym elementem nowych regulacji dotyczącym miejsca przechowywania dokumentacji jest umożliwienie korzystania z usług outsourcingu. Dotychczasowe zapisy określały, *iż dokumentacja wewnętrzna musiała być przechowywana w zakładzie, który ją sporządził.* Zgodnie z nowymi przepisami (§72.1.) *dokumentacja wewnętrzna jest przechowywana przez podmiot, który ją sporządził.* Jest to dość istotna zmiana, zważywszy na wymóg przechowywania przez podmioty dokumentacji medycznej przez okres 20 lat. Ma to szczególne znaczenie w przypadku bardzo dużych podmiotów, udzielających świadczeń zdrowotnych, w wyniku których tworzona jest czasami znaczna ilość dokumentacji medycznej. Poza korzyściami dla podmiotów bazujących jeszcze na dokumentacji w postaci papierowej (zwolnienie zajętych pomieszczeń) widoczne będą korzyści wynikające z możliwości korzystania z usług outsourcingu w przypadku dokumentacji medycznej prowadzonej w postaci elektronicznej. Umożliwienie korzystania z usług dostarczanych przez podmioty zajmujące się profesjonalną archiwizacją danych, zapewniającymi najwyższy poziom bezpieczeństwa dostępu do przechowywanych danych to krok w przyszłość.

Wraz z rozwojem nowych technologii pojawiają się często nowe możliwości podejścia do archiwizacji danych. To kolejny obszar działalności, gdzie usługi zewnętrzne mogą przynieść znaczne oszczędności. Standardowe metody archiwizacji to sposoby ręczne i półautomatyczne, wymagające nakładów czasu i odpowiednich zasobów - przy archiwizacji lokalnej to określone koszty zakupu bądź unowocześnienia sprzętu (rosnąca ilość danych podlegających archiwizacji w określonym czasie wymusi rozbudowę infrastruktury) oraz koszty utrzymania, w tym również zapewnienie bezpiecznego miejsca na składowanie nośników z danymi. Wiąże się to z potrzebą poniesienia kolejnych kosztów - przystosowania archiwum oraz zapewnienia odpowiedniej ochrony (systemy alarmowe, zatrudnienie pracowników ochrony). Kto wie, być może w niedalekiej przyszłości będzie to krok w stronę tak popularnych dzisiaj rozwiązań z zakresu oferowanych usług cloud computing[2].

Z uwagi na konieczność zachowania zgodności rozwiązań prawnych i informatycznych zadbano, aby przedmiotowa regulacja była spójna z zapisami projektu ustawy o systemie informacji w ochronie zdrowia, która obecnie rozpatrywana jest przez Podkomisję Nadzwyczajną Komisji Zdrowia Sejmu RP. Przedmiotowe rozporządzenie definiuje poszczególne rodzaje dokumentacji, umożliwiając jej prowadzenie zarówno w postaci papierowej, jak i elektronicznej. Projekt ww. ustawy przewiduje, że o ile zakres i rodzaje dokumentacji medycznej pozostaną bez zmian, o tyle postać wyłącznie elektroniczna zostanie narzucona od dnia 1 sierpnia 2014 roku. Szczegółowe rozporządzenia wydane na podstawie art. 13 ww. ustawy określi dokładny format dokumentacji medycznej. Ze względu na planowane wprowadzenie w Polsce Elektronicznego Rekordu Pacjenta, którego informacyjnym elementem składowym będą częściowe informacje z elektronicznej dokumentacji medycznej pacjenta, działania podjęte przez Ministerstwo

2 Cloud computing (ang. przetwarzanie w chmurze) – model przetwarzania oparty na użytkowaniu usług dostarczonych przez organizacje zewnętrzne.

Zdrowia są całkowicie przemyślane i racjonalne. Jest to zadanie niełatwe i wymaga pogodzenia oczekiwania pacjentów, środowiska medycznego oraz dostawców rozwiązań IT na rynku medycznym.

Trudno sobie dzisiaj wyobrazić jakąkolwiek placówkę medyczną bez urządzeń komputerowych. Niestety, poza udogodnieniami w zakresie prowadzenia elektronicznej dokumentacji medycznej, obsługi ruchu pacjentów, obsługi profesjonalnej aparatury medycznej wykorzystanie rozwiązań teleinformatycznych niesie za sobą wiele zagrożeń. Bez właściwie zdefiniowanej polityki bezpieczeństwa w tym obszarze łatwo o wyciek/kradzież danych. Tam, gdzie pojawia się dostęp do Internetu, sprawa staje się jeszcze poważniejsza. Mimo iż powszechnie znane są podstawowe przepisy z zakresu ochrony danych osobowych[3], nie wszyscy mają pełną świadomość o powadze zagrożeń wynikających z przechowywania i przetwarzania danych medycznych. Polityka bezpieczeństwa w tym obszarze powinna obejmować możliwie najszersze spektrum bezpieczeństwa, w zależności od specyfiki działania podmiotu, rodzaju i zakresu danych przetwarzanych w systemach. Powinno się to odbywać m.in. przez dokładnie sprecyzowany i restrykcyjny dostęp użytkowników systemów tylko i wyłącznie w granicach uprawnień, jakie są im przypisane przez administratora w systemie. Rejestracja zachowań użytkowników, a także wykonanych przez nich operacji w systemie przy szczególnym uwzględnieniu pełnej niezaprzeczalności i rozliczalności operacji, jest jednym z podstawowych wymagań funkcjonalnych dla każdego nowoczesnego systemu teleinformatycznego. Wszędzie tam, gdzie ma miejsce przetwarzane danych osobowych, jest to konieczne.

Zarówno w szpitalach czy w indywidualnych lub grupowych praktykach lekarskich komputery mogą pełnić wszelakie funkcje - od najprostszych maszyn biurowych począwszy, na niezwykle skomplikowanym technicznie diagnostycznym sprzęcie medycznym skończywszy. Obserwując obecny postęp technologiczny, nie należy przypuszczać, aby tendencja ta miała się zmienić. Należy zatem uświadomić sobie, gdzie mogą wystąpić najczęstsze zagrożenia wycieku lub utraty danych. Przy wielu wykorzystywanych dzisiaj metodach ataków na systemy i bazy danych zwykły użytkownik może nie zauważyć wycieku danych. W dobie afery z portalem WikiLeaks wydaje się to wręcz bezdyskusyjne. Wiedza użytkowników o potencjalnych zagrożeniach, jakie najczęściej mogą prowadzić do wycieku danych, może ustrzec przed takimi ewentualnościami. Poniżej zostało wymienionych zaledwie kilka z nich:

- Niesprawny sprzęt komputerowy - zakupiony sprzęt może działać niestabilnie, często „zawieszając się" i powodując utratę wprowadzonych danych lub uniemożliwiając normalną pracę.
- Nielegalne oprogramowanie lub oprogramowanie z nieznanych źródeł może być przyczyną niestabilnej pracy sprzętu, może być wykorzystane jako oprogramowanie szpiegowskie typu spyweare służące do wykradania danych.
- Brak właściwego zabezpieczenia fizycznego pomieszczeń, w których znajdują się stacje robocze.
- Komputer, w którym przechowywane są dane osobowe, może być narażony na włamanie, kradzież danych lub całego komputera. Dlatego właściwy byłby dwustopniowy poziom bezpieczeństwa, od wykorzystywania indywidualnych kluczy

3 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.).

sprzętowych zaczynając, po logowanie w sieci jako niezaprzeczalny użytkownik kończąc.
- Dane przesyłane za pomocą publicznych mediów telekomunikacyjnych mogą być narażone na ich przechwycenie lub na ich podsłuch.
- Systemy komputerowe pracujące w sieci narażone są na włamania i ataki zewnętrzne oraz wewnętrzne. W przypadku zainfekowania szkodliwym oprogramowaniem jednego z komputerów działających w sieci poza ryzykiem wycieku danych może zostać z nich stworzony tzw. botnet.[4] Komputery wykorzystywane jako kontrolery aparatury medycznej mogą przechowywać część danych osobowych. Należy je zabezpieczać w taki sam sposób jak komputerowe stacje robocze. Potencjalne włamanie do takiego komputera spowoduje kradzież tych danych.
- Wszelkie dane przechowywane na wymienialnych nośnikach narażone są na kradzież całych nośników bądź ich skopiowanie.
- Brak aktualnych baz antywirusowych niesie za sobą szczególne zagrożenie bezpieczeństwa danych ze strony wszelkich wirusów komputerowych.

Sektor medyczny jest szczególnie narażony na różnego rodzaju ataki (np. hakerskie) i wycieki danych, ponieważ dane medyczne mają wymierną wartość rynkową. Dane o zdrowiu obywateli są wartościowe np. dla towarzystw ubezpieczeniowych, firm farmaceutycznych, zakładów pogrzebowych, konkurentów czy rywali politycznych. Informacje te potwierdzają badania przeprowadzone w krajach, w których podobne systemy informacji medycznej zaczęły funkcjonować kilka lat temu. I tak np. według raportu brytyjskiego Komisarza ds. Informacji (brytyjski odpowiednik polskiego GIODO) około 30% najpoważniejszych zgłoszeń związanych z naruszeniem standardów ochrony danych osobowych dotyczyło służby zdrowia. Przypomina to od razu jedną z głośniejszych afer wycieku danych medycznych, które miało miejsce w grudniu 2007 r. w Holandii. Gazeta Trouw poinformowała wtedy, że firmy ubezpieczeniowe ujawniły dane dotyczące zdrowia, danych adresowych i kontaktowych, a także numery ubezpieczeń społecznych swoich klientów. Nieograniczony dostęp do tych danych zyskali wszyscy lekarze i dentyści. Problem dotyczył medycznej bazy The Vecozo, z której w głównej mierze korzystają w Holandii lekarze pierwszej pomocy, chcąc zweryfikować uprawnienia leczonego Holendra do otrzymania świadczenia zdrowotnego. W bazie dostępne są wszystkie wspomniane informacje, a uprawnienia do jej przeglądania, mimo zabezpieczeń w postaci hasła i certyfikatu uwierzytelniającego, ma ponad 80 tysięcy osób. O wyciek wrażliwych informacji nie jest trudno, zwłaszcza że dostępne w bazie są także dane sławnych Holendrów - aktorów, muzyków czy polityków, które są atrakcyjne dla brukowców. Zwłaszcza jeśli znaleźć tam można informacje o przebytych chorobach i leczeniu. Poza tym, dane teleadresowe wraz z numerem ubezpieczenia mogą być wykorzystane przez cyberprzestępców.

Głównymi twórcami danych medycznych pacjentów są oczywiście lekarze. Obowiązek ochrony danych osobowych (w tym danych medycznych) reguluje art. 40 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2005 r. Nr 226, poz. 1943 z późn. zm.), zgodnie z którym

4 Botnet - grupa komputerów zainfekowanych złośliwym oprogramowaniem (np. robakiem), pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu. Kontrola ta pozwala na zdalne rozsyłanie np. spamu oraz inne ataki z użyciem zainfekowanych komputerów.

lekarz musi zachować w tajemnicy informacje uzyskane w związku z wykonywaniem zawodu, a dotyczące pacjenta. Ww. ustawa określa również przypadki, w których tajemnica lekarza nie obowiązuje, stanowiąc w art. 40 ust. 2, że przepisu o obowiązku zachowania tajemnicy nie stosuje się, gdy:

1) tak stanowią inne ustawy,
2) badanie lekarskie zostało przeprowadzone na żądanie uprawnionych, na podstawie odrębnych ustaw, organów i instytucji; wówczas lekarz jest obowiązany poinformować o stanie zdrowia pacjenta wyłącznie te organy i instytucje,
3) zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób,
4) pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy, po uprzednim poinformowaniu o niekorzystnych dla pacjenta skutkach jej ujawnienia,
5) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie, związanych z udzielaniem świadczeń zdrowotnych innemu lekarzowi lub uprawnionym osobom uczestniczącym w udzielaniu tych świadczeń,
6) jest to niezbędne do praktycznej nauki zawodów medycznych,
7) jest to niezbędne dla celów naukowych.

We wszystkich opisanych wyżej przypadkach ujawnienie tajemnicy może nastąpić wyłącznie w niezbędnym zakresie. Lekarz bez zgody pacjenta nie może podać do publicznej wiadomości danych umożliwiających jego identyfikację. Należy podkreślić, iż zgodnie z art. 40 ust. 2 pkt 1 ww. ustawy mamy do czynienia z wyłączeniem obowiązku zachowania tajemnicy w sytuacji, gdy tak stanowią inne ustawy. A zatem w przypadku obowiązywania w tym zakresie stosownych przepisów rangi ustawowej lekarz będzie zwolniony od obowiązku zachowania tajemnicy. Ustawodawcy przewidzieli jednak szereg wyłączeń i sytuacji, w których dane osobowe mogą być przetwarzane lub też mogą być udostępniane na zewnątrz. I tak np. kwestię udostępniania dokumentacji medycznej (będącej zbiorem danych osobowych i jednostkowych danych medycznych), w tym także firmom ubezpieczeniowym, reguluje art. 26 ust. 3 pkt 7 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.). Artykuł 26 ww. ustawy stanowi, że dokumentacja medyczna może być udostępniona pacjentowi, jego przedstawicielowi ustawowemu bądź osobie przez niego upoważnionej. Stąd wynika, że każdy, kto występuje do zakładu opieki zdrowotnej o dokumentację bądź informacje o stanie zdrowia pacjenta, musi legitymować się jego imiennym upoważnieniem w formie pisemnej. Dokumentację medyczną udostępnia się na podstawie decyzji kierownika zakładu opieki zdrowotnej z odpowiednim zastosowaniem przepisów art. 22 ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. Nr 124, poz. 1151 z późn. zm.). Przywołane przepisy stanowią, że zakład opieki zdrowotnej udostępnia dokumentację medyczną zakładom ubezpieczeń tylko i wyłącznie za zgodą pacjenta. Udostępnienie dokumentacji medycznej następuje w trybie zapewniającym zachowanie poufności i ochrony danych osobowych. Określone zostały minimalne wymagania dotyczące wniosku o udostępnienie dokumentacji przez zakład opieki zdrowotnej[5], a mianowicie wniosek o udostępnienie dokumentacji (a także każdej innej informacji o trybie i sposobie leczenia) musi zostać podpisany przez lekarza upoważnionego przez zakład ubezpieczeń. We wniosku firmy ubezpieczeniowej musi być zawarta informacja o posiadaniu przez firmę zgody ubezpieczonego, o którego dane firma ubezpieczeniowa występuje. Zgoda ta powinna

5 Art. 22 ustawy o działalności ubezpieczeniowej (Dz. U. Nr 124, poz. 1151 z późn. zm.).

dotyczyć udostępnienia informacji medycznej (dokumentacji medycznej i innych danych o przebiegu leczenia). W przypadku, gdy firmy ubezpieczeniowe nie stosują się do tej procedury, należy zwrócić wniosek bez udostępnienia dokumentacji.

Wniosek o przekazanie informacji powinien składać się z czterech głównych części i powinien zawierać:

1) dane zakładu ubezpieczeń,
2) podstawę prawną i zakres informacji,
3) dane pacjenta,
4) oświadczenie zakładu o posiadaniu pisemnej zgody zainteresowanego.

Należy podkreślić, iż zakład ubezpieczeń nie może wystąpić o dane dotyczące całej dokumentacji medycznej, lecz w każdym przypadku powinien określić zakres potrzebnej informacji.

Zakład opieki zdrowotnej lub lekarz mają obowiązek przekazać posiadane informacje o stanie zdrowia, o jakie zwrócił się do nich zakład ubezpieczeń, w terminie 14 dni od dnia otrzymania wystąpienia. Za udzielenie informacji pobiera się opłatę w wysokości ustalonej z zakładem ubezpieczeń, z uwzględnieniem kosztów poniesionych na wytworzenie, przekształcenie i udzielenie informacji. Udostępnienie informacji może nastąpić w dowolnej formie, zapewniającej poufność i ochronę danych osobowych. Informacje podpisuje osoba wykonująca zawód medyczny upoważniona przez ZOZ lub lekarza prowadzącego prywatną praktykę albo lekarz prowadzący osobiście prywatną praktykę. W przypadku wydania oryginałów dokumentacji medycznej w placówce należy pozostawić kopię lub pełny odpis wydanej dokumentacji, chyba że zwłoka w wydaniu dokumentacji mogłaby narazić pacjenta na szkodę. Odmowa wydania dokumentacji wymaga zachowania formy pisemnej oraz podania przyczyny.

Poruszone w artykule kwestie dokumentacji medycznej, danych w niej zawartych, szeregu obostrzeń prawnych związanych z jej udostępnianiem, jak również świadomości przeciwdziałania utracie danych wrażliwych mają na celu właściwe wykorzystanie elektronicznej dokumentacji medycznej. Należy pamiętać o korzyściach płynących ze stosowania nowych technologii w codziennym życiu prywatnym czy zawodowym. Zastosowanie narzędzi teleinformatycznych przy zachowaniu podstawowych zasad bezpieczeństwa znacznie usprawnia pracę i przyspiesza obieg informacji bez zbędnego ryzyka wycieku/utraty danych. Od głównych użytkowników tych narzędzi często zależy bezpieczeństwo innych osób. Pamiętajmy, że w nowoczesnym społeczeństwie wyznacznikiem dojrzałości społecznej jest wysoki poziom odpowiedzialności.

Streszczenie

Nowe rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. 2010 nr 252 poz. 1697) wydane na podstawie art. 30 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta określa zasady prowadzenia dokumentacji medycznej, w tym również dokumentacji medycznej prowadzonej w postaci elektronicznej. Nowa regulacja doprecyzowuje minimalne wymagania funkcjonalne dla systemu teleinformatycznego stosowanego do prowadzenia dokumentacji medycznej i w zasadzie umożliwia korzystanie z usług outsourcingu, jeśli chodzi o jej przechowywanie.

Marcin Kędzierski - zastępca Dyrektora Departamentu Organizacji Ochrony Zdrowia w Ministerstwie Zdrowia.

Skuteczne doręczenie elektronicznych dokumentów i oferty w postaci elektronicznej zamawiającemu będącemu podmiotem publicznym

Kinga Telecka

Ustawa z dnia 29 stycznia 2004 roku Prawo zamówień publicznych[1] pozwala na składanie w postępowaniu o udzielenie zamówienia publicznego ofert w postaci elektronicznej, o ile zamawiający wyrazi na to zgodę (art. 82 ust. 2). Rozporządzenie Prezesa Rady Ministrów z dnia 30 grudnia 2009 roku w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane[2], przewiduje możliwość składania przez wykonawców również elektronicznych dokumentów (par. 6 ust. 1).

Zarówno w odniesieniu do postaci elektronicznej oferty, jak i elektronicznych dokumentów, przepisy prawa zamówień publicznych wymagają, aby były one opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu. To jednak nie jedyne ograniczenie dotyczące elektronicznej wymiany oświadczeń i dokumentów pomiędzy wykonawcą i zamawiającym.

Definicja legalna „dokumentu elektronicznego"

Wskazać należy, że definicja dokumentu elektronicznego została zawarta w ustawie z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne[3]. Natomiast w prawie zamówień publicznych (par. 6 rozporządzenia w sprawie dokumentów) posłużono się pojęciem elektronicznego dokumentu jako alternatywy dla składania dokumentów w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez wykonawcę.

Odnosząc się do reguł wykładni językowej, stwierdzić można, że wskazane powyżej wyrażenia: „dokument elektroniczny" i „elektroniczny dokument" stanowią odrębne pojęcia, z których tylko pierwsze zostało zdefiniowane przez ustawodawcę. Argumentu pozwalającego przyjąć prawidłowość takiego stwierdzenia dostarcza reguła wykładni językowej, według której różnym zwrotom nie należy nadawać tego samego znaczenia[4]. W konsekwencji przyjąć należałoby, że wprowadzenie do treści rozporządzenia w sprawie dokumentów pojęcia elektronicznego dokumentu, a nie jak wymagałaby tego ustawa o informatyzacji – dokumentu elektronicznego, było celowym działaniem racjonalnego ustawodawcy. Brakowałoby tym samym podstaw do stosowania w procedurze zamówienia publicznego szczególnych regulacji prawnych, właściwych dla dokumentu elektronicznego.

Rozważyć jednak należy odmienną interpretację, dokonywaną w oparciu o przepisy Pzp i ustawy z dnia 23 kwietnia 1964 r. Kodeks

1 Dz. U. z 2010 r., Nr 113, poz. 759 z późn. zm., dalej w tekście: Pzp.
2 Dz. U. z 2009 r. Nr 226, poz. 1817, dalej w tekście: rozporządzenie w sprawie dokumentów
3 Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm., dalej w tekście: ustawa o informatyzacji.
4 L. Morawski, *Wstęp do prawoznawstwa,* Towarzystwo Naukowe Organizacji i Kierownictwa, Toruń 2002, s. 173-174.

cywilny[5]. Na mocy art. 14 Pzp do czynności w postępowaniu o udzielenie zamówienia publicznego, podejmowanych zarówno przez zamawiającego, jak i przez wykonawcę, mają zastosowanie przepisy KC. Zgodnie z art. 2 pkt 7a Pzp postępowanie o udzielenie zamówienia publicznego to postępowanie, które jest wszczynane w drodze publicznego ogłoszenia (lub przesłania zaproszenia do składania ofert, lub przesłania zaproszenia do negocjacji – w zależności od trybu udzielania zamówienia) w celu dokonania wyboru oferty wykonawcy, z którym zostanie zawarta umowa w sprawie zamówienia publicznego, a w przypadku zamówienia z wolnej ręki – wynegocjowania postanowień wskazanej umowy. Ani przepisy Pzp, ani KC nie stanowią podstawy do wyłączenia stosowania do czynności podejmowanych w postępowaniu o udzielenie zamówienia publicznego przepisów ustawy o informatyzacji wraz z aktami wykonawczymi, w tym rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 roku w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym[6].

Sposób doręczania elektronicznego dokumentu i oferty w postaci elektronicznej

Zgodnie z art. 1 pkt 6 ustawy o informatyzacji „ustawa określa zasady (...) wymiany informacji drogą elektroniczną, w tym dokumentów elektronicznych, pomiędzy podmiotami publicznymi a podmiotami niebędącymi podmiotami publicznymi". Biorąc pod uwagę definicję słownikową wyrazu „wymiana"[7], należy przyjąć, że ustawa o informatyzacji określa zasady komunikacji elektronicznej w obu kierunkach, zatem nie tylko od podmiotu publicznego do podmiotu niebędącego podmiotem publicznym.

W art. 16 ust. 1 ustawy o informatyzacji nałożono na każdy podmiot publiczny przetwarzający dane w systemie teleinformatycznym obowiązek zapewnienia możliwości przekazywania tych danych również w postaci elektronicznej, w formie dokumentów elektronicznych. Wymiana danych może dotyczyć dowolnej sprawy należącej do zakresu działania podmiotu publicznego. Nie została ona tym samym ograniczona jedynie do spraw należących do właściwości lub kompetencji podmiotu publicznego. Regulację warunków organizacyjno-technicznych wymiany dokumentów elektronicznych powierzono Prezesowi Rady Ministrów (art. 16 ust. 3 ustawy o informatyzacji).

Zgodnie z par. 2 ust. 1 rozporządzenia w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym informację w formie elektronicznej dostarcza się do podmiotu publicznego przy użyciu jego elektronicznej skrzynki podawczej, której adres został opublikowany w Biuletynie Informacji Publicznej (par. 5 ust. 2 pkt 1 lit. a), przy wykorzystaniu powszechnie dostępnej sieci teleinformatycznej. Zaznaczyć należy, że ustawodawca nie określił, iż podmiot publiczny jest obowiązany do posiadania tylko jednej elektronicznej skrzynki podawczej, ani też czy ma być ona dostępna dla nadawców pod adresem internetowym poczty elektronicznej, strony internetowej czy też innym, charakterystycznym dla wybranego środka komunikacji elektronicznej.

Uznanie interpretacji dopuszczającej zastosowanie przepisów ustawy o informatyzacji do wymiany informacji określonej

5 Dz. U. z 1964 r. Nr 16, poz. 93 z późn. zm., dalej w tekście: KC.
6 Dz. U. z 2005 r. Nr 200, poz. 1651.
7 Wymiana - danie komuś czegoś i otrzymanie czegoś od kogoś w zamian, zob. Słownik języka polskiego, Wydawnictwo Naukowe PWN SA, http://sjp.pwn.pl/szukaj/wymiana, 16.12.2010.

w prawie zamówień publicznych za prawidłową oznacza, że zamawiający powinien uznać każdy dokument elektroniczny dotyczący prowadzonego postępowania o udzielenie zamówienia publicznego, jeżeli został on dostarczony przy użyciu elektronicznej skrzynki podawczej, o ile zamawiający-podmiot publiczny zorganizował przetwarzanie danych związanych z zamówieniami publicznymi w systemie teleinformatycznym.

Ustawa o informatyzacji wprowadza definicję legalną systemu teleinformatycznego (art. 3 pkt 3) jako zespołu współpracujących ze sobą i podłączonych do sieci telekomunikacyjnej urządzeń informatycznych i oprogramowania zapewniającego w szczególności przetwarzanie i przechowywanie danych. Wskazać należy, że spełnienie tych wymagań jest proste. Tak zdefiniowany system teleinformatyczny stanowią już na przykład dwa komputery, pomiędzy którymi następuje wymiana informacji przy użyciu poczty elektronicznej o adresach dostępnych dla osób z zewnątrz organizacji. Trudno jest więc wyobrazić sobie podmiot publiczny, w odniesieniu do którego nie ma zastosowania art. 16 ustawy o informatyzacji.

Za prawidłowością interpretacji pozwalającej uznać, że rozporządzenie w sprawie dokumentów dotyczy dokumentów elektronicznych w rozumieniu ustawy o informatyzacji, może przemawiać zarówno niejednoznaczność przepisów prawa zamówień publicznych, jak również treść art. 36 ust. 2 pkt 5 Pzp. W przepisach prawa zamówień publicznych występuje brak spójności w odniesieniu do określania sposobu porozumiewania się zamawiającego z wykonawcami za pośrednictwem środków komunikacji elektronicznej. Art. 27 ust. 1 przewiduje elektroniczną drogę przekazywania oświadczeń, wniosków, zawiadomień i informacji. Art. 82 ust. 2 Pzp wskazuje na możliwość złożenia oferty w postaci elektronicznej. Dodatkowo rozporządzenie w sprawie dokumentów dopuszcza możliwość składania dokumentów w jednej z trzech form, w szczególności elektronicznego dokumentu.

Ponadto zgodnie z art. 36 ust. 2 pkt 5 Pzp zamawiający, który dopuszcza porozumiewanie się drogą elektroniczną, jest obowiązany podać w specyfikacji istotnych warunków zamówienia adres poczty elektronicznej lub strony internetowej. Tak sformułowany przepis, w odniesieniu do regulacji zawartej w ustawie o informatyzacji, pozwala przyjąć, że ustawodawca dopuszcza możliwość podania adresu właśnie elektronicznej skrzynki podawczej, która może być zrealizowana jako: konto poczty elektronicznej (na przykład Najwyższa Izba Kontroli[8]), formularz na stronie internetowej (na przykład Urząd Miasta Stołecznego Warszawy[9]) lub rozbudowany serwis WWW (na przykład Główny Urząd Statystyczny[10]).

Skuteczne doręczenie oferty

Zgodnie z art. 60 KC: „z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej". Na podstawie art. 62 KC oświadczenie woli, które jest wyrażone w postaci elektronicznej, przyjmuje się za złożone innej osobie z chwilą, gdy wprowadzono je do środka komunikacji elektronicznej w taki sposób, żeby osoba ta mogła zapoznać się z jego treścią.

8 http://www.nik.gov.pl/kontakt/elektroniczna-skrzynka-podawcza/, 15.12.2010
9 http://bip.warszawa.pl/Menu_przedmiotowe/eUrzad/default.htm, 15.12.2010
10 http://www.stat.gov.pl/gus/5525_PLK_HTML.htm, 15.12.2010

Przepisy KC nie wskazują dopuszczalnych technik komunikacji elektronicznej właściwych do składania oświadczeń woli. Przyjmuje się zatem, że oświadczenie woli może być przekazane w różny sposób, w szczególności przez Internet. Istotne jest natomiast, aby złożone oświadczenie było zrozumiałe.[11]

Na mocy art. 27 ust. 1 Pzp oświadczenia w postępowaniu o udzielenie zamówienia publicznego mogą być, za zgodą zamawiającego, przekazywane drogą elektroniczną. Oferta składana w postępowaniu dodatkowo wymaga opatrzenia bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu. Wskazać należy, że w przypadku złożenia oświadczenia drogą elektroniczną, zgodnie z normą zawartą w art. 27 ust. 2 Pzp, każda ze stron: zamawiający i wykonawca, na żądanie drugiej strony, niezwłocznie potwierdza fakt otrzymania oświadczenia.

Odnosząc powyższe rozważania do projektowanej regulacji dotyczącej w szczególności sporządzania pism w postaci elektronicznej i warunków doręczania dokumentów elektronicznych[12], stwierdzić można, że właściwym i pożądanym narzędziem służącym do składania oferty w postaci elektronicznej zamawiającemu będącemu podmiotem publicznym w rozumieniu ustawy o informatyzacji jest elektroniczna skrzynka podawcza.

Przede wszystkim wskazać należy, że zgodnie z projektowanymi zmianami, oprócz wzorów dokumentów elektronicznych, przewiduje się wprowadzenie ogólnego wzoru elektronicznego, który ma być przeznaczony do tworzenia pism w postaci elektronicznej w następujących sytuacjach, określonych w par. 9 projektu rozporządzenia, gdy:

- w przepisach odrębnych nie został wskazany organ właściwy do określenia wzoru,
- podmiot publiczny będący adresatem podania, żądania, wyjaśnienia lub innej czynności w postaci elektronicznej nie określił wzoru dokumentu elektronicznego, który umożliwiłby załatwienie danej sprawy w tym podmiocie,
- przepisy prawa nie wskazują jednoznacznie, że jedynym skutecznym sposobem przekazania informacji jest jej doręczenie na piśmie w postaci papierowej.

Wskazany ogólny wzór elektroniczny mógłby stanowić wzór wykorzystywany do składania oferty w postępowaniu o udzielenie zamówienia publicznego – formularza ofertowego. W obowiązujących przepisach prawa zamówień publicznych nie został wskazany organ właściwy do określenia stosownego wzoru. Brakuje wzorów określonych przez zamawiających – podmioty publiczne. Przepisy prawa zamówień publicznych nie wskazują jednoznacznie, że jedynym skutecznym sposobem przekazania informacji jest jej doręczenie na piśmie w postaci papierowej, wręcz przeciwnie dopuszczają możliwość złożenia oferty w postaci elektronicznej.

Elektroniczna skrzynka podawcza jest dostępnym publicznie środkiem komunikacji elektronicznej, który zgodnie z par. 19

11 R. Szostak, *Elektroniczne zamówienia publiczne,* w: D. Adamski, P. Litwiński, Cz. Martysz, Z. Okoń, G. Sibiga, R. Szostak, D. Szostek, M. Świerczyński, *E-administracja*. *Prawne zagadnienia informatyzacji administracji*, red. D. Szostek, Presscom Sp. z o.o., Wrocław 2010, s. 105-106.

12 Projekt rozporządzenia Prezesa Rady Ministrów z dnia … 2010 r. w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych, http://bip.mswia.gov.pl/portal/bip/200/19170/Projekt_rozporzadzenia_Rady_Ministrow_z_dnia__2010_r_w_sprawie_sporzadzania_pism.html, 06.12.2010

projektu rozporządzenia stanowi alternatywne rozwiązanie informatyczne służące do doręczania podmiotom publicznym dokumentów elektronicznych. Inny sposób przewiduje doręczenie dokumentu elektronicznego bezpośrednio na informatycznym nośniku danych.

Podkreślić należy, że elektroniczna skrzynka podawcza pozwala również zrealizować wymóg potwierdzania faktu otrzymania oświadczenia przez adresata, o którym mowa w art. 27 ust. 2 Pzp. Jest to możliwe poprzez automatycznie tworzone i udostępniane nadawcy dokumentu urzędowe poświadczenie odbioru.

Doręczenie zamawiającemu będącemu podmiotem publicznym oferty w postaci elektronicznej może jednak dostarczać dodatkowych, praktycznych trudności. Argument, jaki można podnieść przeciwko dopuszczalności składania oferty w postaci elektronicznej, dotyczy objętości pliku z ofertą. W przypadku złożonych postępowań o znaczącej wartości, przede wszystkim dotyczących robót budowlanych, oferta w postaci elektronicznej byłaby całkowicie niepraktyczna lub wymagałaby i tak wydrukowania. Ponadto istnieje ryzyko, że ograniczenia technologiczne standardowego zestawu do składania bezpiecznego podpisu elektronicznego, który przede wszystkim stanowi narzędzie do podpisywania pojedynczych oświadczeń woli o małej objętości, wpłyną niekorzystnie na jego wydajność, w konsekwencji uniemożliwiając złożenie podpisu pod dużym plikiem komputerowym.

Wnioski

Nadal są dokonywane zmiany w kierunku umożliwiającym informatyzację procedur udzielania zamówień publicznych. Jakkolwiek środki komunikacji elektronicznej w prawie zamówień publicznych nie stanowią nowości ani dla zamawiających, ani dla wykonawców, wątpliwości w odniesieniu do praktycznego zastosowania instrumentów elektronicznych przy udzielaniu zamówień jednak nie brakuje.

Streszczenie

Publikacja ma na celu wskazanie konsekwencji braku definicji legalnej elektronicznego dokumentu w przepisach prawa zamówień publicznych oraz uznania przepisów dotyczących informatyzacji działalności podmiotów realizujących zadania publiczne za obowiązujące w postępowaniu o udzielenie zamówienia. W artykule omówiono również zagadnienie skutecznego doręczenia elektronicznego dokumentu i oferty w postaci elektronicznej do zamawiającego będącego podmiotem publicznym. Pomimo iż środki komunikacji elektronicznej w prawie zamówień publicznych nie stanowią nowości, wątpliwości w odniesieniu do praktycznego zastosowania instrumentów elektronicznych przy udzielaniu zamówień nie brakuje.

Kinga Telecka – specjalista w zakresie zamówień publicznych w jednostce samorządu terytorialnego.

Zasada powszechności prawa do informacji publicznej

Dorota Fleszer

Warunkiem aktywnego uczestniczenia w życiu społecznym, politycznym czy też gospodarczym jest posiadanie przez osobę informacji. Szczególne znaczenie ma informacja obejmująca szeroko rozumianą wiedzę dotyczącą działalności władzy publicznej, czyli informacja publiczna. Rola, jaką ona pełni, jest nie do przecenienia. Dlatego też uświadamiając sobie wagę tego rodzaju informacji, osoby podejmują działania mające na celu jej uzyskanie. Również ustawodawca zdaje sobie sprawę ze znaczenia, jaką ma informacja o sprawach publicznych we współczesnym społeczeństwie. W związku z tym tworzy regulacje prawne gwarantujące szeroki do niej dostęp.

W niniejszym opracowaniu prezentuję najważniejsze problemy związane z ustaleniem kręgu podmiotów, które mogą realizować prawo do informacji publicznej. Analizę zagadnienia przeprowadzę w oparciu o powstałe w tej materii orzecznictwo oraz poglądy doktryny.

Komu przysługuje prawo do informacji publicznej

Ustrojodawca ukształtował prawo do informacji publicznej w taki sposób, że nadał mu charakter publicznego prawa podmiotowego, a zatem zapewnił obywatelowi możliwość skutecznego żądania od organów władzy publicznej określonego zachowania, które w wypadku zaistnienia takiej potrzeby jest egzekwowalne w drodze odpowiednich instytucji procesowych. [1]

Jak wynika z art. 61 ust. 1 ustawy z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej[2] - dalej Konstytucja - obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.

Z kolei na gruncie art. 2 ust. 1 ustawy z dnia 6 września 2001 r. o dostępnie do informacji publicznej[3] - dalej u.d.i.p. - prawo do informacji publicznej przysługuje każdemu.

Jak stwierdza NSA, *ratio legis* regulacji zawartej w art. 61 Konstytucji RP, a także w ustawie o dostępie do informacji

1 A. Niżnik-Mucha, *Problematyka zakresu przedmiotowego konstytucyjnego prawa do informacji publicznej,* „Casus" z 2008, lato, s. 15, T. R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej,* Wydawnictwo LexisNexis Warszawa 2008, s. 121, por. wyrok TK z 20.03.2006, 1630/3/A/2006, K 17/05 OTK-A z 2006 Nr 3 poz. 30

2 Dz. U. Nr 78 poz. 483 ze zm.

3 Dz. U. Nr 112, poz. 1198

publicznej, wynika z zasady udziału obywateli w życiu publicznym i sprawowania społecznej kontroli.[4]

Tym niemniej zestawienie zakresu podmiotowego przytoczonych przepisów pozwala na stwierdzenie rozbieżności. O ile na gruncie regulacji konstytucyjnych prawo do informacji przysługuje obywatelowi, to już według stosownego przepisu u.d.i.p. uprawnionym do jego realizacji jest „każdy". Inaczej rzecz ujmując, ustawodawca w regulacji art. 2 ust. 1 u.d.i.p. dokonał rozszerzenia, w porównaniu do art. 61 ust. 1 Konstytucji, kręgu podmiotów uprawnionych do informacji publicznej. A. Obrzut zauważa, że poszerzenie kręgu uprawnionych nastąpiło w stosunku nie tylko do art. 61 Konstytucji, ale także art. 11b ustawy o samorządzie gminnym, art. 8a ustawy o samorządzie powiatowym, art. 15a ustawy o samorządzie województwa, ponieważ zgodnie z nimi prawo dostępu do informacji przysługuje tylko obywatelom polskim, osobom fizycznym.[5]

Wobec powyższego powstaje wątpliwość co do zgodności analizowanego przepisu art. 2 ust. 1 u.d.i.p. z Konstytucją. W. Rygiel jest zdania, że regulacja art. 2 u.d.i.p. nie pozostaje w sprzeczności z postanowieniem art. 61 Konstytucji RP, który zawęża krąg osób, którym przysługuje prawo do informacji, do obywateli RP. U.d.i.p. stanowi bowiem rozszerzenie zakresu podmiotowego prawa do informacji, co w kontekście charakteru tego prawa, jego znaczenia oraz regulacji wspólnotowych należy uznać za dopuszczalne.[6] Również A. Piskorz-Ryń twierdzi, że jest dopuszczalne z konstytucyjnego punktu widzenia, bowiem ustawa zasadnicza zawiera pewien standard minimum, który może być rozszerzony w ustawodawstwie zwykłym.[7] Tezy sformułowane w doktrynie podzielane są w orzecznictwie. Według NSA przepis art. 2 ust. 1 wprowadza zasadę, że każdemu przysługuje prawo dostępu do informacji publicznej zwane „prawem do informacji publicznej". Przepis ten stanowi rozwinięcie treści zapisu art. 61 ust. 1 Konstytucji Rzeczypospolitej Polskiej. [8]

Cudzoziemiec ma prawo do informacji publicznej

Zdaniem Ewy Olejniczak-Szałowskiej zdecydowanie przeważa stanowisko, że Konstytucja nie stoi na przeszkodzie uznaniu, iż adresatem prawa do informacji nie jest wyłącznie obywatel polski. Autorka wskazuje, że zwolennicy tego poglądu powołują się na orzecznictwo Trybunału Konstytucyjnego ukształtowane na początku lat 90, na konieczność respektowania postanowień Powszechnej Deklaracji Praw Człowieka, Międzynarodowego Paktu Praw Obywatelskich i Politycznych, Europejskiej Konwencji Praw Człowieka. Na poparcie owego stanowiska można także przywołać normę zawartą w art. 37 Konstytucji: „kto znajduje się pod władzą Rzeczypospolitej Polskiej, korzysta z wolności i praw zapewnionych w Konstytucji, a wyjątki od

4 Wyrok NSA w Warszawie z 31.05.2004, OSK 205/04, niepubl.

5 A. Obrzut, *Prawo do informacji publicznej. Wybrane problemy.* w (red) S. Dolaty, *Problemy prawne w działalności samorządu terytorialnego,* Wydawnictwo Uniwersytetu Opolskiego, Opole 2002, s. 212

6 W. Rygiel, *Ty nam zgodę, my ci informację. Wzór wniosku z MSWiA: przed wypełnieniem spalić!,* „Rzeczpospolita" z dnia 24.07. 2003, nr 168

7 A. Piskorz-Ryń, *Dostęp do informacji publicznej. Komentarz do ustawy z 6 września 2001 r.*, „Wspólnota" 2001 r. Nr 43 z 27.10.2001, s.40

8 Wyrok NSA Ośrodek Zamiejscowy we Wrocławiu z 5.12.2002, II SA/Wr 1600/02, niepubl., wyrok NSA z 2.07.2003, II S.A. 837/03, niepubl.

tej zasady, odnoszące się do cudzoziemców, określa ustawa".[9] Tak samo twierdzą M. Jabłoński i K. Wygoda. Ich zdaniem odwołanie się przez ustrojodawcę do pojęcia obywatela mogłoby sugerować, że chodzi wyłącznie o prawo obywatela polskiego. Zapis ustawy wyraźnie jednak przeczy wykładni zawężającej, zgodnie z którą uprawnionym do realizacji prawa dostępu do informacji publicznej byłby wyłącznie obywatel polski.[10] E. Jędrzejewska-Siwik podkreśla, że z art. 2 u.d.i.p. nie wynika żaden obowiązek osoby korzystającej z prawa dostępu do informacji publicznej w zakresie wykazania swojego związku z Polską, jak w szczególności zamieszkanie, prowadzenie działalności gospodarczej na jej terytorium itd. Ze względu na przepis art. 13 Konstytucji RP podmioty te muszą jednak działać zgodnie z prawem.[11]

Odmienne stanowisko w tej kwestii reprezentuje A. Niżnik-Mucha. Według niej zakres podmiotowy konstytucyjnego prawa do informacji publicznej to art. 61 ust. 1 Konstytucji RP, który kształtuje owo prawo jako prawo obywatelskie. Podmiotem prawa do informacji publicznej pozostaje zatem „obywatel", a nie „każdy", co z jednej strony – biorąc pod uwagę m.in. obecne zagrożenia terrorystyczne - jest uzasadnione koniecznością zapewnienia bezpieczeństwa państwa, z drugiej jednak strony można zadać pytanie, czy w wypadku przyznania tego prawa „każdemu" ochrona bezpieczeństwa państwa nie byłaby zagwarantowana poprzez ograniczenie ustawowe tegoż prawa, tak jak ma to miejsce w odniesieniu do obywateli.[12] Podnosi się także argument, że „prawo do informacji publicznej to w istocie ‚narzędzie suwerena', dzięki któremu może on sprawować faktyczną kontrolę działalności szeroko rozumianej władzy publicznej. W związku z tym rozwiązanie konstytucyjne polegające na nieprzyznaniu tego prawa cudzoziemcom i bezpaństwowcom – jako podmiotom nieposiadającym uprawnień związanych ze sprawowaniem władzy – należy ocenić pozytywnie."[13]

Przychylam się do twierdzenia P. Szutakiewicza, z którego wynika, że całościowa analiza regulacji prawa do informacji publicznej prowadzi do wniosku, iż zakres podmiotów uprawnionych do żądania informacji publicznej jest zbyt szeroki, zważywszy, że przysługuje również podmiotom, na których sytuację nie wpływa w żaden sposób przejrzystość polskiej administracji, a zatem trudno wskazać *ratio legis* przyznania im wspomnianego prawa.[14]

M. Kłaczyński proponuje wprowadzenie zróżnicowania warunków realizacji prawa do informacji publicznej przez podmioty zagraniczne, przyznając je w pełnym zakresie, jak podmiotom polskim, cudzoziemcom zamieszkałym w Polsce, a od przystąpienia Polski do UE również obywatelom krajów członkowskich Wspólnot, osobom prawnym z siedzibą we wspomnianych krajach oraz obywatelom innych państw zamieszkałym w UE. Pozostałe podmioty zagraniczne (np. cudzoziemiec spoza UE zamieszkały również

9 E. Olejniczak- Szałowska, *Prawo dostępu do informacji publicznej. Zagadnienia wybrane*, (w) red. Ewy Olejniczak – Szałowskiej, *Współczesne problemy administracji publicznej,* Piotrków Trybunalski 2009, s. 17 i podana tam literatura

10 M. Jabłoński, K. Wygoda, *Ustawa o dostępie do informacji publicznej. Komentarz,* Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2002, s. 27

11 E. Jarzęcka-Siwik, *Dostęp do informacji publicznej (Uwagi krytyczne),* „Kontrola Państwowa" 2002, nr 1, s. 26

12 A. Niżnik-Mucha, *Problematyka zakresu przedmiotowego konstytucyjnego...* op. cit., s. 16

13 P. Czarny (w:) P. Sarnecki (red.) *Prawo konstytucyjne RP,* Warszawa 2005, s. 148

14 P. Szustakiewicz, *Zasady ustawy o dostępie do informacji publicznej*, „Jurysta" 2002, nr 1, s. 5-6

poza terytorium jej krajów członkowskich) uzyskiwałyby dostęp do informacji w przypadku wskazania interesu prawnego bądź faktycznego. Prawo do informacji publicznej wynika bowiem z konstytucyjnej zasady zwierzchności narodu, a zatem może ono podlegać ograniczeniu lub wyłączeniu wobec podmiotów zagranicznych.[15] Uwzględniając fakt, że podstawowym sposobem udostępniania informacji publicznej jest jej zamieszczenie na stronach internetowych Biuletynu Informacji Publicznej podmiotu zobowiązanego do udostępniania informacji publicznej, postulat ten wydaje się niewykonalny.

Prawo do informacji publicznej przysługuje każdemu podmiotowi

W oparciu o analizę treści art. 2 ust. 1 u.d.i.p. E. Olejniczak-Szałowska formułuje wniosek, że prawo do informacji publicznej przysługuje każdemu człowiekowi, niezależnie od posiadanego obywatelstwa, a zatem zarówno obywatelom polskim, jak też cudzoziemcom[16] lub też osobie nie posiadającej obywatelstwa żadnego z państw. Z literalnego brzmienia przepisu wynika również, że prawo to przysługuje bez względu na wiek[17], a także zdolność do czynności prawnych.

Jak podkreśla NSA, przepis art. 2 ust. 1 u.d.i.p. stanowi, że każdemu przysługuje prawo dostępu do informacji publicznej, czyli prawo dostępu do wiadomości, wiedzy o sprawach publicznych.[18] Również SKO we Wrocławiu stwierdza jednoznacznie, że przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (art. 2, Dz. U. Nr 112, poz. 1198 z późn. zm.) otwierają jednakowo szeroki dostęp do informacji dla wszystkich zainteresowanych, bez wyodrębnienia szczególnych uprawnień dla radnych.[19]

Dodatkowo w obecnym stanie prawnym zrównano status dziennikarzy i innych podmiotów w zakresie dostępu do informacji publicznej. Dostęp dziennikarzy do informacji publicznej reguluje ustawa z dnia 6 września 2001 r., a nie prawo prasowe, jest to zatem dostęp na prawach ogólnych, zgodnie z treścią art. 2 ust. 1, że prawo dostępu do informacji publicznej przysługuje każdemu.[20]

Warto zwrócić uwagę na fakt, że ustanowione w art. 2 u.d.i.p. prawo dostępu do informacji publicznej nie obejmuje w swej treści prawa dostępu strony do środków masowego przekazu w celu poinformowania członków społeczności gminnej (innej grupy społecznej) o określonych zdarzeniach. Ustawa o dostępie do informacji publicznej w art. 2 nie ustanawia prawa osoby do wypowiedzi za pośrednictwem mediów, czy też prawem członków społeczności gminnej do poinformowania ich o określonych zdarzeniach.[21]

W świetle poczynionych ustaleń można stwierdzić, że realizacja prawa do informacji publicznej przez osobę fizyczną nie budzi zastrzeżeń. Powstaje jednak pytanie, czy w takim samym zakresie przysługuje ono innym podmiotom prawnym np. osobie prawnej.

15 M. Kłaczyński, S, Szuster, *Komentarz do art. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej* (Dz.U.01.112.1198), Lex /el. 2003
16 E. Olejniczak - Szałowska, *Prawo dostępu do informacji publicznej*… op. cit., s. 17
17 A. Obrzut, *Prawo do informacji publicznej*... op. cit., s. 212
18 Wyrok NSA w Warszawie z dnia 20.11.2003, II SAB 372/03, Wokanda z 2004 Nr 5 poz. 33
19 Decyzja SKO we Wrocławiu z dnia 27.05.2008, SKO 4541/6/08, OwSS z 2008 Nr 3 poz.64
20 E. Olejniczak-Szałowska, *Prawo dostępu do informacji publicznej*… op. cit., s. 18
21 Wyrok WSA we Wrocławiu z 17.12.2004, IV SA/Wr 721.04, niepubl.

L. Garlicki stawia tezę, że prawa i wolności konstytucyjne przysługują w zasadzie osobie fizycznej, a nie podmiotowi zbiorowemu. W nauce prawa konstytucyjnego funkcjonuje pogląd, iż „w odniesieniu do osób prawnych prawa prywatnego zawsze konieczne jest postawienie pytania, czy dana osoba prawna (z uwagi na swoją strukturę, zadania i charakter) może być podmiotem określonego prawa lub wolności; jeżeli jednak możliwość taka zachodzi, to nie ma podstaw do odmówienia jej podmiotowości".[22] Według E. Olejniczak-Szałowskiej można przychylić się do poglądu, że na tle rozwiązań konstytucyjnych „faktycznym adresatem prawa do informacji nie jest wyłącznie obywatel polski ani nawet kategoria osób fizycznych, lecz każdy podmiot prawny, który pozostając pod jurysdykcją państwa polskiego, może żądać udzielenia informacji publicznej, zaś ostatecznym potwierdzeniem tego stanowiska jest treść ustawy, która w sposób nie budzący wątpliwości potwierdza, że prawo to ma każdy."[23] Inaczej rzecz ujmując, „adresatem tej normy jest zasadniczo osoba fizyczna. Nie oznacza to jednak, że pominięte zostały inne podmioty działające na terytorium Rzeczypospolitej Polskiej."[24] Stanowisko to podziela E. Jęrzecka-Siwik twierdząc, że ze względu na sformułowanie art. 2 ust. 1 *in principio* u.d.i.p. oraz na fakt, iż w art. 2 ust. 2 u.d.i.p. posłużono się „osobą wykonującą prawo do informacji publicznej", należy przyjąć, iż u.d.i.p. przyznaje prawo do informacji publicznej zarówno osobom fizycznym, jak i prawnym (np. stowarzyszeniom, spółkom kapitałowym). W przypadku jednostek organizacyjnych nieposiadających osobowości prawnej (np. w przypadku stowarzyszenia zwykłego) prawo do informacji publicznej mogą realizować wspólnie bądź osobno ich członkowie. [25]

Również WSA w Warszawie stoi na stanowisku, że pojęcie „każdego" oznacza zarówno osoby fizyczne, osoby prawne, jak i jednostki organizacyjne niemające osobowości prawnej, np. organizacje społeczne. Za takim poglądem przemawia zarówno użyte w art. 2 ust. 1 tej ustawy słowo „każdemu", jak i tendencje występujące w prawie międzynarodowym wynikające przykładowo z rekomendacji Komitetu Ministrów Rady Europy z dnia 25 listopada 1981 r. R81/19 (tekst zawarty w: T. Jasudowicz, *Administracja wobec praw człowieka*, Toruń 1996, s. 99 i n.) czy w prawie unijnym, wynikające z art. 255 Traktatu ustanawiającego Wspólnotę Europejską wprowadzonego Traktatem Amsterdamskim z 2 października 1997 r. (tekst: *Dokumenty Europejskie* w opracowaniu A. Przyborowskiej-Klimczak i E. Skrzydło-Tefelskiej, t. III, Lublin 1999, s. 295-296).[26]

Skoro prawo do informacji publicznej ma każdy podmiot prawa, powstaje pytanie, czy reguła ta ma zastosowanie także do podmiotów władzy publicznej. Zdaniem S. Czarnowa z istoty jawności życia publicznego wynika, że dostęp do informacji publicznej dotyczy wyłącznie relacji między władzą publiczną a podmiotem prywatnym. Tymczasem unormowania u.d.i.p. – zwłaszcza przepisy art. 2 i art. 4 ust. 3, statuujące powszechne prawo ubiegania się o informację i powszechny obowiązanej jej udzielania – wprowadzają pewne pomieszanie pojęć. Sugerują one, że w trybie u.d.i.p. powinna się odbywać wymiana informacji także między organami władzy publicznej. Tak być nie powinno, gdyż organy władzy publicznej potrzebują informacji do wykonywania zadań publicznych,

22 L. Garlicki, *Polskie prawo konstytucyjne, Zarys wykładu,* Warszawa 1998, s. 99
23 E. Olejniczak-Szałowska, *Prawo dostępu do informacji publicznej…* op. cit., s. 18 i podana tam literatura
24 M. Jabłoński, K. Wygoda, *Ustawa o dostępie do informacji publicznej*...op. cit., s. 28
25 E. Jarzęcka-Siwik, *Dostęp do informacji publicznej*...op. cit., s. 26
26 Wyrok WSA w Warszawie z dnia

nie zaś do zaspokojenia własnej ciekawości. Powinny więc mieć dostęp do tych informacji (zarówno jawnych, jak i niejawnych), które są im niezbędne dla wykonywania zadań ustawowych.[27] Inne stanowisko w tej materii reprezentuje orzecznictwo. Według WSA w Poznaniu rada gminy miała prawo do wystąpienia z wnioskiem o udostępnienie informacji publicznej, tak jak przewiduje to art. 2 ust. 1. Wniosek ten może być sformułowany w postaci uchwały.[28] Przychylam się do stanowiska reprezentowanego przez S. Czarnowa. Brak swobodnego przepływu informacji pomiędzy podmiotami realizującymi zadania publiczne i – co warto podkreślić – w zakresie niezbędnym dla prawidłowego ich wykonywania zadań jest przejawem nadmiernej biurokratyzacji administracji.

Osoba fizyczna żądająca informacji nie zawsze może być anonimowa

Jak stanowi art. 10 ust. 1 u.d.i.p., informacja publiczna, która nie została udostępniona w Biuletynie Informacji Publicznej, jest udostępniana na wniosek. Natomiast według ust. 2 art. 10 u.d.i.p. informacja publiczna, która może być niezwłocznie udostępniona, jest udostępniana w formie ustnej lub pisemnej bez pisemnego wniosku.

Przepisy u.d.i.p. nie stawiają żądnych wymogów formalnych dotyczących wniosku o udostępnienie informacji publicznej. Tym niemniej „możliwość udostępnienia informacji publicznej na wniosek jest związana z koniecznością wszczęcia i prowadzenia określonego postępowania w sprawie jej udostępnienia".[29] Powstaje zatem wątpliwość, czy zawsze osoba wykonująca prawo do informacji musi podać swoje dane identyfikacyjne.

Pamiętać jednak trzeba, że na gruncie ustawy o dostępie do informacji publicznej realizacja przyznanego prawa przybiera postać – niezależnie od tego, jak podmiot działa – osobistego wystąpienia lub złożenia wniosku podpisanego przez konkretną osobę fizyczną działającą w imieniu własnym lub też określonego podmiotu prawa. Dlatego też w sytuacji występowania o udostępnienie informacji przez inne podmioty niż osoby fizyczna za prawidłowy wniosek uznać należy tylko taki, który został podpisany przez przedstawiciela uprawnionego (umocowanego) do działania w ich imieniu *de facto*. Z punktu widzenia podmiotu zobowiązanego do udostępnienia informacji przesłanki formalne wskazują, że jest to po prostu realizacja indywidualnego prawa.[30] Należy jednak zgodzić się z twierdzeniem, że ze względu na charakter sposobów udostępniania informacji publicznych sformułowanych w art. 7 u.d.i.p. wymóg ten będzie w praktyce odnosił się przede wszystkim do udostępniania informacji na wniosek pisemny.[31]

W konsekwencji pojęcie „każdy" nie oznacza „anonimowy". Podmiot żądający udostępnienia określonej informacji publicznej powinien podać swoje imię i nazwisko w przypadku podmiotów niebędących

27 S. Czarnow, *Prawo do informacji publicznej w Polsce a wymogi prawa europejskiego*, „Samorząd Terytorialny" z 2007 r., Nr 4, s. 26-27

28 Wyrok WSA w Poznaniu z 5.10.2004, IV SA/Po 876/04 niepubl.

29 M. Jaśkowska, *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002, s. 59-60

30 M. Jabłoński, K. Wygoda, *Ustawa o dostępie do informacji publicznej…* op. cit., s. 28, M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2002, s. 110

31 M. Kłaczyński, S. Szuster, *Komentarz do art. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej…*, op. cit.

osobami fizycznymi.[32] Takie samo stanowisko zajmuje WSA w Warszawie - artykuł 2 ustawy z dnia 6 września 2001 r. o dostępnie do informacji publicznej (Dz. U. Nr 112, poz. 1198) dopuszcza możliwość wystąpienia z wnioskiem o udzielnie informacji publicznej każdemu, bez wykazania interesu prawnego lub faktycznego i w tym sensie nie jest istotnym, kto tej informacji żąda. Natomiast nie oznacza to jednak, że jeżeli z takim wnioskiem występuje osoba prawna, to nie należy badać, czy osoba/osoby w jej imieniu występujące są upoważnione do jej reprezentowania. Jest rzeczą oczywistą, że w sytuacji, w której osoba fizyczna występuje w imieniu osoby prawnej i powołuje się na nią, to działa w jej imieniu jako organ reprezentujący dany podmiot lub pełnomocnik, a nie na własną rzecz.[33]

Jak zauważa A. Matan, przepisy ustawowe w zależności od źródeł umocowania rozróżniają dwa rodzaje przedstawicielstwa. Kodeks cywilny w art. 96 stanowi, że „umocowanie do działania w cudzym imieniu może opierać się na ustawie (przedstawicielstwo ustawowe) albo na oświadczeniu reprezentowanego (pełnomocnictwo)". Pomimo różnych źródeł powstania przedstawicielstwa musi istnieć kompetencja do działania w cudzym imieniu. Podstawę dokonania czynności prawnej przez przedstawiciela stanowi umocowanie dające kompetencję do dokonania czynności prawnych w imieniu reprezentowanego. Źródłem przedstawicielstwa ustawowego jest nie oświadczenie reprezentowanego, lecz oznaczone w ustawie stosunki prawne, np. władza rodzicielska, oparte na ustawie orzeczenia sądu, np. ustanowienie opiekuna albo organu administracyjnego – tak w przypadku ustanowienia przedstawiciela dla nieobecnego, w przypadku konieczności podjęcia czynności nie cierpiącej zwłoki. Przedstawicielami ustawowymi są rodzice dziecka podlegającego ich władzy rodzicielskiej, ustanowiony opiekun lub kurator, wspólnik reprezentujący członków spółki cywilnej lub jawnej.[34]

Posiadanie statusu uczestnika postępowania administracyjnego nie ma wpływu na realizację prawa do informacji publicznej

Nie można dostępu do informacji publicznej, która przysługuje każdemu, zgodnie z art. 2 ust. 1 ustawy o dostępie do informacji publicznej, ograniczyć do osób czy podmiotów ściśle wymienionych w przepisach szczególnych.[35]

Według WSA w Krakowie żadna z ustaw wprost nie wprowadza zakazu udostępniania dokumentów osobie, która była świadkiem w danej sprawie administracyjnej. Nie jest zasadny argument, zgodnie z którym skoro skarżąca posiada status świadka w toku postępowania administracyjnego, to tym samym niedopuszczalnym byłoby udostępnianie jej protokołu (dokumentu sporządzonego w toku postępowania administracyjnego). Taki kierunek argumentacji wprost prowadzi do wniosku, że jakiekolwiek dokumenty sporządzone w toku postępowania administracyjnego mogą zostać udostępnione tylko stronie danego postępowania, ewentualnie w ograniczonym zakresie ustanowionego w danej sprawie biegłemu. Tym samym akta administracyjne w ogóle nie podlegałyby udostępnieniu innym osobom, czyli nie podlegałyby udostępnieniu na podstawie ustawy o dostępie do informacji publicznej. Taki wniosek może wynikać jedynie

32 W. Rygiel, *Ty nam zgodę, my ci informację* ... op. cit.
33 Wyrok WSA w Warszawie z 30.04.2007, II SA/Wa 2404/06, LEX nr 319393
34 A. Matan, *Zastępstwo procesowe w ogólnym postępowaniu administracyjnym,* Katowice 2001, s. 23 i nast.
35 Wyrok WSA w Warszawie z dnia 24.11.2006, II SAB/Wa 99/06, LEX nr 299599

z rozszerzającej wykładni art. 73 i 74 k.p.a. zawężającej dostęp do akt administracyjnej i jest on sprzeczny zarówno z treścią art. 1 i 2 ustawy o dostępie do informacji publicznej, jak i art. 61 ustawy z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. z 1997 r. Nr 78, póz. 483 z późn. zm.), które to przepisy wprowadzają i zarazem gwarantują powszechną dostępność do m.in. wytworzonych w toku postępowania administracyjnego dokumentów, wprowadzając zarazem przypadku odmowy ich udostępnienia.[36]

Podmiotom objętym decyzjami administracyjnymi (podmiotom, do których je skierowano) służy przymiot strony w postępowaniu wywołanym wnioskiem o ich udostępnienie w trybie ustawy o dostępie do informacji publicznej. Przyjąć więc należy dopuszczalność skargi pod względem podmiotowym i uznać legitymację takiej strony do udziału w postępowaniu w omawianej materii.[37]

Osoba żądająca informacji publicznej nie musi uzasadniać potrzeby jej posiadania

Obywatel nie musi przy tym wykazywać interesu prawnego ani faktycznego, nie musi też podawać powodu, dla którego występuje o podanie określonej informacji.[38]

Jak bowiem wynika z treści art. 2 ust. 2 u.d.i.p., od osoby wykonującej prawo do informacji publicznej nie wolno żądać wykazania interesu prawnego lub faktycznego.

Takie sformułowanie wskazuje, że prawo do informacji publicznej może więc być wykorzystywane przez wszystkie podmioty prawa. W tym miejscu warto zaznaczyć, że przyjęta w ustawie zasada jest odejściem od typowej praktyki polskiego ustawodawstwa, uzależniającej występowanie z roszczeniem tylko w sytuacji legitymowania się interesem prawnym lub faktycznym.[39]

Ustawodawca nie określił w przepisach ustawy, co należy rozumieć przez pojęcia „interes prawny" i „interes faktyczny". Terminy te zostały natomiast wyjaśnione w doktrynie i judykaturze. Pojęcie interesu prawnego może być rozumiane jako „obiektywna, czyli rzeczywiście istniejąca potrzeba ochrony prawnej".[40] Według NSA „mieć interes prawny" znaczy to samo, co „ustalić przepis prawa powszechnie obowiązującego, na którego podstawie można skutecznie żądać czynności organu z zamiarem zaspokojenia jakiejś potrzeby albo żądać zaniechania lub ograniczenia czynności sprzecznych z potrzebami danej osoby".[41] W innym orzeczeniu NSA wskazał, że treścią pojęcia „interes prawny" jest prawo podmiotowe rozumiane jako przyznanie przez przepis prawa konkretnych korzyści, które można realizować w postępowaniu administracyjnym. Ten „interes" jest konkretny, indywidualny, aktualny i sprawdzalny obiektywnie, a jego istnienie znajduje potwierdzenie w okolicznościach faktycznych, będących przesłankami zastosowania przepisu prawa materialnego. Tylko przepis prawa materialnego stanowiący podstawę interesu prawnego stwarza dla określonego

36 Wyrok WSA w Krakowie z dnia 18.02.2008, II SA/Kr 942/07 LEX nr 506529
37 Wyrok WSA w Gliwicach z dnia 15.11.2004, IV SA/Gl 664/04, niepubl.
38 A. Niżnik-Mucha, *Problematyka zakresu przedmiotowego konstytucyjnego…* op. cit., s. 15, T. R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej,* Wydawnictwo LexisNexis Warszawa 2008, s. 121, por. wyrok TK z 20.03.2006, 1630/3/A/2006, K 17/05 OTK-A z 2006 Nr 3 poz. 30
39 B. Michalak, *Udostępnienie radnym informacji przetworzonej,* „Nowe Zeszyty Samorządowe" z 2008 r., Nr 6, s. 54
40 T. Rowiński, *Interes prawny w procesie cywilnym i w postępowaniu nieprocesowym,* Warszawa 1971, s. 22
41 Wyrok NSA z dnia 22.02.1984, sygn. akt I SA 1748/83 niepubl.

podmiotu legitymację procesową strony.[42] Szczególną cechą interesu prawnego jest bezpośredniość związku między sytuacją danego podmiotu a wspomnianą normą prawa materialnego, na której budowany jest interes prawny. Oznacza to, że jeżeli sprawa dotyczy dwóch lub więcej podmiotów, to interes prawny mają tylko te z nich, których sytuacja prawna wynika wprost z normy prawa materialnego, a nie powstaje za pośrednictwem drugiego podmiotu. Drugą szczególną cechą interesu prawnego jest jego realność, interes ten musi rzeczywiście istnieć w dacie stosowania danych norm prawa administracyjnego. Nie może to być interes tylko przewidywany w przyszłości ani hipotetyczny.[43] Od tak rozumianego interesu prawnego należy odróżnić interes faktyczny, kiedy to dana osoba jest bezpośrednio zainteresowana rozstrzygnięciem sprawy administracyjnej, a nie może tego interesu poprzeć przepisami prawa powszechnie obowiązującego, mogącego stanowić podstawę skierowanego żądania określonych czynności organu administracyjnego.[44]

Wprowadzenie do u.d.i.p. ust. 2 w art. 2 jest konsekwencją stanowiska ustawodawcy, iż każdy ma prawo do informacji publicznej. Każdy, a zatem nie tylko ten, kto ma w uzyskaniu dostępu do określonej informacji interes prawny lub faktyczny; takie rozwiązanie ograniczałoby bowiem dostęp do informacji publicznej. Intencją ustawodawcy było zatem wzmocnienie charakteru prawa do informacji publicznej jako prawa podmiotowego.[45] W konsekwencji strona, która wystąpiła o udostępnienie informacji publicznej, nie jest zobligowana do uzasadnienia potrzeby uzyskania tego rodzaju informacji.[46]

W związku z powyższym żądanie podmiotu zobowiązanego uzależniające udzielenie informacji od sprecyzowania interesu przez wnioskodawcę będzie sprzeczne z ustawą i może stać się podstawą wszczęcia odrębnego postępowania (nawet o charakterze karnym – jeśli osoba, na której ciąży obowiązek udzielenia informacji publicznej, nie uczyniła tego, powołując się na brak interesu po stronie żądającego.) [47]

Jakkolwiek od osoby wykonującej prawo do informacji publicznej nie żąda się wykazania interesu prawnego lub faktycznego, to konkretne żądanie udzielenia informacji musi podlegać wstępnej ocenie pod kątem tego, czy mamy do czynienia z informacją o sprawach publicznych, ważnych, interesujących dla ogółu, czy też z informacją ważną i przydatną dla konkretnej osoby. Ustawa o dostępie do informacji publicznej nie może być nadużywana i wykorzystywana w czysto prywatnych sprawach. Wymaga to obiektywizacji treści wniosku, gdyż niejednokrotnie osoba go składająca może mieć wrażenie, że to, co ją samą interesuje, jest ważne dla społeczeństwa.[48]

Uwaga ta jest szczególnie istotna z jednego względu. W trakcie wykonywania prawa do informacji publicznej pamiętać

42 Wyrok NSA z dnia 2.06.2000, sygn. akt. I SA 1019/99, LEX nr 78926
43 Wyrok NSA z dnia 19.03.2002, sygn. akt. IV SA 1132/00, LEX nr 81670
44 Wyrok NSA z dnia 6.09.1999, sygn. akt IV SA 2473/98, LEX nr 47873; wyrok NSA z 22.02.1984, sygn. akt. I SA 1748/83, niepubl.
45 T. R. Aleksandrowicz, *Komentarz do ustawy o dostępie do informacji publicznej*... op. cit., s. 124
46 Wyrok WSA w Gliwicach z 16.05.2006, IV SA/Gl 204/05, niepubl.
47 M. Jabłoński, K. Wygoda, Ustawa o dostępie do informacji publicznej… op. cit., s. 30, B. Michalak, *Udostępnienie radnym informacji przetworzonej*… op. cit., s.5548
48 Wyrok WSA w Krakowie z 15.09.2004, II SA/Kr 23/04, niepubl

należy o jednym fundamentalnym wyjątku od określonej powyżej zasady. Dotyczy on sytuacji, w której konkretny podmiot występuje o udostępnienie mu informacji przetworzonej – tu sam ustawodawca nakazuje podanie przez wnioskującego okoliczności wskazujących, iż jest to szczególnie istotne dla interesu publicznego (*in fine* z art. 3 ust. 1 pkt. 1 ustawy). W takiej sytuacji zobowiązany będzie do wykazania istnienia szczególnie istotnego interesu publicznego, którego nie należy jednak utożsamiać z interesem prawnym lub faktycznym danej osoby.[49] Podstawowym elementem pozwalającym na właściwe uzasadnienie szczególnego interesu publicznego będzie wykazanie, że działanie organów i innych podmiotów realizujących zadania publiczne wywołało lub będzie wywoływało skutki obejmujące potencjalnie szeroki krąg adresatów. Wnioskodawca musi więc wykazać, że informacje, które zamierza uzyskać, nie dotyczą wyłącznie jego interesu. Zobowiązany również będzie do takiego nakreślenia okoliczności i faktów, które zostaną uznane za wystarczające do przyjęcia, że działa on w interesie publicznym, a sprawa lub sprawy, o których chce się dowiedzieć, mają szczególne znaczenie.[50]

Reasumując, należy postawić wniosek, że w obowiązującym stanie prawnym zasada powszechności prawa do informacji publicznej jest w pełni realizowana. Na jej podstawie każdy podmiot prawny, niezależnie od struktury organizacyjnej czy też narodowości lub obywatelstwa, ma prawo żądać informacji mającej charakter publiczny, czyli związanej z działalnością władz publicznych. Tak szerokie ujęcie zakresu podmiotowego prawa dostępu do informacji publicznej w pełni odpowiada idei transparentności działań władzy publicznej.

Streszczenie

Warunkiem aktywnego uczestniczenia w życiu społecznym, politycznym, gospodarczym jest posiadanie przez osobę informacji. Dotyczy to także informacji obejmującej szeroko rozumianą wiedzę dotyczącą działalności władzy publicznej. Stąd też prawo do informacji publicznej ma charakter publicznego prawa podmiotowego, na podstawie którego każdy człowiek ma prawo udziału w życiu publicznym i sprawowania kontroli działalności organów władzy publicznej, w szczególności poprzez realizację prawa dostępu do informacji publicznej. Może być ono wykorzystywane niezależnie od posiadanego przez osobę obywatelstwa, zdolności do czynności prawnych, wieku, płci, narodowości. Prawo to przysługuje także osobom prawnym i jednostkom organizacyjnym niemającym osobowości prawnej.

Dr Dorota Fleszer jest pracownikiem Wyższej Szkoły Zarządzania i Administracji w Opolu oraz pracownikiem administracji samorządowej.

49 M. Jabłoński, K. Wygoda, *Ustawa o dostępie do informacji publicznej*...., op. cit. s. 30, decyzja SKO we Wrocławiu z dnia 27 maja 2008 r., SKO 4541/6/08, OwSS z 2008 Nr 3 poz. 64

50 A. Pakuła, *Interes publiczny i użyteczność publiczna jako kryteria zadań samorządu terytorialnego, [w:] Administracja i prawo administracyjne u progu trzeciego tysiąclecia, materiały Konferencji Naukowej Katedry Prawa i Postępowania Administracyjnego,* Łódź 2002, s.106. , M. Jabłoński, K. Wygoda, *Ustawa o dostępie do informacji…,* op. cit. s. 35, decyzja SKO we Wrocławiu z dnia 27.05.2008 r. SKO 4541/6/08, OwSS z 2008 Nr 3 s. 64, B. Michalak, *Udostępnienie radnym informacji przetworzonej…,* op. cit. s.55-56

Program komputerowy jako próbka w świetle przepisów dotyczących zamówień publicznych

Wojciech Kaliński

Program komputerowy czy próbka?

Pojęcie próbki na gruncie regulacji dotyczących zamówień publicznych nie zostało zdefiniowane. Terminem tym ustawa – Prawo zamówień publicznych posługuje się tylko w jednym przepisie. Zgodnie z art. 97 ust. 1. Zamawiający przechowuje protokół wraz z załącznikami przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, w sposób gwarantujący jego nienaruszalność. 2. Zamawiający zwraca wykonawcom, których oferty nie zostały wybrane, na ich wniosek, złożone przez nich plany, projekty, rysunki, modele, próbki, wzory, programy komputerowe oraz inne podobne materiały. Z przepisu tego wynika pośrednio, że w toku postępowania o udzielenie zamówienia publicznego dopuszczalne jest składanie (jak można domniemać - razem z ofertą) m.in. próbek i programów komputerowych. Jak zatem widać, art. 97 pzp różnicuje pojęcie próbki i programu komputerowego, nie utożsamiając tych pojęć. Kolejny ślad dotyczący próbek znajdziemy w przepisach wykonawczych do ustawy. Zgodnie z § 5 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2009 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane. W celu potwierdzenia, że oferowane dostawy, usługi lub roboty budowlane odpowiadają wymaganiom określonym przez zamawiającego, zamawiający może żądać w szczególności:

1) próbek, opisów lub fotografii;
2) opisu urządzeń technicznych, instrukcji obsługi oraz środków stosowanych przez wykonawcę dostaw lub usług oraz opisu zaplecza naukowo-badawczego wykonawcy w celu potwierdzenia zapewnienia odpowiedniej jakości realizowanego zamówienia;
3) zaświadczenia podmiotu uprawnionego do kontroli jakości potwierdzającego, że dostarczane produkty odpowiadają określonym normom lub specyfikacjom technicznym;
4) zaświadczenia niezależnego podmiotu zajmującego się poświadczaniem zgodności działań wykonawcy z normami jakościowymi, jeżeli zamawiający odwołują się do systemów zapewniania jakości opartych na odpowiednich normach europejskich;
5) zaświadczenia niezależnego podmiotu zajmującego się poświadczaniem zgodności działań wykonawcy z europejskimi normami zarządzania środowiskiem, jeżeli zamawiający wskazują środki zarządzania środowiskiem, które wykonawca będzie stosował podczas realizacji zamówienia na roboty budowlane lub usługi, odwołując się do systemu zarządzania środowiskiem i audytu (EMAS) lub norm zarządzania środowiskiem opartych na europejskich lub międzynarodowych normach poświadczonych przez podmioty działające zgodnie z prawem Unii Europejskiej, europejskimi lub międzynarodowymi normami dotyczącymi certyfikacji.

Przedmiotowe rozporządzenie wydane zostało na podstawie delegacji zawartej w art. 25 ustawy, zgodnie z którym to przepisem:

1. W postępowaniu o udzielenie zamówienia zamawiający może żądać od wykonawców wyłącznie oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania. Oświadczenia lub dokumenty potwierdzające spełnianie:
   a) warunków udziału w postępowaniu,
   b) przez oferowane dostawy, usługi lub roboty budowlane wymagań określo-

nych przez zamawiającego
- zamawiający wskazuje w ogłoszeniu o zamówieniu, specyfikacji istotnych warunków zamówienia lub zaproszeniu do składania ofert.

2. Prezes Rady Ministrów określi, w drodze rozporządzenia, rodzaje dokumentów, jakich może żądać zamawiający od wykonawcy oraz formy, w jakich dokumenty te mogą być składane, mając na uwadze, że potwierdzeniem spełniania warunków udziału w postępowaniu o udzielenie zamówienia może być zamiast dokumentu również oświadczenie złożone przed właściwym organem oraz że potwierdzeniem niekaralności wykonawcy może być w szczególności informacja z Krajowego Rejestru Karnego, a potwierdzeniem, że oferowane dostawy, usługi lub roboty budowlane odpowiadają wymaganiom określonym przez zamawiającego, może być w szczególności zaświadczenie podmiotu uprawnionego do kontroli jakości, a także że formy dokumentów powinny umożliwiać udzielanie zamówień również drogą elektroniczną.

W pierwszej kolejności należy zauważyć, że próbka w większości przypadków nie jest ani oświadczeniem, ani dokumentem. Tymczasem z delegacji zawartej w art. 25 ust. 2 pzp wynika, że Prezes Rady Ministrów miał określić „rodzaje dokumentów (...) oraz formy, w jakich dokumenty te mogą być składane". Raczej trudno byłoby uznać za poprawne stwierdzenie, że wykonując zawartą w ustawie delegację, organ wykonawczy określił formę dokumentu w postaci próbki. Bardziej zasadnym wydaje się stwierdzenie, że organ wykonawczy wykroczył poza delegację zawartą w ustawie.

Z treści art. 25 ust. 1 pzp wynika jednoznacznie, że na okoliczność, iż oferowane dostawy, usługi lub roboty budowlane spełniają wymagania określone przez zamawiającego, ten ostatni może żądać wyłącznie oświadczeń bądź dokumentów. O próbkach ani o programach komputerowych nie ma mowy. Widoczna staje się tu niespójność z regulacją art. 79 ust. 2 pzp. Skoro ten ostatni przepis nakazuje zwrot m.in. próbek i programów komputerowych, ale tych zamawiający w toku postępowania nie może żądać, powstaje pytanie, w jaki sposób mogą one znaleźć się w posiadaniu zamawiającego? Trudno bowiem przyjąć, że art. 79 ust. 2 pzp reguluje sytuację, w której wykonawcy sami z siebie, nieproszeni przez zamawiającego dołączyli do ofert próbki czy programy komputerowe. Powstaje więc pytanie, który z przepisów jest błędnie sformułowany? Odpowiedź na tak postawione pytanie wydaje się jedynie pozornie skomplikowana. Bez większych trudów można bowiem stwierdzić, że nieprawidłowa jest redakcja art. 25 pzp. Wystarczy, że porównamy jego brzmienie z pierwowzorem tej regulacji zawartym w art. 48 Dyrektywy 2004/18/WE Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. „*Kwalifikacje techniczne i/lub zawodowe.*

1. Techniczne i/lub zawodowe kwalifikacje wykonawców są oceniane i weryfikowane zgodnie z ust. 2 i 3.

2. W zależności od charakteru, ilości lub znaczenia, a także przeznaczenia robót budowlanych, dostaw i usług dowód możliwości technicznych wykonawcy może stanowić jeden lub kilka z poniższych środków:

a)

i) Wykaz robót budowlanych wykonanych w ciągu ostatnich pięciu lat wraz z zaświadczeniami zadowalającego wykonania najważniejszych robót. Zaświadczenia wskazują wartość, datę i miejsce robót oraz określają, czy roboty zostały wykonywane zgodnie z zasadami sztuki budowlanej i prawidłowo ukończone. W razie konieczności właściwy organ przedkłada takie zaświadczenie bezpośrednio instytucji zamawiającej.

ii) Wykaz głównych dostaw lub usług zrealizowanych w ciągu ostatnich

trzech lat, z podaniem kwot, dat wykonania oraz odbiorców, publicznych lub prywatnych. Dowody dostaw i usług należy przedstawić:

- *w przypadku gdy odbiorcą była instytucja zamawiająca - w formie zaświadczeń wydanych lub poświadczonych przez właściwy organ;*
- *w przypadku gdy odbiorcą był nabywca prywatny - w postaci zaświadczenia wystawionego przez nabywcę, a w razie braku takiego zaświadczenia - w postaci oświadczenia wykonawcy.*

b) Wskazanie zaangażowanych pracowników technicznych lub instytucji technicznych, niezależnie od tego, czy są one częścią przedsiębiorstwa danego wykonawcy, w szczególności tych, odpowiedzialnych za kontrolę jakości, zaś w przypadku zamówień na roboty budowlane - tych, którymi ten przedsiębiorca budowlany będzie dysponował do wykonania robót budowlanych.

c) Opis urządzeń technicznych oraz środków zastosowanych przez dostawcę lub usługodawcę w celu zapewnienia jakości oraz opis zaplecza naukowo-badawczego przedsiębiorstwa.

d) W przypadku gdy produkty lub usługi, które mają zostać dostarczone, mają charakter złożony lub wyjątkow, mają szczególne przeznaczenie, instytucje zamawiające lub w ich imieniu właściwy organ urzędowy kraju, w którym dostawca lub usługodawca ma siedzibę lub miejsce zamieszkania, z zastrzeżeniem zgody tego organu, przeprowadza kontrolę możliwości produkcyjnych dostawcy lub możliwości technicznych usługodawcy, a w razie konieczności także dostępnych mu możliwości naukowych i badawczych, jak również środków kontroli jakości, z których będzie korzystał.

e) Wykształcenie i kwalifikacje zawodowe usługodawcy, przedsiębiorcy budowlanego lub personelu zarządzającego przedsiębiorstwem, w szczególności osoby lub osób odpowiedzialnych za świadczenie usług lub kierowanie robotami budowlanymi.

f) W odniesieniu do zamówień publicznych na roboty budowlane oraz zamówień publicznych na usługi oraz wyłącznie w stosownych przypadkach wskazanie środków zarządzania środowiskiem, które wykonawca będzie mógł zastosować podczas realizacji zamówienia.

g) Oświadczenie na temat wielkości średniego rocznego zatrudnienie u usługodawcy lub przedsiębiorcy budowlanego oraz liczebność personelu zarządzającego w ostatnich trzech latach.

h) Oświadczenie na temat narządzi, wyposażenia zakładu i urządzeń technicznych dostępnych usługodawcy lub przedsiębiorcy budowlanemu w celu realizacji zamówienia.

i) Wskazanie części zamówienia, której realizację usługodawca zamierza ewentualnie zlecić podwykonawcy.

j) W odniesieniu do produktów, które mają zostać dostarczone:

- ***próbki*, opisy lub fotografie, których autentyczność musi zostać zaświadczona na żądanie instytucji zamawiającej***;
- *zaświadczenia sporządzone przez uznane, właściwe urzędowe instytuty lub agencje kontroli jakości i wyraźnie potwierdzające zgodność produktów przez odniesienie do specyfikacji lub norm."*

Jak zatem widać, art. 48 Dyrektywy nie wymaga, by kwalifikacje techniczne i zawodowe, co z grubsza odpowiada zakresowi regulacji art. 25 pzp, musiały być potwierdzane wyłącznie oświadczeniami i dokumentami. Wiele rozwiązań zawartych w art. 48 Dyrektywy nie znalazło się w przepisach polskiej ustawy, natomiast w sposób pośredni zostało implementowane regulacjami rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2009 r.

w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy oraz form, w jakich te dokumenty mogą być składane. Poza zakresem dalszych rozważań pozostaje kwestia, czy taki sposób implementacji Dyrektywy jest na pewno poprawny.

Co ciekawe, Dyrektywy – w przeciwieństwie do art. 79 ust. 2 pzp - nie posługują się pojęciem programu komputerowego. Program taki może zatem być wymagany przez zamawiających co najwyżej jako próbka.

Oceniając relacje pomiędzy art. 25 pzp i §5 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2009 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy, oraz form, w jakich te dokumenty mogą być składane, a art. 79 ust. 2 pzp, wydawać by się mogło, że domaganie się przez zamawiającego załączenia do oferty lub zaprezentowania w toku procedury oceny ofert programu komputerowego znajdzie samodzielną, niezależną od próbki podstawę prawną. Wniosek ten mógłby z jednej strony znaleźć podstawę w treści art. 79 ust. 2 pzp, który próbkę i program komputerowy traktuje oddzielnie, z drugiej zaś w treści § 5 ust. 1 rozporządzenia, który nie zawiera zamkniętego katalogu dokumentów, oświadczeń i innych przedmiotów, które mogą potwierdzić zgodność oferowanego przez wykonawcę świadczenia z wymaganiami zamawiającego, posługując się określeniem „w szczególności". Jednak czytając polskie regulacje w kontekście cytowanego wcześniej art. 48 Dyrektywy „klasycznej", należy zauważyć, że Dyrektywa nie pozwala na swobodne domaganie się przez zamawiających „dowodów" potwierdzających zgodność oferty z wymaganiami zamawiającego. Przyjmując więc pro-wspólnotową wykładnię polskich przepisów (co w świetle nieszczęśliwie sformułowanego art. 25 pzp wydaje się wręcz koniecznością), uznać należy, że zamawiający mogą domagać się od wykonawców załączenia programów komputerowych wyłącznie jako próbek.

Odmienne stanowisko zajęła Krajowa Izba Odwoławcza w wyroku z dnia 17 maja 2010 r., sygn. akt KIO 758/10, stwierdzając: „*zdaniem Izby podstawą prawną do żądania przez zamawiającego przeprowadzenia prezentacji systemu jest § 5 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2009 roku w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawc, oraz form, w jakich te dokumenty mogą być składane (Dz. U. nr 226, poz. 1817). Ustawodawca w przywołanym przepisie rozporządzeni, przez użycie słów 'w szczególności' określił katalog otwarty dokumentów i oświadczeń, które potwierdzają, że oferowane dostawy, usługi czy roboty budowlane odpowiadają wymaganiom określonym przez zamawiającego. Taka konstrukcja przepisu pozwala zamawiającemu żądać także innych niż wprost w nim wymienionych dokumentów i oświadczeń potwierdzających oferowane parametry. W ocenie Izby demonstracji systemu nie można zaliczyć do zwykłej próbki przedmiotu zamówienia, za którą należy uznać raczej część produktu gotowego. Tymczasem zdaniem Izby prezentacja systemu jest specyficznym rodzajem 'dokumentu', potwierdzającym spełnienie oferowanych funkcjonalności, stosowanym przy dokonywaniu zamówień na systemy i oprogramowania komputerowe. Z uwagi na specyfikę tego 'dokumentu', jakim jest demonstracja systemu, należy go zaliczyć raczej do innych 'dokumentów', niewymienionych wprost w § 5 ust. 1 przywołanego rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2009 roku w sprawie rodzajów dokumentów (...).*" Pogląd ten, jak wskazałem wyżej, nie zasługuje na aprobatę, albowiem opiera się wyłącznie na wykładni polskich przepisów rozporządzenia Prezesa Rady Ministrów i pozostaje w sprzeczności z art. 48 Dyrektywy „klasycznej".

Razem z ofertą czy w toku oceny ofert?

W postepowaniach o udzielenie zamówienia publicznego ukształtowały się dwa mechanizmy prezentowania programów komputerowych jako próbki. Pierwszy z nich zakłada dołączenie nośnika z programem do złożonej przez wykonawcę oferty, drugi zaś prezentację programu komputerowego przez wykonawcę w ramach procedury oceny ofert, przy czym sama prezentacja jest nagrywana bądź protokołowana przez zamawiającego. Należy zauważyć, że tylko pierwszy z mechanizmów jest w świetle przepisów prawa zamówień publicznych poprawny i to z kilku względów. Po pierwsze, zgodnie z art. 29 ust. 1 pzp, przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. Ewentualne późniejsze uzupełnienie tych wymagań, np. poprzez udostępnienie danych, jakie mają być zaimplementowane w programie komputerowym, oznacza, że wymagania stawiane wykonawcom na etapie opisu przedmiotu zamówienia nie zostały opisane wyczerpująco, a zatem praktyka taka narusza cytowany przepis. Po drugie, jak stanowi §5 ust. 1 rozporządzenia, zamawiający może żądać m.in. próbek w celu potwierdzenia, że oferowane dostawy, usługi lub roboty budowlane odpowiadają wymaganiom określonym przez zamawiającego. Co prawda rozporządzenie wprost nie wskazuje, w jakim momencie zamawiający może żądać próbek czy innych dokumentów, jednak powszechnie przyjmuje się, że jest to moment składania oferty. Po trzecie, dopuszczenie późniejszej prezentacji opartej o materiały niezałączone od oferty może prowadzić do naruszenia zasady równego traktowania wykonawców, gdyż niektórzy z nich mogą przygotowywać swoje „próbki" dopiero po złożeniu oferty. Wreszcie należy podnieść, że dopuszczenie prezentacji z jej protokołowaniem czy nawet rejestrowaniem przebiegu za pomocą urządzeń nagrywających dźwięk i obraz nie pozwala na praktyczne zrealizowanie zasad kontroli w drodze postępowania odwoławczego. Istota kontroli realizowanej przez Krajową Izbę Odwoławczą polega na tym, że Izba zapoznaje się dokładnie z tym samym materiałem, jakim dysponował zamawiający przy podejmowaniu decyzji o rozstrzygnięciu przetargu. Oznacza to, iż zapoznanie się z próbką musi być zarówno powtarzalne, jak i dotyczyć dokładnie tej samej próbki jaką dysponował zamawiający, a nie próbki, którą po prezentacji mógł wykonawca zmodyfikować. Nawet nagrywanie przebiegu prezentacji nie rozwiązuje problemu, albowiem dzięki nagraniu można ocenić co do zasady prawidłowość postępowania zamawiającego i – znów co do zasady - zgodność tego, co było prezentowane z wymaganiami SIWZ. Nie da się jednak w ten sposób ocenić elementów prezentacji, które zostały pominięte przez zamawiającego i tym samym nie doszło do zweryfikowania wszystkich wymagań stawianych wykonawcom. Dlatego gotowe prezentacje programów lub same programy powinny być dołączane do składanych przez wykonawców ofert.

Możliwość uzupełnienia próbki

W wyroku z dnia 17 maja 2010 r., sygn. akt KIO 758/10 Krajowa Izba Odwoławcza uznała, że możliwość uzupełnienia (powtórzenia) prezentacji programu komputerowego co do zasady istnieje, jednak nie we wszystkich przypadkach. Krajowa Izba stwierdziła bowiem, że „z *okoliczności sprawy wynika, że w dniu wyznaczonym na prezentację, tj. w dniu 16 kwietnia 2010 roku, przedstawiciele przystępującego stawili się w siedzibie zamawiającego, jednak nie zgodzili się na przeprowadzenie prezentacji z zachowaniem zasady jawności, zatem stanowisko takie należy ocenić jako odmowę przeprowadzenia prezentacji systemu na warunkach wymaganych przez zamawiającego, co nie pozwala na przyjęcie, że spełniona została przesłanka określona w art. 26 ust. 3 ustawy Pzp zobowiązująca*

zamawiającego do wezwania do uzupełnienia dokumentów. Odmowę przeprowadzenia prezentacji na określonych przez zamawiającego warunkach, w wyznaczonym przez niego terminie nie można uznać za równoznaczną z 'brakiem dokumentu' lub 'dokumentem zawierającym błąd', a zatem brak w przedmiotowej sprawie zaistnienia okoliczności, od których uzależnione jest wszczęcie procedury z art. 26 ust. 3 ustawy Pzp. Przepis art. 26 ust. 3 ustawy Pzp jako wyjątek od zasady - obowiązku potwierdzania spełniania warunków udziału w postępowaniu oraz potwierdzenia spełnienia przez oferowane dostawy wymagań określonych przez zamawiającego w terminie wyznaczonym na składnie ofert - należy interpretować ściśle. W rozpatrywanych okolicznościach sprawy oświadczenie przedstawicieli przystępującego o odmowie przeprowadzenia w dniu 16 kwietnia 2010 roku jawnej prezentacji systemu nie może być ocenione jako 'niezłożenie dokumentu' lub 'złożenie dokumentu zawierającego błąd'. W tym zakresie stanowisko Izby uznać należy za błędne. Z punktu widzenia art. 26 ust 3 pzp powód niezłożenia dokumentu lub oświadczenia nie ma najmniejszego znaczenia. O konieczności wezwania decyduje fakt obiektywny – brak prawidłowego dokumentu.

Innym problem jest natomiast kwestia relacji art. 26 ust. 3 pzp do kwestii próbki. Art. 26 ust. 3 pzp nakazuje bowiem wezwanie do uzupełnienia dokumentów, oświadczeń i pełnomocnictw. Tymczasem próbka nie jest żadnym z tych przedmiotów. Czy zatem dopuszczalne jest wezwanie do jej uzupełnienia? Wydaje się, że podobnie jak miało to miejsce wcześniej, należy posłużyć się wykładnią funkcjonalną. Skoro na gruncie art. 25 pzp pojęcie dokumentów i oświadczeń należy interpretować szerzej w kontekście art. 48 Dyrektywy, to również art. 26 ust. 3 pzp należy interpretować w analogicznym duchu, uznając, że zamawiający ma obowiązek wezwać do uzupełnienia wszelkich elementów (przedmiotów), jakich zamawiający mógł żądać na potwierdzenie spełniania przez wykonawców warunków udziału w postepowaniu. Dzięki takiej interpretacji uzyskamy spójne rozumienie obydwu regulacji.

Próbka jako tajemnica przedsiębiorstwa

Wywód należy ponownie rozpocząć od cytatu z wyroku z dnia 17 maja 2010 r., sygn. akt KIO 758/10 Krajowej Izby Odwoławczej: „*zgodnie bowiem z treścią art. 8 ust. 3 ustawy Pzp wykonawca może zastrzec informacje stanowiące tajemnicę przedsiębiorstwa nie później niż w terminie składania ofert lub terminie składania wniosków o dopuszczenie do udziału. Zatem najpóźniej w dniu składania ofert wykonawca winien poczynić starania w celu zachowania poufności danych, które w jego ocenie mogłyby stanowić tajemnicę przedsiębiorstwa. Zastrzeżenie tajemnicy przedsiębiorstwa w terminie późniejszym należy uznać za bezskuteczne. O ewentualnej możliwości zastrzeżenia tajemnicy przedsiębiorstwa wykonawcy zostali poinformowani przez zamawiającego w pkt 13.3 siwz. Ponadto przystępujący, składając ofertę, miał już wiedzę o konieczności przeprowadzenia demonstracji systemu celem potwierdzenia funkcjonalności i cech, które zadeklarował w treści oferty. Ponieważ demonstracja miała jedynie zweryfikować dane zadeklarowane w ofercie (załączniku nr 5), zatem przystępującemu najpóźniej w dniu składania ofert znana była zarówno procedura oceny parametrów systemu, jak również ewentualny zakres funkcji i jego cech, które mogły być przedmiotem przeprowadzonej demonstracji. Stąd okoliczność przekazania przez zamawiającego w terminie późniejszym (w dniu składania ofert) tzw. 'scenariusza demonstracji', który określa jedynie porządek i kolejność weryfikacji poszczególnych funkcji systemu, nie stanowi w ocenie Izby wystarczającego*

uzasadnienia dla braku możliwości zastrzeżenia już na etapie składania oferty tajemnicą przedsiębiorstwa mającej się odbyć demonstracji systemu. Ponadto Izba wskazuje, że demonstracja jak każdy dokument złożony *w postępowaniu o zamówienie publiczne, objęty tajemnicą przedsiębiorstwa podlega ocenie przez zamawiającego co do skuteczności dokonanego przez wykonawcę zastrzeżenia. Następstwem stwierdzenia bezskuteczności zastrzeżenia jest wyłączenie zakazu ujawniania zastrzeżonych informacji, na co wskazał również Sąd Najwyższy w uchwale z dnia 21 października 2005 roku, sygn. III CZP 74/05.*" W tym zakresie wydaje się, że wnioski Izby sięgają zbyt daleko. W pierwszej kolejności należy zauważyć, że prezentacja programu komputerowego oznacza pokazanie jego standardowych funkcjonalności, a zatem informacji postrzegalnych przez jego użytkownika. Ponieważ należy zgodzić się z poglądami, zgodnie z którymi jako próbki można żądać jedynie standardowego programu komputerowego, niedostosowanego do potrzeb zamawiającego, oznacza to, że pokazywane informacje winny być dostępne dla każdego posiadacza programu. To z kolei oznacza, **że co do zasady brak jest podstaw do traktowania prezentacji programu komputerowego jako tajemnicy przedsiębiorstwa.** Gdyby w szczególnych okolicznościach pewne informacje zawarte w prezentacji wykraczałyby poza to, co jest dostępne dla użytkowników systemu, to co najwyżej te konkretne informacje lub fragmenty można by uznać za tajemnicę. W żadnym jednak wypadku nie daje to podstawy do utajnienia całej próbki (podobnie jak ma to miejsce w przypadku oferty). Wreszcie wywody KIO dotyczące terminu zastrzeżenia poufności można byłoby uznać za prawidłowe, gdyby uznać, że prezentacja miała być dołączona do oferty. Skoro jednak KIO dopuściło późniejszą prezentację próbki niezałączonej do oferty, to powinno dopuścić również późniejsze zastrzeżenie tajemnicy przedsiębiorstwa. Gdyby bowiem uznać pogląd KIO za słuszny, niedopuszczalne byłoby zastrzeżenie tajemnicy przedsiębiorstwa w odniesieniu do dokumentów i wyjaśnień składanych przez wykonawców, np. w trybie art. 26 ust. 3 i 4 pzp, które to dokumenty i wyjaśnienia nie sposób zastrzec na etapie składania ofert.

Streszczenie

Pojęcie próbki nie zostało zdefiniowane. Jedynie art. 97 ust. 2 pzp stanowi, że zamawiający zwraca wykonawcom, których oferty nie zostały wybrane, na ich wniosek, złożone przez nich plany, projekty, rysunki, modele, próbki, wzory, programy komputerowe oraz inne podobne materiały. Z przepisu tego wynika pośrednio, że w przetargu dopuszczalne jest składanie m.in. próbek i programów komputerowych.

W praktyce ukształtowały się dwa mechanizmy prezentowania programów komputerowych jako próbki: 1) dołączenie nośnika z programem do złożonej przez wykonawcę oferty, 2) prezentację programu komputerowego w ramach procedury oceny ofert. Tylko pierwszy z mechanizmów jest w świetle przepisów prawa zamówień publicznych poprawny.

Co do zasady brak jest podstaw do traktowania prezentacji programu jako tajemnicy przedsiębiorstwa. Nie ma też podstawy do utajnienia całej próbki, a jedynie do jej „tajnych" fragmentów.

Dr Wojciech Kaliński - asystent w Katedrze Prawa Cywilnego Uniwersytetu Jagiellońskiego, wspólnik w kancelarii Maruta i Wspólnicy sp. j.

Jak generować klucze dla podpisu osobistego

Przemysław Kubiak

Uzasadniana poniżej odpowiedź jest krótka: w sposób weryfikowalny, w myśl zasady: ,,Zaufanie jest dobre, lecz kontrola jeszcze lepsza''.

A przecież w przypadku dowodów osobistych mechanizmy kontroli procesu wytwarzania mają zasadnicze znaczenie.

Generowanie klucza RSA na karcie

Paragraf 32 ustęp 1 projektu [1] rozporządzenia do art. 15 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych stanowi, że dane do składania podpisu osobistego są generowane przez dowód osobisty na żądanie posiadacza.

Podpis osobisty ma być zaimplementowany z wykorzystaniem algorytmu RSA (por. paragraf 3, ustęp 5).

Zapisy projektu rozporządzenia (paragraf 20, ustęp 3 projektu [1]) rozumieć można jako wymóg, by podpis osobisty był podpisem z mediatorem [19]. Schemat z mediatorem ma wiele zalet (por. [2], [3]) jak np. użyteczna możliwość czasowego zawieszenia przez właściciela dowodu możliwości składania tym dowodem podpisu osobistego. Schemat podpisów RSA może być zrealizowany w ten sposób, że będzie to podpis deterministyczny (nie zawsze podpis RSA jest deterministyczny, np. w przypadku użycia kodowania PSS [4] używa się pewnej zmiennej o nazwie ,,salt'', której wartość może być losowa). Determinizm jest zaletą, nie pozwala na podprogowy wyciek informacji [5] w podpisach.

Jednak sam klucz RSA niesie w sobie bardzo dużo losowych bitów. Jak pokazano w pracach [6], [7] część z nich można wykorzystać do przemycania informacji o faktoryzacji modułu RSA. Atak z pracy [6] jest bardzo wyrafinowany, a jednocześnie efektywny (w wersji opisanej w [8] okazał się szybszy od standardowego mechanizmu generowania kluczy RSA). Producent karty umieszcza w niej asymetryczny klucz dla protokołu Diffie-Hellmana uzgadniania klucza. Ów asymetryczny klucz pełni rolę analogiczną do klucza publicznego w protokołach wykonywanych publicznie takich jak DHIES [9] czy jak procedura chip authentication [10]. Czyli klucz ten pozwala na przeprowadzenie protokołu Diffie-Hellmana uzgadniania klucza w przypadku, gdy jedna ze stron (tutaj producent) jest stroną statyczną, tj. nie wpływa aktywnie na postać „uzgadnianego'' klucza.

Producent posiada klucz prywatny, który zachowuje jedynie dla siebie. W efekcie nawet w przypadku otwarcia zainfekowanego urządzenia i wykrycia tylnej furtki nie mamy wglądu w chroniony kluczem asymetrycznym przekaz podprogowy - możemy jedynie domyślać się, że w kluczu publicznym RSA urządzenie umieściło dla producenta informację o kluczu prywatnym. Ta informacja to tak naprawdę zarodek dla generatora ciągów pseudolosowych, od których jest zależny jeden z czynników pierwszych generowanego przez kartę modułu. Zarodek, czyli klucz sesyjny, jest ustalany z pomocą wspomnianej powyżej wersji protokołu Diffie-Hellmana. Przesyłana do producenta informacja, ciąg bitów, z którego, posiadając

klucz prywatny, odtworzy zarodek, jest zawarta w górnej połówce (bardziej znaczące bity) modułu RSA. Zastosowany w [6] mechanizm zapewnia, że ten ciąg jest ciągiem bitów o własnościach idealnie losowych - wystąpienia konkretnych wartości tego ciągu binarnego mają jednostajny rozkład prawdopodobieństwa. Nie można więc wykryć mechanizmu poprzez analizę statystyczną ciągów binarnych w generowanych modułach RSA.

Opisany w [6] atak jest bardzo elegancki - bardzo oszczędnie używa bitów wygenerowanych z zarodka, który będzie odtworzony przez producenta. Nie wszystkie bity jednego z dzielników pierwszych modułu RSA są wygenerowane z tego zarodka. A przecież mogłyby, upraszczając tym samym procedurę odtwarzania klucza RSA. Autorzy pracy [6] uznali, że część bitów w generowanym dzielniku będzie także dla producenta losowa - przynajmniej do momentu odtworzenia przez niego faktoryzacji. W pracy [6] nie wyjaśniono powodu takiego oszczędnego postępowania (być może chodzi tutaj o matematyczną elegancję i skuteczność ataku). Po bliższej analizie okazuje się, że owe „losowe'' bity, czyli bity dzielnika nieprzewidywalne dla producenta na początku procesu odtwarzania przez niego faktoryzacji modułu można wykorzystać jako nośnik przeznaczonego dla producenta szyfrogramu. Bity „tekstu jawnego'' zainfekowana karta może sksorować z kolejnymi bitami wyjścia z generatora ciągów losowych. W wyniku otrzymujemy szyfr strumieniowy, który po odtworzeniu faktoryzacji zostanie przez producenta odtworzony, a znając wyjście z generatora ciągów pseudolosowych, producent może odtworzyć także bity „tekstu jawnego'' - czyli informację, która wyciekła w module RSA, a która z kluczem RSA związana nie jest.

Także inne bity generowanego modułu RSA można wykorzystać jako nośnik szyfrogramu. Pojemność wynikowego kanału (kanału kleptograficznego) jest bardzo duża. Oznaczmy przez |N| długość modułu N algorytmu RSA. W projekcie [1] rozporządzenia określono (paragraf 3, ustęp 5), że ma to być co najmniej 2048 bitów (tj. |N| nie mniejsze niż 2048). Jeśli zainfekowane karty mają dawać jednostajny rozkład generowanych kluczy RSA, to dla ok. 1/4 kluczy kanał ten ma pojemność ok. (3|N|/4)-245 bitów szyfrogramu, a dla ok. 3/4 kluczy pojemność ok. (|N|/2)-215 bitów szyfrogramu. Szyfrogramu, który przenosi informację niezwiązaną z faktoryzacją modułu RSA - informacja umożliwiająca producentowi faktoryzację przenoszona jest niezależnie, wystarczy dla niej 211 bitów.

Praca [6] znana jest od kilku lat. Minęło zatem sporo czasu, by (hipotetycznie) móc dopracować implementację ataku i dopasować do siebie wzajemnie dwie partie kart w ten sposób, by partia kart mająca podlegać certyfikacji miała takie same charakterystyki (pobór energii, widmo elektromagnetyczne) jak karty zainfekowane i by jedynie przez inspekcję wnętrza urządzenia można było wykryć różnicę.

Wróćmy ponownie do projektu [1] rozporządzenia. Jak wspomnieliśmy na początku, paragraf 32, ustęp 1 mówi, że dane do składania podpisu osobistego są generowane przez dowód osobisty na żądanie posiadacza. Ponieważ domniemywać można, że żądanie to może być wyrażone także po personalizacji dokumentu (personalizacja odbywa się w zaufanym centrum, jeszcze przed dostarczeniem dokumentu do urzędu gminy), domniemywać też można, że klucz RSA do podpisu osobistego generowany będzie na karcie już po osadzeniu na niej klucza prywatnego do generowania informacji uwierzytelniającej oraz klucza prywatnego do generowania informacji uwierzytelniającej ograniczonej identyfikacji.

Przedstawiony powyżej kanał kleptograficzny jest wystarczająco pojemny, by wyprowadzić w module RSA czytelną jedynie dla producenta informację o jego faktoryzacji, klucz prywatny do generowania informacji uwierzytelniającej

oraz klucz prywatny do generowania informacji uwierzytelniającej ograniczonej identyfikacji (realizacja punktu 2 ustępu 1 paragrafu 7 oraz realizacja ustępu 2 paragrafu 24 projektu [1] preferuje w rzeczywistości wykorzystanie protokołu Diffie-Hellmana do generowania tych dwóch rodzajów informacji uwierzytelniającej, ale nawet w przypadku zastosowania algorytmu RSA do generowania informacji uwierzytelniającej karta może zdradzać górną połowę bitów jednego z czynników pierwszych modułu RSA, wówczas statystycznie dla jednej czwartej modułów możliwa jest ich faktoryzacja przez producenta - por. [6], a w konsekwencji także odtworzenie klucza prywatnego do generowania informacji uwierzytelniającej). W takim przypadku warstwa elektroniczna dowodu i zawarte tam klucze nie stanowią już żadnego zabezpieczenia przed producentem karty.

Opisana powyżej funkcjonalność kanału kleptograficznego, u przynajmniej części kart, staje się zatem bardzo atrakcyjna dla służb specjalnych państw obcych.

Zauważmy, że projekt rozporządzenia nie zabrania wycieku w module RSA klucza do generowania informacji uwierzytelniającej ani klucza do generowania informacji uwierzytelniającej ograniczonej identyfikacji. Ustęp 3 paragrafu 31 odnosi się jedynie do procesu tworzenia i instalacji danych, o których mowa w paragrafie 31, czyli dotyczy wyłącznie procesu tworzenia i instalacji obu wspomnianych kluczy do generowania informacji uwierzytelniających.

Zauważmy ponadto, że w powyższym ataku w ogóle nie wykorzystano wykładnika publicznego RSA, który, jeśli nie jest narzucony z zewnątrz, także może przenosić zaszyfrowaną informację.

Opisany powyżej mechanizm ataku na schemat RSA jest niezależny od sposobu realizacji paragrafu 20, ustęp 3 projektu [1] rozporządzenia. Z drugiej strony rezygnacja z RSA i użycie probabilistycznego schematu podpisów niesie z sobą niebezpieczeństwo wycieku informacji w samych podpisach.

Generowanie kluczy RSA w sposób scentralizowany

Wymóg generowania kluczy przez kartę może być próbą zabezpieczenia obywateli przed kopiowaniem kluczy prywatnych przez obsługę systemu w przypadku generowania ich przez centralny serwer.

Z drugiej strony pamiętać należy, że karta przed dostaniem się w ręce obywatela przechodzi przez system centralny, w którym jest personalizowana. W systemie tym (hipotetycznie) osadzona może być na karcie aplikacja powodująca, że generowane później przez kartę klucze będą i tak na końcu procesu ich generacji zastąpione kluczami zapisanymi w pamięci karty podczas procesu jej personalizacji. Dla obywatela warstwa elektroniczna dowodu to i tak czarna skrzynka, która generuje komunikaty, które wcale nie muszą być zgodne z tym, co dzieje się w jej wnętrzu.

Zabezpieczenie się przed powyższym atakiem, czyli przed rodzajem zawirusowania kart wraz ze wszczepieniem im znanych atakującemu kluczy prywatnych, polega w dużej mierze na wdrożeniu odpowiednich procedur organizacyjnych. Jest to zatem sytuacja podobna do zabezpieczania się przed kopiowaniem kluczy z serwera centralnego: w jednym przypadku atakujący wprowadza swoje klucze do systemu, w drugim przypadku wyprowadza klucze skopiowane.

Zabezpieczając się przed kopiowaniem kluczy, kontrolować należy moduły HSM (Hardware Security Module), na których wytwarzany jest materiał kryptograficzny. Czyli należy kontrolować fizyczny stan tych urządzeń oraz środowisko ich pracy: czy nie było prób ataku typu „fault injection" poprzez np. skoki napięcia dostarczanej

energii oraz czy np. w otoczeniu HSM nie pojawiły się urządzenia do pomiaru emisji elektromagnetycznej, natężenia dźwięku [20], poboru mocy. Ponadto zapewnić należy, by dostęp do HSM był bardzo restrykcyjny, monitorowany oraz rozliczalny dla całego okresu ich posiadania.

W sytuacji drugiego z ataków, tj. „zawirusowywania" kart, bezpieczeństwo systemu nie jest skupione na jednym jego komponencie. Aby w sposób wydajny i powtarzalny wprowadzać oprogramowanie na karty, atakujący powinien posiadać podpis pod tym oprogramowaniem (zakładamy, że karta wymaga, by oprogramowanie było podpisane), a także uzyskać dostęp do czytnika komunikującego się z przetwarzanymi w systemie kartami lub samodzielnie wprowadzić do systemu taki czytnik (karty posiadają interfejs bezstykowy). Jeśli producent kart zadbał o to, by rzeczywiście w każdej sytuacji podpis pod instalowanym na karcie oprogramowaniem był przez kartę wymagany i by był to jedynie podpis składany przez wyznaczoną do tego jednostkę w MSWiA (czyli producent kart nie zostawił w nich tylnej furtki w postaci akceptacji przez kartę także jego podpisów), to sytuacja atakującego nie jest łatwa - w co najmniej dwóch miejscach musi zmienić stan systemu.

W jaki sposób uniknąć scenariusza wycieku w module RSA informacji o jego faktoryzacji, jeśli urządzeniem generującym klucz RSA jest nie karta, ale centralny moduł HSM? Jednym z rozwiązań jest generowanie klucza RSA nie przez pojedynczy moduł HSM, ale przez zbiór takich modułów. Istnieją algorytmy rozproszonego generowania klucza RSA (por. np. [12], [13], [14]). Działają one w ten sposób, że żadna ze stron nie poznaje wynikowego sekretu, tj. klucza prywatnego (lub równoważnie: faktoryzacji wygenerowanego modułu, por. [15]). Jeśli zbiór modułów HSM dobrany będzie od różnych producentów, to można zabezpieczyć się przed omawianym w podrozdziale 1 atakiem.

Z drugiej strony generowanie kluczy w sposób rozproszony jest dużo wolniejsze niż generowanie ich w sposób scentralizowany - pojedynczy zbiór HSMów do rozproszonego generowania klucza może nie sprostać wymogom wydajnościowym. Wyjściem jest wdrożenie kilku, kilkunastu gniazd generacji w sposób rozproszony lub generowanie kluczy w scentralizowany (jądro systemu na pojedynczym HSM), ale jednocześnie weryfikowalny sposób [18].

Aby proces mógł być zweryfikowany, jego przebieg musi być ściśle zdeterminowany, łącznie ze sposobem generowania ciągów (tutaj pseudo-) losowych. Z problemem weryfikowalności procesu od dawna stykają się projektanci protokołów wyborów elektronicznych - dobry protokół wyborczy powinien zapewnić możliwość weryfikacji przestrzegania tegoż protokołu przez maszynę (czy np. maszyna nie zmienia głosów oddanych przez wyborców). Wymóg taki nie jest rezultatem czysto akademickich rozważań - por. np. słabości maszyn wyborczych opisane w [16].

Okazuje się, że znaleziono już dobre rozwiązanie problemu weryfikowalnego generowania ciągów pseudolosowych. W pracy [11] zaproponowano, by generować ciągi pseudolosowe z podpisu deterministycznego. Podpis cyfrowy jest nieprzewidywalny - jeśli potrafimy przewidzieć wartość podpisu bez posiadania klucza tajnego, to oznacza to, że potrafimy sfałszować podpis pod wiadomością. Z drugiej strony jeśli zobaczymy podpis, to łatwo sprawdzić, że rzeczywiście jest on podpisem. Zatem otrzymujemy narzędzie, które łączy oba oczekiwania: nieprzewidywalność (czyli pseudolosowość) z weryfikowalnością czysto deterministycznego procesu.

Przedstawmy bardziej szczegółowo ten mechanizm. Urządzenie posiada klucz prywatny do generowania podpisów z wykorzystaniem deterministycznego schematu podpisów (RSA). Klucz weryfikacji podpisu

posiada strona sprawdzająca. Jako argument urządzenie z zewnątrz otrzymuje numer seryjny, który podpisuje. Ów podpis, lub jego skrót, stanowi zarodek dla generatora ciągów pseudolosowych. Aby zweryfikować, czy urządzenie rzeczywiście przestrzega procedury, podaje się mu na wejściu dwa numery seryjne i dla każdego z nich urządzenie przeprowadza procedurę, przekazując na wyjście wyniki. Następnie strona sprawdzająca wskazuje losowo wybrany przez siebie numer seryjny, dla którego zweryfikowany będzie proces: urządzenie ma przekazać na zewnątrz podpis tego numeru seryjnego. Poprawność podpisu jest weryfikowana, a ponieważ podpis służy do wygenerowania zarodka ciągów pseudolosowych użytych wewnątrz urządzenia, sprawdzający może na zewnątrz urządzenia wygenerować taki sam ciąg i dla wskazanego numeru seryjnego powtórzyć dokładnie procedurę, którą wykonało urządzenie. Jeśli wynik procesu weryfikacji zgadza się z tym, co wygenerowało urządzenie jako jeden z wyników, to, ponieważ nie wie ono, który numer seryjny będzie zweryfikowany, przyjmujemy, że dla drugiego z pary numerów seryjnych urządzenie też zadziałało uczciwie. Wynik dla tego drugiego numeru seryjnego jest ostatecznym wynikiem pojedynczej rundy protokołu.

Prawdopodobieństwo, że urządzenie oszuka stronę weryfikującą, zależy od tego, czy wybory dokonywane przez sprawdzającego są przewidywalne dla urządzenia, czy nie. Jeśli są zupełnie nieprzewidywalne, to prawdopodobieństwo uniknięcia wykrycia oszustwa polegającego na przestrzeganiu protokołu w stosunku do tylko jednego z numerów seryjnych użytych w rundzie, jest w przypadku 20 prób oszustwa (czyli 20 nieuczciwie wykonanych rund) mniejsze niż jeden do miliona, w przypadku 30 prób oszustwa mniejsze niż jeden do miliarda i maleje wykładniczo szybko w stosunku do liczby podejmowanych przez urządzenie prób oszukania strony sprawdzającej.

Łatwo powyższy protokół uogólnić na przetwarzanie nie dwóch, ale większej liczby numerów seryjnych w rundzie, z weryfikowaniem jednego, wskazywanego przez stronę sprawdzającą numeru.

Bezpieczeństwo procesu zależy od bezpieczeństwa kluczy podpisu użytych przez urządzenie. W jaki zatem sposób generowane powinny być klucze RSA do podpisywania zarodków przez urządzenie? Jak pamiętamy, można je generować w sposób rozproszony - czyli niezależny od pojedynczego urządzenia. Co więcej, rozproszone generowanie może przebiegać także w sposób odporny na wprowadzanie błędów do protokołu [17], [12]. Ponadto dla podpisów używanych przez HSM do generowania zarodków nie trzeba generować wielu kluczy podpisu w krótkim czasie.

Zauważmy, że urządzenie, którego determinizm weryfikowaliśmy, oprócz kluczy publicznych dla dowodów musi generować odpowiadające im klucze prywatne. Ale sprawdzający nie musi poznawać klucza prywatnego, wystarczy, że zweryfikuje czy procedura generowania klucza publicznego jest ściśle deterministyczna - klucz prywatny musi odpowiadać kluczowi publicznemu.

W przypadku implementacji schematu z mediatorem [19] należy uwzględnić reprezentację klucza prywatnego w postaci sumy dwóch elementów: pierwszy z nich jest wygenerowany niezależnie przez mediatora, drugi jest dobrany przez urządzenie generujące klucze tak, że po zsumowaniu z pierwszym elementem otrzymujemy klucz prywatny podpisu. Drugi z elementów jest przekazywany karcie.

Aby uniknąć wycieku kleptograficznego ze strony HSM mediatora, należy wymagać, by:

1) albo mediator generował swój składnik klucza w sposób weryfikowalny,

2) albo by najmłodszy bit generowanych przez mediatora składników dla kolejnych kluczy miał zawsze tę samą wartość, np. by był zawsze ustawiony (uzasadnienie tego wymagania wykracza poza ramy niniejszego artykułu).

W przypadku (2) wymagać ponadto należy, by weryfikacja składnika mediatora dla weryfikowanego numeru seryjnego była przeprowadzana przez urządzenie inne niż te, które podejmuje decyzję o tym, który numer seryjny sprawdzać. Numer seryjny do weryfikacji składnika mediatora powinien być przekazywany kanałem jednokierunkowym od urządzenia podejmującego decyzję.

Podsumowanie

Oprócz generowania kluczy RSA na karcie po przeprowadzeniu procesu personalizacji lub generowania ich w sposób scentralizowany rozważyć można alternatywne scenariusze.

Pierwszym z nich jest generowanie przez kartę klucza RSA podczas procesu personalizacji, ale jeszcze przed osadzeniem na karcie kluczy prywatnych do generowania informacji uwierzytelniających. W ten sposób klucze prywatne do generowania informacji uwierzytelniających są oczywiście chronione przed wyciekiem w kluczu publicznym RSA. Pomijając nawet kwestię kleptograficznego wycieku informacji nt. faktoryzacji modułu, taki scenariusz generowania kluczy może się okazać wąskim gardłem w systemie - generowanie klucza RSA zajmuje karcie kilkadziesiąt sekund (ciekawy przegląd technik generowania przez kartę kluczy RSA oraz osiąganej 9 lat temu wydajności znaleźć można w pracy [21]).

Innym podejściem jest generowanie klucza RSA z wykorzystaniem protokołu rozproszonego (np. [13]) bezpośrednio przez kartę i przez mediatora. Protokół taki byłby jednak na pewno wolniejszy niż samodzielne generowanie klucza przez kartę. Przeprowadzany nawet po otrzymaniu karty przez użytkownika absorbowałby serwer centralny przez długi czas. Zatem to rozwiązanie nie wydaje się dobrze skalowalne.

Biorąc zatem pod uwagę skalowalność procesu, a także możliwość jego kontroli, najlepszym rozwiązaniem wydaje się generowanie kluczy RSA w sposób scentralizowany, ale jednocześnie w pełni weryfikowalny.

Aby jednak nie skupiać bezpieczeństwa w jednym elemencie systemu, klucze prywatne do składania informacji uwierzytelniających należy generować w odrębnych modułach HSM. Aby zagwarantować spełnienie warunku z paragrafu 31 ustęp 3 projektu [1] rozporządzenia, należy każdy z takich kluczy generować w sposób rozproszony, z wykorzystaniem co najmniej dwóch HSM (w przypadku kluczy dla protokołu Diffie-Hellmana rozproszona generacja jest prosta i szybka).

Idąc krok dalej w tym kierunku, można wykorzystać tzw. podpis wewnętrzny, szerzej opisany w [3], [22].

Wspomniana na początku niniejszego artykułu zmienna „salt'' używana w kodowaniu PSS [4] jest odtwarzana z podpisu RSA w trakcie jego weryfikacji. Standard [4] jest jednocześnie dość elastyczny co do zakresu długości tej zmiennej. Zmienna „salt'' może zatem przenosić dodatkowy podpis pod tą samą wiadomością co zawierający ją podpis RSA. Deterministyczne algorytmy generowania wystarczająco krótkich podpisów można znaleźć w pracach [23], [24]. Problemy, na których bazują schematy [23], [24], mimo że uważane za problemy trudne, nie mają tak długiej historii podejmowanych na nie prób ataku jak problem faktoryzacji. Ponadto oprogramowanie weryfikujące podpisy jest dla schematu RSA powszechne, a dla schematów [23], [24] nie.

Dlatego właściwym wykorzystaniem algorytmu [23] lub [24] wydaje się wykorzystanie go jako dodatkowego, a nie zasadniczego, komponentu bezpieczeństwa - czyli wykorzystanie go do przenoszenia podpisu w zmiennej „salt'' kodowania PSS użytego w podpisach RSA. Aby było to możliwe, karta musi wspierać zarówno podpisy RSA, jak i arytmetykę krzywych eliptycznych (takie karty są dostępne).

Zatem jeśli karta oprócz podpisu RSA realizuje także protokół podpisu wewnętrznego, to generowanie kluczy można przeprowadzić następująco:

1) Jeszcze przed osadzeniem na karcie kluczy do generowania informacji uwierzytelniających, o których mowa w paragrafie 31 ustęp 1 projektu [1]:
   - osadzana jest na karcie krzywa eliptyczna do podpisu wewnętrznego oraz punkt bazowy na tej krzywej (krzywa oraz punkt bazowy mogą być wspólne dla wielu użytkowników),
   - klucz prywatny do podpisu wewnętrznego generowany jest przez kartę jako losowy ciąg bitów ustalonej długości,
   - zwracany jest przez kartę klucz publiczny do podpisu wewnętrznego (certyfikat do tego klucza nie będzie wydawany samodzielnie, ale jedynie jako pole rozszerzeń certyfikatu dla podpisu RSA). Klucz publiczny to iloczyn punktu bazowego przez skalar, będący kluczem prywatnym - zatem generacja przebiega bardzo szybko.
2) Osadzane są na karcie informacje, o których mowa w paragrafie 31 ustęp 1 projektu [1].
3) Klucz do podpisu RSA generowany jest w scentralizowany sposób.

Zauważmy, że cały punkt (1) powyższej procedury można nawet zrealizować jeszcze u producenta kart: producent powinien jedynie otrzymać zbiór możliwych krzywych eliptycznych i punktów bazowych na nich. Zwraca natomiast zbiór kart oraz podpisane przez siebie klucze publiczne podpisu wewnętrznego poszczególnych kart.

Jak widać, istnieje potencjalnie możliwość realizacji protokołu, w którym ani karta, ani centralny HSM generujący klucze RSA nie mają z osobna pełnego wpływu na materiał kryptograficzny pozwalający na wygenerowanie podpisu weryfikowalnego certyfikatem podpisu osobistego.

Literatura

1. MSWiA, *Projekt rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia ...2011 r. w sprawie wymagań technicznych dla warstwy elektronicznej dowodu osobistego oraz protokołu komunikacji elektronicznej z dowodami osobistymi* (w wersji skierowanej do uzgodnień międzyresortowych, z 7-terminem na zgłaszanie uwag). Biuletyn Informacji Publicznej MSWiA http://bip.mswia.gov.pl/portal/bip/218/19372/ (data publikacji 15.02.2011)
2. M. Tabor, *Electronic signature – easy as card transactions*. w: *Polskie Karty 2011 almanach,* Medien Service Sławomir Cieśliński, s. 331-335, ISBN 978-83-924201-1-8
3. P. Błaśkiewicz, P. Kubiak, M. Kutyłowski, *Digital signatures for e-government - a long-term security architecture,* China Communications, 7(6), s. 64–70, December 2010
4. RSA Laboratories, *PKCS #1 v2.1*, RSA Cryptography Standard, June 2002
5. A. Young, M. Yung, *The dark side of black-box cryptography, or: Should we trust capstone?* In N. Koblitz ed., CRYPTO, Volume 1109 of LNCS., Springer (1996) 89–103
6. A. Young, M. Yung, *A space efficient backdoor in RSA and its applications*, In B. Preneel, S.E. Tavares eds., Selected Areas in Cryptography, Volume 3897 of LNCS., Springer (2005) 128–143
7. A. Young, M. Yung, *Space-Efficient Kleptography Without Random Oracles*, Information Hiding 2007, 112-129
8. A. Young, M. Yung, *A Timing-Resistant Elliptic Curve Backdoor in RSA*, Inscrypt (2007) 427-441
9. M. Abdalla, M. Bellare, P. Rogaway, *The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES,* CT-RSA 2001, 143-158

10. BSI, *Advanced Security Mechanisms for Machine Readable Travel Documents 2.05,* Technische Richtlinie TR-03110 (2010)
11. D. Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, IEEE Security & Privacy 2(1), 38-47 (2004)
12. J. Algesheimer, J. Camenisch, V. Shoup, *Efficient Computation Modulo a Shared Secret with Application to the Generation of Shared Safe-Prime Products*, CRYPTO 2002, 417-432
13. M. H. Ibrahim, *Eliminating Quadratic Slowdown in Two-Prime RSA Function Sharing,* I. J. Network Security 7(1), 106-113 (2008)
14. I. Damgard, G.L. Mikkelsen, *Efficient, Robust and Constant-Round Distributed RSA Key Generation,* TCC 2010, 183-200
15. J.-S. Coron, A. May, *Deterministic Polynomial-Time Equivalence of Computing the RSA Secret Key and Factoring,* J. Cryptology 20(1), 39-50 (2007)
16. T. Kohno, A. Stubblefield, A. D. Rubin, D. S. Wallach, *Analysis of an Electronic Voting System,* IEEE Symposium on Security and Privacy 2004
17. Y. Frankel, P. D. MacKenzie, M. Yung, *Robust Efficient Distributed RSA-Key Generation*, PODC 1998, 320
18. M. Kutyłowski, Prywatna korespondencja nt. weryfikowalnego generowania kluczy RSA
19. Wikipedia, Podpis elektroniczny z mediatorem, http://pl.wikipedia.org/wiki/Podpis_elektroniczny_z_mediatorem
20. A. Shamir, E. Tromer, *Acoustic cryptanalysis, On nosy people and noisy machines*, http://people.csail.mit.edu/tromer/acoustic/
21. C. Lu, A. L. M. Santos, F. R. Pimentel, *Implementation of fast RSA key generation in Smart Cards*, in Proceedings of the 2002 ACM Symposium on Applied computing, 214–220, ACM Press
22. P. Kubiak, *Długofalowe bezpieczeństwo podpisu osobistego*, Czas Informacji Nr 4(5)/2010
23. D. Boneh, B. Lynn, H. Shacham, *Short signatures from the Weil pairing*, J. Cryptology 17(4) (2004) 297–319
24. F. Zhang, R. Safavi-Naini, W. Susilo, *An Efficient Signature Scheme from Bilinear Pairings and Its Applications*, Public Key Cryptography 2004, 277-290

Abstract

How to generate keys for personal signature functionality of the polish id cards

The answer given in the paper is short: in a verifiable way, according to the rule „trust is good, control better". The first part of the paper discuss some extended attack made by malicious implementation of the RSA key generation procedure. The basic attack is known in the cryptographic literature for a few years and allows to leak trapdoor to factorization of the RSA module in the module itself. Moreover, the trapdoor looks completely random and it is readable exclusively by the malicious implementator of the procedure. Simple extension of the basic attack allows to leak additional information, like for example keys for the chip authentication procedure. The second part of the paper depicts how this kind of attacks could be prevented: centralized and verifiable generation of RSA keys is proposed for the Polish ID-cards. Verifiability is achieved with help of tools known from e-voting protocols.

Dr Przemysław Kubiak jest adiunktem na Politechnice Wrocławskiej, jego zainteresowania naukowe dotyczą kryptografii z kluczem publicznym.

Ściśle tajne czy zastrzeżone – nowe regulacje dotyczące informacji niejawnych

Anita Jackiewicz

Od 2 stycznia 2011 r. obowiązuje ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. Nr 182, poz. 1228). Ustawa ta wprowadza nowe zasady ochrony informacji niejawnych. Zastąpiła obowiązująca przez ponad dziesięć lat ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2005 r. Nr 196 poz. 1631). Przepisy nowej ustawy mają zastosowanie m.in. do przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy. Chronione są tylko informacje dotyczące interesów państwa.

Ustawa wprowadza ogólną definicję informacji niejawnych. Do informacji takowych zaliczamy informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania (niezależnie od formy i sposobu ich wyrażania). Ochronie podlegają tylko informacje dotyczące interesów państwa, a nie, jak dotychczas, także informacje, których ujawnienie mogłoby spowodować szkodę. Dotychczasowe pojęcia jak „tajemnica państwowa" i „tajemnica służbowa" zastąpiono czterema klauzulami tajności: „ściśle tajne", „tajne", „poufne" i „zastrzeżone". Podstawowym kryterium przyporządkowania jest kryterium szkody dla interesów państwa, jaką mogłoby spowodować nieuprawnione ujawnienie informacji. Każda klauzula zawiera dodatkową charakterystykę.

Informacjom niejawnym nadaje się klauzulę „ściśle tajne", jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że m.in. zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskie lub zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej, zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej.

Informacjom niejawnym nadaje się klauzulę „tajne", jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że m.in. uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej lub pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi bądź zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej.

Informacjom niejawnym nadaje się klauzulę „poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że m.in. utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej lub utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej bądź zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli.

Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ

na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Nowa ustawa o ochronie informacji niejawnych zawiera także wiele istotnych przepisów dotyczących przedsiębiorców. Warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa jest zdolność do ochrony takich informacji. Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej jest świadectwo bezpieczeństwa przemysłowego. Wydawane jest przez Agencję Bezpieczeństwa Wewnętrznego (ABW) lub Służbę Kontrwywiadu Wojskowego (SKW) po przeprowadzeniu postępowania bezpieczeństwa przemysłowego. W przypadku przedsiębiorcy wykonującego działalność jednoosobowo i osobiście zdolność do ochrony informacji niejawnych potwierdza poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli tajności „poufne" lub wyższej, wydawane przez ABW albo SKW i zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych, wydawane przez ABW albo SKW. W przypadku, gdy przedsiębiorca zamierza wykonywać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", świadectwo nie jest wymagane.

Ustawa zawiera szereg rozwiązań mających na celu uproszczenia systemu ochrony informacji niejawnych, a także dostosowania tegoż systemu do panujących standardów międzynarodowych.

W art. 1 ustawy określono zakres obowiązywania ustawy oraz podmioty, do których ma ona zastosowanie. W nowej ustawie, w art. 2 zostały doprecyzowane m.in. takie definicje, jak przedsiębiorca, kierownik przedsiębiorcy, przetwarzanie informacji niejawnych, ryzyko, szacowanie ryzyka i zarządzanie ryzykiem. Uregulowany został katalog postępowań, do których mają zastosowanie przepisy Kodeksu postępowania administracyjnego, a wśród nich znalazły się postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego. Art. 4 oraz 8 regulują zasady udostępniania informacji niejawnych oraz zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych.

Art. 5 to podział i charakterystyka nowych klauzul tajności. Największa zmiana dotyczy dotychczasowej „tajemnicy służbowej", ponieważ zrezygnowano z oznaczania klauzulami „poufne" lub „zastrzeżone" informacji chronionych na podstawie innych ustaw, a definicje tych klauzul odniesiono jedynie do ewentualnych szkód, które ujawnienie informacji mogłoby przynieść dla bezpieczeństwa i interesów RP. Art. 6 określa zasady znoszenia lub zmiany klauzuli tajności. W ustawie zrezygnowano ze zdefiniowanych okresów obowiązywania klauzul tajności na rzecz możliwości ich zniesienia lub zmiany w przypadku ustania, lub zmiany ustawowych przesłanek ochrony. Art. 7 określa ścisły katalog informacji podlegających ochronie bez względu na upływ czasu, w stosunku do których zniesienie klauzuli tajności nie będzie możliwe. Są to informacje mogące identyfikować funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania czynności operacyjno-rozpoznawczych, a także osoby udzielające pomocy w wykonywaniu tych czynności.

Ustawa wprowadza także w art. 9 możliwość odwołania się odbiorcy materiału od decyzji wytwórcy dotyczącej nadania klauzuli tajności do ABW lub SKW, a w przypadku sporu z jedną z tych służb – do Prezesa Rady Ministrów. W dotychczasowym systemie

odbiorca mógł tylko apelować do wytwórcy o zmianę nieprawidłowej klauzuli. Ta możliwość powinna wpłynąć na ograniczenie liczby przypadków bezpodstawnego zawyżania lub zaniżania klauzul tajności.

W rozdziale 3 ustawy, a więc w art. 10-18, określono zadania ABW, SKW, kierowników jednostek organizacyjnych oraz pełnomocników i pionów ochrony. Wprowadzona została instytucja jednej krajowej władzy bezpieczeństwa, odpowiedzialnej za ochronę informacji niejawnych wymienianych z NATO i Unią Europejską. Funkcję krajowej władzy bezpieczeństwa pełni Szef ABW, natomiast jej zadania wobec podmiotów sfery wojskowej będą wykonywane za pośrednictwem Szefa SKW. W jasny sposób zostały uregulowane zasady prowadzenia przez ABW i SKW kontroli stanu zabezpieczenia informacji niejawnych. Uzupełniono także zakres kontroli o możliwość żądania udostępnienia systemów teleinformatycznych nieposiadających akredytacji, ale wyłącznie w przypadku uprzedniego ustalenia okoliczności wskazujących na przetwarzanie w tych systemach informacji niejawnych. Rozszerzono także zakres kontroli prawidłowości postępowań sprawdzających. Do tej pory takiej kontroli podlegały wyłącznie postępowania prowadzone przez pełnomocników ochrony. Postępowania prowadzone przez ABW i SKW nie podlegały kontroli, z wyjątkiem postępowania odwoławczo-skargowego w przypadku odmowy lub cofnięcia poświadczenia bezpieczeństwa. Proponowane zapisy przewidują możliwość kontrolowania postępowań prowadzonych przez ABW i SKW – przez Prezesa Rady Ministrów.

Zasady prowadzenia szkoleń poprzedzających udostępnienie informacji niejawnych zostały uregulowane w art. 19-20. Wszystkie osoby mające dostęp do informacji niejawnych będą szkolone w zakresie ochrony tych informacji nie rzadziej niż co 5 lat. Potwierdzeniem odbycia szkolenia jest zaświadczenie. Obowiązkowym szkoleniom podlegają kierownicy jednostek organizacyjnych. Pełnomocnicy ochrony mają obowiązek przeprowadzenia szkoleń pracowników w zakresie ochrony informacji niejawnych.

Tryb prowadzenia postępowań sprawdzających wobec osób mających uzyskać dostęp do informacji niejawnych został określony w art. 21-34. Zniesiony został obowiązek prowadzenia postępowań sprawdzających wobec osób, które mają uzyskać dostęp do informacji niejawnych o klauzuli „zastrzeżone". Dostęp do informacji niejawnych o klauzuli „zastrzeżone" jest możliwy na podstawie pisemnego upoważnienia kierownika jednostki organizacyjnej po odbyciu stosownego przeszkolenia. Nowa ustawa wprowadza dwa rodzaje postępowań sprawdzających. Zwykłe postępowania sprawdzające będą prowadzone przez pełnomocników ochrony wobec osób ubiegających się o dostęp do informacji niejawnych o klauzuli „poufne". Poszerzone postępowania sprawdzające będą prowadzone przez ABW lub SKW wobec osób ubiegających się o dostęp do informacji niejawnych o klauzuli „tajne" i „ściśle tajne", a w niektórych przypadkach również „poufne". Stronami postępowań będą wszyscy kierownicy jednostek organizacyjnych, niezależnie od klauzuli. W art. 24-27 określono cele postępowania sprawdzającego, czynności prowadzone w toku postępowania sprawdzającego, przyczyny zawieszenia takiego postępowania oraz podstawy jego zakończenia. Art. 29 określa, co zawiera i kiedy jest wydawane poświadczenie bezpieczeństwa. W art. 30 precyzuje przyczyny odmowy wydania poświadczenia bezpieczeństwa. Art. 33 reguluje zasady prowadzenia kontrolnego postępowania sprawdzającego w przypadku ujawnienia informacji kwestionujących dawanie rękojmi zachowania tajemnicy przez osobę posiadającą poświadczenie bezpieczeństwa. Wprowadzona została procedura wstępnej weryfikacji niepotwierdzonych

negatywnych informacji dotyczących osoby sprawdzanej. Sprecyzowano, który organ jest właściwy do wszczęcia kontrolnego postępowania sprawdzającego, stwierdzając, że jest to ten organ, który byłby właściwy do wszczęcia w danym momencie kolejnego postępowania sprawdzającego. Art. 34 z kolei precyzuje, kiedy nie przeprowadza się postępowania sprawdzającego wobec osób legitymujących się ważnym poświadczeniem bezpieczeństwa do danej klauzuli. Do katalogu osób mających dostęp do informacji niejawnych bez postępowania sprawdzającego została dopisana osoba wybrana na urząd Prezydenta RP ze względu na szczególną pozycję takiej osoby w systemie władzy państwowej. Postępowania sprawdzające wobec kandydatów na wysokie stanowiska państwowe będą kończyły się wydaniem poświadczenia bezpieczeństwa, a nie opinii, ponieważ niejednokrotnie zdarzało się, że osoby, które uzyskały pozytywną opinię, ale nie zostały powołane na stanowisko, po upływie krótkiego czasu musiały ponownie poddawać się postępowaniu sprawdzającemu w celu uzyskania poświadczenia bezpieczeństwa.

Postępowanie odwoławcze i skargowe oraz podstawy wznowienia postępowania określa rozdział 6 ustawy. Art. 34 reguluje tryb oraz termin odwoływania się od decyzji o odmowie lub cofnięciu poświadczenia bezpieczeństwa oraz składania skarg do sądu administracyjnego na decyzję organu odwoławczego. W art. 39-41 wprowadzono także możliwość wznowienia zakończonego ostateczną decyzją postępowania sprawdzającego lub kontrolnego. Art. 35 precyzuje, że odwołanie do Prezesa Rady Ministrów od decyzji o odmowie lub cofnięciu poświadczenia bezpieczeństwa przysługuje nie tylko osobom, wobec których postępowanie było prowadzone przez ABW lub SKW, ale także w przypadku postępowań prowadzonych przez służby uprawnione do samodzielnego prowadzenia poszerzonych postępowań sprawdzających. Art. 36 jednoznacznie określa, jakie decyzje lub postanowienia mogą zostać wydane przez organ odwoławczy.

Zasady organizacji kancelarii tajnych i środki bezpieczeństwa fizycznego, do wdrożenia których są zobowiązane jednostki organizacyjne przetwarzające informacje niejawne, regulują art. 42-47 w rozdziale 7 ustawy. Wprowadzony został obowiązek ustalenia przez kierowników jednostek organizacyjnych poziomu zagrożenia ujawnienia informacji niejawnych i szacowania ryzyka. Obowiązek organizacji kancelarii tajnej będą miały jedynie jednostki organizacyjne dysponujące informacjami oznaczonymi klauzulami „ściśle tajne" lub „tajne". Zasady obiegu informacji niejawnych oznaczonych klauzulą „poufne" będzie określał kierownik jednostki organizacyjnej – art. 42-43. Na kierowniku jednostki organizacyjnej spoczywa obowiązek informowania odpowiednio ABW lub SKW o utworzeniu lub likwidacji kancelarii tajnej z określeniem klauzuli tajności informacji będących w dyspozycji tej jednostki. Wykaz jednostek organizacyjnych, które zorganizowały kancelarie tajne, będzie dostępny dla wszystkich zainteresowanych podmiotów. Określenie poziomu zagrożeń nieuprawnionego dostępu do informacji niejawnych oraz stosowanie środków ochrony fizycznej odpowiednich do tego poziomu nakazują art. 43 i 45. Możliwe jest także tworzenie komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, podstawy takie przewiduje art. 44.

Zasady ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych unormowane zostały w art. 48-53. Art. 48 wprowadza nową zasadę polegającą na tym, że akredytacji bezpieczeństwa teleinformatycznego dla systemów przetwarzających informacje oznaczone klauzulą „zastrzeżone" udziela kierownik jednostki organizacyjnej, w której funkcjonuje system lub

- w przypadku systemu obsługującego wiele podmiotów – kierownik jednostki organizującej system. Obowiązkiem kierownika jednostki organizacyjnej, który udzielił akredytacji dla systemu przetwarzającego informacje oznaczone klauzulą „zastrzeżone", będzie przekazanie ABW lub SKW – zgodnie z kompetencją – dokumentacji bezpieczeństwa teleinformatycznego akredytowanego systemu. Nowością jest wprowadzenie świadectwa akredytacji bezpieczeństwa teleinformatycznego, które jest potwierdzeniem udzielenia przez ABW lub SKW akredytacji dla systemu przetwarzającego informacje niejawne o klauzuli „poufne" lub wyższej Świadectwo akredytacji zastąpi dotychczasowy certyfikat akredytacji. Najistotniejszym elementem dokumentu szczególnych wymagań bezpieczeństwa jest ocena ryzyka dla bezpieczeństwa informacji niejawnych oraz zarządzanie tymże ryzykiem. Art. 50 określa zasadę, że urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych podlegają procesowi certyfikacji prowadzonej przez ABW lub SKW. Certyfikacji podlegają urządzenia i narzędzia kryptograficzne służące do ochrony informacji niejawnych od klauzuli „zastrzeżone". Wprowadzono także zasadę certyfikowania środków ochrony elektromagnetycznej przeznaczonych dla informacji niejawnych o klauzuli „poufne" lub wyższej. Certyfikacja środków ochrony elektromagnetycznej oraz urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych prowadzona będzie przez ABW lub SKW. Art. 51 wyłącza z obowiązku akredytacji bezpieczeństwa teleinformatycznego systemy teleinformatyczne, których istotą jest to, że służą wyłącznie do pozyskiwania i przekazywania w sposób niejawny informacji uzyskanych w trakcie czynności operacyjno-rozpoznawczych przez uprawnione do tego podmioty. Z akredytacji wyłączono też systemy teleinformatyczne wykorzystywane przez służby wywiadowcze poza granicami RP podczas wykonywania czynności operacyjno-rozpoznawczych oraz wydzielone stanowiska na terytorium RP służące służbom wywiadowczym do odbierania i przetwarzania tych informacji. Art. 52 określa zakres zadań kierownika jednostki organizacyjnej. Natomiast art. 53 to podstawa do ustalania wysokości opłat związanych z bezpieczeństwem teleinformatycznym.

Bezpieczeństwo przemysłowe uregulowane jest w art. 54-71, w których określono zasady ochrony informacji niejawnych przekazywanych przedsiębiorcom podczas wykonywania umów albo zadań wynikających z przepisów prawa. W zależności od stopnia zdolności do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej wydaje się świadectwo odpowiednio: pierwszego stopnia – potwierdzające pełną zdolność przedsiębiorcy do ochrony tych informacji, drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych, a także trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach – art. 55. Postępowanie bezpieczeństwa przemysłowego jest prowadzone na wniosek przedsiębiorcy. Wniosek nie wymaga uzasadnienia. We wniosku przedsiębiorca określa stopień świadectwa oraz klauzulę tajności informacji niejawnych, których zdolność do ochrony ma potwierdzać świadectwo. Do wniosku przedsiębiorca dołącza m.in. kwestionariusz bezpieczeństwa przemysłowego – art. 56-58. Postępowanie bezpieczeństwa przemysłowego obejmuje sprawdzenie przedsiębiorcy i postępowania sprawdzające wobec określonych osób. Postępowanie bezpieczeństwa przemysłowego powinno być zakończone w terminie nie dłuższym niż 6 miesięcy, licząc od dnia przedłożenia wszystkich dokumentów niezbędnych do jego przeprowadzenia. ABW albo SKW zawiesza lub podejmuje postępowanie bezpieczeństwa przemysłowego na wniosek przedsiębiorcy. ABW albo SKW

może z urzędu zawiesić postępowanie bezpieczeństwa przemysłowego w przypadku: wydania przez inny organ decyzji nakazującej przedsiębiorcy wstrzymanie prowadzenia działalności gospodarczej, wszczęcia postępowania upadłościowego wobec przedsiębiorcy, nieuregulowania w terminie zobowiązań publicznoprawnych oraz uzależnienia wyniku oceny zdolności przedsiębiorcy do ochrony informacji niejawnych od uprzedniego rozstrzygnięcia zagadnienia wstępnego przez inny organ lub sąd. ABW albo SKW podejmuje z urzędu postępowanie bezpieczeństwa przemysłowego zawieszone na podstawie wymienionych wyżej przypadków po ustaniu przyczyn zawieszenia. Postępowanie bezpieczeństwa przemysłowego kończy się wydaniem przez ABW albo SKW świadectwa zgodnie z wnioskiem przedsiębiorcy albo decyzją o odmowie wydania świadectwa lub decyzją o umorzeniu postępowania bezpieczeństwa przemysłowego – art. 59-67.

W rozdziale 10 doprecyzowano zasady tworzenia i prowadzenia ewidencji i udostępnianie danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego - art. 72-73.

Ankieta Bezpieczeństwa Osobowego jest załącznikiem do ustawy.

Nowa ustawa wprowadza zmiany w wielu obowiązujących ustawach, w których znajdziemy regulacje dotyczące informacji niejawnych. Przeredagowano pojęcia „służby ochrony państwa" – zastępując je sformułowaniem „ABW lub SKW" oraz pojęcia „tajemnica państwowa" i „tajemnica służbowa" – zastąpiono określeniami poszczególnych klauzul albo terminem „informacje niejawne".

Wszystkie poświadczenia, zaświadczenia i świadectwa wydane pod rządami starej ustawy zachowają ważność na okres w nich wskazany. Na organy nałożono obowiązek przeprowadzenia w ciągu trzech lat przeglądu wszystkich materiałów wytworzonych pod rządami starej ustawy pod kątem ewentualnej zmiany lub zniesienia klauzuli tajności.

Anita Jackiewicz - prawnik z wykształcenia, specjalizuje się w prawie pracy i prawie europejskim.

Zapraszamy do udziału

WARSZTATY
KREDYT KONSUMENCKI W NOWYM KSZTAŁCIE, CZYLI O IMPLEMENTACJI DYREKTYWY 2008/48/WE W POLSCE
12 maja 2011 r., Warszawa

Dlaczego warto wziąć udział w warsztatach?
- Dowiedzą się Państwo o zmianach, które rewolucjonizują rynek kredytów konsumenckich.
- Dowiedzą się Państwo o zmianach, które odnoszą się bezpośrednio do działalności nie tylko instytucji finansowych (banków), ale wszystkich przedsiębiorców udzielających kredytów konsumenckich.
- Dowiedzą się Państwo o przygotowywanych zmianach, które wkraczają w finalny etap, a wymagają przemyślenia strategii postępowania już dziś.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Jaka będzie przyszłość elektronicznej administracji? Część I - trendy

Dariusz Bogucki

Niezmiernie ważnym, nie tylko dla polskiej branży ICT, wydarzeniem Polskiej Prezydencji w UE będzie odbywająca się co dwa lata Konferencja Ministerialna UE nt. administracji elektronicznej (eGovernment). Komisja Europejska traktuje konferencje jako ważny element kreowania polityki w zakresie społeczeństwa informacyjnego zarówno na szczeblu ogólnoeuropejskim, jak i polityk krajowych. Tegoroczna VI Konferencja ma odbyć się w dniach 17-19 listopada 2011 roku w Poznaniu. Warto zatem bacznie przyjrzeć się, co dzieje się w obszarze zwanym elektroniczna administracją (albo eGovernment). Bo dzieje się naprawdę wiele.

Co to jest elektroniczna administracja?

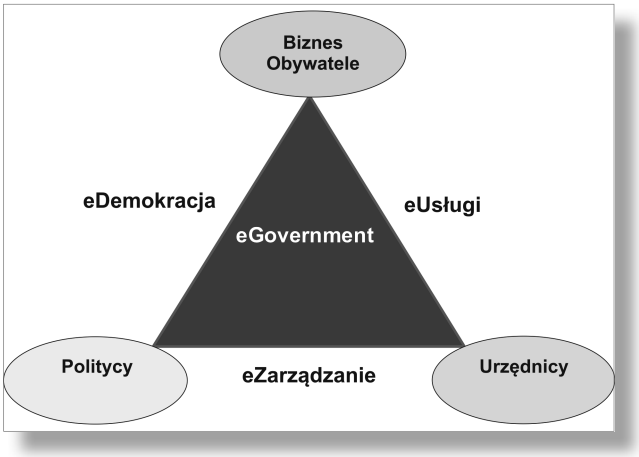
W polskiej administracji publicznej pojęcie elektronicznej administracji (eGovernment) utożsamiane jest od wielu lat z usługami świadczonymi na drodze elektronicznej przez urzędy (eUsługi). Na tle trendów ogólnoświatowych należy uznać, że jest to podejście zachowawcze. Faktycznie, u podstaw elektronicznej administracji leżała idea wykorzystania możliwości technologii ICT do usprawnienia funkcjonowania administracji w kontaktach z firmami/obywatelami. Jednak już Jane E. Fountain w fundamentalnej dla eGovernment książce z 2001 r. *"Building the Virtual State"* widziała rozwój e-administracji znacznie szerzej: jako proces dostosowania struktury administracji i sposobu rządzenia (governance) do zmian społecznych będących skutkiem rewolucji, jaką niosą technologie teleinformatyczne.

Także badacze związani z ONZ i Bankiem Światowym uważają utożsamianie eGovernment z samymi usługami elektronicznymi za zdecydowanie przestarzałe. Warto tu zacytować Sharon Dawes, Dyrektor Centrum Nowych Technologii dla Administracji z Uniwersytetu w Albany, która w publikacji *„The Future of E-Government"* formułuje następującą definicję: „eGovernment jest to proces wykorzystania technologii informatycznych zmierzający do poprawy procesu rządzenia, większego zaangażowania obywateli i świadczenia usług administracji."

W krajach Unii Europejskiej od czasu uruchomienia inicjatywy strategicznej i2010 utrwaliło się pojmowanie eGovernment jako wszystkich **form kontaktu klienta z administracją wykorzystujących technologie ICT** (co przytacza nawet polska Wikipedia - http://pl.wikipedia.org/wiki/E-government). Administracja publiczna, będąc zarówno odbiorcą, jak i dostawcą rozwiązań ICT (nie tylko eUsług), przyczynia się w znacznym stopniu do rozwoju sektora ICT, stymulując wykorzystanie technologii teleinformatycznych wśród obywateli i podmiotów gospodarczych. Dlatego w opinii Komisji elektroniczna administracja jest ważnym czynnikiem budowy gospodarki opartej na wiedzy.

W tym kierunku idzie znacznie szerszy model zaproponowany w projekcie badawczym PRISMA[1] i rozwinięty później przez Vinnova (Szwedzka Agencja Innowacji w Administracji). Przywoływany tu eGovernment definiuje on jako **taki sposób kontaktu obywatela z urzędem**, **który dzięki**

1 Realizowanego w ramach 5 Programu Ramowego UE na rzecz badań i rozwoju.



Rys. 1

możliwościom technologii teleinformatycznych zapewnia aktywny dialog obydwu stron kontaktu.

Tę bardzo pojemną definicję najlepiej ilustruje powyższy trójkątny diagram (za Vinnowa Report VR 2006: 11 „*The future of eGovernment, Scenarios 2016*" oraz Vinnova Report VR 2009: 28 *„eGovernment of Tomorrow, Future Scenarios for 2020").*

Innymi słowy rozwoju eGovernment dziś nie można już sprowadzić tylko i wyłącznie do jednego wymiaru – do wdrażania usług elektronicznych. Nie tylko dlatego, że równie istotne są funkcje z pozostałych boków diagramu:

- **eDemokracji**, związane z wykorzystaniem technologii ICT do stymulowania funkcji społeczeństwa obywatelskiego, niesprowadzające się tylko do kwestii tzw. e-Wyborów,
- **eZarządzania** (eManagement), czyli systemów umożliwiających przy pomocy ICT wykorzystywanie machiny państwowej do sprawnego zarządzania państwem (governance).

Ale prawdziwa wartość dodana powstaje „pomiędzy" bokami powyższego trójkąta.

Rząd Zjednoczonego Królestwa intensywnie rozwija system e-petycji, dzięki którym wnioski obywatelskie zgłaszane via Internet popierane przez 100 tys. osób staną się przedmiotem debat w Izbie Gmin. Najcelniejsze mają się zmieniać w pilotowane przez posłów ustawy. Niewątpliwie dużą trudnością jest wyławianie cennych inicjatyw obywatelskich w morzu petycyjnego spamu. Co więcej, system ten pozwala też na bieżąca ocenę jakości funkcjonowania poszczególnych aktów prawnych – problemów, jakie wiążą się z ich wykonaniem w praktyce tak, aby stanowione prawo było coraz lepsze i doskonalsze. Nie jest to więc system, który można zaliczyć jednoznacznie do któregoś z „boków trójkąta, a takich przykładów jest więcej.

Nowy paradygmat funkcjonowania elektronicznej administracji

Jak już wspomniano, wraz z przygotowaniem inicjatywy i2010 Komisja Europejska zmieniła paradygmat rozwoju elektronicznej administracji: **miejsce wspierania rozwoju eUsług (eServices) zastąpiło wspieranie wykorzystania technologii ICT do wzrostu wartości usług administracji.** Ta zmiana jest mocniej eksponowana w nowych dokumentach strategicznych, jakie Komisja Europejska przygotowuje na okres finansowania do roku 2020, by wymienić tylko inicjatywy

„Europejska Agenda Cyfrowa" czy „Unia Innowacji". Warto dlatego przyjrzeć się temu bliżej.

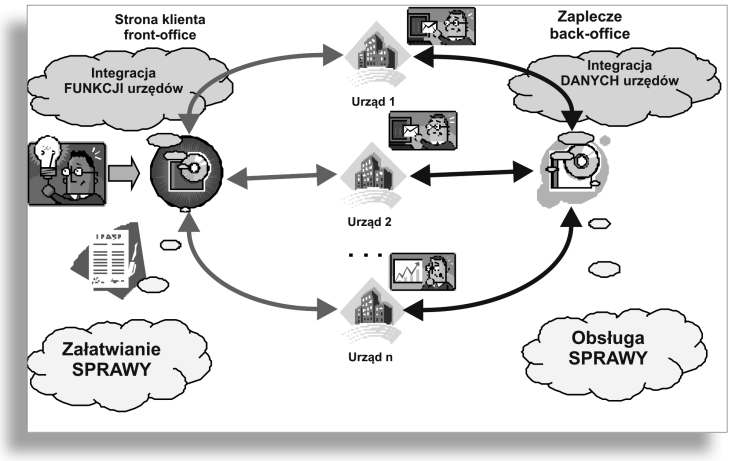
Przyczyny tej zmiany wyjaśniają Jeremy Millard i Edwin Horlings w opracowaniu *„Value for Citizens. A vision of public governance in 2020"* wykonanym na zlecenie Komisji Europejskiej na bazie wspomnianego projektu PRISMA. Wskazują oni, że badania nt. eUsług w krajach UE potwierdzały, że samo wdrażanie eUsług nie prowadziło do poprawy jakości w kontaktach klienta z urzędem, a jedynie do informatyzacji funkcji urzędu. Dlatego też uważają, że miejsce wdrażania eUsług winno zastąpić budowanie zintegrowanego „Urzędu Sieciowego", wspierającego innowacyjne podejście do usług administracji i ich transformacji zgodnie z potrzebami klientów. Ich zdaniem w ten sposób dzięki ICT powstanie „wartość dodana", wyrażająca się w jakości funkcjonowania państwa. Millard i Horlings wskazują, że owa wartość będzie kreowana w wielu płaszczyznach: w **wymiarze prywatnym** (w interakcji klientów-obywateli + firm z urzędem), w **wymiarze wspólnym** – związanych ze wspólnymi potrzebami klientów (społecznościom) i **publicznym**, generowanym przez dobrze i sprawnie funkcjonujący aparat państwa.

Przyjęcie tego paradygmatu zmienia kompletnie ramy budowania systemów IT dla administracji, zmieniając „aksjomat" autonomii funkcjonowania urzędów i ich **systemów sektorowych** (w nomenklaturze Komisji Europejskiej). W administracji traktowanej całościowo oprócz systemów sektorowych funkcjonować muszą wspólne dla wszystkich **systemy horyzontalne** – integrujące sługi „po stronie klienta" i dane „od strony zaplecza urzędów" (patrz poniższy rysunek).

Taka infrastruktura umożliwia z jednej strony wprowadzenie nowych kategorii usług, a z drugiej wprowadza czytelne mechanizmy sprzyjające przejrzystości funkcjonowania administracji.

Wartość wdrożonych usług w miejsce korzyści z wdrażania eUsług

Opisane wyżej zmiany wpisują się w głębszy proces, zgodnie z którym idea Nowego Zarządzania Publicznego (New Public



Rys. 2

Management - NPM), która zdominowała myślenie o administracji w ciągu ostatnich dziesięciu lat, jest stopniowo zastępowana nowymi ideami, z których najdynamiczniej rozwija się **Zarządzanie Wartością Publiczną (Public Value Management – PVM)**.

Przypomnijmy, że pod pojęciem New Public Management była rozwijana od lat połowy 80 na podstawie doświadczeń nowozelandzkich (J. Boston, J. Martin, J. Pallot, P. Walsh, *"Public Management: The New Zealand Model"* 1996) idea implementacji metod zarządzania firm komercyjnych do poprawy funkcjonowania administracji. Początkowo mianem NPM było określane przedsiębiorcze zarządzanie instytucjami publicznymi przeciwstawiane zbiurokratyzowanemu zarządzaniu, opartemu na hierarchicznej strukturze organów władzy oraz ich funkcjonalnej specjalizacji. W procesie doskonalenia systemu zarządzania w sektorze publicznym nastąpiło nie tylko adaptowanie metod i technik zarządzania z sektora prywatnego, ale także otwarcie na sektor organizacji non-profit oraz włączenie ich do realizacji zadań publicznych.

Teoria NPM stawiała w szczególności tezę, że tzw. „orientacja na rynek" (klienta) w sektorze publicznym przyczyni się do większej efektywności finansowej funkcjonowania administracji, bez negatywnych skutków ubocznych dla innych zadań administracji.

Rezultatem zmiany filozofii rządzenia sektorem publicznym było podjęcie szeregu reform, których celem miało być lepsze wykorzystanie zasobów znajdujących się pod kontrola państwa. Wysiłki skoncentrowane zostały na:

- ograniczeniu bezpośredniego udziału sektora publicznego w gospodarce,
- intensyfikacji prywatyzacji własności publicznej,
- zwiększeniu efektywności w obszarze klasycznych dóbr i usług publicznych,
- wzmocnieniu pozycji obywatela na rynku dóbr i usług, a w szczególności zastąpieniu obywatela-pasywnego płatnika podatków obywatelem-konsumentem,
- zmniejszenie aparatu państwowego oraz oddzieleniu różnych centralnych instytucji państwowych podejmujących decyzje w zakresie alokacji dóbr i usług od instytucji peryferyjnych w postaci agencji i innych pozarządowych organizacji, których zadaniem jest działalność operacyjna.

Wadą NPM było mechaniczne adaptowanie reguł panujących w biznesie do hierarchicznych zasad administracji, co prowadziło niekiedy do dziwacznych oszczędności skutkujących pogorszeniem obsługi klienta przez urząd. Tak było np. w przypadku systemów ICT urzędu (Patrick Dunleavy, Helen Margetts et al, *„New public management is dead: Long live digital era governance*").

Idea PVM zakłada, że dzięki ICT formy kontaktu pomiędzy obywatelami, biznesem i administracją przestają być jednowymiarowe i ograniczone tylko do „załatwiania spraw". Istotna jest zatem nie sama usługa, ale wartość jaką daje społeczeństwu. System budowania owej wartości prowadzi docelowo do nowej formy zarządzania państwem, bazującej na społecznym konsensusie.

W tym sensie pojęcie elektronicznej administracji wykracza zdecydowanie poza sensu stricte eUsługi, obejmując szeroko pojęte kwestie demokratycznej odpowiedzialności rządzących, społecznego uczestnictwa w zarządzaniu państwem, przejrzystości i legalności działań administracji, demokracji uczestniczącej w kontekście wykorzystania ICT. PVM zakłada, że możliwości nowych technologii tworzą pole dla nowych jakościowo usług i głębokiej transformacji

obecnych stosunków w duchu instytucjonalnej innowacyjności. Jednym z filarów idei PVM jest to, że administracja musi sprawować swoje funkcje wobec obywateli fizycznie rozrzuconych po całym świecie (vide „województwo londyńskie"). Praktycznie oznacza to, że cała administracja będzie wkrótce świadczyć usługi transgraniczne w reżimie 24/7!

Identyczne, całościowe podejście prezentują od roku 2008 badacze ONZ opracowujący raporty *„eGovernment Readiness Index",* co wyraża się tym, że aspekt rozwiązań integrujących funkcje i dane jest bardzo wysoko w nim ważony. Praktyczny brak takich rozwiązań w Polsce jest główna przyczyną głośno komentowanego w kraju spadku Polski aż o 12 pozycji w rankingu z roku 2010.

Nowy model dojrzałości eUsług

Istotne zmiany następują też w samym pojmowaniu eUsług administracji. Klasyczny już model dojrzałości usług świadczonych przez administrację zaproponowany przez Gartner Group w roku 2002 (Andrea Di Maio *"Four phases of eGovernment"*) wyróżniał cztery poziomy zaawansowania:

1. **Informacja** (Presence), sprowadzający się do „zaistnienia urzędu w Sieci poprzez stronę WWW. Komunikacja jest jednokierunkowa i obejmuje informacje o charakterze ogólnym, np. dane kontaktowe.
2. **Interakcja** (Interaction), w którym strona Urzędu zawiera informacje niezbędne do załatwiania konkretnych spraw, np. znajdują się tam linki do formularzy elektronicznych, które klient może wydrukować i wypełnić, a także łącza do stron innych urzędów związanych z dana sprawą.
3. **Transakcja** (Transaction), gdy sprawa może być już całkowicie załatwiona poprzez złożenie wniosku poprzez Sieć w oparciu o dane, jakie już posiada na ten temat Urząd (np. przedłużenie prawa jazdy, złożenie aplikacji do pracy itd.).
4. **Transformacja** (Transformation), w którym systemy urzędu pozwalają, aby sprawa była załatwiona całkowicie via Internet w komunikacji dwukierunkowej pomiędzy urzędem a klientem.

Praktyka pokazała, że osiągnięcie poziomu czwartego jest znacznie trudniejsze niż to się dzieje np. w systemach elektronicznego handlu. Di Maio w 2009 r. w *"Blurring of government"* wskazuje na następujące czynniki:

- Jedna sprawa klienta najczęściej składa się z kilku drobnych spraw załatwianych przez poszczególne urzędy. Mamy zatem do czynienia z rozproszeniem danych dotyczących jednej sprawy w wielu systemach urzędów, co bez integracji systemów urzędów uniemożliwia praktycznie realizację takiego scenariusza.
- Zmiany systemu wartości i oczekiwań, zwłaszcza młodego pokolenia, jakie niesie masowe wykorzystanie systemów zaliczanych do Web 2.0, np. portali społecznościowych, co rodzi rosnący nacisk na skuteczność, ale i przejrzystość funkcjonowania tradycyjnie zorganizowanej hierarchicznie administracji.

Dlatego też obecnie mówi się o piątym poziomie dojrzałości usług:

5. **Personalizacja** (personalization), zakładająca że po stronie administracji (nie pojedynczego urzędu) funkcjonują mechanizmy bezpośredniej, osobistej interakcji z klientem, opierającej się na przejrzystym działaniu urzędu i budowaniu zaufania np. system kont osobistych, kanały kontaktu ze specjalistą wspierającym załatwianie sprawy itd.

Trzeba tu wspomnieć o jeszcze jednym ważnym aspekcie: w większości krajów UE architekci elektronicznej administracji zdają sobie sprawę, że już niedługo jej głównym klientem będą seniorzy. Ludność Europy starzeje się wszak w szybkim tempie: prognozy demograficzne dla krajów EU-27 wskazują,

że w latach 2010–2030 wraz z przechodzeniem na emeryturę pokolenia wyżu demograficznego liczba osób w wieku między 65 a 80 lat wzrośnie prawie o 40%, by w 2050 roku stanowić ok. 30% populacji! Dlatego też w większości krajów UE wdrażane są coraz liczniejsze przykłady udanych rozwiązań eGovernment dostosowanych do specyfiki ludzi starszych. W tych systemach wielką role odgrywa osobisty kontakt klienta z partnerem z drugiej strony, nie tyle przedstawicielem urzędu, ale właśnie partnerem w załatwianiu spraw życiowych.

Stawia to w zupełnie nowym świetle kwestie tzw. kompetencji cyfrowych. W Polsce mamy sytuację, że z Internetu korzysta już ponad połowa Polaków w wieku 16+ (50,9% w marcu 2009 r. wg. *„Diagnozy Społecznej 2009”*). Wskaźnik ten nie rozkłada się równo w kategoriach wiekowych i geograficznych. Różnice pomiędzy osobami, które korzystają z technik informacyjno-komunikacyjnych i tymi, które z nich nie korzystają, są olbrzymie. W „*Diagnozie Społecznej 2009”* dr Dominik Batorski stawia wręcz tezę, że mamy w tej chwili dwie Polski:

- jedną mniejszą, nowoczesną, młodą, dobrze wykształconą,
- drugą starszą, znacznie większą, tradycyjną, słabo wykształconą i słabo radzącą sobie w obecnych czasach.

Doświadczenia innych krajów UE pokazują jednoznacznie, że bez podjęcia zdecydowanych działań na rzecz podniesienia poziomu kompetencji cyfrowych ludzie „drugiej grupy” nigdy nie skorzystają z usług elektronicznej administracji, co stanie się wkrótce poważną barierą wzrostową.

Podsumowanie

W kwietniu 2010 roku Organizacja Narodów Zjednoczonych opublikowała raport „*United Nations E-Goverment Survey 2010. Leveraging e-goverment at a time of financial and economic crisis”*, stanowiący analizę postępów we wdrażaniu rozwiązań eGovernment. Polska od poprzedniego rankingu z roku 2008 spadła aż o 12 pozycji i jest 45 – przedostatnia spośród krajów UE (46 jest Rumunia). To pozycja zdecydowanie nieodpowiadająca potencjałowi naszego kraju. Zwłaszcza że na poprzednich edycjach Konferencji Ministerialnej w 2003 i 2005 roku polskie systemy eGovernment (Celina i KSI ZUS) zdobywały nagrody.

Opisane w artykule trendy wskazują, że elektroniczna qdministracja przechodzi obecnie głęboką zmianę. Pomysły na to, jak papierowy urząd przenieść do Internetu, umarły śmiercią naturalną podobnie jak tzw. 20 podstawowych usług e-Administracji, o których Komisja Europejska już dawno zapomniała (sformułowano je w… 2002 roku!).

Powstają za to nowe, innowacyjne rozwiązania, które tradycyjnie pojmowany urząd zastępują nową treścią i formą, ale o tym napiszemy w kolejnej części opracowania.

Dr inż. Dariusz Bogucki - Dyrektor ds. Sektora Publicznego, EFICOM SA.

Podpis urzędniczy 2.0

Michał Tabor

Wstęp

W trakcie budowy rozwiązania dla nowego - elektronicznego dowodu osobistego, w ramach projektu pl.ID, powstał pomysł wykorzystania podpisu osobistego nie tylko do kontaktu obywatela z urzędami, ale także jako narzędzie urzędnika lub lekarza do wykonywania jego obowiązków służbowych. Implementacja tego pomysłu znalazła swoje odzwierciedlenie w Kodeksie Postępowania Administracyjnego znowelizowanym Ustawą o dowodach osobistych. Wskazana nowelizacja wejdzie w życie 1 lipca 2011 roku.

Analiza samej inicjatywy wykorzystania dowodu osobistego jako narzędzia pracy urzędnika wydaje się interesująca i należy ją przedyskutować. Skoro wydaje się publiczne pieniądze na narzędzie elektronicznego uwierzytelniania w imię re-używalności efektów projektów finansowanych z pieniędzy publicznych i najlepszego wykorzystania powstałego potencjału technologicznego, należy wykorzystać go w możliwie szerokim spektrum zastosowań. Aby potwierdzić lub zaprzeczyć rzeczywistym zyskom z połączenia dowodu osobistego z elektronicznym identyfikatorem urzędnika, konieczne jest wykonanie analizy bezpieczeństwa wykorzystania dowodu osobistego do składania podpisów przez urzędników oraz przeglądu technologii, w ramach której zaimplementowany ma być podpis osobisty. W tym kontekście także należy zastanowić się, czy obowiązek prawny wykorzystania dowodu osobistego do wykonywania czynności służbowych nie stanowi ważnego precedensu, który będzie powielany nie tylko w zakresie administracji publicznej, ale także w obszarze biznesu.

Dowód osobisty urzędnika

Dowód osobisty jest dokumentem stwierdzającym tożsamość i obywatelstwo, a jego zawartość elektroniczna ma stanowić uzupełnienie podstawowych funkcji tego dowodu. Dowód osobisty, jak czytamy w „Studium wykonalności", ma gwarantować uwierzytelnienie obywatela zgodne z unijnymi koncepcjami narodowego dokumentu identyfikacyjnego (eID) w systemach IT jednostek sektora publicznego, pozwalające na jednoznaczne uwierzytelnienie posiadacza dokumentu tożsamości. A zatem podstawowym celem jest dostarczenie osobie prywatnej narzędzia do wykonywania przez nią jej praw i obowiązków obywatelskich.

Rozdzielenie sfery działania prywatnego od działania służbowego jest jednym z podstawowych praw każdej osoby, niezależnie od tego czy pracuje w firmie prywatnej, jest lekarzem lub urzędnikiem. W ramach każdej z tych sfer, podejmując zobowiązania, ponosi się różną odpowiedzialność prawną. Obywatel, składając podpis, musi mieć pełną świadomość tego, w ramach jakiej sfery działa i z jaką wiąże się to odpowiedzialnością.

Poza ewentualnym zyskiem finansowym związanym z zobowiązaniem urzędników do wykorzystywania przez nich dowodu osobistego z wykonywaniem czynności służbowych wiąże się szereg wątpliwości zarówno w zakresie bezpieczeństwa takiego rozwiązania, jak i jego strony formalnej.

Wykorzystanie narzędzia, jakim jest warstwa elektroniczna dowodu osobistego, do realizacji zadań przez obywateli będących urzędnikami nie może ograniczać praw, ani dawać większej odpowiedzialności związanej z użyciem dowodu osobistego niż ma osoba niebędąca urzędnikiem posługując się tym dokumentem.

Należy jeszcze rozważyć, czy skoro PESEL jest numerem umożliwiającym uzyskanie z rejestru pełnej informacji o danej osobie fizycznej, należy tą daną osobową udostępniać wszystkim adresatom pism urzędowych. Certyfikat służący do weryfikacji podpisu osobistego będzie tą daną zawierał, toteż każde pismo sygnowane podpisem osobistym będzie nie tylko ujawniało pełną datę urodzenia osoby fizycznej, ale także umożliwiało łatwy dostęp do pozostałych danych osobowych danego urzędnika, łącznie z adresem jego zamieszkania.

Weryfikowalność podpisu

Podpis osobisty będzie weryfikowany certyfikatem zawierającym imię, nazwisko i numer PESEL jego posiadacza, a co za tym idzie, będzie identyfikował osobę fizyczną posiadającą obywatelstwo polskie. Natomiast certyfikat nie będzie zawierał informacji dotyczących podmiotu, w imieniu którego podpis został złożony, co w zasadzie stanowi znaczące utrudnienie dla weryfikacji, czy podpis został złożony przez urzędnika działającego w ramach swoich uprawnień, czy przez obywatela w ramach spraw prywatnych. Stosowanie podpisu przez urzędnika czy lekarza wymaga jasnego wskazania, w imieniu jakiego organu on występuje.

Brak wiarygodnego wskazania w imieniu jakiego podmiotu został złożony podpis, może stanowić ważne źródło zagrożeń dla prób posługiwania się dokumentami, pod którymi podpisy zostały złożone przez osoby niebędące urzędnikami oraz poza ich kompetencjami. Natomiast próby zastosowania zabezpieczeń w tym zakresie wymagają utworzenia rejestru urzędników i pełnomocnictw oraz mogą pozbawić urzędnika prawa do prywatności wyrażonego konstytucją i prawem do ochrony danych osobowych.

Zabezpieczenie tego, aby dokumenty sygnowane podpisem osobistym były wiarygodne dla podmiotów je weryfikujących, wymaga zastosowania „pieczęci elektronicznej" urzędu lub innych zabezpieczeń potwierdzających źródło pochodzenia. Na dzień dzisiejszy stosowanie „pieczęci elektronicznej" urzędu nie ma podstawy prawnej zarówno w ustawie o podpisie elektronicznym, jak i ustawie definiującej pieczęcie urzędowe i państwowe (Ustawa o godle). Postawienie wymagania stosowania „pieczęci elektronicznej" wobec wszystkich podmiotów publicznych staje się trudne organizacyjnie i kosztowne.

Użycie podpisu

Podejmując zobowiązania, musimy mieć świadomość, w jakiej roli i w ramach jakich uprawnień je realizujemy. Zdarza się, że występując w tym samym miejscu, raz występujemy prywatnie, a innym służbowo (np. będąc jednocześnie mieszkańcem gminy i urzędnikiem urzędu tejże gminy), inne także ma znaczenie ten sam list wysłany przez osobę prywatną, a inne przez burmistrza lub prezydenta. Obywatel, który jest zobowiązany do posiadania przy sobie dowodu osobistego, np. kupując alkohol w sklepie, nie może ponosić ryzyka, że to samo narzędzie może być użyte do podpisania rozporządzenia. Dlatego konieczne wydaje się rozdzielenie funkcji podpisu osobistego od podpisu urzędniczego, gdzie nie tylko sam fakt złożenia podpisu ma znaczenie, ale także jego rola. Natomiast narzędzie, którym jest dowód osobisty, którego posiadanie przy sobie jest często obowiązkiem prawnym, podlega innym regułom

bezpieczeństwa niż legitymacja służbowa, której zgubienie lub którą posługiwanie się w barze może mieć inne znaczenie.

Dla przykładu, idąc za koncepcją wykorzystania dowodu osobistego jako legitymacji służbowej, można doprowadzić do sytuacji, w której osoba pełniąca obowiązki urzędnicze zawsze jest identyfikowana jako urzędnik, co daje możliwość wywierania nieuprawnionego nacisku w sprawach pozasłużbowych, a z drugiej strony może naruszać prawo do prywatności obywatela.

Nadzór nad podpisami

Dowodu osobistego nie może odebrać osobie fizycznej jego przełożony w przypadku zwolnienia lub zmiany zakresu obowiązków. W tym kontekście stosowanie dowodu osobistego nie daje łatwej fizycznej kontroli nad uprawnieniami poszczególnych pracowników typu: *Jest pan zwolniony – proszę oddać swoją kartę służbową umożliwiającą składanie podpisów w imieniu urzędu.* Stosowanie mechanizmów dowodu osobistego wymagałoby znacznie większej świadomości przełożonych w zakresie stosowanych przez ich pracowników narzędzi do składania podpisu elektronicznego i rodziłaby duże ryzyka związane z tym, że osoby zwalniane miałyby do końca ważności dowodu osobistego możliwość składania podpisów w imieniu organu, w którym pracowały.

Jak pokazują światowe statystyki w zakresie bezpieczeństwa systemów teleinformatycznych, systemy opierające się na bezpieczeństwie logicznym (zapisie uprawnień w bazie danych) w ponad 30% nie likwidują kont i uprawnień zwalnianych pracowników, pozostawiając im dostęp do zasobów. Analizy administracji publicznej w tym zakresie wskazywały na jeszcze większy brak zachowania elementarnych procedur bezpieczeństwa. Natomiast podmioty mają wdrożone i stosowane mechanizmy związane z fizycznym odbieraniem kluczy i identyfikatorów, a odsetek podmiotów, które tego nie realizują, jest niższy niż 5%.

Dowód osobisty jako narzędzie pracy

Utrata dowodu osobistego wymaga zgłoszenia tego faktu, złożenia wniosku o nowy dowód, a następnie otrzymania takiego dokumentu. Proces ten trwa w najlepszym wypadku kilkanaście dni i nie należy się spodziewać jego zasadniczego skrócenia. Jednak utrata dowodu osobistego zazwyczaj nie wpływa na możliwość wykonywania swojej pracy. Stosowanie dowodu osobistego jako narzędzia pracy mogłoby doprowadzić do sytuacji, w której jego utrata i czas potrzebny na wydanie nowego uniemożliwia pełnienie obowiązków służbowych. Do narzędzia służącego do złożenia podpisów służbowych można zastosować zupełnie inną i uproszczoną procedurę wydania i inne mechanizmy chroniące przed utratą (np. możliwość pozostawienia w sejfie). W szczególności procedura potwierdzania tożsamości może opierać się o wewnętrzne kadry i przełożonych, a sama personalizacja takiego identyfikatora może być lokalna lub w najbliższym urzędzie powiatowym.

Podpis osobisty

Dowód osobisty wyposażony w mikroprocesor, który ma być efektem prowadzonego projektu „pl.ID" zgodnie z Ustawą o dowodach osobistych, ma zawierać funkcję umożliwiającą składanie tzw. popisu osobistego. Pełna ustawowa definicja podpisu osobistego ma następującą treść:

Podpis osobisty –dane w postaci elektronicznej, złożone za pomocą danych, służących do składania podpisu osobistego, zawartych w ważnym dowodzie osobistym, które:

- wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, pozwalają na identyfikację posiadacza dowodu osobistego,

- są przyporządkowane wyłącznie do posiadacza dowodu osobistego,
- są powiązane z danymi, do których się odnoszą, w taki sposób, że każda późniejsza zmiana tych danych jest wykrywalna,
- są uzupełnione przez ministra właściwego do spraw wewnętrznych danymi pozwalającymi na określenie czasu złożenia tego podpisu.

Wśród innych cech określonych niniejszą ustawą należy wymienić:

Art. 13. 1. Warstwa elektroniczna dowodu osobistego zawiera:

2) (…) dane służące do składania podpisu osobistego weryfikowane za pomocą certyfikatu podpisu osobistego (…)

Art. 19. 2. Aktywacja certyfikatu podpisu osobistego jest dobrowolna i następuje na wniosek posiadacza dowodu osobistego.

4. Ważność certyfikatu podpisu osobistego jest tożsama z ważnością dowodu osobistego, z zastrzeżeniem art. 22.

5. Certyfikat podpisu osobistego można zawiesić, a następnie wznowić na wniosek posiadacza dowodu osobistego.

6. Zawieszenie certyfikatu podpisu osobistego nie wpływa na ważność dowodu osobistego.

7. Podpis osobisty złożony w okresie zawieszenia certyfikatu podpisu osobistego nie wywołuje skutków prawnych.

Zestawienie tych wszystkich cech wymaga, aby podpis osobisty był realizowany w sposób odmienny od typowego podpisu elektronicznego – tj. w sposób zapewniający kontrolę ważności certyfikatów i uczestnictwo systemu ministra właściwego do spraw wewnętrznych w procesie składania podpisu. Innymi słowy podpis taki jest składany on-line, a aplikacja podpisująca kontaktuje się z systemem MSWiA w procesie powstawania tego podpisu i uzupełniania ten podpis o dane umożliwiające określenie czasu jego złożenia.

Nie można tutaj także mówić o zastosowaniu całkowicie standardowego modelu składania podpisu opartego o Infrastrukturę Klucza Publicznego i mechanizmy oparte o znakowanie czasem i listy OCSP, ponieważ te mechanizmy nie wspierają potwierdzenia czasu złożenia podpisu, a jedynie potwierdzenie, że podpis został złożony przed określoną datą. W standardowym modelu Infrastruktury Klucza Publicznego nie są wspierane mechanizmy weryfikacji tego, czy podpis nie został złożony w okresie zawieszenia certyfikatu.

Dla podpisu osobistego wymagane jest zastosowanie mechanizmu, w którym podpis może być utworzony tylko i wyłącznie wtedy, gdy zostaną spełnione warunki określone ustawą, tj. certyfikat podpisu osobistego jest ważny i nie jest zawieszony, a do podpisu dołączone są dane MSWiA umożliwiające stwierdzenie czasu złożenia podpisu. O takim rodzaju podpisu, tzw. podpisie potwierdzonym, pisałem w artykule „Podpis potwierdzony". Umożliwia on nie tylko weryfikację cech podstawowych, jakimi są ważność certyfikatu, jego aktywacja czy weryfikacja, ew. zawieszenia jego funkcjonowania, ale także szereg innych cech związanych ze środowiskiem i uprawnieniami składającego podpis.

Podpis potwierdzony powstaje przy współudziale tzw. Urzędu Podpisu, bez którego udziału podpis nie może uzyskać swojej

kompletnej i weryfikowalnej postaci. Główną zaletą takiego podpisu jest to, że zaufanie do niego opiera się w głównej mierze na weryfikacji jego integralności certyfikatem i nie wymaga stosowania dodatkowych potwierdzeń dla złożonych podpisów. Ustawa nie wskazuje dodatkowych cech, więc należy zakładać, że stosownie podpisu osobistego będzie ograniczone do podstawowych weryfikacji związanych z ważnością lub ew. zawieszeniem certyfikatu, skutkującymi brakiem możliwości złożenia poprawnie weryfikującego się podpisu osobistego.

Zastosowanie mechanizmów podpisu potwierdzonego dla podpisu osobistego stanowi bardzo ważne wyjście dla uproszczenia procesu weryfikacji podpisów i łatwego modelu budowania zaufania. Zastosowane w podpisie osobistym konieczności współudziału systemu MSWiA w procesie podpisywania daje możliwość zmniejszenia środków ochrony podpisu po stronie weryfikującego.

PKI 2.0

Zastosowanie mechanizmów wykorzystywanych w podpisie osobistym w przyszłej implementacji popisu urzędnika jest kierunkiem, który może w znaczący sposób uprościć mechanizmy podpisu elektronicznego przy jednoczesnym zwiększeniu poziomu bezpieczeństwa jego wykorzystania – zarówno dla podpisującego, jak i strony ufającej. Wykorzystanie mechanizmów podpisu potwierdzonego jest w stanie dostarczyć nowej jakości, rozszerzając proces składania podpisu elektronicznego o możliwości bezpośredniej kontroli nad tym procesem i połączenia go z wewnętrznymi systemami IT zarządzającymi uprawnieniami i dokumentami. Dodatkowo poza podstawową cechą, jaką jest prawo do złożenia podpisu, można kontrolować całe środowisko i szereg cech związanych z samym podpisem elektronicznym w procesie jego tworzenia (M. Tabor, *Podpis elektroniczny powszechnie stosowany - łatwy jak transakcja kartą bankową*, 2010).

Podpis potwierdzony

Podpis potwierdzony jest mechanizmem, w którym warunkiem koniecznym dla jego utworzenia jest uczestniczenie w procesie Urzędu Podpisu (ang. *Signature Authority*), który jest w stanie kontrolować uprawnienia podpisującego i cechy związane z samym podpisywanym dokumentem. W szczególności takimi cechami są:

- sprawdzona data i czas utworzenia podpisu,
- zweryfikowana ważność certyfikatów, które będą służyły do weryfikacji podpisu,
- zweryfikowane uprawnienia osoby podpisującej,
- załączenie wszystkich wymaganych dokumentów do podpisu,
- występowanie dokumentu w systemie EOD urzędu,
- przygotowanie pisma zgodnie z obowiązującym wzorem,
- spełnienie kryteriów akceptacyjnych dokumentu – np. weryfikacja go przez przełożonych,
- miejsce (np. adres ip) komputera, w którym podpis jest składany.

Lista cech weryfikowanych w trakcie składania podpisu może być dynamiczna, zależna od przyjętego rozwiązania i sposobu podpisywania, a jednocześnie dynamicznie zarządzana wewnątrz podmiotu publicznego.

Technologia podpisu potwierdzonego nie wymaga tego, aby Urząd Podpisu (SA) był zaimplementowany wewnątrz podmiotu publicznego, który go używa. Urząd taki może być centralny u ministra właściwego ds. administracji, tak jak to ma miejsce przy podpisie osobistym lub może być współdzielony przez grupę podmiotów, np. w ramach

podziału terytorialnego. Natomiast sama decyzja autoryzacyjna może zależeć od wewnętrznych dla każdego podmiotu publicznego systemów zarządzających uprawnieniami lub wewnętrznego EOD.

Podpis kontrolowany przez EOD

Sprawy prowadzone w urzędach w postaci dokumentów elektronicznych mają odzwierciedlenie w Elektronicznych Systemach Obiegu Dokumentów. W systemach tych zgodnie z instrukcją kancelaryjną proces załatwiania sprawy oraz powstająca dokumentacja powinna mieć odzwierciedlenie w systemie obiegu dokumentów. Urząd, który posiada system obiegu dokumentów, może ustanowić kryterium złożenia podpisu przez urzędnika, ograniczając podpisy tylko do takich dokumentów, które zostały zarejestrowane w EOD i procedura akceptacji jest realizowana zgodnie z regułami wskazanymi w tym systemie. Takie postawienie sprawy uniemożliwia powstanie podpisanego dokumentu poza systemem EOD, zapewnia pełną kontrolę nad wszystkimi procesami związanymi z prowadzeniem sprawy. Jednocześnie obywatel, który otrzyma pismo sygnowane tego rodzaju podpisem, może bez ograniczeń czasowych, konieczności stosowania dodatkowych zabezpieczeń i obawy przed utratą ważności pisma się nim posługiwać, mając jednocześnie referencję do systemu obiegu dokumentów, w którym znajduje się pierwowzór otrzymanego dokumentu.

Podpis z kontrolą uprawnień

Pełnomocnictwo do podpisania dokumentu, w szczególności pełnomocnictwo wydane urzędnikowi przez organ celem jego reprezentowania, określa zakres spraw, uprawnień, zobowiązań, które dany urzędnik może realizować, reprezentując organ. Urzędnik, podpisując pismo, musi mieć świadomość posiadanych przez siebie uprawnień, natomiast te uprawnienia powinny zostać skontrolowane w momencie wydawania pisma. Mechanizmy sprawdzania tych uprawnień w terminie późniejszym przez adresatów pism nie dają wystarczającego poziomu bezpieczeństwa i narażają dane osobowe podpisujących na nieuprawniony dostęp. Jednocześnie zdarzają się sytuacje, w których pominięcie elementów procedury czy występowanie urzędnika poza przydzielonymi mu uprawnieniami jest podstawą do unieważnienia decyzji urzędowych. W związku z powyższym weryfikacja uprawnień urzędnika do wykonania danej czynności służbowej ma zasadnicze znaczenie w momencie składania przez niego podpisu. Model podpisu potwierdzonego umożliwia zablokowanie składania podpisów pod pismami powstałymi poza procedurą lub poza uprawnieniami danego urzędnika. Adresat pisma sygnowanego podpisem potwierdzonym ma pewność, że podpis powstał w kontrolowanym środowisku, w ramach posiadanych przez podpisującego uprawnień i obowiązującej procedury.

Podpis z informacją do przełożonego

W podmiotach administracji publicznej cały czas znaczący problem stanowi wiedza zarówno samego urzędnika, jak i jego przełożonych na temat, jakie i kiedy złożono podpisy. Brak kontroli nad tym umożliwia omijanie systemu przez antydatowanie dokumentów oraz podpisywanie dokumentów poza obowiązującą procedurą i systemem kancelaryjnym. Zastosowanie podpisu potwierdzonego stanowi poważne zabezpieczenie przed realizacją takich praktyk w mechanizmach podpisu elektronicznego. Podpis potwierdzony nie może być złożony bez współuczestniczenia Urzędu Podpisu, a co za tym idzie, każdy złożony podpis ma odzwierciedlenie w rejestrach zdarzeń dostępnych zarówno dla samego popisującego, jak i dla jego przełożonych.

Zbieranie informacji o złożonych podpisach, w zależności od implementacji, może mieć odzwierciedlenie w wewnętrznym

EOD lub innym systemie rejestrującym podpisy (np. centralnym rejestrze podpisów urzędników). Zastosowanie tego typu mechanizmów, które wchodzą z zakres zaawansowanych usług PKI 2.0, umożliwia dostęp do dodatkowej usługi dostępnej dla strony ufającej – potwierdzenia, że Urząd Podpisu brał udział w walidacji i utworzeniu danego podpisu.

Podpis dodatkowo zabezpieczony

Poza weryfikacją uprawnień podpis potwierdzony może wymagać dodatkowych autoryzacji przez osobę go składającą. W przypadku decyzji o ogromnym znaczeniu i wymagających szczególnego bezpieczeństwa podpisowi może towarzyszyć konieczność weryfikacji biometrycznej podpisującego lub np. uczestniczenie dwóch osób w procesie podpisywania. W takim wypadku Urząd Podpisu wstrzymuje potwierdzenie złożenia podpisu do czasu, w którym nastąpi dodatkowe potwierdzenie chęci jego złożenia – dla przykładu przez umieszczenie palca w czytniku biometrycznym Finger Vein. Tę cechę może mieć podpis potwierdzony składany przez osobę odpowiedzialną za udzielanie pełnomocnictw innym osobom lub za publikację dziennika urzędowego.

Podsumowanie

Zastosowanie podpisu osobistego dla urzędników ma bardzo słabe podstawy merytoryczne i posiada bardzo wiele zagrożeń. W szczególności należy tutaj wskazać ograniczenie praw obywatela do posługiwania się dowodem osobistym do tego, do czego został stworzony – czyli spraw obywatelskich i osobistych, a jednocześnie zwiększa ryzyko związane z utratą tego dowodu dla osoby, która jest urzędnikiem. Natomiast sama technologia zastosowana w podpisie osobistym, gwarantująca kontrolę nad procesem podpisywania i uczestnictwo w tym procesie Urzędu Podpisu daje kontrolę czasu i ważności certyfikatów w procesie podpisywania realizowanym przez urzędnika, a co za tym idzie, łatwiejsze zaufanie do tego podpisu przez jego adresata.

Należy tutaj wskazać, że opisane ustawą o dowodach wymagania podpisu osobistego dotyczące czasu i ważności podpisu dla pełnego bezpieczeństwa podpisów urzędników mogą być niewystarczające i należy zapewnić ich rozszerzenie poprzez zastosowanie podpisu potwierdzonego opisanego w PKI 2.0. Takie podejście da możliwości pełnego panowania nad składanymi podpisami i zapewnienia bardzo szerokiego spektrum zabezpieczeń i informacji zawartych w podpisie przy jednoczesnej przezroczystości tego mechanizmu dla samego podpisującego. Podpisujący posługuje się narzędziem do składania podpisu w taki sam sposób, jak ma to miejsce przy składaniu podpisu kwalifikowanego, natomiast wszystkie weryfikacje, w tym sprawdzenie, czy podpis powstał zgodnie z obowiązującą procedurą oraz w ramach uprawnień podpisującego, jest przezroczyste.

Informatyzacja podmiotów publicznych to nie tylko narzędzia prawne, ale także dostarczenie narzędzi technicznych wspierających budowę eAdministracji – łatwej w użyciu, ale bezpiecznej. Zastosowanie w procesach administracyjnych nowoczesnych mechanizmów podpisu elektronicznego, które zapewnią zaufanie do powstających w administracji publicznej dokumentów, jest działaniem koniecznym i wymagającym unifikacji w zakresie całej administracji. Jest to szczególnie ważne w kontekście nowej instrukcji kancelaryjnej i spodziewanego zwiększenia zainteresowania elektronicznym dostępem do urzędu obywateli w wyniku wprowadzenia elektronicznego dowodu osobistego.

Bibliografia

1. Rozporządzenie Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, Dz.U.2011.14.67
2. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, Dz.U.1960.30.168
3. R. Poznański, *Implementation of biometric technology in PKI 2.0*, Wrocław 2011, http://pki2.eu/images/Publications/20110120_en_PKI_2_0_Partners_IMM.pdf
4. *Studium wykonalności dla projektu „pl.ID – polska ID karta"*
5. M. Tabor, *Podpis elektroniczny powszechnie stosowany - łatwy jak transakcja kartą bankową*, pobrano z lokalizacji PKI 2.0: http://pki2.eu/images/Publikacje/101207_en_art_podpis_elektroniczny_latwy_jak_transakcja_karta.pdf
6. M. Tabor, *Podpis potwierdzony*, Czas informacji 2010, 3(4), str. 63-71
7. Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych, Dz.U.10.167.1131
8. Ustawa z dnia 31 stycznia 1980 r. o godle, barwach i hymnie Rzeczypospolitej Polskiej oraz o pieczęciach państwowych, Dz.U.05.235.2000 tekst jednolity

Michał Tabor – dyrektor operacyjny Trusted Information Consulting Sp. z o. o., ekspert w zakresie podpisu elektronicznego, bezpieczeństwa informacji oraz zarządzania dokumentami elektronicznymi, michal.tabor@ticons.pl.

Polecamy

SEMINARIUM
SYSTEMY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W JEDNOSTKACH REALIZUJĄCYCH ZADANIA PUBLICZNE
11 maja 2011 r., Warszawa

Zarządzanie bezpieczeństwem informacji to nowa dziedzina z pogranicza informatyki, prawa, organizacji i zarządzania, zajmująca się definiowaniem aspektów bezpieczeństwa jednostki i jej systemów teleinformatycznych. Zarządzanie bezpieczeństwem to ciągły i złożony proces umożliwiający bezpieczną realizację zadań, które są postawione przed jednostką realizującą zadania publiczne. Wchodzimy w erę społeczeństwa informacyjnego - instytucje publiczne stają się coraz bardziej uzależnione od szybkiego, niezawodnego, a przede wszystkim bezpiecznego przetworzenia ogromnych ilości informacji. Rosnąca ilość informacji powoduje wzrost zagrożeń dla nich, stąd niezwykłej wagi problemem stała się ochrona systemów teleinformatycznych i przetwarzanych w nich informacji. Wraz z rozwojem systemów rozwijano technologię zabezpieczeń, jednak dziś same zabezpieczenia już nie wystarczają. Dobór zabezpieczeń powinien zostać poprzedzony starannym określeniem celów bezpieczeństwa dla jednostki i jej systemów, uwzględniających realizację zadań w sytuacji występowania zagrożeń. Wdrożenie zabezpieczeń nie oznacza jeszcze osiągnięcia zaplanowanego poziomu bezpieczeństwa. Równie ważnymi zadaniami są: zdefiniowanie zasad bezpiecznego przetwarzania informacji, szkolenie i uświadamianie pracowników, monitorowanie aktualnego stanu bezpieczeństwa oraz stałe doskonalenie i adaptacja systemów.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Informatyzacja służby zdrowia – czy się wreszcie powiedzie?

Piotr Kociński

Jak informatyzowano służbę zdrowia

Od ponad dekady państwo polskie, posługując się różnymi instytucjami, niekiedy tworzonymi wyłącznie w tym celu, wdraża rozwiązania informatyczne w obszarze szeroko pojętej służby zdrowia do..., no właśnie do końca nie wiadomo, do czego. Nazwa tworu, który już od ponad dekady zaprząta umysły kolejnych zastępów informatyków, teoretyków zarządzania, lekarzy i urzędników, zmienia się. Na początku owe coś, a właściwie jego kluczowy element, nazywało się Rejestrem Usług Medycznych (RUM), czyli owe coś miało być oprogramowaniem, którego , jak się domyślamy, istotnym elementem miała być baza danych zawierająca rejestr usług medycznych. Wokół tej bazy danych miały się pojawić moduły realizujące usługi, z których mieli korzystać lekarze, ubezpieczyciele, pacjenci. Naturalnie poza bazą danych RUM pojawić się miały i inne bazy danych. W zależności od zamysłu miały to być bazy danych leków, recept, zdarzeń medycznych itd. Całość miała:

A. umożliwić efektywniejsze wykorzystanie środków łożonych na służbę zdrowia przez państwo, a raczej przez podatników,
B. uczynić kontakt pacjenta z „służbą zdrowia" wygodniejszym,
C. zwiększyć efektywność wykonywania procedur leczniczych.

RUM jednak nie powstał i to pomimo dostępnych od dłuższego czasu znacznych środków finansowych z Unii Europejskiej. Warto przypomnieć, że w tym samym czasie większość szpitali zdołała wdrożyć w większym lub mniejszym stopniu narzędzia informatyczne wspomagające różne aspekty ich działalności.

W chwili, gdy stoimy przed kolejną wielką próbą zmierzenia się z informatyzacją służby zdrowia na szczeblu centralnym, warto przyjrzeć się różnym koncepcjom informatyzacji oraz przyczynom, dla których dotąd niewiele się udało zrobić. Przemyśleć w jakim stopniu dokonywane przez lata wybory poszczególnych koncepcji przyczyniły się do tak miernych efektów, a w jakim stopniu zadecydowały inne czynniki, takie jak na przykład częste zmiany uwarunkowań instytucjonalnych działania służby zdrowia. Na koniec rozważań wskażemy, co należy zrobić teraz, gdy:

- na poziomie poszczególnych szpitali co nie co się jednak wydarzyło w obszarze informatyzacji,
- w ciągu ostatnich dziesięciu lat internet stał się w Polsce czymś oczywistym, łatwo dostępnym i czymś, z czego instytucje komercyjne, również te działające w służbie zdrowia, intensywnie korzystają.

Nowe koncepcje informatyczne remedium na zastój w informatyzacji służby zdrowia

Zacznijmy od przypomnienia, że pod pojęciem informatyzacji rozumiemy zestaw działań, których celem jest uruchomienie programów komputerowych, dzięki którym łatwiej, lepiej, szybciej wykonujemy grupy czynności specyficzne dla danej dziedziny życia. Dodajmy, że zakup komputerów, nawet bardzo dużych, czy pakietów oprogramowania nie jest informatyzacją, a jedynie może być uznany za jedno z działań, które w ramach informatyzacji

należy podjąć. Jest to o tyle ważna konstatacja, że w Polsce w ostatnich dwudziestu latach pod hasłem informatyzacji urzędy państwowe ograniczały się do zakupu wielkich superkomputerów , ewentualnie z pakietami oprogramowania takimi jak SAP, Oracle, a już nie starczało im sił, wiedzy, determinacji do wykonania tych najważniejszych działań składających się na informatyzację, a więc określenia grup czynności uporządkowanych w procesy, a następnie stworzenia programów komputerowych, dzięki którym owe procesy będą procedowane łatwiej, lepiej, szybciej. Niekiedy czynnikiem uniemożliwiającym dokonanie sensownej informatyzacji była któraś tam wersja ustawy o zamówieniach publicznych, która być może (choć trudno to dostrzec) uniemożliwia korupcję, natomiast bez wątpienia jeśli nie uniemożliwia całkowicie, to w każdym razie szalenie utrudnia, zważywszy zwłaszcza na powszechnie stosowany sposób jej wykorzystania, wdrażanie wszelakich nowoczesnych rozwiązań technicznych w instytucjach publicznych.

W przypadku informatyzowania służby zdrowia na szczeblu centralnym na przeszkodzie informatyzacji stanęła jeszcze jedna rzecz, mianowicie niespójna polityka państwa wobec służby zdrowia przejawiająca się w dramatycznych zmianach w organizacji sposobu działania służby zdrowia zachodzących na przestrzeni ostatnich 11 lat, od centralnego systemu do jego rozproszenia, następnie powtórnej centralizacji i degeneracji tego ostatniego w stronę swoistej quasi-decentralizacji, którą obserwujemy obecnie. Te gwałtowne zmiany spowodowały, że udane przykłady informatyzacji dokonane na poziomie regionalnym, czyli poziomie pośrednim pomiędzy poziomem szpitali, ośrodków zdrowia, aptek a poziomem centralnym, nie mogły zostać zaaplikowane w całym kraju.

Pomimo tego wszystkiego wydaje się, że akurat w obszarze zdrowia zdołano, w końcu, podjąć najważniejsze prace, czyli:

D. wskazano cele strategiczne – patrz punkty A, B, C powyżej,
E. podejmowano próby określenia i formalnego opisania podstawowych procesów (uporządkowanych grup czynności) niezbędnych do zrealizowania powyższych celów,
F. debatowano nad najlepszą z punktu widzenia zidentyfikowanych procesów architekturą rozwiązania.

Określono więc, lepiej lub gorzej, „zwierzę, na które należy zapolować" i wskazano dość ogólnie jak winno się „polować", natomiast, trzymając się metafory łowieckiej, nie kupiono na szczęście różnych drogich „sztucerów", z których część z pewnością okazałaby się zupełnie niepotrzebna (jak już mówiliśmy, podejście polegające na rozpoczynaniu wszelkich polowań od zakupu najlepszych strzelb – czyli dużych i bardzo dużych komputerów – jest zmorą dotychczas podejmowanych działań). W tym więc aspekcie nie jest źle, a jednak się nie udało. Dlaczego? Zacznijmy od stwierdzenia, że cele A, B, C wydają się sensowne, a procesy (patrz punkt E), choć tylko niektóre, zostały wstępnie opisane. Odbyto też niezliczoną liczbę narad i konferencji na temat architektury rozwiązania. W tym miejscu zatrzymajmy się i zanim zagłębimy się w dociekanie innych przyczyn niepowodzenia, przeanalizujemy dwa najpopularniejsze pomysły architektoniczne. Wydaje się, że co najmniej jeden z tych pomysłów architektonicznych, który ze względów choćby historycznych był brany pod uwagę na początku, mógł przyczynić się do impasu, z jakim mamy do czynienia w kwestii informatyzacji.

W dobie przedinternetowej programy komputerowe były w stanie komunikować się na odległość, stosowano nawet więcej protokołów sieciowych niż obecnie, gdy dominuje protokół komunikacyjny TCP/IP. Modelowano rozwiązania składające się

z wielu małych modułów klienckich, uruchamianych na rozproszonych komputerach klasy PC oraz jednego, uruchomionego na centralnym, na ogół dużym serwerze programu głównego (tzw. architektura klient-serwer). Centralny moduł świadczył usługi na rzecz modułów-klientów, przetwarzał zadania w oparciu o informacje, które dostarczały moduły klienckie. Całość działała autonomicznie, tzn. była samodzielnym bytem, którego nie dało się „zlepić" z innym, było się skazanym, w określonym obszarze, wyłącznie na funkcjonalność oferowaną przez taki program. Tak skonstruowano większość aplikacji działających kiedyś w bankach, firmach ubezpieczeniowych, instytucjach publicznych. Klasycznym przykładem takiej konstrukcji jest rządowy system unikatowych identyfikatorów osobowych PESEL. Dodajmy, że zarysowana powyżej architektura jest skuteczna i niezwykle efektywnie wykorzystywała dostępne technologie, a raczej technologie dostępne wtedy determinowały taki a nie inny kształt architektury. Podkreślmy, że warunkiem koniecznym dla jej skuteczności jest precyzyjne i w miarę kompletne określenie funkcji, które winna aplikacja zbudowana w takiej architekturze spełniać. Jeśli lista realizowanych przez aplikację funkcji rozmija się z potrzebami czy oczekiwaniami zamawiającej ją instytucji, to o efektywnym działaniu nie będzie mowy, co gorsza wprowadzanie zmian i modyfikacji do takiej aplikacji było trudne i kosztowne. Jeśli więc do tego obrazu dołożymy kwestię częstej zmiany uwarunkowań instytucjonalnych, w jakich funkcjonuje służba zdrowia w Polsce, a więc częstej zmiany wymaganych funkcji, to staje się jasne, dlaczego niewiele osiągnięto. Próbowano wdrożyć rozwiązanie w architekturze, która wymaga stabilnego otoczenia prawno-biznesowego w dłuższej perspektywie czasowej.

Zanim przejdziemy do próby nakreślenia, jak należy zinformatyzować służbę zdrowia, wskażmy na jeszcze jeden czynnik, który gdyby nawet udało się wdrożyć jakieś rozwiązanie na poziomie rządu centralnego dla służby zdrowia, mógłby powodować, że pożytek z rozwiązania i tak był niewielki. Otóż rozwiązanie główne miało (w każdym razie tak odczytywać można intencje rządu sprzed 11 już lat) koncentrować się wokół bazy danych zawierającej rejestr usług medycznych. Było to skądinąd naturalne w kraju, gdzie nie istniały mechanizmy wyceny usług ani referencyjne rejestry tych usług, co traktowano jako jedną z najważniejszych przyczyn nieefektywnego kosztowo funkcjonowania służby zdrowia. W chwili więc, gdy chciano zaaplikować nowoczesne narzędzia informatyczne do „chorej" służby zdrowia, postanowiono zacząć, od jak się wydawało, najbardziej „chorego" miejsca. Niestety taki tryb w kontekście informatyzacji był zły, niezgodny z metodami stosowanymi w komercyjnej informatyce. Żeby zrozumieć, jaki tryb byłby z informatycznego punktu widzenia sensowny, przyjrzyjmy się instytucjom finansowym, które wszędzie, również w Polsce, obok firm telekomunikacyjnych przecierają nowe, dotąd niezbadane ścieżki w adaptowaniu dla swoich potrzeb nowoczesnych technik teleinformatycznych. Otóż w bankach, które chcą, między innymi:

G. umożliwić efektywniejsze wykorzystanie środków klientów zdeponowanych w banku,
H. uczynić kontakt klienta z bankiem wygodniejszym,
I. zwiększyć efektywność banku w zakresie jego statutowych działań

wdraża się rozwiązania, które zawierają m.in.:

- bazę danych klientów,
- bazę danych oferowanych produktów,
- system wyceny produktów,
- rejestr transakcji,
- systemy analityczno-sprawozdawcze, których wyniki kieruje się do zarządu czy zewnętrznych ciał kontrolnych takich jak Komisja Nadzoru Finansowego.

Naturalnie istnieje zawsze program komputerowy, który spaja wszystkie powyższe elementy w jedną, spójnie działającą całość. Tak czy owak najważniejszym elementem systemu bankowego jest ten pierwszy na powyższej liście, czyli baza danych klientów. Jest to dość oczywiste zważywszy na fakt, że bez klientów bank po prostu nie będzie funkcjonował. Rejestr produktów też jest elementem, ale nie jest wyróżniony, jest jednym z wielu koniecznych elementów, które winny złożyć się na całość. Zwróćmy teraz uwagę, że wymagania „bankowe" (G, H, I) można odwzorować na, odpowiednio, wymagania (A, B, C) wskazane powyżej, stawiane systemowi informatycznemu wspomagającemu służbę zdrowia (dodajmy, że odwzorowanie jest dwukierunkowe). Po dodatkowym porównaniu całej funkcjonalnej otuliny systemów finansowego i zdrowia widać, że system dla służby zdrowia winien składać się m.in. z:

J. bazy danych uczestników systemu:
   a) pacjentów,
   b) lekarzy,
   c) personelu,

K. bazy danych oferowanych produktów:
   d) rejestru usług medycznych (RUM),
   e) rejestru leków,

L. systemu wyceny produktów,

M. rejestru wykonanych usług medycznych,

N. systemu analityczno-sprawozdawczego, których wyniki kieruje się do NFZ czy zewnętrznych ciał kontrolnych takich jak Ministerstwo Zdrowia.

W takim ujęciu RUM „spada z piedestału" i staje się jednym z wielu. Być może więc ta próba wdrażania narzędzi informatycznych w służbie zdrowia ze źle określonym punktem startu była skazana na niepowodzenie, zwłaszcza jeśli dodamy do tego szybkozmienne otoczenie prawne, a co za tym idzie funkcjonalne. Zatem widać, że powszechnie stosowana 11 lat temu architektura rozwiązania informatycznego nie była wystarczająco elastyczna, żeby akomodować te wszystkie szybko następujące zmiany.

Tak więc RUM nie powstał, a Centrum Systemów Informacyjnych Ochrony Zdrowia (CSIOZ) podejmuje w tej chwili trud budowy sensownego rozwiązania. Jak należy dalej postępować? Czy zakładając, że uchwalane właśnie regulacje prawne dotyczące służby zdrowia przetrwają dużej niż 5 lat, wystarczy ograniczyć się do precyzyjnego określenia niezbędnych funkcji systemu, a następnie jego budowy w architekturze klient-serwer , ze składnikami J-N jak powyżej? Otóż nie, gdyż stare (10 lat!) technologie narzucały jednak spore ograniczenia na rozwiązania, które były mało elastyczne, a do tego pojawiły się nowe czynniki (choćby Internet), które dekadę temu nie wydawały się tak istotne.

W nowym, wspaniałym świecie Internetu systemy informatyczne wyglądają inaczej

W tej chwili dostępne technologie umożliwiają budowę lepszych, bo elastyczniejszych, rozwiązań, wykorzystujących przy tym dobrodziejstwo zjawiska, jakim jest Internet. Pojęcie „elastyczny system informatyczny" w przypadku instytucji komercyjnych takich jak banki oznacza, że:

a) posługując się takim systemem, możemy szybko udostępnić klientowi (wprowadzić na rynek) nowy produkt w konkurencyjnej cenie, udostępnić na wiele sposobów, przede wszystkim za pośrednictwem Internetu,
b) możemy oferować w Internecie hybrydowe produkty, tj. usługi, których celem jest udostępnienie klientowi pakietu składającego się z własnego produktu i produktu oferowanego przez firmę trzecią, również dostępnego w Internecie,
c) generalnie szybko reagujemy na zmieniające się środowisko biznesowe (prawo, sytuacja na rynku kredytowym, podatki, mody itp.).

W przypadku służby zdrowia w Polsce powyższe trzy punkty można przetłumaczyć na następujące cechy, możemy między innymi:

d) szybko udostępnić pacjentom informację o nowych usługach medycznych,
e) wskazywać, gdzie jakie usługi mogą być wykonane w jakim czasie, dokonywać rejestracji,
f) umożliwiać pacjentowi śledzenie procesu jego leczenia,
g) ułatwić dostęp do leków poprzez lepsza informację na temat ich dostępności,
h) ułatwić lekarzom swobodny (niezależnie od miejsca przebywania lekarza) dostęp do informacji o pacjencie, do dokumentacji o przebiegu choroby (z zastrzeżeniem co do różnicowania praw dostępu do określonych danych).

Produkt w przypadku służby zdrowia ma inny charakter niż w przypadku instytucji finansowej, a i pacjent jest dość specyficznym typem klienta. Naturalnie rozwiązanie ciągle winno gwarantować takie funkcje jak:

i) zapewnienie rozliczalności wszystkich działań,
j) gromadzenie i przetwarzanie właściwych danych,
k) zarządzanie logiką działania instytucji.

Zwróćmy uwagę, że w powyższych punktach, choć nie wymienione wprost, przewija się pojęcie Internetu. Bez wątpienie zjawisko Internetu jawi się jako konstytutywne dla współczesnego sposobu działania w dowolnej sferze życia. Przywołajmy te cechy Internetu, które wydają się istotne. Internet dostarcza możliwość:

O. prezentowania na komputerze Y treści składowanej na komputerze X pod warunkiem, że oba komputery są podłączone do Internetu, czyli że są podłączone do siebie w sposób pośredni; pośrednikiem jest tu globalna sieć – to tzw. informacyjny tryb pracy (ang. *Informational services*),
P. wywoływania określonej usługi udostępnionej na jakimś firmowym portalu i zlecania jej wykonania (klasycznym przykładem jest tu bankowość internetowa) – to tzw. transakcyjny tryb pracy (ang. *transactional services*),
Q. wywoływania określonej usługi, której początek udostępniony jest na portalu ***x*** należącym do instytucji X, ale której realizacja wymaga kolaboracji, za pośrednictwem Internetu, wielu systemów różnych instytucji (ang. *connected services*),
R. adresowania, co oznacza, że portale uruchomione na różnych komputerach niepołączonych ze sobą bezpośrednio są w stanie się odnaleźć, posługując sie mechanizmami opisanym *w Internet Protocol* (IP), w oparciu o specyficzne książki adresowe, które zapisane są na tzw. ruterach i częściowo na tychże komputerach.

Zwróćmy uwagę, że pojęcia takie jak „connected services" czy „transactional services", a właściwie środowiska informatyczne o cechach opisanych tymi pojęciami są stosowane przez instytucje międzynarodowe do oceny stopnia informatyzacji sektora publicznego w danym kraju. W rzeczywistości cechy powyższe (przede wszystkim O-Q) są tak naprawdę cechami tzw. sieci globalnej (ang. *world wide web* – www) korzystającej z protokołu udostępniania treści o nazwie HTTP, która korzysta z wcześniejszego wynalazku, jakim jest Internet, czyli kolaboracja komputerów „wpiętych" do sieci zarządzanej zgodnie z protokołami TCP/IP. Przyjęło się jednak mówić o zjawisku sieci globalnej www jako o Internecie.

W świecie Internetu aplikacje mogą być niejako „rozpięte" na komputerach niepołączonych ze sobą bezpośrednio, a jedynie za pośrednictwem Internetu. Połączenie „klienta" z „serwerem" zostaje przerwane. W tej

sytuacji „klient" niejako usamodzielnia się, nabiera wielu cech zastrzeżonych dotąd dla programów typu „serwer". Linia podziału pomiędzy programami zaczyna przebiegać gdzie indziej. Programy stają się więc albo *dawcami usług* (ang. *services providers*) albo *biorcami usług* (ang. *services requestors*). Programy uruchamiamy na potencjalnie różnych, często bardzo odległych od siebie komputerach, „sczepionych" za pośrednictwem Internetu. Usługi wspierają odpowiednie czynności, które, jak pisaliśmy wyżej, składają się na jakiś proces, biznesowy bądź administracyjny. Możemy przestać więc myśleć w kategoriach wdrażania wyłącznie bardzo dużych programów o szerokiej funkcjonalności, a zacząć myśleć w kategoriach elektronicznych zbiorów usług. Program X, dawca, „wystawia" w Internecie kilka usług realizujących jakieś konkretne wąsko zdefiniowane czynności. Program Y, biorca, korzystając z dobrodziejstw protokołów Internetowych (IP i HTTP), trafia do tej grupy usług, podaje im dane wejściowe, usługi te przekazują dane do programu X, gdzie następuje przetwarzanie, a następnie wyniki przetwarzania są przekazywane za pośrednictwem tychże usług do programu Y. Tak naprawdę usługę wykonał w tym przypadku program X, a ów „mały" program wystawiony w Internet i zwany usługą (ang. *service*) był tylko pośrednikiem pomiędzy programami, biorcą i dawcą. Jednak przyjęło się właśnie te programy pośredniczące nazywać usługami i dalej w tekście tę konwencję będziemy stosować. Zbiór usług niejako „wisi" w Internecie i inne programy mogą z tych usług korzystać. Mogą korzystać z nich wybiórczo, w różnej sekwencji itp. System zbudowany w architekturze opartej na usługach (ang. *services oriented architecture* – SOA) jest systemem elastycznym tzn. spełniającym wymagania a-c, d-h podane powyżej. Jest też systemem otwartym, można dodawać do niego różne programy, które będą wzbogacały paletę dostępnych usług. Im szerszy zbiór usług tym więcej nowych, złożonych produktów może być zbudowanych i zaoferowanych klientom/pacjentom. Udostępnienie klientom produktu to zwykle sekwencja kilku, kilkunastu czynności. Gdy programy były zamkniętymi konstrukcjami (choć o niekiedy szerokiej funkcjonalności), to było wysoce prawdopodobne, że do wsparcia jakiejś sekwencji czynności program się nie nadawał, gdyż po prostu brakowałoby wśród jego funkcji takich, którymi można było wesprzeć wszystkie czynności konkretnego procesu. W nowej architekturze wiele programów biorców dostarcza usługi dostępne w protokole HTTP i z tych usług można w dowolny sposób konstruować informatyczne wsparcie dla różnych procesów. Wsparcie nowego procesu (stojącego za nowym produktem) najczęściej nie wymaga już więc kosztownych, żmudnych i ryzykownych, z punktu widzenia rezultatu końcowego, modyfikacji dużego programu zbudowanego w starej architekturze, a jedynie wyboru odpowiednich i dostępnych usług, następnie ułożenia ich w określonej sekwencji. Do ułożenia usług we właściwej sekwencji i zarządzania ich działaniem wprowadzono programy klasy zarządzania procesem (ang. *process management*). Dla usprawnienia funkcjonowania rozwiązań zbudowanych w oparciu o architekturę zorientowaną na usługi mamy często do czynienia z pakietami, które:

- grupują pewne usługi,
- umożliwiają zarządzanie procesami,
- są tym miejscem, do którego zgłaszają się programy biorcy, gdy chcą skorzystać z jakiś usług, są więc pośrednikiem (ang. *broker*) pomiędzy programami dawcami i programami biorcami.

Są to tzw. szyny usługowe (ang. *services bus*). Zwróćmy uwagę na inną ważną funkcję szyny. Mianowicie gdy jest wiele programów dawców i wiele dostępnych usług, to gdy dysponujemy szyną, nie trzeba się trudzić z „wiązaniem" wszystkich ze wszystkim, ale dla programów dawców jest przeznaczony jeden protokół korzystania z usługi (o różnych interfejsach naturalnie) wystawionej teraz

niejako z szyny usługowej, a dla programów biorców jest stworzony jeden protokół na dodawanie usług do szyny serwisowej.

Dodajmy, że nawet stare aplikacje można łatwo przystosować zwłaszcza do roli programów dawców usług dostępnych w Internecie. Tak więc architektura ta świetnie się nadaje do sytuacji, gdy mamy środowisko wielu działających, acz nie kolaborujących ze sobą, starych programów. Należy je przystosować do roli programów dawców, dodać programy biorcy umożliwiające nowoczesne formy komunikacji użytkownika (klient, pacjent) z systemem IT, takie jak portale czy IVR i w ten sposób stworzyć środowisko informatyczne oparte o architekturę zorientowaną na usługi. Od kilku programów, wprawdzie dobrze działających i sprawdzonych, ale uniemożliwiających szybkie ich dostosowywanie do zmiennego otoczenia, przechodzimy bez likwidacji tychże programów, a wprost przeciwnie wykorzystując je, do nowoczesnego i elastycznego systemu IT.

W służbie zdrowia mamy na szczeblu szpitali czy aptek wiele dobrze działających programów. Jednak wszystkie te programy nie są w stanie efektywnie współpracować, gdyż zbudowano je w oparciu o stare paradygmaty architektoniczne. Dodajmy, że centralne instytucje pełniące funkcje kontrolne i zarządcze w stosunku do szpitali nie mają systemu informatycznego zdolnego wesprzeć je w działaniach. W świetle powyższych rozważań architektonicznych odpowiedź, jak postępować dalej, wydaje się oczywista.

Co należy zrobić – nie zapominajmy o interoperacyjności

Wydaje się, że system informatyczny do wspierania funkcjonowania służby zdrowia w Polsce na różnych jej szczeblach winien być otwartym, zbudowanym w architekturze zorientowanej na usługi. Aby tak się mogło stać, należy na początku:

- podjąć trud identyfikacji i formalnego opisu (Unified Modelling Language) wszelkich procesów administracyjnych niezbędnych dla funkcjonowania służby zdrowia na różnych szczeblach i potrzebnych do realizacji celów strategicznych wskazanych na początku niniejszego artykułu w punktach A-C oraz ocenienia, które z nich (bądź które ich części) winny być wspierane informatycznie,
- zinwentaryzować wszelkie programy funkcjonujące w obrębie służby zdrowia oraz ocenić jakie usługi mogą te programy udostępnić w Internecie i jakim kosztem to udostępnienie może być wykonane,
- stworzyć katalog potencjalnie dostępnych usług, a następnie zbadać, czy usługi te w różnych konfiguracjach są w stanie realizować zidentyfikowane i opisane procesy,
- zidentyfikować, które procesy nie mogą być realizowane i w oparciu o ten zbiór nierealizowalnych procesów określić, jakie usługi (a więc programy dawcy, które określone usługi udostępniają) winny być zrealizowane,
- stworzyć środowiska aplikacyjne, w których będzie można uruchomić poszczególne programy.

Następnie należy „złożyć" z posiadanych kawałków system informatyczny. Dodajmy jeszcze raz, że poza programami, których zadaniem będzie dostarczanie potrzebnych usług na szczeblu lokalnym, winniśmy dodać na poziomie centralnym:

S. szynę usługową o charakterystyce, jak pokazaliśmy wyżej,
T. program zabezpieczający, czyli mechanizmy zabezpieczania danych, ochrony dostępu do danych czy wystawionych w Internecie usług, różnicowania praw dostępu do danych czy usług, rejestrowania aktywności itd.,
U. centralny zbiór znaczeń,
V. systemy udostępniające usługi, które z kolei dostarczają kluczowe informacje,

a więc takie systemy IT, jak centralny rejestr pacjentów, centralny rejestr leków, centralny rejestr lekarzy, generalnie systemy wskazane powyżej w punktach J-N.

W całym systemie będzie mnóstwo różnych programów, które nagle będą musiały kolaborować ze sobą. Kolaboracja oznacza wymianę danych i nie jest to li tylko zabieg techniczny, gdyż odpowiednio sformatowane dane są informacją, która ma znaczenie decydujące o sensowności działania danego systemu. Z dużym prawdopodobieństwem można stwierdzić, że na ogół formaty, w których dane są przechowywane w różnych systemach, są odmienne. Chodzi więc o to, żeby program X przekazujący do programu Y daną $\boldsymbol{x}$ nadał tą daną wartość właściwej danej z systemu Y. To ostatnie oznacza, że informacja związana z daną $\boldsymbol{x}$ zapisaną w formacie f_x winna mieć takie same znaczenie jak dana z programu Y, zapisywana w formacie f_y. Wdrożenie mechanizmów gwarantujących zgodność semantyczną przekazywanych danych pomiędzy programami nie jest trywialne, a na ogół przygotowanie programów konwertujących z formatu na format, stworzenie zbiorów znaczeń jest kosztowne. Zanim więc podejmie się wysiłek wdrożeniowy, warto starannie zbadać potencjalny poziom interoperacyjności, czyli innymi słowy zgodności semantycznej informacji przetwarzanej w dwóch systemach [1].

Na koniec, gdy posługując się dobrymi wzorcami architektonicznymi, stworzyliśmy już aplikacyjne elementy środowiska opartego na usługach, wykorzystujące również dotychczasowe programy (po ich niewielkiej modyfikacji polegającej na wystawieniu z nich usług i udostępnienia tychże usług w Internecie), musimy zadecydować na jakich środowiskach sprzętowych winniśmy uruchomić całość. Choć rozpoczęliśmy niniejszy tekst od krytyki dotychczasowej praktyki nabywania dużych i bardzo dużych serwerów, to jednak w tym miejscu wskazujemy, że warto rozważyć zakup dużego serwera , na którym będzie można umieścić szereg elementów, takich jak te wymienione powyżej w punktach S, T, U, V.

Nakreślony powyżej sposób postępowania zakładający zmianę paradygmatów architektonicznych poprzez wskazywanie celów strategicznych oraz definiowanie procesów, staranne i szczegółowe określenie „po co robimy to wszystko" wydaje się zwiększać prawdopodobieństwo choćby umiarkowanego sukcesu we wdrażaniu narzędzi informatycznych w służbie zdrowia. Warto dodać na koniec, że wykonując te wszystkie prace, winniśmy od razu stworzyć wskaźniki, za pomocą których będziemy mierzyć efektywność, również efektywność kosztową, funkcjonowania całego systemu [2].

A nuż tym razem się powiedzie?

Literatura

1. Grzegorz Bliźniuk, *Biuletyn Instytutu Systemów Informatycznych*, 3 X-X(2009)
2. Piotr Kociński, *Czy państwo potrzebuje architektury korporacyjnej?*, Czas Informacji**,** 2(3)/2010

Piotr Kociński - z wykształcenia dr fizyki, od 13 lat w branży I/T. Obecnie w Accenture.

Informacja w transgranicznej opiece zdrowotnej. Polska na tle przepisów wspólnotowych oraz USA

Bartłomiej Michalak

Wprowadzenie

Legislacja pojęcia informacji medycznej w polskim systemie ochrony zdrowia jest problem, na który składa się wiele czynników. Niepewność w reformowaniu całości systemu ochrony zdrowia nie ułatwia wdrażania standardów informacji medycznej jako rzetelnego narzędzia całościowej konsultacji w celu ochrony i poprawy zdrowia ludzkiego. Zobowiązania względem członkostwa w Unii Europejskiej oraz niewspółmierne do potrzeb środki zmuszają rząd polski do wdrożenia narzędzia zapewniającego bezpieczeństwo systemu prawnego, jak i aktualizacji niezbędnych przy projektowaniu zasobów finansowych, kadrowych czy też określeniu niezbędnej infrastruktury materialnej.

Polska informacja opieki zdrowotnej poprzez uzasadnienie projektu ustawy o systemie informacji w ochronie zdrowia odwołuje się do rozwiązań wspólnotowych kontynentu europejskiego. Wśród tych rozwiązań można wskazać na tzw. Strategię lizbońską z 2000 r., plan eEurope 2005 ze szczytu w Sewilli, Decyzję 1786/2002/WE Parlamentu Europejskiego i Rady z dnia 23 września 2002 r., komunikat Komisji Europejskiej z dnia 30 kwietnia 2004 r. (COM(2004) 356), zalecenia Komisji Europejskiej 9185/04, Dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. (INSPIRE). Natomiast z polskich rozwiązań, wskazanym zarówno w projekcie ustawy, jak i w uzasadnieniu, podstawowym aktem jest ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, nie mniej ważna jest ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz dokument MSWiA „Nowoczesna infrastruktura informacyjna podstawą taniego i przyjaznego państwa obywatelskiego. Program reformy infrastruktury informacyjnej państwa i strategii informatyzacji sektora publicznego" z 2005 r. Ciekawym może wydawać się fakt, iż w tym samym czasie w USA podejmuje się próby, na poziomie rządowym, całościowego wdrożenia elektronicznej dokumentacji medycznej Medicare i Medicaid zarówno dla szpitali, jak i lekarskiej opieki specjalistycznej.

Celem budowy europejskiego społeczeństwa informacyjnego jest osiągnięcie wysokiego poziomu ochrony zdrowia ludzkiego. Jednocześnie Komisja Europejska zobowiązała kraje członkowskie do uruchomienia m.in. elektronicznych usług medycznych (e-recepta, telekonsultacje), elektronicznych ubezpieczeń zdrowotnych oraz e-Health.

Ustawodawca krajowy w głównym projekcie informatyzacji polskiego systemu ochrony zdrowia za cel przyjął stworzenie warunków i stabilizację dla informacji w ochronie zdrowia, a co za tym idzie, zmniejszenie luki informacyjnej oraz uporządkowanie i poprawę funkcjonowania systemu. Ma to spowodować optymalizację nakładów finansowych i przywrócenie właściwych relacji pomiędzy podmiotami systemu ochrony zdrowia.

W Polsce prowadzenie dokumentacji medycznej miało na celu analizę wyników i związków przyczynowych związanych z procesem

leczenia. Obecnie dokumentacja medyczna jest prowadzona głównie do celów formalno-prawnych i finansowych, będąc umiarkowanie przydatną do celów naukowo-medycznych.

Modele wdrożeń EHR

Opisując modele wdrożeń informacji w ochronie zdrowia poprzez „01" dokumentację medyczną, posłużę się podziałem prawnych form działania administracji publicznej autorstwa Jerzego Supernata.

Rząd USA, wprowadzając elektroniczny rekord, zastosował instrument finansowy, wspierając go instrumentem informacyjnym. Z kolei UE postawiła na instrument organizacyjny, wspierając go instrumentem informacyjnym. Wydaje się, że w Polsce żaden z powyższych modeli nie zostanie wprowadzony i najprawdopodobniej, jak miało to miejsce w poprzednich reformach informacji w ochronie zdrowia, rząd RP posłuży się instrumentem władczym, wspierając go instrumentem informacyjnym.

Stany Zjednoczone, wdrażając elektroniczną dokumentację medyczną (EHR) Medicare i Medicaid, posłużyły się programami motywacyjnymi, zachęcając specjalistów i szpitale wysokimi płatnościami w przypadku przyjęcia, wdrożenia, modernizacji czy wykazaniu stosowania kwalifikowanych technologii Electronic Health Record (zamiennie używa się Electronic Medical Record). Jak zauważył Charles E. Lindblom, zakres dóbr wymiennych na pieniądze jest niemal nieograniczony. Wskazał, iż takie nie nadające się do transakcji handlowych dobra jak życzliwość są kupowane i sprzedawane. Wierność, podległość, uznanie publiczne itp. - wszystko to jest niekiedy na sprzedaż, a wymiana rynkowa dosięga każdego aspektu życia.

Przy zasobach organizacyjnych systemu ochrony zdrowia główne znaczenie odgrywa osobowo-rzeczowy substrat, z którego korzysta administracja wspólnotowa. Jak zauważa Adam Podgórecki, samo działanie administracji nie jest w zasadzie społecznie produktywne, a usprawiedliwione jest jedynie przez wywołanie skutków aktów normatywnych, które administracja wprowadza w życie społeczne i zazwyczaj kontroluje. Takim aktem może stać się dyrektywa Parlamentu Europejskiego i Rady w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej. Obok zagwarantowania dostatecznej jasności na temat prawa do zwrotu kosztów opieki zdrowotnej udzielonej w innym państwie członkowskim położono również nacisk, by zostały spełnione konieczne wymagania w zakresie wysokiej jakości, bezpieczeństwa i skuteczności opieki zdrowotnej. Niesie to konieczność wymiany odpowiednich danych na temat zdrowia pacjentów między upoważnionymi organizacjami oraz pracownikami służby zdrowia w różnych państwach członkowskich. Dane dotyczące zdrowia pacjentów są uważane za dane wrażliwe i podlegają ściślejszym zasadom ochrony danych zgodnie z art. 8 dyrektywy 95/46/WE.

Władztwo administracyjne pozwala nakazywać i zakazywać, ostrzegać, określać, obiecywać, prowadzić, zalecać, pozwalać, orzekać, zatwierdzać, potwierdzać, rejestrować, udzielać akredytacji, postanawiać, ustalać, poświadczać, opiniować itp. Najprawdopodobniej rząd RP postawi na władcze instrumenty przy wdrażaniu informacji w systemie ochrony zdrowia. Kazimierz Strzyczkowski wskazuje, iż władztwo może być stopniowalne, gdzie element przymusu państwowego zostaje wyłączony. W ciekawy sposób do władztwa podchodzi również Irena Lipowicz, wskazując na kres zafascynowania władczością państwa oraz podkreśla normatywny i stopniowalny charakter władztwa administracyjnego, z drugiej zaś strony zaznacza, że może być skutecznym narzędziem ochrony podmiotów słabszych, np. konsumentów. Z kolei

w sytuacji kryzysu czy katastrofy powraca z całą mocą, służąc ochronie życia i zdrowia lub przetrwania wspólnoty państwowej. Jak dotąd charakter stopniowalny władztwa można było zauważyć przy wprowadzaniu formatu XML. Format ten służy do kontaktu z NFZ i obejmuje jedynie świadczenia zdrowotne finansowane ze środków publicznych. Przy wdrożeniu formatu XML nie istniał przymus państwowy, jednakże w przypadku niespełnienia wymagań płatnika nie mogło dojść do wymiany informacji świadczeniodawca – płatnik.

W. Cezary Włodarczyk wskazuje, że nawet w pełni merytorycznie uzasadnione idee napotykają na opór. Taka mobilizacja sprzeciwu może zachodzić na etapie projektu, ale równie dobrze może nastąpić, gdy udało się przeprowadzić propozycje przez drogę legislacyjną. Stąd istnieje konieczność stałego pozyskiwania wsparcia opinii publicznej i tych segmentów społeczeństwa, które mają szansę poprawy swojego położenia w wyniku proponowanych zmian.

Stąd instrumenty informacyjne są nieodzownym składnikiem wdrożeń „01" dokumentacji medycznej. Administracja może wykorzystywać informacje w celu oddziaływania na swoje otoczenie i realizację zadań publicznych. W. Berka wskazuje, że sprawowanie administracji w obecnym czasie za pomocą informacji zyskało wyraźnie na znaczeniu. Autor wiąże to z trudnościami w sterowaniu współczesnym społeczeństwie za pomocą regulacji władczych. W demokratycznym państwie prawa procesy reformatorskie XX i XXI wieku wytworzyły pojęcie dobrej administracji (*good administration*). To dzięki tej zasadzie, bez aktywności z naszej strony, otrzymujemy od administracji publicznej informację spersonalizowaną, z której dowiadujemy się o programach zdrowotnych, badaniach profilaktycznych. Stąd można śmiało wskazać na instrumenty informacyjne, które w XXI wieku są nieodzownym składnikiem wdrożeń technologii medycznych.

Kreatorzy zmian, czyli podmioty odpowiedzialne za wdrożenie technologii medycznych

Nadzór nad polską informacją w ochronie zdrowia sprawuje minister właściwy do spraw zdrowia. Jednakże ograniczenia organizacyjne i kadrowe ministerstwa spowodują potrzebę zlecania kontroli jednostkom ze sfery ochrony zdrowia (np. instytutom badawczym). Projekt ustawy o systemie informacji w ochronie zdrowia wskazuje, iż ta kontrola miałaby być przeprowadzona z punktu widzenia legalności, celowości i rzetelności. Nie zostało jednak wyjaśnione zastosowanie takiej kompilacji. Konstytucja Rzeczypospolitej Polskiej w rozdziale IX „Organy kontroli państwowej i ochrony prawa" w art. 203 przedstawia katalog przesłanek, jakimi kieruje się Najwyższa Izba Kontroli. I tak:

- organy administracji rządowej, Narodowy Bank Polski, państwowe osoby prawne i państwowe jednostki organizacyjne podlegają kontroli z punktu widzenia – legalności, gospodarności, celowości i rzetelności;
- organy samorządu terytorialnego, komunalne osoby prawne i komunalne jednostki organizacyjne podlegają kontroli z punktu widzenia – legalności, gospodarności i rzetelności;
- jednostki organizacyjne i podmioty gospodarcze wykorzystujące majątek lub środki państwowe lub komunalne oraz wywiązują się z zobowiązań finansowych na rzecz państwa podlegają kontroli z punktu widzenia – legalności i gospodarności.

Rodzi się pytanie, na jakiej podstawie zastosowano przesłanki sprzeczne z konstytucyjnym katalogiem kontrolnym. Tym bardziej, że zrezygnowano z zamieszczania przepisów karnych

w projekcie ustawy ze względu na dostateczne regulacje zawarte w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

W sposób przejrzysty określono podmiot odpowiedzialny za integrację rejestrów medycznych oraz działania edukacyjno-informacyjne, wskazując na Centrum Systemów Informacyjnych Ochrony Zdrowia, które jest de facto odpowiedzialne za opracowanie podwalin systemu informacji w ochronie zdrowia. Jest także quasi-stroną w finansowaniu przedsięwzięcia. Warto zaznaczyć, że źródłem finansowania działań związanych z informacją w ochronie zdrowia są środki Europejskiego Funduszu Rozwoju Regionalnego (stanowiące 85%) oraz środki krajowe (stanowiące 15%).

Na szczeblu Unii Europejskiej można wskazać na Komisję Wspólnot Europejskich, Parlament Europejski, Radę Unii Europejskiej, Komitet Ekonomiczno-Społeczny oraz Komitet Regionów, które są odpowiedzialne za wspieranie stosowania technologii informacyjno-komunikacyjnych w sektorze zdrowia. Komisja WE w Komunikacie z dnia 4 listopada 2008 r. (KOM (2008) 689) zwraca uwagę, że nie zgromadzono jeszcze wystarczającej liczby dowodów na potwierdzenie tezy, że usługi telemedyczne świadczone na szeroką skalę są skuteczne i efektywne pod względem kosztów. Nie istnieją również powszechnie akceptowalne metody oceniania tej skuteczności.

Unia Europejska boryka się również z problemem statusu prawnego czynności medycznej, która jest uzależniona od obecności pacjenta i pracownika służby zdrowia w tym samym miejscu (takim przykładem może być Polska). Omawiając status prawny czynności medycznej, należy podkreślić, że dane medyczne należą do specjalnej kategorii danych, która – jak zauważa Europejski Inspektor Ochrony Danych Osobowych w Opinii z dnia 6 czerwca 2009 r. (2009/C 128/03) – zasługuje na szczególną ochronę.

Ważnym dla funkcjonowania na gruncie wspólnotowym jest projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej, który został przyjęty przez Parlament Europejski w dniu 19 stycznia 2011 r. Jeszcze musi zostać zatwierdzony przez Radę UE, po czym rozpocznie się okres 30-miesięczny, w którym to kraje członkowskie są zobowiązane przyjąć przepisy. W tym celu Komisja wspiera europejską współpracę pomiędzy pracownikami służby zdrowia i pacjentami, w szczególności dotyczącej zwiększenia zaufania do telemedycyny i jej akceptacji, uwzględniając przy tym kwestie etyczne i dotyczące prywatności.

Na najwyższym szczeblu rządowej administracji do spraw zdrowia w USA stoi Sekretarz Stanu HHS (Health and Human Services). W jego strukturze znajduje się Urząd Narodowego Koordynatora do spraw Informacji w Ochronie Zdrowia (ONC), który stoi na czele administracji *health information technology*. ONC jako główny federalny koordynator ma na celu wdrażanie i stosowanie najbardziej zaawansowanych technologii informacyjnych i elektronicznej wymiany na temat zdrowia, a także zarządzanie Ogólnonarodową Siecią Informacji Zdrowia. Stanowisko ONC powstało w 2004 r., jednakże ustawowe upoważnienie do podejmowania działań nastąpiło w 2009 r. za sprawą ustawy o technologiach informacyjnych w ochronie zdrowia, finansowaniu i planowaniu leczenia oraz opieki nad pacjentem (HITECH). Oprócz tego, że ONC wspiera wdrażanie HITECH, zajmuje się również inicjatywami ułatwiającymi przyjęcie krajowych ram HIT. Ustawa naprawcza The American Recovery and Reinvestment

Act z 2009 r. (Arra), przewiduje utworzenie Komitetu Politycznego HIT, który jest odpowiedzialny za formułowanie zaleceń dla ONC w ramach polityki na rzecz rozwoju i przyjęcia ogólnokrajowej infrastruktury na temat zdrowia, w tym standardów wymiany informacji medycznych pacjenta. Również w 2009 r. powstały tzw. Grupy Robocze, np. ds. wymiany informacji, ds. prywatności i bezpieczeństwa, ds. rejestrowania.

Arra przewiduje również utworzenie Komitetu Standardów HIT, który wydaje zalecenia do ONC w zakresie norm, specyfikacji oraz kryteriów certyfikacji elektronicznej wymiany informacji i korzystania z opieki zdrowotnej. Początkowo Komitet Standardów HIT skupił się na politykach opracowanych przez Komitet Polityczny HIT, a przy okazji powstały również tzw. Grupy Robocze, np. ds. wdrożeń, ds. standardów klinicznych.

Warto wskazać jeszcze na publiczny system informacji medycznej (AHIC) działający w latach 2005-2008, doradzający Sekretarzowi Stanu HHS, zalecający podjęcie konkretnych działań w celu osiągnięcia wspólnych ram interoperacyjności dla HIT. Efektem jest coraz częstsza sytuacja, kiedy pacjent podczas wizyty lekarskiej ogląda na monitorze swoje wyniki z laboratorium, przez co może lepiej zrozumieć, co się dzieje z jego stanem zdrowia.

Podsumowanie

Jak zauważa W. Cezary Włodarczyk, w poszukiwaniu dostatecznych środków (ich doboru) istnieje naturalna tendencja do zadowalania się rozwiązaniami znanymi z przeszłości albo łatwo dostępnymi. I nawet kiedy nastąpił już dobór środków i udało się zgromadzić wystarczające środki finansowe na realizację działań związanych z informacją w ochronie zdrowia, może uwydatnić się jeszcze jeden problem. Tym problemem jest pozyskanie odpowiedniej liczby dobrze przygotowanych kadr, które potrafią i chcą realizować przyjęte zadania. Ale opór w pozyskiwaniu informacji może pojawić się po stronie pacjentów, tym bardziej że coraz częstszym celem polityki zdrowotnej jest podwyższenie kapitału zdrowotnego, który jest wykorzystywany jako jeden z czynników produkcji.

Bartłomiej Michalak - prawnik, wykładowca, wdrożeniowiec, szef HELP-MED Outsourcing Medyczny, członek KSS Kamsoft SA, help-medi@wp.pl.

Proponujemy

SEMINARIUM
DATA CENTER - ASPEKTY TECHNOLOGICZNE I PRAWNE
10 maja 2011 r., Warszawa

W programie:
- aspekty prawne komercyjnego funkcjonowania Data Center,
- wykorzystanie wolnego oprogramowania (OS) w Data Center,
- bezpieczne Data Center - bezpieczne, czyli po prostu działające,
- przykładowy proces budowy Data Center - dostępne technologie, uwarunkowania techniczne,
- po czym poznać dobrą serwerownię - elementy infrastruktury Data Center decydujące o bezawaryjnym funkcjonowaniu serwerowni.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

ICT w inicjatywach przewodnich UE „Mobilna Młodzież" oraz „Program na rzecz nowych umiejętności i zatrudnienia"

Dariusz Bogucki

Wprowadzenie

Wśród 7 inicjatyw przewodnich, które przygotowała Komisja Europejska, przyjmując 3 marca 2010 roku Strategię Europa 2020 (Komunikatem COM(2010) 2020 „EUROPA 2020 – Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu"), są dwie inicjatywy skupiające się na szeroko pojętych umiejętnościach:

- **„Młodzież w drodze"** – projekt na rzecz radykalnej poprawy wyników systemów kształcenia oraz ułatwiania młodzieży wejścia na rynek pracy;
- **„Program na rzecz nowych umiejętności i zatrudnienia"** – projekt na rzecz modernizacji rynków pracy i wzmocnienia pozycji obywateli poprzez rozwój kwalifikacji przez całe życie w celu zwiększenia współczynnika aktywności zawodowej i lepszego dopasowania popytu do podaży na rynku pracy, między innymi dzięki mobilności siły roboczej.

Są one bardzo interesujące z punktu widzenia rozwoju ICT, albowiem w bardzo ciekawy sposób podchodzą do możliwości, jakie niosą technologie społeczeństwa informacyjnego i dlatego, jak się wydaje, warto się z nimi bliżej zapoznać.

„Mobilna młodzież"

Badania i analizy, jakie były podstawą do uruchomienia Inicjatywy Europa2020, szczególnie krytycznie odnosiły się do stanu wykształcenia i umiejętności młodych Europejczyków. Obecnie w krajach UE zbyt wiele osób kończy edukację szkolną przedwcześnie, a zbyt niewiele podejmuje studia wyższe, zwłaszcza w kierunkach ścisłych i technicznych. Europa kształtuje się w tym ostatnim aspekcie niekorzystnie nie tylko na tle USA, Japonii czy Chin, ale i Rosji, Indii a nawet Brazylii. Stanowi to poważne zagrożenie dla przyszłej europejskiej bazy zasobów umiejętności.

„Mobilna młodzież" ma być ważnym narzędziem w realizowaniu głównych celów zawartych w strategii Europa 2020, jakimi są obniżenie odsetka osób przedwcześnie kończących edukację szkolną z 15% do 10% oraz zwiększenie udziału osób posiadających wyższe wykształcenie lub jego odpowiednik z 31% do co najmniej 40% do roku 2020. Działania programu „Mobilna młodzież" pomogą również państwom członkowskim w osiągnięciu w ciągu następnego dziesięciolecia unijnego celu 75% poziomu zatrudnienia poprzez zapewnienie młodym ludziom możliwości zdobycia umiejętności odpowiednich do pracy w przyszłości.

Badania przeprowadzone przez Komisję wykazują, że do 2020 r. 35% nowych miejsc pracy wymagać będzie wysokich kwalifikacji, a 50% wymagać będzie kwalifikacji na średnim poziomie, a wspólnym czynnikiem jest konieczność sprawnego poruszania się w możliwościach, jakie dają technologie informacyjne. Kryzys finansowy i gospodarczy utrudnił młodym Europejczykom dostęp do rynku pracy – obecnie wskaźnik bezrobocia wśród młodzieży UE sięga bisko 21%.

Te wyzwania wymagają wspólnego działania i sprawnej koordynacji polityki w celu wskazania działań koniecznych na poziomie

UE i państw członkowskich. Komisja będzie wspierać państwa członkowskie w opracowaniu polityki mającej na celu pomoc osobom najbardziej zagrożonym bezrobociem, skuteczniejszą zachętę dla młodych innowacyjnych przedsiębiorców oraz pokonanie prawnych i administracyjnych przeszkód na drodze do mobilności edukacyjnej i zawodowej.

Niezależne badania pokazują, że ponad 40% pracodawców przywiązuje wagę do doświadczenia zdobytego w czasie studiów i pracy za granicą, które nie tylko obejmują poprawę znajomości języków obcych lecz także innych wysoko cenionych umiejętności, zwłaszcza z obszaru ICT.

Komisja Europejska zaproponowała w inicjatywie 10 najważniejszych działań, m.in.:

- **Uruchomienie specjalnego serwisu internetowego „Mobilna młodzież”**, gdzie będzie można uzyskać informacje na temat możliwości podjęcia studiów lub zdobycia doświadczenia zawodowego za granicą, w tym również porady dotyczące grantów unijnych i indywidualnych praw. Opierać się będzie na zasobach takich jak portal Możliwości Kształcenia w Europie (PLOTEUS), ale kompletnie przeredagowany i przebudowany w kierunku portalu społecznościowego.
- Związany z poprzednim **Projekt pilotażowy „Twoja pierwsza praca z EURES-em**”, w ramach którego będzie można znaleźć porady, możliwości zatrudnienia i wsparcie finansowe dla młodych ludzi poszukujących pracy, którzy chcieliby pracować za granicą oraz dla firm - zwłaszcza małych i średnich przedsiębiorstw. Projekt zarządzany będzie przez EURES, sieć europejskich publicznych służb zatrudnienia i zacznie funkcjonować w 2011 r.
- **Tablica wyników mobilności**, gdzie będą notowane i mierzone postępy w dziedzinie usuwania prawnych i technicznych przeszkód na drodze do mobilności edukacyjnej przez poszczególne kraje UE. Szczególnie wysoko oceniane będzie wspieranie zdobywania przez młodzież umiejętności związanych z technologiami ICT.
- Komisja we współpracy z Europejskim Bankiem Inwestycyjnym bada możliwość utworzenia **europejskiego systemu pożyczek studenckich**, które miałyby udzielać wsparcia studentom planującym naukę lub szkolenia za granicą.
- Trwają prace nad opracowaniem **nowego wielowymiarowego globalnego systemu rankingu dla uniwersytetów**, który ma zapewnić pełniejszy i bardziej realistyczny obraz osiągnięć szkolnictwa wyższego niż ten, który prezentują obecne rankingi. Komisja zakłada, że szczególnie promowane będą kierunki ścisłe i techniczne.
- Trwają prace nad opracowaniem **Karty „Mobilna Młodzież”**, oferującej młodym ludziom różne korzyści i rabaty, w szczególności w trakcie podróżowania i nabywania nowych umiejętności.
- Nowa inicjatywa Komisji - **europejski instrument mikrofinansowy** na rzecz zatrudnienia i włączenia społecznego Progress, który zapewni młodym przedsiębiorcom finansowe wsparcie w zakładaniu i rozwoju firm, szczególnie w obszarze innowacyjnego wykorzystania nowych technologii.
- Komisja zaproponuje Europejski paszport umiejętności oparty na projekcie Europass (Europejskie CV online), aby umożliwić uporządkowany i przejrzysty zapis umiejętności. Start: jesień 2011 r.

„Program na rzecz nowych umiejętności i zatrudnienia”

Ściśle związany z poprzednią inicjatywą jest „Program na rzecz nowych umiejętności i zatrudnienia”. Program ten ma pomóc Komisji w podniesieniu do 75% wskaźnika zatrudnienia mężczyzn i kobiet należących do grupy wiekowej 20-64 lata do roku 2020. Obecna stopa bezrobocia w UE przekroczyła 10%. Niewątpliwie

jest to wynik kryzysu gospodarczego, natomiast niepokojąca jest jego struktura, to, że dotyka głownie ludzi młodych. Europejskie społeczeństwo starzeje się, dlatego utrzymanie modelu społecznego UE uzależnione jest od wzrostu zatrudnienia i tego, aby pracownicy mieli kwalifikacje, jakie potrzebne będą na rynkach pracy w perspektywie roku 2020.

Komisja proponuje trzynaście konkretnych działań, które mają usprawnić funkcjonowanie rynków pracy w Europie, które wpisują się w następujące działania:

- Przyspieszenie reformy rynku pracy dla poprawy elastyczności i bezpieczeństwa rynków pracy („flexicurity").
- Odpowiednie mechanizmy zachęcające przedsiębiorstwa i osoby indywidualne do inwestowania w szkolenia, aby stale podnosić poziom umiejętności zgodnie z zapotrzebowaniami rynku pracy, zwłaszcza w zakresie umiejętności związanych z ICT.
- Aby zapewnić przyzwoite warunki pracy przy równoczesnej poprawie jakości prawodawstwa w zakresie zatrudnienia, Komisja przedstawi wnioski dotyczące przeglądu dyrektywy w sprawie czasu pracy oraz wystąpi z inicjatywą legislacyjną na rzecz poprawy wdrażania dyrektywy o delegowaniu pracowników. Promowane będą elastyczne formy zatrudnienia jak np. telepraca.
- Zapewnienie odpowiednich warunków na rynku pracy sprzyjających tworzeniu nowych miejsc pracy, w tym zmniejszanie obciążeń administracyjnych i obniżanie podatków związanych z zatrudnieniem i mobilnością, co jest szczególnie ważne dla szybko rozwijających się sektorów, na przykład prowadzących prace badawczo-rozwojowe, nowych technologii itd.

W nawiązaniu do opisanych wyżej programów Komisja rozpoczęła tworzenie założeń nowych programów w zakresie wspierania szkolnictwa wyższego. Nowe programy mają wspierać te kierunki studiów, które wpisują się w realizację strategii Europa 2020, a więc w rozwój gospodarki opartej na wiedzy, badaniach i innowacjach. Programy powinny pomóc Europejczykom:

- dostosować się do rynku pracy, na którym większość miejsc pracy wymaga wysokiego lub średniego poziomu umiejętności i na którym jest coraz mniej miejsc pracy dla osób bez solidnego przygotowania zawodowego, ze szczególnym podkreśleniem umiejętności w zakresie ICT;
- funkcjonować w społeczeństwie, w którym coraz więcej ludzi korzysta z usług on-line i wykonuje codzienne czynności za pośrednictwem Internetu;
- zdobyć najważniejsze w XXI umiejętności (znajomość języków obcych, przedsiębiorczość, obeznanie z technologiami ICT), które są istotne w obecnym życiu zawodowym i prywatnym.

Wnioski dla Polski

Z powyższego opisu widać, że Komisja konsekwentnie programuje głębokie zmiany obecnych ram wsparcia UE dla krajów członkowskich. Zmienią się, jak widać, ramy nie tylko na „twarde projekty" z obszaru innowacyjności, badań i rozwoju, ale i na „miękkie projekty" związane z edukacją i umiejętnościami. Ważne jest natomiast, jak wielką rolę opisane wyżej inicjatywy przykładają do wiedzy i umiejętności związanych z technologiami społeczeństwa informacyjnego.

Z jednej strony potwierdza to opinię, że nowa perspektywa finansowa będzie zdecydowanie trudniejsza w realizacji od obecnej. Tym niemniej szerokie wsparcie UE dla ICT, ze szczególnym podkreśleniem umiejętności związanych z nimi, otwiera nowe, interesujące możliwości.

Dr inż. Dariusz Bogucki - Dyrektor ds. Sektora Publicznego, EFICOM SA.

Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne – część V

Wojciech Kaliński

Rekomendacja 2: zarządzanie informatyką w organizacji zgodnie z najlepszymi praktykami i standardami

Przedmiotowe rekomendacje sprowadzają się w ogólnym zarysie do obowiązku wprowadzenia przez zamawiających jednolitych norm, metodyk i standardów w zakresie zarządzania podstawowymi procesami IT. Urząd Zamówień Publicznych wskazuje w tym zakresie dwie zasadnicze grupy błędów popełniane przez zamawiających. Pierwszy z nich stanowi połączenie i uzależnienie procesów rozwoju systemu (zarządzanie zmianą) i jego bieżącego utrzymania (zarządzanie konfiguracją, zarządzanie incydentem). Jako uzasadnienie wskazuje się na fakt, że *„utrzymanie systemu wymaga odmiennych kompetencji aniżeli prowadzenie jego rozbudowy. W większości przypadków nie wymaga też dostępu do kodów źródłowych, do których wyłączne prawa posiada niekiedy autor systemu (w zależności od zapisów umownych), co jest stanem odwrotnym niż w przypadku rozwoju systemu. W efekcie połączenie tych dwóch istotnie różnych usług w jednym zamówieniu przenosi ograniczenie konkurencji wynikające z praw wyłącznych przysługujących podmiotowi rozwijającemu system na usługi utrzymania systemu, co do których brak jest ograniczeń prawnych i technicznych uniemożliwiających ich wykonanie przez podmiot inny aniżeli wykonawca prac rozwojowych."* Z powyższą tezą nie do końca można się zgodzić. Nie jest bowiem do końca prawdą, że utrzymanie systemu wymaga odmiennych kompetencji niż jego rozbudowa. Kompetencje te w pewnych aspektach rzeczywiście są trochę różne, ale nie aż tak, jak wydaje się to wynikać z interpretacji Urzędu. Po drugie, stanowisko Urzędu zapomina o jednej istotnej korzyści wynikającej ze skumulowania utrzymania i rozwoju systemu w jednym ręku: zamawiający ma w takim wypadku jeden podmiot odpowiedzialny za obydwa procesy i eliminuje tym samym zarówno konflikty między wykonawcami na styku ich kompetencji, jak i przerzucanie się między innymi odpowiedzialnością za nieprawidłowe działanie systemu. Z punktu widzenia sprawności działania organizacji oraz bezpieczeństwa IT nie jest to kwestia banalna. Zgodzić się natomiast należy z dwoma pozostałymi wnioskami Urzędu, a mianowicie że do utrzymania systemu nie jest potrzebny dostęp do kodów źródłowych oraz że utrzymanie systemu nie uprawnia do udzielania na nie zamówienia z wolnej ręki, a zatem łączenie tych usług z rozwojem systemu jest niepotrzebnym ograniczaniem konkurencji. To ostatnie zdanie wymaga jedynie uzupełnienia o stwierdzenie, że zasada ta dotyczy udzielania zamówień w trybach niekonkurencyjnych, a nie rozpisania przetargu na budowę systemu wraz z jego utrzymaniem i rozwojem.

Jako drugi błąd Urząd wskazuje udzielenie zamówienia na administrację systemem, obsługę incydentów, wsparcie eksploatacji systemu wykonawcy świadczącemu gwarancję na wykonany system lub dotychczasowemu wykonawcy w trybie wyłączającym konkurencję, tj. w trybie z wolnej ręki, uzasadniając to tezą, że „*zgodnie ze standardami zarządzania systemami informatycznymi*

i dobrą praktyką procesy reagowania na incydenty i wsparcie eksploatacji systemu powinny być oddzielone od procesów wprowadzania zmian w systemie (stanowi element świadczenia gwarancji), wymagają także odmiennego zakresu wiedzy i kompetencji. Brak jest zatem przesłanek pozwalających na udzielenie zamówienia w trybie z wolnej ręki." W przypadku tego zastrzeżenia, o ile można zgodzić się z główną tezą Urzędu, iż „zamówienia na administrację systemem, obsługę incydentów, wsparcie eksploatacji systemu" nie spełniają przesłanek udzielenia zamówienia z wolnej ręki, o tyle samo uzasadnienie tej tezy oparte o standardy zarządzania i dobre praktyki już nie przekonuje. Zwłaszcza że takie podejście oznacza brak jednego ośrodka decyzyjnego i odpowiedzialnego za prawidłowe działanie systemu.

Na podstawie tych zastrzeżeń Urząd przedstawił 6 rekomendacji:

Rekomendacja R.2.1. Rekomendacja organizacyjna: zarządzanie systemami informatycznymi winno być prowadzone zgodnie z odpowiednimi standardami (np. ITIL, ISO 20000, COBIT) i dobrymi praktykami w tym zakresie. Zaleca się certyfikację organizacji w zakresie zgodności systemu zarządzania usługami/systemami IT z odpowiednimi normami, w szczególności zamawiającym użytkującym/rozwijającym systemy o znacznej wartości.

Powyższa rekomendacja raczej nie powinna budzić zastrzeżeń. Co więcej wyraźnie wskazuje, że dopuszczalne jest stawianie przez zamawiających wymagań w postępowaniach, by wykonawcy stosowali określone metodyki zarządzania i by posiadali na dowód tego określone certyfikaty. Jest to więc dobry argument „obronny" na wypadek podnoszenia przez wykonawców zarzutów bezpodstawnego wymagania certyfikatów czy znajomości określonych metodyk zarządzania. Oczywiście należy sobie zdawać sprawę, czy wymóg posiadania określonego certyfikatu jest wymaganiem dyskryminującym podmioty, które np. posiadają własne metodyki. Dlatego wymagania tego należy używać bardzo ostrożnie, z dużą znajomością danego rynku IT tak, by nie wyeliminować niepotrzebnie znaczącej konkurencji. Podobnie za zbyt daleko idący wymóg należy uznać postawienie wymagania dopuszczającego tylko jednego z możliwych certyfikatów. Takie wymaganie stanowiłoby nieuzasadnione ograniczenie konkurencji.

Rekomendacja R.2.1.a Rekomendacja organizacyjna: procesy zarządzania zmianami (prowadzenie prac rozwojowych i rozwiązywania problemów) powinny być realizowane oddzielnie od procesów bieżącego utrzymania i konserwacji systemu (procesy zarządzania incydentami i konfiguracją). Podstawowe wnioski wynikające z tej rekomendacji zostały już omówione w ramach analizy zagadnień wstępnych. Należy jedynie powtórzyć, że wadą tego rozwiązania jest brak jednego podmiotu odpowiedzialnego za wszystkie elementy zarządzania systemem. Z tego względu przy konstruowaniu tego typu postępowań i określaniu warunków umów należy baczną uwagą zwrócić na zapewnieniu czytelnych kompetencji między jednym i drugim wykonawcą (co wbrew pozorom nie jest takie proste) oraz na wprowadzenie mechanizmów zapewniających niezbędny poziom współpracy między poszczególnymi wykonawcami (co jest jeszcze trudniejsze). Często w takich przypadkach stosuje się mechanizmy prawne pozwalające jednemu z wykonawców domagać się od drugie

określonego działania i to bez konieczności osobistej ingerencji i pośrednictwa zamawiającego. Oczywiście wprowadzenie takiego rozwiązania zależy od wielu czynników: zasad wynagradzania wykonawców - ryczałt czy w oparciu o stawkę (by inny wykonawca nie zaciągał w imieniu zamawiającego zobowiązań finansowych), zakresu obowiązków wykonawców (by uniknąć zagrożenia, że wykonawca będzie starał się przerzucić na drugiego wykonawcę swoje obowiązki kontraktowe), zakresu czynności, które mogą być „zlecane" bezpośrednio itd.

Rekomendacja R.2.1.b Rekomendacja organizacyjna: wprowadzanie zmian w systemie powinno odbywać się w ramach dobrze zdefiniowanych i realizowanych procesów zarządzania zmianą, problemem i wydawaniem, których celem jest zminimalizowanie liczby i prawdopodobieństwa powstania zakłóceń w działaniu systemu wskutek zmian i uzupełnień wprowadzanych w systemie. Przedmiotowa rekomendacja ma stosunkowo mniejsze znaczenie prawne. Jakkolwiek w uzasadnieniu tej rekomendacji stwierdzono, że *„zastosowanie tej rekomendacji zmierza do rozdzielenia prac prowadzących do zmian w konstrukcji i działaniu systemu od prac administracyjno-konserwacyjnych*", jednak spostrzeżenia zawarte w rekomendacji mają charakter bardziej uniwersalny i odnoszą się do każdego procesu wprowadzania zmian bez względu na to, w jakim trybie postępowania doszło do udzielenia zamówienia na dokonywanie zmian w systemie oraz czy wprowadzanie tych zmian jest, czy też nie jest powiązane z innymi pracami w zakresie administrowania systemem.

Rekomendacja R.2.1.c Rekomendacja organizacyjna: zmiany przed wprowadzeniem do środowiska produkcyjnego powinny być testowane na oddzielnym środowisku (deweloperskim i/lub testowym) i po pozytywnym wyniku testów zatwierdzone do wprowadzenia (w przypadku dużych systemów IT rekomenduje się korzystanie z 3 środowisk: deweloperskiego, testowego i produkcyjnego). Podobnie jak w przypadku poprzedniej rekomendacji sama rekomendacja nie do końca pokrywa się z jej uzasadnieniem. W uzasadnieniu stwierdza się bowiem: „*zalecenie to podobnie jak R.2.1.a i R.2.1.b zmierza do uniezależnienia prac rozwojowych lub innych prac wymagających zmian w budowie systemu od prac o charakterze utrzymaniowym*." Szczerze powiedziawszy, trudno zrozumieć, na czym miałby polegać związek pomiędzy zasadami testowania oprogramowania na wydzielonym środowisku a uniezależnieniem prac rozwojowych lub innych prac wymagających zmian w budowie systemu od prac o charakterze utrzymaniowym. Wskazane w rekomendacji zasady testowania zmian można bowiem prowadzić zarówno w przypadku, gdy wprowadzanie zmian stanowiło przedmiot odrębnego postępowania, jak i w sytuacji gdy było ono traktowane łącznie z innymi usługami. Niezależnie od tej kwestii należy jednak pamiętać, że budowa równolegle dwóch środowisk, które muszą być do siebie jak najbardziej zbliżone, jest rozwiązaniem bardzo kosztownym, zwłaszcza przy bardziej złożonych systemach. Dotyczy to w szczególności konieczności zapewniania licencji na oprogramowanie bazodanowe, które rzadko bez nabycia dodatkowych licencji może być jednocześnie wykorzystywane jako oprogramowanie dla potrzeb systemu produkcyjnego i jednocześnie testowego, co automatycznie podwaja koszty takiego rozwiązania. Warto mieć tę kwestię na uwadze, decydując się na budowę dwóch równoległych środowisk. Z drugiej oczywiście strony dwa środowiska zapewniają znacząco większe bezpieczeństwo przy rozwoju systemu.

Rekomendacja R.2.1.d Rekomendacja organizacyjna: zaleca się, by wiedza o sposobach rozwiązania problemów i właściwych reakcjach na incydenty była gromadzona w sposób zaplanowany i uporządkowany. Jak Urząd wskazuje w uzasadnieniu tej rekomendacji, „*zgromadzona wiedza o sposobach rozwiązywania problemów i reakcjach na incydenty pozwala zamawiającemu uniezależnić się w zakresie utrzymania systemu od jego wykonawcy. Warunkiem osiągnięcia tego celu jest zapewnienie przepływu informacji między zespołami realizującymi te dwa zadania.*" Jakkolwiek z samą tezą rekomendacji nie sposób się nie zgodzić, o tyle uzasadnienie jej stosowania wydaje się momentami zbyt optymistyczne. Zgromadzona wiedza o sposobach rozwiązywania problemów i reakcjach na incydenty może zmniejszyć uzależnienie zamawiającego od wykonawcy w zakresie utrzymania systemu, ale zależności tej całkowicie nie wyeliminuje. Zawsze może pojawić się incydent, który wcześniej nie występował. Takie zdarzenia mają często miejsce w wypadku zmian w systemie lub w przypadku wprowadzania nowych rozwiązań informatycznych współpracujących z systemem. Nie zmienia to jednak faktu, że gromadzenie wiedzy o incydentach i sposobie ich rozwiązywania jest jak najbardziej pożądane.

Dr Wojciech Kaliński - asystent w Katedrze Prawa Cywilnego Uniwersytetu Jagiellońskiego, wspólnik w kancelarii Maruta i Wspólnicy sp. j.

Zapraszamy do udziału

WARSZTATY

WALKA Z PRANIEM PIENIĘDZY PO NOWEMU, CZYLI O PROBLEMACH IMPLEMENTACJI NOWYCH ROZWIĄZAŃ W PRAKTYCE

Dlaczego warto wziąć udział w warsztatach?

- Poznacie Państwo fundamentalne zmiany wprowadzane do systemu prawnego przez dużą nowelizację do polskiej Ustawy w sprawie "prania pieniędzy", a także zmiany wprowadzane przez III Dyrektywę w sprawie "prania pieniędzy".
- Przedstawiony zostanie Państwu stan dyskusji na temat sposobu wdrażania nowych rozwiązań związanych z "praniem pieniędzy" i podstawowych kłopotów dotyczących tego procesu.
- Dowiecie się Państwo, jak wasza instytucja może być narażona na "pranie pieniędzy".
- Jakie obowiązki ciążą na "instytucjach obowiązanych" i ich pracownikach, a także jaka jest osobista odpowiedzialność członków zarządów "instytucji obowiązanych".
- Zaprezentowane zostaną Państwu niezgodności pomiędzy prawem polskim i wspólnotowym, a także ich praktyczne następstwa.
- Zaprezentowaną zostaną zalecenia i rekomendacje Generalnego Inspektora Informacji Finansowej i bieżąca praktyka sądowa w zakresie procederu "prania pieniędzy" oraz ochrony danych osobowych.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Artykuł 27 czy paragraf 22?

Robert Podpłoński

Wstęp

W lutym 2011 r. minęła druga rocznica chaosu na rynku telekomunikacyjnym związanego z wydawanymi przez Prezesa UKE decyzjami w sprawie zmian umów o połączeniu sieci. Decyzjami tymi Prezes UKE obniża stawki za zakańczanie połączeń w sieciach poszczególnych operatorów. Niestety, wbrew dotychczasowej praktyce, decyzje te nie obniżyły stawek symetrycznie i u obu kontrahentów jednocześnie, lecz odrębnie u każdego z nich. Każdy na zmianę swoich stawek musiał czekać. Każdy dzień oczekiwania na decyzję Prezesa UKE to kilkaset tysięcy złotych strat. W związku z tym narażeni na tak duże straty operatorzy telekomunikacyjni starali się uniknąć doręczenia im decyzji i doczekać drugiej, korzystnej dla nich. Należy zauważyć, że takimi rozstrzygnięciami Prezes UKE zaskoczył wszystkich uczestników rynku. Każdy z operatorów oczekiwał wydania jednej decyzji regulującej wzajemne stawki, zgodnie z dotychczasową linią UKE. Tymczasem Prezes UKE rozstrzygał o stawkach u jednego operatora, a umarzał postępowanie w zakresie obniżenia stawek u drugiego operatora. Doprowadziło to do kompletnego chaosu. Pierwszą ofiarą Prezesa UKE miała paść PTK Centertel. Prezes UKE wydał decyzję na korzyść PTC, a przeciwko PTK Centertel, a następnie przeciwko Polkomtel, nadając im rygor natychmiastowej wykonalności. Obie firmy skutecznie unikały doręczenia im tych decyzji, zmieniając pełnomocników. Wreszcie Polkomtel doczekał się swojej decyzji przeciwko PTC i to PTC zaczęła unikać doręczenia jej decyzji korzystnej dla Polkomtel, także stosując sprawdzony sposób zmiany pełnomocnika. Następnie zapadła decyzja na korzyść PTK przeciwko PTC. Od kwietnia 2009 r. każdy operator unikał doręczenia mu jednej decyzji i jednocześnie niecierpliwie czekał na doręczenie konkurentowi drugiej. Mogło się nawet okazać, że PTC, której wydawało się, że z nieba spadło jej kilkanaście milionów złotych, na całej operacji straci, jeżeli decyzje konkurentów zostałyby jej doręczone wcześniej. Nie było również wykluczone, że pozostając w przekonaniu o doręczeniu decyzji do PTK i Polkomtel, skupiła ruch innych operatorów i transmitowała go do sieci PTK i Polkomtel po nowych, niższych stawkach z marżą. Gdyby za ten ruch nie mogła zastosować obniżonych stawek, to mogło się okazać, że na tej operacji także – zamiast spodziewanych zysków – poniesie straty.

Decyzje te wreszcie zostały doręczone, jednak nie musiało to zakończyć chaosu, lecz mogło być ledwie początkiem dla niego, jeśli decyzje te zostaną poddane pod rozstrzygnięcie sądowe. Różne składy i w różnych terminach będą rozstrzygać odrębnie o każdej z nich. Teoretycznie mogą zapaść różne rozstrzygnięcia w podobnych sprawach. Uchylenie lub zmiana każdej z nich w różnym czasie może zobowiązać strony do wstecznych rozliczeń przy jednoczesnym obowiązku stosowania decyzji, co do której sąd jeszcze się nie wypowiedział. Jeżeli dołożyć do tego fakt, że UKE ma zwyczaj nie spieszyć się z przekazywaniem akt do sądu, okres, za który spółki będą się musiały rozliczyć, może wynosić kilka lat. Jak się pomnoży pół miliona dziennych strat przez tak długi

okres, sprawa przestaje być bardzo poważna, a zaczyna być poważna kosmicznie. Konieczność zwrotu kilkuset milionów złotych może doprowadzić spółki na skraj bankructwa.

Powyższe zdarzenia i ryzyka skłoniły autora niniejszego artykułu do przeprowadzenia rozważań prawnych dotyczących przyjętego przez Prezesa UKE trybu postępowania oraz interpretacji stosowanych w 2009 r. przepisów.

Analiza prawna

Pojęcie negocjacji

Zgodnie z art. 26 ust. 1 prawa telekomunikacyjnego (PT)[1] „operator publicznej sieci telekomunikacyjnej jest obowiązany do prowadzenia negocjacji w sprawie zawarcia umowy o dostępie telekomunikacyjnym na wniosek innego przedsiębiorcy telekomunikacyjnego lub podmiotów, o których mowa w art. 4 pkt. 1, 2, 4, 5, 7 i 8, w celu świadczenia publicznie dostępnych usług telekomunikacyjnych oraz zapewnienia interoperacyjności usług.". Jednocześnie zgodnie z art. 27 ust. 1 PT „Prezes UKE może, na pisemny wniosek każdej ze stron negocjacji o zawarcie umowy o dostępie telekomunikacyjnym albo z urzędu, w drodze postanowienia określić termin zakończenia negocjacji o zawarcie tej umowy, nie dłuższy niż 90 dni, licząc od dnia wystąpienia z wnioskiem o zawarcie umowy o dostęp telekomunikacyjny." Wreszcie na podstawie art. 30 PT[2] do zmian umów o dostępie telekomunikacyjnym przepisy te stosuje się odpowiednio.

Dla przedmiotowej sprawy niezwykle istotne jest rozstrzygnięcie zakresu uprawnienia wnioskodawcy z art. 27 ust. 1 oraz uprawnienia Prezesa UKE w tym zakresie, a także ustalenie pojęcia negocjacji, o którym mowa w tych przepisach.

Mając na uwadze fakt, że pojęcie negocjacji nie zostało zdefiniowane w PT, dokonując wykładni jego zakresu pojęciowego, należy sięgnąć po instytucję rokowań, które regulowane są w art. 72 k.c. Trafne w tym zakresie wydają się być wywody zawarte w wyrok Sądu Apelacyjnego w Warszawie[3] na temat zakresu pojęciowego negocjacji. W ocenie sądu: „definicja pojęcia *'negocjować'*, zawarta w Uniwersalnym słowniku języka polskiego, Wydawnictwo Naukowe PWN, Warszawa 2003, tom 2, str. 878, jest następująca: *'targować się w celu uzyskania niższej ceny lub korzystniejszych warunków zakupu'*. Można zatem stwierdzić, że istotą negocjacji (rokowań) jest dochodzenie do porozumienia w kwestiach spornych, w celu sfinalizowania określonej czynności, na warunkach satysfakcjonujących potencjalnych kontrahentów." Aktualne pozostają również teza i uzasadnienie zawarte w wyroku Sądu Najwyższego - Izba Cywilna[4], w których Sąd słusznie stwierdza, że: „*rokowania różnią się i to zasadniczo od zawierania umowy przez złożenie oferty i jej przyjęcie. W wypadku oferty oferentowi przypada rola formułowania treści zamierzonej umowy, a oblatowi rola akceptanta. Natomiast w rokowaniach* ***role obu stron są takie same****. Rokowania znamionują się stopniowym „ucieraniem się" stanowisk obu stron, a skutki ich działań wynikają z samej ich doniosłości lub nawet upływu czasu.* ***Czynności te pozostają ze sobą***

1 Art. 26 ust. 1 nie obowiązuje od 6 lipca 2009 r., ale pozostaje to bez większego wpływu na prowadzone rozważania.
2 Obecnie art. 30 ust. 1 PT.
3 Wyrok z dnia 12 stycznia 2006 r., sygn. I ACa 672/2005.
4 Wyrok z dnia 16 grudnia 2003 r., sygn. II CK 335/02.

w nierozerwalnym związku. *Rokowania, będące typowym sposobem zawarcia umowy, polegają na wzajemnym oddziaływaniu stron w celu osiągnięcia wiążącego porozumienia (zawarcia umowy). Strony, przystępując do rokowań, mają wolę zawarcia umowy, lecz* ***dopuszczają kilka wariantów jej treści*** *i jednocześnie względem alternatywnych wariantów tej treści mają niezgodne preferencje. Każda z nich dąży do ukształtowania umowy według własnych potrzeb.*"

Zgodnie z powyższym należy stwierdzić, że przywołane orzecznictwo i doktryna uznają, że negocjacje to ciągły i jednolity proces uzgadniania treści umowy w celu osiągnięcia konsensusu. Należy stwierdzić, że wykładnia tego pojęcia w zasadniczy sposób wpływa na zakres upoważnienia wnioskodawcy, a przede wszystkim uprawnień Prezesa UKE, w związku z art. 27 ust. 1 PT. Przepis ten jednoznacznie wskazuje, że Prezes UKE może postanowieniem określić termin zakończenia negocjacji o zmianę umowy. Jak wynika z powyższego, negocjacje **to proces jednolity i niepodzielny**. Przedmiotem negocjacji w rozumieniu art. 27 PT jest zmiana umowy w takim zakresie, w jakim strony przedstawiały swoje propozycje. Każdej ze stron przysługują takie same prawa i żadnej nie mogą zostać przyznane szczególne uprawnienia względem drugiej zarówno na mocy prawa cywilnego, jak i administracyjnego. Stąd brak jest podstaw do uznania, że Prezesowi UKE przysługuje uprawnienie do ustalenia zakresu negocjacji, a nawet wydzielenia ich części. Nie można też wywieść takich twierdzeń z przepisów k.p.a. regulujących pojęcie wniosku o wszczęcie postępowania administracyjnego. Przyznanie stronie negocjacji lub Prezesowi UKE upoważnienia do określenia zakresu negocjacji jest sprzeczne z prawem telekomunikacyjnym, prawem cywilnym i Konstytucją RP, a do tego konieczny byłby jednoznaczny przepis prawny. Należy przypomnieć, że obowiązująca w prawie administracyjnym zasada związania organu wnioskiem strony, nie ma charakteru bezwzględnego. W przypadku załatwienia sprawy w drodze ugody administracyjnej zakres wniosku wszczynającego postępowanie nie wpływa na treść ugody w takim stopniu jak na wydanie decyzji, w szczególności dopuszczalne jest zawarcie ugody wykraczającej poza wniosek o wszczęcie postępowania, a granicą treści ugody jest stosunek administracyjno-prawny objęty kompetencjami organu zatwierdzającego ugodę, przepisy prawa, stanowisko organu oraz interes społeczny bądź słuszny interes stron. W przedmiotowej sprawie Prezes UKE nie rozstrzyga o stosunku administracyjnym, a między stronami a organem nie ma stosunku nadrzędności, charakterystycznego dla tego typu stosunków, żadna ze stron nie zwraca się o przyznanie uprawnień lub nałożenie obowiązków o charakterze publicznoprawnym. Na mocy szczególnego przepisu Prezes UKE rozstrzyga spór cywilny, a postępowanie ma charakter kontradyktoryjny. Zawarcie przez strony umowy powoduje konieczność umorzenia postępowania, a wydana decyzja przestaje wiązać strony, jeżeli – nawet po jej doręczeniu – strony odmiennie ukształtują swój stosunek cywilnoprawny. Nie narusza to oczywiście szczególnych uprawnień Prezesa UKE wynikających z art. 29 PT, jednak w przedmiotowej sprawie podstawą rozstrzygnięcia jest art. 27 PT. Kontradyktoryjność postępowania oraz cywilny charakter sporu wpływają w istotnym stopniu na zakres kompetencji Prezesa UKE oraz zakres uprawnień stron. Jak już podniesiono powyżej, stronie nie przysługują uprawnienia, które mogłyby ograniczać wpływ drugiej strony na wynik postępowania. W tym też kontekście należy rozpatrywać wnioski o ustalenie terminu zakończenia negocjacji oraz wnioski o wydanie decyzji, o których mowa w art. 27 ust. 1 i 2 PT.

Warto również w tej kwestii przytoczyć wyrok Naczelnego Sądu Administracyjnego[5], w którym sąd stwierdza: „*interpretacje i zastosowanie*

5 Wyrok z dnia 29 stycznia 2002 r., sygn. I SA 1207/2001, LexPolonica nr 394901.

przepisów prawa powinny wynikać z ich treści, odnoszącej się do konkretnego stanu faktycznego, a nie wymyślonych koncepcji oderwanych od treści przepisu i stanu faktycznego sprawy, gdyż takie koncepcje podważają zaufanie obywateli do organów Państwa (art. 8 kpa)".

Prawo do złożenia wniosku o wydanie decyzji w sprawie rozstrzygnięcia kwestii spornych lub określenia warunków współpracy w trybie art. 27 ust. 2 PT nie przyznaje wnioskodawcy roszczenia materialno-prawnego, nie stwarza ono bowiem możliwości żądania od drugiej strony zachowania się w określony sposób. Trudno też uznać je za uprawnienie prawokształtujące, skoro zainteresowana strona sama w drodze jednostronnego oświadczenia woli nie może ukształtować nowego stanu prawnego.

W przedmiotowych sprawach PTK, PTC i Polkomtel składały sobie propozycje zmiany umowy o połączeniu sieci w zakresie wzajemnych rozliczeń z tytułu zakańczania połączeń w swoich sieciach. Do dnia złożenia wniosku o ustalenie terminu zakończenia negocjacji strony wymieniały się swoimi propozycjami zmian oraz prowadziły negocjacje mające na celu uregulowanie wzajemnych stosunków, w tym również w zakresie stawek za zakańczanie połączeń w obu sieciach. Stawki za zakańczanie połączeń miały być symetryczne. Co nie może dziwić, gdyż stawki te wynikają nie tyle z woli stron, co z doręczonych im wcześniej decyzji MTR[6]. Tak więc przedmiot i zakres negocjacji na dzień składania wniosków o określenie terminu zakończenia negocjacji obejmował wszelkie propozycje stron, w szczególności określone w składanych wzajemnie aneksach. Jednakże mimo formalnej zgodności co do wzajemnych stawek za zakańczanie połączeń do zawarcia umowy nie doszło, gdyż zgodnie z art. 72 k.c. jeżeli strony prowadzą negocjacje w celu zawarcia oznaczonej umowy, umowa zostaje zawarta, gdy strony dojdą do porozumienia co do wszystkich jej postanowień, które były przedmiotem negocjacji. Wobec braku uzgodnienia pozostałych postanowień negocjacje nie mogły zakończyć się zmianą umowy.

Prezes UKE w odpowiedzi na wnioski PTC ustalał termin zakończenia negocjacji. Godne jest przywołać sentencję tych postanowień: „**postanawiam określić na dzień …… termin zakończenia negocjacji zmian Umowy rozpoczętych w dniu …….. wraz z doręczeniem do PTK/Polkomtel wniosku PTC**." Sentencja postanowień jednoznacznie wskazuje, że Prezes UKE postąpił zgodnie ze swoimi uprawnieniami i ustalał termin zakończenia negocjacji rozpoczętych wnioskami PTC. Wnioski te obejmowały rozliczenia wzajemne, a dalsze działania stron także zmierzały w tym celu. Tak więc należy uznać, że zakres rokowań obejmował całą negocjowaną zmianę umowy o połączeniu sieci, w tym stawki za zakańczanie połączeń w obu sieciach. Znajduje to także potwierdzenie w uzasadnieniach do przedmiotowych decyzji, w których Prezes UKE potwierdził, że negocjacje w zakresie warunków rozliczeń za zakańczanie połączeń w sieci PTC także rozpoczęły się w tym dniu właśnie na skutek tego samego pisma. W tym samym postanowieniu Prezes UKE stwierdza, że termin zakończenia negocjacji wyznaczył na dzień, który w jego ocenie „jest wystarczający, **aby Strony mogły swobodnie ukształtować łączący je stosunek prawny**", potwierdzając sentencję postanowienia, że ustalony termin zakończenia negocjacji dotyczy ich jako całości, a nie bliżej nieokreślonej części.

Co więcej, każda ze stron pozostawała w przekonaniu, że postanowienia ustalały termin zakończenia negocjacji w całości,

6 Decyzje ustalające stawki za zakończenie połączeń.

a nie w części. Znajduje to potwierdzenie w stanowiskach stron, składanych aneksach oraz wnioskach o wydanie decyzji.

Tymczasem Prezes UKE w uzasadnieniu decyzji wydanej na podstawie art. 27 PT w wyniku braku uzgodnień kończących negocjacje dokonał w sposób nieuprawniony i z naruszeniem art. 27 PT oraz m.in. zasad:

1) praworządności, wynikającej z art. 7 Konstytucji i art. 6 k.p.a.,
2) zaufania do organów Państwa, wynikającej z art. 8 k.p.a.

interpretacji własnego postanowienia, ustalając nie tylko termin zakończenia negocjacji, ale także ich zakres. Mimo jednoznacznej wykładni językowej i funkcjonalnej art. 27 ust. 1 **Prezes UKE uzurpował sobie kompetencje do rozstrzygania postanowieniem także o zakresie prowadzonych negocjacji, a nawet do wyodrębnienia z nich części i poddania jej osobnemu postępowaniu administracyjnemu**. Działanie Prezesa UKE pozostało w jaskrawej sprzeczności z treścią art. 27 ust. 1 PT. Żadnej ze stron ani Prezesowi UKE – działającemu z urzędu czy na wniosek – nie przysługuje prawo do ustalania zakresu negocjacji ani do wyodrębniania ich części. Zakres negocjacji jest kształtowany wolą obu stron i wynika ze złożonych wzajemnie oświadczeń i propozycji. Rolą Prezesa UKE jest jedynie zdopingowanie stron do ich wcześniejszego zakończenia. Różny interes prawny stron, aktywność w negocjacjach czy ich zainicjowanie nie mają żadnego wpływu na zakres negocjacji ani na prawa stron je prowadzące.

Mając na względzie fakt, że stronie negocjacji nie przysługuje prawo do jednostronnego określania zakresu negocjacji ani wnioskowania o ustalenie terminu ich zakończenia tylko w części, należy uznać, że wniosek o takiej treści:

1) powinien prowadzić do ustalenia terminu zakończenia negocjacji w całości zgodnie z uprawnieniami Prezesa UKE wynikającymi z art. 27 ust. 1 albo
2) powinien zostać uznany za niedopuszczalny lub niepełny i Prezes UKE winien wezwać do jego usunięcia braków formalnych wniosku w trybie art. 64 §2 k.p.a.

Należy również zauważyć, że Prezes UKE, rozstrzygając spór wyłącznie w zakresie zakańczania połączeń w sieci PTK, zupełnie pominął fakt, że przedmiotem rozstrzygnięcia jest spór w zakresie zmiany umowy, a nie ustalenie stawek. Co istotne, strony na każdym etapie postępowania podkreślały konieczność ustalenia stawek symetrycznych. Tak więc nawet gdyby przyjąć, że Prezes UKE miał prawo rozstrzygnąć spór wyłącznie w przedmiocie zmiany umowy w zakresie rozliczeń za zakańczanie połączeń w sieci, to nie ma uzasadnienia dla odmowy ustalenia stawek za zakańczanie połączeń w obu sieciach, skoro było to zgodne z propozycją samego wnioskodawcy i mieściło się w ustaleniu zmiany w umowie zasad rozliczeń za zakańczanie połączeń w sieci. Każda ze stron od początku proponowała stawki symetryczne we wzajemnej współpracy, a do wniosku o wydanie decyzji załączyła aneks zawierający symetryczne stawki i określający zakres sporu, o którym mowa w art. 27 ust. 3 PT. Prezes UKE dokonał jednak kolejnej interpretacji swojego postanowienia o ustaleniu terminu zakończenia negocjacji i uznał, że PTC nie mogło w ramach negocjacji zasad rozliczeń za zakańczanie połączeń w sieci PTK/PTC zaproponować również symetrycznej stawki za zakańczanie połączeń w sieci PTC, uznając, że nie mieści się to w zakresie negocjacji warunków rozliczeń za zakańczanie połączeń w sieci PTK. Stoi to w oczywistej sprzeczności z wyraźnie oświadczoną wolą stron i samego wnioskodawcy. Tym bardziej że propozycja PTC, jak i całe negocjacje, były podyktowane wyłącznie treścią wcześniejszej decyzji MTR.

Wreszcie należy zauważyć, że Prezes UKE ustalił stawki za zakańczanie połączeń w sieci PTK/PTC także od dnia 1 lipca 2009 r. Tymczasem na żadnym etapie negocjacji ani postępowania administracyjnego PTC nie wnosiło o ustalenia stawek w tym zakresie ani w tej wysokości. Prezes UKE wykroczył więc poza zakres negocjacji, postanowienie o ustaleniu terminu zakończenia negocjacji oraz wniosek o wydanie decyzji, a także poza propozycje aneksu, rozstrzygając ponad żądanie PTC i jednostronnie na jej korzyść. Do takiego rozstrzygnięcia można ewentualnie znaleźć podstawę w art. 29 PT, ale nie w art. 27. W związku z tym rozstrzygnięcie w tym zakresie należy uznać za nieważne.

Działania Prezesa UKE ewidentnie wykraczają poza przewidziane prawem kompetencje. Warto zwrócić uwagę, że:

1) przed wydaniem decyzji przeciwko PTK toczyło się już postępowanie (z ostrożności procesowej) w sprawie ustalenia terminu zakończenia negocjacji w sprawie zakańczania połączeń w sieci PTC,
2) na 10 dni przed wydaniem decyzji przeciwko Polkomtel zostało już wszczęte postępowanie w sprawie wydania decyzji w sprawie zakańczania połączeń w sieci PTC, a Polkomtel złożył wniosek o połączenie spraw.

Mimo to Prezes UKE, zasłaniając się koniecznością niezwłocznego załatwienia sprawy, odmówił połączenia spraw i wydał przedmiotowe decyzje. Zaprezentowane w przedmiotowych decyzjach stanowisko prowadzi do wniosku, że każde negocjacje zmiany umowy mogą – wnioskiem strony lub z urzędu postanowieniem Prezesa UKE – zostać podzielone na dowolną liczbę części i dla każdej z nich może być ustalony inny termin ich zakończenia, a każdy spór dotyczący części negocjacji wydzielonej postanowieniem Prezesa UKE winien zostać rozstrzygnięty odrębną decyzją wydaną w różnym czasie. Stoi to w oczywistej sprzeczności z ideą negocjacji, jednością stosunku cywilnoprawnego oraz rolą regulatora. Co więcej, żadna ze stron nie ma żadnego wpływu na działania Prezesa UKE ani na wynik sprawy. **Nawet składanie równolegle takich samych wniosków przez każdą ze stron nie gwarantuje, że spór obejmujący całość negocjacji zostanie rozstrzygnięty w tym samym czasie i w sposób uwzględniający interesy stron czy ich obowiązki regulacyjne**. Nawet wydanie w tym samym dniu dwóch odrębnych decyzji o analogicznej treści, z których każda regulowałaby zakańczanie połączeń w jednej z sieci, także narusza prawa stron w sposób oczywisty i prowadzi do nierównego ich traktowania. Wydane decyzje wiążą bowiem strony z chwilą ich doręczenia. Oznacza to, że nawet kilkudniowa[7] zwłoka w doręczeniu którejkolwiek z nich może spowodować wielomilionowe straty jednej ze stron. Straty niczym nieuzasadnione i niewynikające ani z obowiązujących przepisów prawa, ani ciążących na stronach obowiązków regulacyjnych, ani woli stron czy z merytorycznego rozstrzygnięcia Prezesa UKE, lecz będące skutkiem przypadku, pomyłki, odległości od siedziby UKE czy zaniedbania lub innych

7 Odrębnych i bardzo pogłębionych rozważań wymaga kwestia chwili związania stron decyzją o zmianie umowy. Zazwyczaj strony wiążą się umową albo z chwilą jej zawarcia, albo z początkiem danego dnia, ewentualnie z inną chwilą uzgodnioną przez strony. W przypadku wyroków ustalających (art. 189 k.p.c.) lub zmieniających stosunek cywilny (art. 3571 k.c.) zmiana treści stosunku cywilnego następuje z początkiem dnia, w którym orzeczenie się uprawomocni. Rozliczenia za zakańczanie połączeń to proces ciągły, wydaje się, że jest dopuszczalne związanie stron zmianą umowy w ciągu dnia. Jeżeli przyjąć taką koncepcję dla doręczania decyzji wydanych na podstawie art. 27 PT, oznaczać to może straty liczone nie w milionach, lecz dziesiątkach tysięcy złotych za każdą godzinę różnicy w terminie doręczenia.

nieistotnych okoliczności, które doprowadziły do niejednoczesnego doręczenia decyzji. Co więcej, taki skutek będzie prawdopodobnie także niezgodny z wolą Prezesa UKE i jego polityką regulacyjną, a wynikać będzie wyłącznie z przyjęcia przez Prezesa UKE niezgodnego z prawem trybu postępowania. Właściwie można zaryzykować twierdzenie, że przedstawiony tryb postępowania zawsze będzie prowadził do bezprawnego pokrzywdzenia jednej ze stron negocjacji. Jest to absolutnie nie do pogodzenia z zasadami demokratycznego państwa prawnego (art. 2 Konstytucji RP).

Prezes UKE, dokonując rozstrzygnięcia, stwierdził, że w zakresie zakańczania połączeń w sieci PTC negocjacje nadal trwają. Pomijając powyższe wywody, Prezes UKE nie wyjaśnił, na czym opiera swoje twierdzenia. Na czym miałyby polegać te negocjacje między telekomami i co strony mogą sobie w ich ramach zaoferować, skoro oczekiwania jednej z nich zostały już uwzględnione przez Prezesa UKE. Co więcej, niezależnie od odwołania się przez każdą ze stron od decyzji MTR należy stwierdzić, że w ramach negocjacji strony przy ustalaniu stawek za zakańczanie połączeń kierowały się wyłącznie tą decyzją. Można nawet stwierdzić, że dla stron stawki te były sztywne i żadna ze stron na żadnym etapie negocjacji nie proponowała innej ich wysokości niż ustalona w decyzji MTR. Nie bez znaczenia pozostaje również fakt, że żadna ze stron nie prowadziłaby tych negocjacji i nie byłaby zainteresowana zmianą umowy, gdyby nie została do tego zmuszona decyzją MTR. Te wszystkie fakty nie pozostają bez wpływu na rozstrzygnięcie sprawy.

Nie można również zapominać, że Prezes UKE, rozstrzygając w przedmiotowych sprawach, postąpił niezgodnie ze swoją dotychczasową praktyką. Warto w tym miejscu powołać się na stanowisko Prezesa UKE wyrażone w decyzji z dnia 21 stycznia 2009 r. nr DHRT-WWM-60600-227/08 (9) w sprawie uregulowania stawek pomiędzy PTC i Netią. Uzasadniając swoją decyzję, „*Prezes UKE uznał, iż przedłużanie się negocjacji i brak zawartego Aneksu do Umowy wprowadzającego stawki MTR zgodne z Decyzją MTR, a co się z tym wiąże niewykonywanie przez PTC nałożonego na nią mocą Decyzji MTR obowiązku regulacyjnego,* ***stanowi przypadek wyjątkowy i powoduje bezpośrednie i poważne zagrożenie zarówno dla konkurencyjności, jak i dla interesów użytkowników****. Nie może ulegać wątpliwości, iż stosowanie przez PTC w stosunkach z Netią stawki MTR niezgodnej z nałożonymi na PTC obowiązkami* ***powoduje poważne zaburzenia w konkurencyjności na całym rynku świadczenia usług telekomunikacyjnych****. Z jednej strony należy wskazać, iż działania PTC* ***mogą doprowadzić do sytuacji, w której stawka, jaką Netia obowiązana jest uiszczać PTC za zakończenie połączenia w ruchomej sieci PTC, będzie inna niż stawki MTR, które PTC stosuje w relacjach z innymi przedsiębiorcami telekomunikacyjnymi*** *(...). Aby* ***zabezpieczyć zarówno interesy użytkowników końcowych, jak i zapobiec poważnym zaburzeniom konkurencyjności na rynku telekomunikacyjnym****, działanie Prezesa UKE musi być natychmiastowe, tak aby* ***w możliwie maksymalny sposób zneutralizować wyżej wskazane negatywne skutki wynikające z niewykonywania przez PTC obowiązków na nią nałożonych***”. Na takie same argumenty powołał się Prezes UKE w decyzji przeciwko Polkomtel, pomijając, że decyzjami MTR nałożył na PTC, PTK i Polkomtel identyczne obowiązki.

W przedmiotowych sprawach PTC stanęła na stanowisku, iż Prezes UKE, wydając decyzję, powinien wydać analogiczne decyzje z tą samą datą obowiązywania w stosunku do wszystkich operatorów sieci telefonii ruchomej i stacjonarnej. Prezes UKE, odnosząc się do tego postulatu,

wyraził pogląd, że „*stawki MTR są wprowadzane do umów międzyoperatorskich w formie indywidualnych decyzji administracyjnych, po wnikliwym i wszechstronnym rozpatrzeniu konkretnych okoliczności danej sprawy. (...) Oczekiwanie na zakończenie postępowań prowadzonych w innych sprawach dotyczących zmian stawek MTR w celu skorelowania momentu wydania decyzji dla wszystkich operatorów stanowiłoby nieuzasadnione przedłużenie danego prowadzonego postępowania. (...) Prezes UKE nie byłby zatem w stanie ustalić terminu jednoczesnego wydania decyzji dla wszystkich operatorów.* ***Przychylając się więc do wniosku PTC, Prezes UKE mógłby zatem narazić się na zarzut niezałatwienia sprawy w terminie***”.

Jak wynika z powyższego, Prezes UKE wyraził zaniepokojenie przedłużającą się realizacją decyzji MTR. Co więcej, podkreślił, że stan ten oraz stosowanie przez operatorów telefonii mobilnej stawek niezgodnych z decyzjami MTR ***stanowi przypadek wyjątkowy i powoduje bezpośrednie i poważne zagrożenie zarówno dla konkurencyjności, jak i dla interesów użytkowników oraz powoduje poważne zaburzenia w konkurencyjności na całym rynku świadczenia usług telekomunikacyjnych***. Prezes UKE wydaje się podzielać pogląd, że najlepszym rozwiązaniem byłoby objęcie wszystkich operatorów jedną stawką w jednym czasie, ubolewając jednak, że nie ma wystarczających możliwości prawnych w tym zakresie.

Niestety, wydając decyzje w zakresie ustalenia zasad rozliczeń za zakańczanie połączeń pomiędzy PTK i PTC oraz Polkomtel i PTC, Prezes UKE zajął całkowicie odmienne stanowisko. Decyzjami bowiem wprowadził jednostronną asymetrię w rozliczeniach, a jednocześnie usiłował wykazać, że jest to korzystne dla użytkowników i pozytywnie wpływa na konkurencyjność na rynku usług telekomunikacyjnych. Pominął również wszystkie wymienione powyżej zagrożenia. Co więcej, mimo że był zobowiązany do objęcia decyzją całego stosunku prawnego, jak również dysponował możliwościami prawnymi pozwalającymi mu na to, postąpił zupełnie przeciwnie.

Powyższe działanie należy rozważać nie tylko w świetle norm prawnych z zakresu prawa telekomunikacyjnego, prawa cywilnego czy Konstytucji RP, ale także z uwzględnieniem art. 8 k.p.a., a mianowicie zasady pogłębiania zaufania obywateli do organów Państwa oraz świadomości i kultury prawnej obywateli. Z całą pewnością narusza realizację zasady pogłębiania zaufania obywateli do organów Państwa podejmowanie w tej samej sprawie przeciwstawnych działań przez organy Państwa[8], dokonywanie skrajnie różnej oceny tego samego stanu faktycznego przez organy administracji[9], jak również zmienność rozstrzygnięć podejmowanych w sprawie przez organy administracji[10]. Jak stwierdzono w wielu orzeczeniach sądów administracyjnych[11]: „*zmienność poglądów prawnych wyrażonych w decyzjach organów administracji w odniesieniu do tego samego adresata, wydanych na tle takich samych stanów*

8 Por. wyrok NSA z 26 listopada 1999 r., sygn. V SA 978/99 – LEX nr 49942.

9 Por. np. wyrok NSA OZ w Gdańsku z 3 lutego 1999 r., sygn. I SA/Gd 370/97 – LEX nr 38664.

10 Zob. np. teza druga wyroku NSA z 28 kwietnia 1999 r., sygn. IV SA 895/97 – LEX nr 47186; wyrok NSA OZ we Wrocławiu z 23 czerwca 1994 r., SA/Wr 98/94 - POP 1996, nr 1, poz. 3.

11 Zob. np. wyrok NSA OZ w Łodzi z 8 kwietnia 1998 r., I SA/Łd 652/97 - ONSA 1999, nr 1, poz. 27; wyrok WSA w Gliwicach z dnia 23 sierpnia 2007 r., IV SA/Gl 1221/2006 LexPolonica nr 1919412; podobnie wyrok Naczelnego Sądu Administracyjnego - Ośrodek Zamiejscowy w Gdańsku z dnia 20 czerwca 1985 r., sygn. SA/Gd 478/85 LexPolonica nr 308276.

faktycznych, ze wskazaniem tej samej podstawy prawnej decyzji i bez bliższego uzasadnienia takiej zmiany, stanowi niewątpliwie naruszenie art. 8 k.p.a.". Naruszeniem zasady pogłębiania zaufania obywateli do organów Państwa jest także **odmienne traktowanie stron w takiej samej sytuacji faktycznej i prawnej** przez różne organy administracji[12].

Art. 8 k.p.a. statuuje zasadę, zgodnie z którą organy administracji publicznej obowiązane są prowadzić postępowanie w taki sposób, aby pogłębiać zaufanie obywateli do organów Państwa oraz świadomość i kulturę prawną obywateli. Zasada ta nie może być rozumiana jedynie jako postulat określonego zachowania, lecz stanowi ona obowiązującą normę prawa, z której wynikają konkretne dyrektywy wiążące organy administracji publicznej w toku podejmowanych przez nie czynności procesowych. **Strona, znając wcześniejszą decyzję organu i dokonaną w niej interpretację obowiązujących przepisów prawa, powinna móc działać w zaufaniu do tej decyzji**.

Czyniąc powyższe wywody, nie można zapomnieć o wyroku Naczelnego Sądu Administracyjnego w Warszawie[12], który podzielił pogląd WSA uznający, iż „*powyższe postanowienie Prezesa URTiP nie rozstrzyga sprawy co do istoty ani też nie kończy postępowania w sprawie, gdyż dotyczy jedynie zakończenia terminu negocjacji* ***i nie ma jakiegokolwiek wpływu na treść umowy o połączeniu sieci***.". NSA dalej stwierdza, że „*postanowienie Prezesa URTiP w przedmiocie terminu zakończenia negocjacji (art. 27 ust. 1 i art. 28 ust. 4 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, Dz. U. z 2004 r. Nr 171, poz. 1800 ze zm.)* ***nie rozstrzyga istoty sprawy,*** *gdyż taka sprawa jest rozstrzygana dopiero decyzją Prezesa URTiP, o jakiej mowa w art. 27 ust. 2 Prawa telekomunikacyjnego. Niezawarcie zaś umowy w terminie określonym przez Prezesa stanowi jedną z kilku przesłanek formalnych do wydania decyzji w sprawie rozstrzygnięcia kwestii spornych lub określenia warunków współpracy.* ***Postanowienie to nie determinuje bezpośrednio treści decyzji wydawanej w postępowaniu głównym i nie stanowi elementu materialnego przyszłego rozstrzygnięcia***". Podobnie orzekł Naczelny Sąd Administracyjny wyrokiem z dnia 10 listopada 2005 r.[13]. Sąd stwierdził, że „*postanowienie Prezesa UKE określające termin zakończenia negocjacji o zawarcie umowy o dostępie telekomunikacyjnym, wydane na podstawie art. 27 ust. 1 pr. tel., nie dotyczy samodzielnej kwestii i* ***nie rozstrzyga o istocie autonomicznej sprawy. Postanowienie to jedynie obliguje strony negocjacji do zakończenia w określonym terminie tych negocjacji przez zawarcie umowy. Nie jest ono zatem oderwane od istoty sprawy, którą jest zawarcie umowy cywilnoprawnej pomiędzy stronami negocjacji***."

Uprawnienia Prezesa UKE z art. 27

Wreszcie należy rozważyć charakter prawny uprawnień oraz decyzji Prezesa UKE wydawanych na podstawie art. 27 ust. 2. Nie ma wątpliwości, że Prezes UKE rozstrzyga w trybie administracyjnym spór o charakterze cywilnym. Zakres jego uprawnień oraz zakres orzekania, a także charakter orzeczenia muszą być interpretowane przede wszystkim w świetle zasad obowiązujących w prawie cywilnym. Stąd za trafny należy uznać pogląd – wyrażony odnośnie analogicznych uprawnień Prezesa URE – sformułowany w wyroku przez Sąd Antymonopolowy[15]. W świetle

12 Por. Wyrok NSA OZ w Białymstoku z 8 maja 1998 r., sygn. SA/Bk 655/97 - Biul. Skarb. 1998, nr 4, poz. 26.
13 Wyrok NSA z dnia 19 października 2005 r., sygn. II GSK 232/05.
14 Sygn. II GSK 275/2005, niepubl.
15 Wyrok z dnia 7 kwietnia 1999 r., sygn. XVII Ama 85/98/E, Opubl.: Orzecznictwo w Sprawach Gospodarczych rok 2005, Nr 3, poz. 48, str. 87.

tego wyroku „*w razie braku zgody jednej ze stron na zawarcie umowy druga strona może żądać w trybie postępowania administracyjnego, aby treść umowy została ustalona przez Prezesa URE w trybie art. 8 ust. 1 omawianej ustawy, a więc w drodze decyzji administracyjnej*. ***Żądanie strony, która wszczyna postępowanie administracyjne, zbliżone jest swym charakterem do funkcjonującego na gruncie odrębnych przepisów powództwa o ustalenie (ukształtowanie) stosunku prawnego.*** *W następstwie takiego wniosku Prezes URE uzyskuje ustawową legitymację do ukształtowania między stronami spornej umowy,* ***w granicach przysługującej stronom swobody kontraktowania.*** *Decyzja Prezesa URE, wydana w trybie art. 8 ust. 1 Prawa energetycznego, niejako zastępuje oświadczenie woli obu stron w przedmiocie zawarcia umowy (por. w drodze analogii art. 64 k.c.). Innymi słowy, do Prezesa URE odnoszą się te wszystkie ograniczenia odnoszące się do zasady swobody umów, które przysługują stronom (art. 353[1] kc). W świetle tego przepisu strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego. Decyzja ustalająca treść umowy i orzekająca jej zawarcie ma charakter konstytutywny (prawotwórczy). Złożenie wniosku wszczynającego postępowanie administracyjne w sprawie zawarcia decyzją administracyjną spornej umowy nie daje stronie prawa do uzyskania decyzji w pełni uwzględniającej jej propozycje*."

Należy również zgodzić się z poglądem wyrażonym w wyroku Sądu Najwyższego – Izba Administracyjna, Pracy i Ubezpieczeń Społecznych[16] i aktualnym dla interpretacji analogicznych uprawnień Prezesa UKE określonych w art. 27 PT. W ocenie Sądu „**istotą regulacji szczególnej umów przewidzianych w ustawie Prawo energetyczne jest zastąpienie środkami administracyjnymi mechanizmów rynkowych. Ustalając treść umowy, Prezes URE powinien przyjmować jako miarę zachowanie abstrakcyjnego, racjonalnego przedsiębiorcy działającego na rynku konkurencyjnym. Ustalona treść umowy powinna zatem odpowiadać treści umowy, jaką zawarliby *'racjonalni przedsiębiorcy działający na rynku konkurencyjnym.'*"** Jest oczywiste, że racjonalny operator publicznej sieci telekomunikacyjnej działający na rynku konkurencyjnym nie zawarłby umowy o treści określonej przez Prezesa UKE. Decyzja ta w sposób jednoznaczny i istotny uprzywilejowuje jednego z konkurentów kosztem drugiego, narażając go w sposób nieuzasadniony na wielomilionowe straty, a konkurentowi przyznając nieuprawnione wielomilionowe zyski.

Sąd cywilny, rozstrzygając spór o ustalenie (ukształtowanie) stosunku prawnego, np. na podstawie art. 189 k.p.c. czy 357[1] k.c., jest zobowiązany ukształtować całość stosunku prawnego z uwzględnieniem obowiązującego prawa i po rozważeniu interesów stron oraz zgodnie z zasadami współżycia społecznego. Jest oczywiste, że nie jest możliwe wydanie w tym zakresie wyroku częściowego, o którym mowa w art. 317 k.p.c. Konieczne jest całościowe ukształtowanie stosunku prawnego, co nie stoi w sprzeczności z odmową sądu uwzględnienia części czy nawet całości żądań jednej ze stron. Prezes UKE, rozstrzygając spór na podstawie art. 27 ust. 2 PT, jest zobowiązany – obok kryteriów przewidzianych w PT – do uwzględnienia tych właśnie zasad. Niestety, Prezes UKE nie zastosował się do tych wymagań w najmniejszym stopniu.

16 Wyrok z dnia 9 marca 2004 r., sygn. III SK 18/04, opubl.: Orzecznictwo Sądu Najwyższego Izba Administracyjna, Pracy i Ubezpieczeń Społecznych rok 2004, Nr 24, poz. 429, str. 1144.

Wreszcie należy podnieść, że dokonywanie jednostronnych rozstrzygnięć ogranicza uprawnienia kontrolne Sądu Ochrony Konkurencji i Konsumentów. Rozpatrując bowiem odwołanie od każdej z decyzji z osobna, nie może dokonać merytorycznego rozstrzygnięcia o całości sporu. Co więcej, nawet merytorycznie poprawne decyzje mogą zostać wyeliminowane z obrotu prawnego np. na skutek ułomności proceduralnych. Prowadziłoby to po raz kolejny do niczym nieuzasadnionej straty podmiotu, którego uprawnienia zostałyby uchylone, a który musiałby wykonywać symetryczne obowiązki wynikające z drugiej, niewadliwej formalnie decyzji.

Wypaczone rozumienie wyroku SOKiK

Nie jest wykluczone, że Prezes UKE, podejmując wadliwe decyzje, zasugerował się interpretacją wyroku SOKiK[17]. Otóż ten skądinąd w całości prawidłowy wyrok w najmniejszym stopniu nie może uzasadniać przyjętego przez Prezesa UKE trybu postępowania. Wyrok zapadł w innym stanie faktycznym. Sąd stwierdził bowiem, że od rozpoczęcia negocjacji nie minął termin 90 dni, a jednocześnie nie zostało wydane postanowienie o określeniu terminu ich zakończenia. Analiza treści uzasadnienia wyroku skłania wręcz do przeciwnego wniosku. Wyrokiem tym sąd zmienił zaskarżoną decyzję i umorzył postępowanie, odmawiając Prezesowi UKE prawa do wszczęcia postępowania w trybie art. 27 PT w przypadku, gdy strony nie zakończyły negocjacji, wobec niespełnienia warunku przewidzianego bezwzględnie obowiązującymi przepisami prawa – art. 26 ust. 1 w zw. z art. 30 PT i art. 27 ust. 2 PT. SOKiK w uzasadnieniu podkreśla równouprawnienie stron negocjacji i wskazuje, że negocjacje trwają tak długo, jak strony wymieniają się swoimi stanowiskami, a zakres negocjacji wynika z propozycji stron. SOKiK zauważa w uzasadnieniu, że rozpoczęte negocjacje w sprawie zmiany umowy nie zostały zakończone, gdyż zostały przez jedną ze stron przerwane w sposób nieznajdujący uzasadnienia dla takiego działania. Strona ta bowiem, nie odnosząc się do propozycji złożonej przez drugą stronę, złożyła wniosek o wydanie decyzji w trybie art. 27 ust. 2. Tym samym sąd potwierdził, że żadna ze stron nie może jednostronnie decydować o czasie trwania i zakresie negocjacji ani ograniczać uprawnień drugiej strony czy determinować zakresu postępowania w sprawie wydania decyzji. W uzasadnieniu podniesiono również, że przedmiotem negocjacji jest umowa lub jej zmiana, a nie stawka za zakańczanie połączeń.

Sąd słusznie odmówił Prezesowi UKE prawa do ingerowania w stosunek cywilnoprawny stron tak długo, jak mogą go ułożyć samodzielnie, wskazując m.in. na zasadę wolności gospodarczej, podkreślając, że priorytetem jest wola stron. Przyjęty przez Prezesa UKE tryb postępowania nie tylko nie znajduje – choćby w najmniejszym stopniu – potwierdzenia w przywołanym wyroku, ale wręcz jest z nim sprzeczny. Podobnie jak jest sprzeczny z dotychczasową linią orzeczniczą SOKiK. W żadnym bowiem przypadku SOKiK nie uchylił ani nie zmienił decyzji Prezesa UKE, ani nie umorzył postępowania na tej podstawie. Ani z tego, ani z innych dotychczasowych wyroków SOKiK nie można wyprowadzić więc wniosku, że:

1) Prezes UKE jest uprawniony czy zobowiązany – na wniosek czy z urzędu – do wyodrębnienia z negocjacji ich części i poddania ich odrębnemu postępowaniu administracyjnemu,
2) strona ma prawo jednostronnie określać zakres negocjacji czy determinować zakres postępowania administracyjnego, w którym pozostaje w sporze z drugą stroną.

17 Wyrok z dnia 29 grudnia 2008 r., sygn. akt XVII AmT 78/07.

Co prawda w nomenklaturze operatorów telekomunikacyjnych wyróżnia się jednostronne i dwustronne wnioski o wydanie decyzji w trybie art. 27 ust. 2 czy wnioski o wydanie postanowienia w trybie art. 27 ust. 1 PT. Podział ten jednak nie ma żadnego waloru prawnego. Każdy wniosek o wydanie decyzji jest bowiem wnioskiem o zawarcie/zmianę umowy i jego zakres określa treść prowadzonych negocjacji i zakres sporu między stronami. Podział ten wynika wyłącznie z interesu ekonomicznego strony. Jest oczywiste, że z reguły stroną inicjującą negocjacje, postępowanie w sprawie określenia terminu ich zakończenia czy wydania w sprawie decyzji zmieniającej umowę będzie ta, której się to będzie opłacać. W przypadku spraw z zakresu ustalania stawek MTR zainteresowanym będzie operator, który z decyzji MTR odnosi korzyść i oczekuje jej realizacji poprzez zmianę umowy. Nie można tego jednak utożsamiać z jednostronnym uprawnieniem strony do określania zakresu postępowania administracyjnego, negocjacji czy wyodrębnienia ich części. W każdym przypadku Prezes UKE – rozstrzygając spór – jest zobowiązany uwzględnić stanowiska, interesy oraz obowiązki regulacyjne każdej ze stron.

Należy zauważyć, że Prezes UKE może wydać decyzję w trybie art. 27 ust. 2 także w przypadku odmowy podjęcia negocjacji przez jedną ze stron. W takim przypadku z całą pewnością sytuacja prawna inicjującego postępowanie jest lepsza. Nawet jednak w tym przypadku Prezes UKE nie może ograniczyć się do rozstrzygnięcia zgodnie z wnioskiem strony. Jest on bowiem związany pierwotną propozycją negocjacyjną strony inicjującej (druga strona bowiem odmówiła negocjowania właśnie jej), a nadto musi kierować się podobnymi przesłankami jak w przypadku wydawania decyzji po przeprowadzeniu negocjacji. W przypadku podjęcia przez stronę negocjacji jej sytuacja prawna nie może być gorsza niż podmiotu, który odmówił ich podjęcia.

Umorzenie

Odnosząc się do powoływania się przez Prezesa UKE w uzasadnieniu decyzji na orzecznictwo sądów administracyjnych mające potwierdzić prawidłowość postępowania Prezesa UKE w przedmiocie umorzenia postępowania, należy uznać, że przywołane orzeczenia potwierdzają tezę całkowicie przeciwną. Tezy z szeregu orzeczeń sądów administracyjnych[18] potwierdzają nietrafność wywodów Prezesa UKE.

Podsumowanie

Podsumowując, wydaje się, że decyzje Prezesa UKE są dotknięte następującymi, bardzo poważnymi wadami prawnymi:

1. ani wnioskodawca, ani Prezes UKE nie są uprawnieni do zawężania zakresu negocjacji pomiędzy stronami umowy o połączenie sieci, w szczególności żadna ze stron nie może swoim wnioskiem ograniczać lub w inny sposób wpływać na prawa i obowiązki oraz pozycję negocjacyjną drugiej strony,
2. Prezes UKE dokonał bezprawnej i nieuzasadnionej interpretacji postanowień o ustaleniu terminu negocjacji, które wydał wbrew jednoznacznemu brzmieniu ich sentencji,
3. naruszył art. 105 k.p.a. przez jego niewłaściwą wykładnię i zastosowanie,

18 Wyrok Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 9 października 2007 r., sygn. VI SA/Wa 1338/07; wyrok Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 1 czerwca 2005 r., sygn. I SA/Wa 677/04; wyrok Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 16 maja 2006 r., sygn. VII SA/Wa 37/06; wyrok Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 29 sierpnia 2007 r., sygn. VII SA/Wa 774/07.

4. naruszył art. 27 ust. 1 przez ustalenie terminu negocjacji zmiany umowy tylko w ich części,
5. naruszył art. 27 ust. 2 przez rozstrzygnięcie tylko części kwestii spornych, w pozostałym zaś zakresie nie rozstrzygając lub umarzając postępowania,
6. naruszył art. 28 PT, rozstrzygając sprzecznie z:
   1) interesem użytkowników sieci telekomunikacyjnych,
   2) obowiązkami nałożonymi na przedsiębiorców telekomunikacyjnych,
   3) obowiązkiem zapewnienia:
      a) integralności sieci oraz interoperacyjności usług,
      b) niedyskryminujących warunków dostępu telekomunikacyjnego,
      c) rozwoju konkurencyjnego rynku usług telekomunikacyjnych,
   4) obowiązkiem uwzględnienia pozycji rynkowych przedsiębiorców telekomunikacyjnych, których sieci są łączone,
7. naruszył zasadę praworządności wynikającą m.in. z art. 7 Konstytucji i art. 6 k.p.a.,
8. naruszył zasadę zaufania do organów Państwa wynikającą z art. 8 k.p.a.,
9. naruszył 31 ust. 3 Konstytucji RP poprzez nieuprawnioną ingerencję w swobodę działalności gospodarczej, w szczególności poprzez dokonanie interpretacji rozszerzającej w zakresie swoich kompetencji wbrew powszechnie przyjętemu poglądowi – zarówno w judykaturze, jak i doktrynie – że treść norm prawnych ograniczających uprawnienia bądź nakładających określone obowiązki powinna być interpretowana w sposób ścisły.

Robert Podpłoński jest radcą prawnym specjalizującym się w prawie nowych technologii.

Polecamy

SEMINARIUM

ARCHIWIZACJA DANYCH CYFROWYCH - TECHNOLOGIE DOBRE PRAKTYKI, UWARUNKOWANIA PRAWNE

19 kwietnia 2011 r., Warszawa

Przechowywanie danych cyfrowych stało się jednym z ważniejszych problemów zarządzania dokumentami elektronicznymi. Z tego powodu znajomość norm i standardów archiwizacji danych elektronicznych jest podstawowym warunkiem optymalizacji dostępu do cyfrowego archiwum. W tym zakresie istotne są zarówno problemy technologiczne, jak i wszelkie uwarunkowania prawne. Proponowane seminarium ma zadanie przybliżyć zagadnienia backupu danych cyfrowych.

W programie:

- podstawowe narzędzia backupu danych cyfrowych,
- sposoby przechowywania zasobów elektronicznych w bibliotekach cyfrowych - zalety i ograniczenia,
- zarządzanie dostępem do cyfrowego archiwum, normy i standardy archiwizacji danych elektronicznych,
- archiwum elektroniczne - pokaz "na żywo" oprogramowania ELO uwzględniającego nową instrukcję kancelaryjną,
- archiwizacja zbiorów audiowizualnych,
- usługa powszechnej archiwizacji (zabezpieczanie i archiwizacja danych),
- cyfrowa archiwizacja publikacji naukowych - cyfrowe repozytoria nauki.

Więcej: www.cpi.com.pl

cpi
centrum promocji informatyki

Nowelizacja ustawy o ochronie danych osobowych – konsekwencje i nowe wyzwania

Monika Krasińska

W dniu 18 listopada 2010 r. Prezydent RP podpisał uchwaloną przez Parlament ustawę o zmianie ustawy o ochronie danych osobowych i niektórych innych ustaw. Zakończeniu w ten sposób uległ żmudny proces zmiany niektórych z dotychczas istniejących zapisów w sferze prawa do ochrony danych osobowych. Przypomnieć bowiem należy, iż przedstawiony przez Prezydenta RP projekt ustawy o zmianie ustawy o ochronie danych osobowych wpłynął do laski marszałkowskiej w dniu 21 grudnia 2007 r. i w toku procedowania spotkał się z ostrą krytyką wielu środowisk. Potrzeba zmian mających na celu zagwarantowanie skuteczniejszej niż dotychczas ochrony danych osobowych determinowana była wieloletnim okresem obowiązywania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 ze zm.), zwanej dalej ustawą, której regulacje okazały się niewystarczające dla zapewnienia skutecznych rozwiązań w kwestii egzekwowania prawa o ochronie danych osobowych wynikających z Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym obiegu tych danych. Wiele z zaproponowanych pierwotnie rozwiązań miało wyłącznie charakter porządkujący. Zasadniczą różnicą jakościową w odniesieniu do dotychczasowych rozwiązań była zaproponowana w projekcie prezydenckim możliwość nakładania przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w drodze decyzji administracyjnej kar pieniężnych o równowartości od 1000 do 100000 euro na podmioty niewykonujące decyzji wydanych przez ten organ. Przy czym decyzja, której niewykonanie stanowiło przesłankę nałożenia kary pieniężnej, miała mieć charakter bezwzględnie obowiązujący, co oznaczało pozostawienie jej w obiegu prawnym po ewentualnej i zainicjowanej przez stronę kontroli instancyjnej i sądowej. Nałożenie kary pieniężnej poddane zostało nadzorowi sądu administracyjnego.

Kary pieniężne stanowią integralny element oddziaływania na administratorów danych uchylających się od stosowania zasad ochrony danych osobowych w wielu krajach Unii Europejskiej, m.in. w Czechach, Słowacji, Hiszpanii, Włoszech, Portugali, Austrii, Niemczech czy Francji. Coroczne sprawozdania GIODO z wykonywania swojej działalności dobitnie pokazują, iż składane zawiadomienia o popełnieniu przestępstw stypizowanych w ustawie o ochronie danych osobowych nie są efektywne i w większości przypadków postępowania albo nie są wszczynane, albo wszczęte podlegają umorzeniu przez organy ścigania z powołaniem na niski stopień społecznej szkodliwości czy brak znamion czynu zabronionego. Tylko w nielicznych przypadkach sprawcy czynów zabronionych ponoszą odpowiedzialność karną. Takie z kolei podejście organów ścigania i wymiaru sprawiedliwości do sfery prawa do prywatności nie sprzyja budowie poczucia bezpieczeństwa osób poszkodowanych, czyniąc iluzoryczną ochronę ich praw wynikających z przepisów o ochronie

danych osobowych. Projekt prezydencki zakładał konieczność wzmocnienia tych praw a ww. rozwiązanie miało wypełnić lukę prawną, jaka powstała wobec braku norm dla wyegzekwowania wykonalności decyzji administracyjnych organu ochrony danych osobowych. W projekcie prezydenckim zaproponowano także instytucję tzw. wystąpień, które, mając walor edukacyjny, podnosiłyby zarówno poziom wiedzy administratorów danych, jak i inspirowały do zmian niedoskonałych przepisów prawa. Przewidziana została również możliwość tworzenia jednostek zamiejscowych Biura GIODO celem zapewnienia obywatelom łatwiejszego dostępu do organu ochrony danych osobowych.

Wątpliwości wyrażane podczas prac nad nowelą ustawy o ochronie danych osobowych zarówno przez rząd, jak i przez przedstawicieli wielu instytucji, doprowadziły do zmian projektowanej regulacji. W konsekwencji mająca wejść w życie 7 marca 2011 r. ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych i niektórych innych ustaw (Dz. U. Nr 229, poz. 1497)[1] nadaje Generalnemu Inspektorowi Ochrony Danych Osobowych status organu egzekucyjnego i nowe uprawnienia przez stosowanie środków egzekucyjnych przewidzianych w ustawie o postępowaniu egzekucyjnym w administracji. Zrezygnowano tym samym z możliwości nakładania kar pieniężnych. Otwarte pozostaje pytanie, na ile powyższe środki okażą się skutecznym instrumentem prawnej ochrony danych osobowych i czy przyczynią się do wzmocnienia pozycji organu ochrony danych osobowych, ale przede wszystkim wzmocnienia praw jednostki, w tym prawa do zapewnienia lepszej jakości danych, dostępu do nich czy wreszcie do „prawa bycia zapomnianym". Jest to pytanie o tyle istotne, iż właśnie powyższe aspekty jako priorytetowe cele są przedmiotem trwających aktualnie dyskusji nad zmianą europejskich ram ochrony danych osobowych.

Niewątpliwie w tok dyskusji nad „prawem do bycia zapomnianym" wpisuje się zaproponowana w nowelizacji możliwość wycofania zgody na przetwarzanie danych przez osobę, której dane dotyczą. Takie rozwiązanie nie było wprost przewidziane w dotychczasowych przepisach o ochronie danych osobowych, choć nie jest wyjątkiem w polskim prawodawstwie. Możliwość odwołania zgody przewidziana została m.in. w ustawie Prawo telekomunikacyjne, ustawie o świadczeniu usług drogą elektroniczną czy ustawie Prawo bankowe.

W praktyce administratorzy danych oświadczenia o wycofaniu zgody interpretowali jako sprzeciw osoby wobec dalszego przetwarzania jej danych osobowych i zaprzestawali przetwarzania danych osobowych, ale wyłącznie w celach marketingowych lub przekazywania danych innemu administratorowi danych, pozostawiając sobie określony w ustawie zakres informacji o wnoszącym sprzeciw.

Nowe przepisy wymuszą na administratorze danych konieczność dokonywania każdorazowej oceny, czy w istocie przesłanka zgody, która w każdym czasie może być wycofana, jest jedyną uzasadniającą legalność procesu przetwarzania danych osobowych, a jeżeli nie, czy celowym jest w ogóle jej pozyskiwanie. Weryfikacja procesu pozyskiwania zgody na przetwarzanie danych osobowych jest szczególnie uzasadniona, gdy administratorzy danych operują nimi w oparciu o inne podstawy, np. przepis prawa (art. 23 ust. 1 pkt 2 ustawy) czy z uwagi na konieczność realizacji umowy z podmiotem danych (art. 23 ust. 1

1 Niniejszą ustawą zmienia się ustawy: ustawę z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, ustawę z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym oraz ustawę z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych.

pkt 3 ustawy), a zgoda jest pozyskiwana niejako „na wszelki wypadek", „na zapas". Odwołanie zgody udzielonej w takich warunkach nie powinno prowadzić do sparaliżowania działalności administratora.

Przykładowo - organ administracji publicznej prowadzący postępowanie administracyjne nie może wskutek odwołania pozyskanej uprzednio zgody zaprzestać przetwarzania danych osobowych, gdyż w ten sposób naruszyłby przepisy procedury administracyjnej i naraził się na zarzut bezczynności. Z kolei dla wierzyciela, jako strony stosunku obligacyjnego, odwołanie zgody nie może oznaczać uniemożliwienia dochodzenia roszczeń z umowy na drodze cywilno-prawnej, łącznie z prawem do kontroli wykonania zobowiązania przez sąd.

Wielu administratorów danych łączy zgodę na przetwarzanie danych osobowych z realizacją obowiązku informacyjnego, mimo iż taka praktyka nie wynika z obowiązujących przepisów. Również poprzez złożenie jednego oświadczenia o wyrażeniu zgody administratorzy danych próbują zalegalizować przetwarzanie danych w różnych celach. W interesie administratora danych osobowych stanie się zatem uściślenie celu, dla którego zgoda została wyrażona, tak aby w przypadku jej odwołania doszło do zaprzestania przetwarzania danych osobowych tylko w celu, którego dotyczył zakres wcześniejszej zgody.

Do istotnych uprawnień GIODO zagwarantowanych mocą noweli ustawy o ochronie danych osobowych należy kierowanie wystąpień, których adresatami będą organy państwowe, organy samorządu terytorialnego, państwowe i komunalne jednostki organizacyjne, podmioty niepubliczne realizujące zadania publiczne, osoby fizyczne i prawne, jednostki organizacyjne niebędące osobami prawnymi oraz inne podmioty (art. 19a). Wystąpienia te oraz wnioski do właściwych organów o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych mają na celu zapewnić skuteczniejszą ochronę danych osobowych. Ustawa wprawdzie dotychczas wprost nie przewidywała dla GIODO takiej kompetencji, jednakże w praktyce wystąpienia, zwane również sygnalizacjami, wpisywały się w nurt działalności edukacyjnej organu ochrony danych osobowych i stanowiły istotny element podnoszenia stanu wiedzy na temat zasad ochrony danych osobowych zarówno wśród administratorów danych, jak i kształtowania w tym zakresie świadomości osób, których dane dotyczą. Wprowadzenie powyższej regulacji wzmacnia rolę GIODO jako rzecznika ochrony danych osobowych, który pozostaje jednocześnie organem administracji publicznej wyposażonym w atrybuty władztwa publicznego (możliwość wydawania nakazów w drodze decyzji administracyjnych, przeprowadzania kontroli itd.).

Zmianą, która tylko pozornie ma charakter porządkujący- ale w istocie wymusza rewizję podejścia do zasad udostępniania danych osobowych- jest rezygnacja w nowych przepisach z dotychczas obowiązującego art. 29 ustawy. Stanowił on wyjątek od ogólnych zasad przetwarzania danych określonych w art. 23 i 27 ustawy i różnicował sytuację prawną odbiorcy danych tylko dlatego, iż proces przetwarzania dotyczył czynności udostępnienia mu danych w celach innych niż włączenie do zbioru. Przepis art. 29 ustawy dawał administratorowi danych szereg „podpowiedzi" - po spełnieniu jakich kryteriów przez wnioskodawcę może mu udostępnić dane osobowe (uwiarygodnienie potrzeby posiadania danych, nienaruszenie praw i wolności osoby, której dane dotyczą, wniosek pisemny zawierający informacje umożliwiające wyszukanie w zbiorze żądanych danych, konieczność wskazania zakresu i przeznaczenia żądanych danych, obowiązek wykorzystania pozyskanych danych wyłącznie z przeznaczeniem, dla którego zostały udostępnione). Pozostawienie procesu udostępniania danych jednorodnemu reżimowi znajduje uzasadnienie w świetle zasad Dyrektywy 95/46/WE. Komisja Europejska, odnosząc się do treści art. 29, podkreślała, że zwolnienie z zasady ograniczonego celu

jest dopuszczalne jedynie w celu utrzymania porządku publicznego, a wiarygodne uzasadnienie potrzeby posiadania danych nie powinno stanowić samoistnej przesłanki udostępnienia danych osobie trzeciej. Wobec uchylenia komentowanego przepisu administratorzy danych będą zobowiązani do oceny legalności udostępnienia danych na zasadach ogólnych, z których nie wynika np. forma wniosku, co może stwarzać większe pole niepewności interpretacyjnej.

Ustawą o zmianie ustawy o ochronie danych osobowych i niektórych innych ustaw wprowadzono także nowy rodzaj czynu zabronionego, polegającego na udaremnianiu lub utrudnianiu wykonywania czynności kontrolnej przez inspektora. Brak w tym zakresie sankcji karnych powodował, iż Generalny Inspektor Ochrony Danych Osobowych nie mógł w wielu przypadkach zbadać procesu przetwarzania danych osobowych w siedzibie administratora danych. Istotne jest także to, iż przepis ten adresowany jest do każdego podmiotu, który utrudnia bądź uniemożliwia przeprowadzenie kontroli, a nie tylko do administratora danych.

Z kolei do zmian wyłącznie porządkujących dotychczasowe rozwiązania prawne należy rezygnacja z niektórych przepisów wobec obowiązywania w ustawie innych norm konsumujących te przepisy (m.in. art. 33, art. 50).

Przepisy ustawy o zmianie ustawy o ochronie danych osobowych wpisują się w kalendarz zmian, jakie aktualnie są szykowane w ustawodawstwie europejskim w związku z rozwojem nowoczesnych technik informacyjnych i globalizacją. Podkreślić bowiem należy, iż współczesne metody przetwarzania danych osobowych, a w szczególności ich pozyskiwania, gromadzenia i udostępniania, stają się coraz bardziej wyrafinowane i trudniej wykrywalne. Nowe technologie w sposób coraz bardziej agresywny ingerują w przestrzeń prywatności człowieka, a istniejące dotychczas gwarancje ustawowe dla jej ochrony stają się niewystarczające.

W związku z powyższym Komisja Europejska rozpoczęła proces modernizacji istniejących dotychczas ram prawnych w zakresie ochrony danych osobowych, którego wyrazem jest m.in. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów - „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”[2].

Jednym z głównych założeń postawionych w powyższym dokumencie jest dążenie do wzmocnienia praw osób fizycznych i zapewnienie procesowi ich przetwarzania większej przejrzystości, jak również poprawy osób, których dane dotyczą, nad procesem ich przetwarzania. Uznano, iż istotne jest pogłębianie świadomości społeczeństwa w zakresie zagrożeń związanych z procesem przetwarzania danych przy wsparciu mających efektywne instrumenty kontroli organów ochrony danych osobowych. Jako szczególnie ważna została także zaakcentowana potrzeba wzmocnienia odpowiedzialności administratorów danych i podejmowania przez nich dalszych inicjatyw samoregulacyjnych. Polska ustawa o ochronie danych osobowych wraz z dokonanymi w niej zmianami niewątpliwie nie spełnia wszystkich postulatów, o których mowa w ww. dokumencie i choć stanowi wyraz realizacji wielu istotnych założeń wynikających z ustawodawstwa europejskiego, wymaga dalszych pilnych zmian, nad którymi prace rozpoczął Generalny Inspektor Ochrony Danych Osobowych.

Monika Krasińska - Dyrektor Departamentu Orzecznictwa, Legislacji i Skarg w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

2 KOM (2010) 609/3

Postanowienie Krajowej Izby Odwoławczej z 22 kwietnia 2010 r., sygn. akt KIO/UZP 600/10

Wojciech Kaliński

Teza 1. W chwili ogłoszenia informacji o wyborze oferty najkorzystniejszej, rankingu ofert, ofertach odrzuconych itd. oczywiste jest, że Zamawiający zakończył [badanie ofert], a tym samym podjął w stosunku do tych ofert wszystkie czynności, których zamierzał dokonać – zatem albo uznał zastrzeżone informacje za stanowiące tajemnicę przedsiębiorstwa, albo też zaniechał ich odtajnienia. Dlatego od tej chwili jednoznacznie można mówić o zaniechaniu.

Teza 2. [Inaczej byłoby gdyby wcześniej] wykonawcy złożyli wniosek o odtajnienie lub protest w tym zakresie, do których ustosunkowując się, Zamawiający musiałby zająć stanowisko.

Cytowane postanowienie odnosi się po raz kolejny do wielokrotnie poruszanej wcześniej problematyki upływu terminu na wniesienie odwołania na odmowę odtajnienia przez zamawiającego części oferty innego wykonawcy, która zdaniem odwołującego się nie powinna była zostać utajniona. Mimo wielu orzeczeń kwestia ta w dalszym ciągu sprawia wiele problemów w praktyce.

W zakresie problematyki odtajnienia przez zamawiającego fragmentów oferty innego wykonawcy istnieje pewna zasada oraz wyjątki od tejże zasady. Poczynając od zasady, jak słusznie zauważyła Krajowa Izba, jeżeli zamawiający dokonał wyboru najkorzystniejszej oferty oznacza to, iż wykonał wszystkie przewidziane przez siebie czynności w ramach procedury oceny ofert. Jeśli więc po dokonaniu wyboru najkorzystniejszej oferty zamawiający odmawia innemu wykonawcy udostępnienia fragmentów oferty konkurencji z uwagi na zastrzeżoną tajemnicę przedsiębiorstwa, oznacza to, iż w dniu wyboru oferty ocenił, że zastrzeżenie poufności tych fragmentów było skuteczne. Innymi słowy data wyboru najkorzystniejszej oferty jest równocześnie datą ewentualnego zaniechania odtajnienia nieprawidłowo zastrzeżonych fragmentów ofert. Interpretacja ta ma niezwykle istotne znaczenie dla wykonawców, którzy po zapoznaniu się z wynikami postępowania zwracają się następnie do zamawiającego o udostępnienie ofert konkurencji. Po pewnym czasie, ok. 2-4 dniach, dostają wgląd do ofert, jednak z wyłączeniem niektórych fragmentów tychże ofert stanowiących tajemnicę przedsiębiorstwa danego wykonawcy. W reakcji na taką sytuację wykonawcy często składali dwa odwołania: pierwsze na czynność wyboru najkorzystniejszej oferty oraz drugie, którego

termin liczyli od dnia otrzymania „niekompletnej" oferty, na zaniechanie jej odtajnienia. Analizowane orzeczenie wskazuje na nieprawidłowość takiej praktyki. Termin na wniesienie obydwu odwołań (a precyzyjniej na podniesienie obydwu zarzutów, zarówno co do rozstrzygnięcia przetargu, jak i zaniechania ujawnienia zastrzeżonych fragmentów oferty) biegnie bowiem równolegle od dnia rozstrzygnięcia postępowania.

Inaczej przedstawia się sytuacja, w której przed dokonaniem wyboru najkorzystniejszej oferty miały miejsce zdarzenia, które skutkują koniecznością zajęcia przez zamawiającego stanowiska w kwestii prawidłowości zastrzeżenia tajemnicy przedsiębiorstwa przez wykonawcę. W analizowanym postanowieniu Krajowa Izba Odwoławcza wskazała na złożenie przez wykonawcę wniosku o odtajnienie lub protestu w tym zakresie jako czynności, które zmuszają zamawiającego do ustosunkowania się do tych czynności i tym samym wcześniejszego podjęcia decyzji w tym zakresie. W takim przypadku termin na wniesienie odwołania od zaniechania ujawnienia utajnionych fragmentów ofert biegnie odpowiednio wcześniej. W tym miejscu konieczna jest jedna szczegółowa uwaga, mająca niezwykle istotne znaczenie dla ustalania terminów na wniesienie odwołania na czynność zaniechania odtajnienia ofert konkurencji. W zamówieniach publicznych często bowiem mamy do czynienia z następującymi scenariuszami: po otwarciu ofert poszczególni wykonawcy zwracają się do zamawiającego o udostępnienie im do wglądu ofert konkurencji. Oferty te otrzymują, jednak z wyłączeniem części niejawnych ofert. Część wykonawców nie reaguje na ten fakt, kwestię „walki" o odtajnienie ofert pozostawiając na później. Druga grupa wykonawców składa następnie do zamawiającego wniosek o odtajnienie oferty, a następnie w razie otrzymania odpowiedzi negatywnej wnosi odwołanie do Krajowej Izby Odwoławczej, licząc termin na wniesienie odwołania od dnia odmowy zamawiającego przychylenia się do wniosku o odtajnienie oferty. Obie praktyki są błędne. Ich zwolennicy zapominają bowiem o treści art. 182 ust. 3 odpowiednio pkt 1 lub 2, zgodnie z którym odwołanie wnosi się w odpowiednim terminie, licząc od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia. Zamawiający, udostępniając oferty, już wtedy winien ocenić, czy utajnienia pewnych ich fragmentów było zasadne czy też nie. Udostępniając fragmenty niekompletnych ofert, zamawiający pośrednio informuje, że albo nie podjął czynności zmierzających do oceny prawidłowości utajnienia ofert, albo że takie działania podjął, lecz nie znalazł podstaw do zmiany decyzji wykonawców utajniających swoje oferty. Nie jest tu zatem potrzebny żaden dodatkowy wniosek ze strony wykonawcy o odtajnienie ofert. W obydwu bowiem przypadkach (niepodjęcie działań zmierzających do oceny prawidłowości utajnienia ofert bądź decyzja negatywna w kwestii odtajnienia) termin na wniesienie odwołania od zaniechania odtajnienia ofert winien być liczony albo od dnia udostępnienia wykonawcy niekompletnych ofert, albo od ewentualnej wcześniejszej informacji od zamawiającego o braku zamiaru odtajnienia ofert, np. pisma zamawiającego wyznaczającego termin udostępnienia ofert, które to pismo zawiera informację, że pewne fragmenty ofert nie zostaną udostępnione wykonawcy z uwagi na treści art. 8 ust. 3 pzp. O zasadach tych warto pamiętać. Ich nieprzestrzeganie skutkować bowiem będzie upływem terminu na wniesienie odwołania od zaniechania odtajnienia ofert innych wykonawców.

Edwin Bendyk

Cyfrowe społeczeństwo otwarte i jego wrogowie

Jedną z najważniejszych książek inspirujących opozycję w PRL było „Społeczeństwo otwarte i jego wrogowie" Karla Rajmunda Poppera. Filozof we właściwy sobie, klarowny sposób argumentował, dlaczego tylko system demokratyczny oparty na otwartym dostępie do wiedzy i informacji oraz na wolności krytyki najlepiej może zaspokoić aspiracje nowoczesnego społeczeństwa i jego obywateli. Wszelkie drogi na skróty, polegające na przekonaniu, że ktoś uzbrojony w znajomość rzekomych praw rozwoju dziejowego wie lepiej, jaki jest cel tego rozwoju, a więc wie także, jak ów cel osiągnąć, doprowadzić mogą jedynie do katastrofy.

Ba, demokracja nie jest jednak celem – jest tylko narzędziem, które wymaga obrony i ciągłego odnawiania. Podobnie jak stojąca u podstaw demokracji idea otwartości. Warto pamiętać, że proces ucieczki od realnego socjalizmu rozpoczął się w 1989 r., a więc polska demokratyczna rewolucja zaczęła się dziać dokładnie w tym samym czasie, kiedy rozpoczynała się wielka przemiana technologiczna – wtedy jeszcze niemal nikomu nieznany uczony Timothy Berners-Lee szkicował w podgenewskim Laboratorium Fizyki Cząstek CERN założenia systemu zarządzania wiedzą, który dziś znamy pod nazwą WWW.

W Polsce zaczęliśmy z Internetu korzystać oficjalnie 20 lat temu. Kroniki donoszą, że pierwsze połączenie w protokole TCP/IP miało miejsce w sierpniu 1991 r. między uniwersytetami w Warszawie i Kopenhadze.

Można więc bez przesady stwierdzić, że polska demokracja i polski Internet rozwijały się wspólnie i razem osiągnęły dojrzałość. Ich związek będzie trwał, bo trudno wyobrazić sobie dziś polityczną wolność bez możliwości wolnego komunikowania się w Sieci. I nie trzeba się przekonywać, że w krajach, gdzie brakuje wolności, również kiepsko dzieje się z Internetem. Demokracja i Internet są więc skazane na siebie, najlepszy nawet jednak związek wymaga odświeżania – nic tak nie zabija relacji jak rutyna.

Największy walor Internetu polega na tym, że jest wielką, otwartą platformą innowacyjną. Zaprasza swoich użytkowników, by przychodzili ze swoimi pomysłami i realizowali marzenia, tworząc nowe usługi, serwisy i aplikacje. W efekcie powstają dzieła wielkie, zmieniające rzeczywistość jak Wikipedia i godne pogardy jak Redwatch. Powstają wielkie przedsięwzięcia biznesowe jak Google i wielkie inicjatywy społeczne jak ruch związany z oprogramowaniem GNU/Linux.

Kreatywna energia Sieci wynika zarówno z trwającego w niej współzawodnictwa, jak i nieustannej współpracy. Byłaby jednak bezproduktywna gdyby nie główna zasada nakazująca dzielenie się zasobami i traktowanie tworzonej przez internautów wiedzy jako dobra publicznego.

Ekonomiści przez długi czas mieli problem z dobrami publicznymi, bo wychodziło im z racjonalnej analizy, odwołującej się do klasycznych teorii ekonomii klasycznej, że coś takiego nie może istnieć. Jak w realnym socjalizmie, co wspólne to niczyje – więc zamiast być przedmiotem wspólnej troski staje się celem grabieży. Rzeczywistość okazała się jednak bardziej złożona, zwłaszcza w przestrzeni wirtualnej. Dobra niematerialne, jak wiedza, mają to do siebie, że nie grozi im możliwość rozgrabienia – można je powielać dowoli, w epoce cyfrowej na dodatek praktycznie za darmo.

Ta łatwość powielania jest zmorą dla prywatnych wytwórców treści, którzy muszą walczyć ze złodziejami nielegalnie używającymi ich utworów. Dla twórców pragnących się dzielić, jak np. programiści Linuksa lub autorzy Wikipedii, to sytuacja idealna, ich dzieło ma bowiem szansę na optymalne wykorzystanie - optimum zarówno twórcy, jak i optimum społeczne, polega w tym przypadku na jak największym upowszechnieniu dzieła.

Tyle nauczył nas otwarty Internet. Jaki stąd wniosek dla demokracji? Czy nie można zastosować podobnych rozwiązań, by zreformować sferę relacji między demokratyczną władzą a obywatelami? Władza wspólnie z obywatelami tworzy olbrzymie zasoby danych: zasilamy je często sami, wszyscy zaś z podatków finansujemy rozliczne repozytoria wiedzy wspomagające pracę administracji publicznej. Dla nikogo nie jest tajemnicą, nawet dla samej administracji, że zasoby informacji publicznej nie są wykorzystywane efektywnie. Czemu więc ich nie otworzyć? Ale nie na niby, za pomocą takich rozwiązań jak Biuletyn Informacji Publiczny, tylko na serio, w sposób technologicznie adekwatny, czyli za pomocą protokołów API umożliwiających pobieranie danych wprost z repozytoriów.

Tak zrobili Amerykanie i pokazali, że otwarty dostęp do zasobów informacji publicznej wyzwala innowacyjność w taki sam sposób jak inne otwarte inicjatywy w Sieci. Efektem są serwisy i usługi tworzone przez obywateli, organizacje społeczne, firmy, o których samej administracji nawet się nie śniło. Jednocześnie jednak otwartość informacji publicznej uniemożliwia ukrywanie niewygodnych faktów, a więc zwiększa się zakres społecznej kontroli nad władzą.

W Polsce także rozpoczęły się prace nad cyfrowym otwarciem publicznych zasobów danych administracji, wiedzy i kultury, ich koordynacji podjął się Michał Boni. Nie jest łatwo, rozwiązania, które uważane są dziś za oczywiste w Stanach Zjednoczonych czy Wielkiej Brytanii, w naszym kraju wzbudzają opór. Kto się boi otwartości i dlaczego?

Bibliografia zagadnień prawno-informatycznych 2010

Wojciech R. Wiewiórowski

Abramowicz Witold, Filipowska Agata, Łazaruk Szymon: *Integracja heterogenicznych baz danych z wykorzystaniem technologii semantycznych dla platform e-government* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Adamska Izabela, Wojsyk Kajetan: *Zmiany KPA wprowadzone nową ustawą o informatyzacji - część I*, „Czas Informacji" 2/2010

Adamska Izabela, Wojsyk Kajetan: *Zmiany KPA wprowadzone nową ustawą o informatyzacji - część II*, „Czas Informacji" 3/2010

Adamska Izabela: *Czy nowela ustawy o informatyzacji i KPA zrewolucjonizuje e-administrację?,* „Czas Informacji" 1/2010

Adamska Izabela: *Informacja podstawowym źródłem wiedzy*, „Czas Informacji" 3/2010

Adamska Izabela: *Potwierdzenie tożsamości w elektronicznym obrocie gospodarczym a elektroniczna administracja*, „Czas Informacji" 4/2010

Adamski Andrzej: *Internet - medium, prasa czy środowisko komunikacyjne?* „Zeszyty Prawnicze UKSW" 1/2010, s. 247-264

Adamski Andrzej: *Studia podyplomowe jako forma kształcenia ustawicznego prokuratorów w dziedzinie prawa nowych technologii informacyjnych na przykładzie Podyplomowych Studiów Problemów Przestępczości Komputerowej UMK w Toruniu* [w:] Jacek Gołaczyński [red:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Badanie potencjału innowacyjnego województwa łódzkiego w zakresie ICT - identyfikacja luk kompetencyjnych, Miasta w Internecie 2010*,* http://mwi.pl/download/category/9-raporty-i--analizy.html?download=73:raport-dzki

Bajor−Stachańczyk Małgorzata: *Informacja prawna na temat możliwości prowadzenia internetowych zakładow bukmacherskich oraz działań rządu ukierunkowanych na zwalczanie hazardu w Internecie*, „Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu" 3/2010, s. 148-155

Balcarczyk Justyna: *Prasa internetowa - rejestracja?*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 1/2010, s. 13-18, http://cbke.prawo.uni.wroc.pl/files/pme/PME_1_2010.pdf

Bal-Domańska Beata, Salus Aneta: *Wstęp do e-administracji. E-obieg dokumentów w administracji publicznej z wykorzystaniem el-DOK-systemu*, Akademia Ekonomiczna Wrocław 2010

Bałos Iga: *Stosowanie artykułu 52 konwencji o udzielaniu patentów europejskich w części dotyczącej programów komputerowych,* Akademia Frycza Modrzewskiego Kraków 2010

Banasiński Daniel, Karpiński Krzysztof: *Monitoring wizyjny - spojrzenie eksperckie* [w:] Włodzimierz Fehler [red.:] *Bezpieczeństwo publiczne w przestrzeni miejskiej*, Arte 2010

Bar Gabriela: *Recenzja monografii autorstwa dra Tomasza Romana Smusa pt. „Spełnianie świadczeń pieniężnych za pomocą pieniądza elektronicznego",* „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 68-71, http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Barbaszewski Tomasz: *Zamówienia publiczne na oprogramowanie. Aspekty technologiczne i finansowe,* Fundacja Wolnego i Otwartego Oprogramowania 2010

Barecki Tomasz: *Metodyka audytu bezpieczeństwa systemu teleinformatycznego przetwarzającego informacje niejawne* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 15-28

Barta Janusz, Markiewicz Ryszard, *Prawo autorskie w Internecie* [w:] *Prawo autorskie.* Wyd. II, Wolters Kluwer 2010

Bendyk Edwin: *Krytyka rozumu cyfrowego*, „Opcje" 1/2010, s. 10-13

Bernaczyk Michał, Presz Anna: *Karnoprawna ochrona dostępu do informacji publicznej w działalności prokuratury i sądów powszechnych. Część I*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 1/2010, s. 50-61, http://cbke.prawo.uni.wroc.pl/files/pme/PME_1_2010.pdf

Bernaczyk Michał, Presz Anna: *Karnoprawna ochrona dostępu do informacji publicznej w działalności prokuratury i sądów powszechnych. Część II*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 54-67, http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Bernaczyk Michał: *Udostępnianie informacji publicznych w postaci elektronicznej w orzecznictwie sądów administracyjnych* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Białek Tadeusz, Marzec Agnieszka: *Ustawa o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych. Komentarz*, Wolters Kluwer 2010

Bidziński Mariusz, Chmaj Marek, Szustakiewicz Przemysław: *Ustawa o dostępie do informacji publicznej komentarz,* C.H. Beck 2010

Bińkowska-Artowicz Beata: *Przetwarzanie danych osobowych stanowiących tajemnicę bankową w świetle orzecznictwa sądów administracyjnych*, „Czas Informacji" 4/2010

Bodnar Adam, Jagielski Michał: *Informacja kredytowa a ochrona danych osobowych* [w:] Krzysztof Markowski, Marek Wierzbowski [red.:] *Prawne uwarunkowania wymiany informacji – nowe wyzwania*, Stowarzyszenie Absolwentów WPiA UW 2009 [pozycja ukazała się jesienią 2010], s. 119-138

Bogucki Dariusz: *Inicjatywa Wspólnotowa Ambient Assisted Living AAL*, „Czas Informacji" 3/2010

Bogucki Dariusz: *Program Ramowy na rzecz Innowacyjności i Konkurencyjności a wspieranie rozwoju technologii informacyjnych i komunikacyjnych CIP ICT PSP*, „Czas Informacji" 4/2010

Bogucki Dariusz: *Sieć Szerokopasmowa Polski Wschodniej*, „Czas Informacji" 2/2010

Bogucki Dariusz: *Unia Innowacji*, „Czas Informacji" 4/2010

Bojek Ernest, Haręza Adam: *The legal personality of government in the face of technological development and security* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 11-24

Borcuch Artur: *Cyfrowe społeczeństwo w elektronicznej gospodarce,* CeDeWu, 2010

Borowiecki Ryszard, Czekaj Janusz [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Brodzicki Tomasz: *Ochrona informacji niejawnych w jednostce samorządowej* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 29-34

Brzozowska Monika: *Prawo autorskie w administracji publicznej*, Presscom 2010

Brzozowski Maciej: *Organizacja wirtualna*, PWE 2010

Bubiło Jarosław: *Prawnomiędzynarodowe regulacje dotyczące prawa do prywatności - na tle dorobku zagranicznej doktryny i judykatury* [w:] Waldemar Bednaruk [red.:] *Polska w Strefie Schengen*, KUL 2010

Budziewicz-Guźlecka Agnieszka, *Istota wykluczenia społecznego w społeczeństwie informacyjnym* [w:] Iwona Chomiak-Orsa, Adam Nowicki, Henryk Sroka [red.:] *Informatyka ekonomiczna. Systemy informacyjne w zarządzaniu. Przegląd naukowo-dydaktyczny nr 17*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu 2010, s. 241-249

Bulut Cevdet: *Data protection in Austria* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 105-110

Byczkowski Maciej: *Zarządzanie bezpieczeństwem informacji i systemów* [w:] Janusz Zawiła-Niedźwiedzki, Katarzyna Rostek, Artur Gąsiorkiewicz [red.:] *Informatyka gospodarcza. Tom 4*, C.H. Beck 2010

Byrski Jan: *Elektronicznie z urzędem skarbowym*, „IT w Administracji" 5/2010

Byrski Jan: *Tajemnica prawnie chroniona w działalności bankowej*, C.H. Beck 2010

Bytniewski Andrzej: *Systemy informatyczne organizacji jako czynnik rozwoju społeczeństwa informacyjnego* [w:] Jerzy Korczak, Iwona Chomiak-Orsa, Henryk Sroka [red.:] *Systemy informacyjne w zarządzaniu*, s. 170-181, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu 2010

Celarek Krystyna: *Prawne aspekty informatyzacji administracji,* WSB Dąbrowa Górnicza 2010

Celiński Piotr: *Interfejsy. Cyfrowe technologie w komunikowaniu*, Wydawnictwo UMCS 2010

Chmielarz Witold: *Stan i dynamika rozwoju elektronicznej administracji w Polsce na tle tendencji europejskich* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Chmielewski Jacek Maria, Szomański Bolesław, Waćkowski Kazimierz: *Przegląd wybranych standardów i norm stosowanych w informatyce* [w:] Janusz Zawiła-Niedźwiedzki, Katarzyna Rostek, Artur Gąsiorkiewicz [red.:] *Informatyka gospodarcza. Tom 4*, C.H. Beck 2010

Chwalba Jakub: *Prawo prasowe a publikacje internetowe,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 109/2010, s. 87-109

Ciborowski Leopold: *Rzeczowa postać informacji oraz jej funkcje i właściwości* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Cieślak Łukasz: *Selected issues of data protection in the Visegrad Group States and in Austria* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 25-38

Cieślak Sławomir: *Elektroniczne postępowanie upominawcze*, „Monitor Prawniczy" 7/2010, s. 359-369

Cieślik Artur: *Skuteczna ochrona urzędu*, „IT w Administracji" 11/2010

Cisek Rafał: *Spór o domenę „świstak.pl"*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 77-78, http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Cisek Rafał: *Śladami e-sądów*, „IT w Administracji" 2/2010

Cisek Rafał: *Wypełnienie formularza rejestracyjnego nie jest chwilą zawarcia umowy on-line*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 1/2010, s. 62-66, http://cbke.prawo.uni.wroc.pl/files/pme/PME_1_2010.pdf

Citko Adam G.: *Dokument elektroniczny w życiu administracji,* Edukacja Prawnicza – Serwis Internetowy, 2010, http://www.edukacjaprawnicza.pl/index.php?mod=m_aktualnosci&cid=69&id=1394

Cybulka Jolanta: *Metoda tworzenia ontologii na potrzeby systemu wspomagającego prace dochodzeniowo-śledcze w sprawach przestępstw gospodarczych* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Cygan Tomasz: *Umowa normalnie poufna* , „IT w Administracji" 8/2010

Cygan Tomasz: *Urzędowa polityka*, „IT w Administracji" 11/2010

Czekaj Janusz, Ćwiklicki Marek, Obora Hubert: *Ekonomika informacji v. infonomika* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Czubik Agnieszka: *Prawo do prywatności w travaux preparatoires Europejskiej Konwencji Praw Człowieka*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 7/2009, s. 111-120

Czyżak Mariusz: *Karnoprawny charakter odpowiedzialności biura informacji gospodarczej za udzielenie nieprawdziwych lub nieaktualnych informacji gospodarczych,* „Wojskowy Przegląd Prawniczy" 1/2010, s. 33-41

Danielewicz Michał: *Wikipedia – socjologiczny reportaż z miejsca zdarzeń*, „Studia Socjologiczne" 2/2010, s. 127-156

Dąbkiewicz Krzysztof: *Ochrona prawnokarna niektórych usług elektronicznych*, „Prokuratura i Prawo" 1/2011, s. 68-85

Dela Mirosław: *Rejestracja zbioru danych osobowych*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 47-53 http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Dębicka Olga: *Informatyczne systemy zarządzania* [w:] Jacek Winiarski [red.:] *Gospodarka elektroniczna współczesne przedsiębiorstwo na rynku globalnym*, Wydawnictwo Uniwersytetu Gdańskiego 2010

Domaszk Arkadiusz, *Ochrona danych osobowych - obowiązek duszpasterski*, „Prawo Kanoniczne" 2/2010

Drachal Janusz: *Zagadnienia sądowej ochrony prawa do informacji,* Zeszyty Naukowe Sądownictwa Administracyjnego 5-6/2010*,* s. 100-119

Drajewicz Dariusz: *Dowodowe wykorzystanie wyników kontroli operacyjnej w postępowaniu karnym,* „Prokuratura i Prawo" 7-8/2010, s. 165-181

Draniewicz Bartosz: *Elektroniczne postępowanie upominawcze*, „Edukacja Prawnicza" 5/2010, s. 6-10

Drelichowski Ludosław: *Uwarunkowania rozwoju zastosowań wiedzy w zarządzaniu publicznym* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Dudzie Adam: *Przyszłość formuły Schengen jako gwaranta bezpieczeństwa w Unii Europejskiej po przyjęciu programu sztokholmskiego* [w:] Zbigniew Ciekanowski [red.:] *Infrastruktura bezpieczeństwa publicznego ogólnokrajowe i lokalne wyzwania cywilizacyjne*, Wyższa Szkoła Zarządzania i Prawa Warszawa 2010

Dutko Maciej, Karciarz Magdalena: *Informacja w Internecie,* PWN 2010

Dyląg Łukasz: *Elektroniczna forma oświadczenia woli*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 1/2010, s. 19-24, http://cbke.prawo.uni.wroc.pl/files/pme/PME_1_2010.pdf

Dzierżanowski Włodzimierz, Grzebalska Marta: *Mechanizmy finansowania partnerstwa publiczno-prywatnego w kontekście ustawy o partnerstwie publiczno prywatnym i ustawy o koncesjach,* „Czas Informacji" 2/2010

Dzioba Krzysztof, Rybicki Rafał: *Cyber-Terrorism and Cyber-Warfare. Virtual Reality – true menance* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 39-48

Europejska Agenda Cyfrowa: program rozwoju społeczeństwa informacyjnego w Unii Europejskiej w latach 2010-2015: Wprowadzenie i główne dokumenty, Wyd. II, MSWiA 2010

Fajgielski Paweł: *Kontrola i audyt przetwarzania danych osobowych*, Presscom 2010

Felchner Krzysztof: *Kompleksowa regulacja zwalczania przesyłania spamu w projekcie nowelizacji prawa telekomunikacyjnego*, „Radca Prawny" 6/2010

Fischer Bogdan: *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich*, Wolters Kluwer 2010

Formella Zbigniew: *Cyberbulling: zagrożenie, prewencja, wyzwania edukacyjne* [w:] Bis Dorota, Rynio Alina [red.:] *Media w wychowaniu chrześcijańskim*, Wydawnictwo KUL 2010, s. 475-490

Franciszek Danielewski: *Specyficzność informacji w działaniach wojennych* [w:] Mirosław Kwieciński [red.:] *Bezpieczeństwo informacji i biznesu zagadnienia wybrane*, Akademia Frycza Modrzewskiego Kraków 2010

Francuz Piotr: *Zastosowanie współczesnych technologii informatycznych i Internetu w szkolnictwie wyższym* [w:] Bis Dorota, Rynio Alina [red.:] *Media w wychowaniu chrześcijańskim*, Wydawnictwo KUL 2010, s. 651-662

Frankowski Paweł: *Darmowy Intranet dla urzędników*, „IT w Administracji" 8/2010

Frankowski Paweł: *Urząd w każdej komórce*, „IT w Administracji" 6/2010

Frączkiewicz-Wronka Aldona, Saryusz-Wolska Hanna: *E-administracja w praktyce funkcjonowania małej gminy: raport z badań 'Rzeczywistość skrzeczy'* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Gacki Grzegorz: *Ciemna strona sądu*, „IT w Administracji" 2/2010

Gacki Grzegorz: *E-okienko u sołtysa*, „IT w Administracji" 8/2010

Gajos Małgorzata [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010

Galewska Ewa [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010

Gałęska-Śliwka Anita: *Kalifornijska Baza DNA*, „Prokuratura i Prawo" 7-8/2010, s. 240-248

Ganczar Małgorzata: *Wpływ technologii komunikacyjno-informacyjnych na postępowanie administracyjne na przykładzie wnoszenia i doręczania pism w formie elektronicznej* [w:] Stanisław Wrzosek, Michał Domagała, Jan Izdebski, Tadeusz Stanisławski [red.:] *Współzależność dyscyplin badawczych w sferze administracji publicznej*, C.H. Beck 2010

Gapska Edyta: *Wykorzystanie technologii informatycznych w cywilnym postępowaniu sądowym*, [w:] Piotr Pogonowski, Paweł Cioch, Edyta Gapska, Joanna Nowińska [red.] *Współczesne przemiany postępowania cywilnego*, Wolters Kluwer 2010

Garlicki Leszek: *Wolność wypowiedzi dziennikarza – przywileje i odpowiedzialność,* „Europejski Przegląd Sądowy" 1/2010, s.12-17

Gladysz Anna: *Analiza danych tekstowych wraz z zastosowaniem sieci semantycznej jako narzędzia reprezentacji wiedzy dziedzinowej* [w:] Witold Chmielarz, Tomasz Parys, Jerzy Kisielnicki [red:] *Informatyka w przyszłości*, Wydział Zarządzania Uniwersytetu Warszawskiego 2010

Gliszczyńska Justyna, Śliwińska Magdalena: *Tajemnica bankowa w praktyce*, Bodie 2010

Gliściński Konrad: *Wyodrębnianie się nowych pól eksploatacji i ich wpływ na obrót prawami do utworów,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 109/2010, s. 45-60

Głaz Sławomir: *Ochrona danych osobowych w ZOZ-ach*, „IT w Administracji" 1/2010

Golat Rafał: *Krajowa strategia cyfryzacji dziedzictwa narodowego* [w:] Henryk Hollender [red.:] *Cyfrowy świat dokumentu. Wydawnictwa, biblioteki, muzea, archiwa*, Centrum Promocji Informatyki 2010

Golonka Anna: *Granice dopuszczalnego monitoringu pracownika przy wykorzystaniu jego danych biometrycznych oraz audiowizualnych form nadzoru* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Gołaczyński Jacek [red.:] *Elektroniczne postępowanie upominawcze. Komentarz*, Wolters Kluwer 2010

Gołaczyński Jacek [red:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Gołaczyński Jacek, Kotecka Sylwia: *Kolejny etap informatyzacji postępowania cywilnego. Uwagi na tle projektu zmiany ustawy – kodeks postępowania cywilnego. Część I,* „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 14-18 http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Gołaczyński Jacek: *Informatyzacja postępowania w sprawie europejskiego nakazu zapłaty i w sprawie drobnych roszczeń w prawie polskim. Wnioski de lege ferenda* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Gołuchowski Jerzy, Filipczyk Barbara: *Wiedza i komunikacja w innowacyjnych organizacjach. Systemy ekspertowe wczoraj, dziś jutro*, Uniwersytet Ekonomiczny w Katowicach 2010

Gołuchowski Jerzy, Frączkiewicz-Wronka Aldona [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Gorazdowski Krzysztof: *Kontrola korespondencji e-mailowej pracownika* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Goździaszek Łukasz: *Elektroniczne orzeczenia sądowe* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Goździaszek Łukasz: *Podpis elektroniczny w prawie amerykańskim*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 1/2010, s. 44-49, http://cbke.prawo.uni.wroc.pl/files/pme/PME_1_2010.pdf

Goździaszek Łukasz: *Zasada bezpośredniości i pisemności postępowania dowodowego w świetle nowelizacji Kodeksu postępowania cywilnego z dnia 5 grudnia 2008 r.*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 26-30, http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Góral Zbigniew [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Górny Andrzej, Zygmunt Agata: *Para w Sieci*, „Opcje" 1/2010, s. 45-50

Grabowski Mariusz, *Kierunki interdyscyplinarnej wizji systemów informacyjnych zarządzania* [w:] Iwona Chomiak-Orsa, Adam Nowicki, Henryk Sroka [red.:] *Informatyka ekonomiczna. Systemy informacyjne w zarządzaniu. Przegląd naukowo-dydaktyczny nr 17*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu 2010, s. 290-298

Groń Maciej: *Elektroniczne dzienniki urzędowe. Wpływ wymagań technicznych dla dokumentów elektronicznych zawierających akty normatywne i inne akty prawne na ich treść* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Gródek Zofia: *Sieci informacyjne dla przedsiębiorczości - czynnik przewagi konkurencyjnej opartej na informacji* [w:] Ryszard Borowiecki, Janusz Czekaj [red.:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki,* Difin 2010

Gruza Ewa: *Czy badania wariograficzne są skuteczną kontrolą prawdomówności pracownika* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Grzybko Leszek: *Szerokopasmowy Internet standardem w 2015 roku?,* „Czas Informacji" 3/2010

Grzymkowska Magdalena: *The threats arise from Legal Information Systems* [w:] Ewa Galwska [red.:] *European Information Law. Good Governance in the Public Sector*, CBKE 2010, s. 49-56

Haręża Adam: *Recenzja książki autorstwa Joanny Kuleszy pt. „Ius internet. Między prawem a etyką"*, „Kwartalnik Naukowy - Prawo Mediów Elektronicznych" 2/2010, s. 72-76, http://cbke.prawo.uni.wroc.pl/files/pme/PME_2_2010.pdf

Herbowski Piotr: *Badania poligraficzne pracownika - szanse i zagrożenia* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Hernas Adam: *Bezpieczeństwo informacji, bezpieczeństwo teleinformatyczne i polityka bezpieczeństwa - trzy wymiary ochrony informacji i danych osobowych* [w:] Mirosław Kwieciński [red.:] *Bezpieczeństwo informacji i biznesu zagadnienia wybrane*, Akademia Frycza Modrzewskiego Kraków 2010

Hoc Stanisław: *Bezpieczeństwo informacyjne. Wybrane problemy* [w:] Sokolewicz Wojciech [red.:] *Krytyka Prawa. Niezależne studia nad prawem. Tom II. Bezpieczeństwo*, WAIP 2010

Hoc Stanisław: *Geneza ustawy o ochronie informacji niejawnej* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 35-56

Hoc Stanisław: *Ustawa o ochronie informacji niejawnych. Komentarz,* Lexis Nexis 2010

Hollender Henryk [red.:] *Cyfrowy świat dokumentu. Wydawnictwa, biblioteki, muzea, archiwa*, Centrum Promocji Informatyki 2010

Hołyst Brunon, Pomykała Jacek: *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 1/2011, s. 5-34

Hoppe Łukasz, Semeniuk Tomasz, Wąsek Łukasz: *SWDOP – System Wspomagania Działań Operacyjno-Procesowych* [w:] Małgorzata Gajos [red.:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały z VI Kongresu*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych / Uniwersytet Śląski 2010, s. 213-216

Ignac-Nowicka Jolanta: *Rozwój technicznych środków zabezpieczeń w obrębie systemów monitoringu wizyjnego miejsc publicznych* [w:] Włodzimierz Fehler [red.:] *Bezpieczeństwo publiczne w przestrzeni miejskiej*, Arte 2010

Iszkowski Wacław: *Teleinformatyka ICT w czterech obszarach*, „Czas Informacji" 4/2010

Izdebski Krzysztof: *Uwolnić dane publiczne*, „IT w Administracji" 11/2010

Jacek Mirecki: *Identyfikacja biometryczna jako element optymalizacji procesu e-learningu w administracji publicznej* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Jach Mariusz, *Wpływ strategii informacyjnej na proces outsourcingu technologii informacyjnych* [w:] Iwona Chomiak-Orsa, Adam Nowicki, Henryk Sroka [red.:] *Informatyka ekonomiczna. Systemy informacyjne w zarządzaniu. Przegląd naukowo-dydaktyczny nr 17*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu 2010, s.299-308

Jackiewicz Anita: *Nowe dowody osobiste - zmiany na lepsze czy na gorsze?*, „Czas Informacji" 3/2010

Jackiewicz Anita: *W oczekiwaniu na elektroniczne akty prawne*, „Czas Informacji" 4/2010

Jagielski Mariusz: *Prawo ochrony danych osobowych. Standardy europejskie*, Wolters Kluwer 2010

Janasova Eva, Ardielli Jifi: *The Usage of Public Information Systems In the Czech Health Service* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Janczy Mariola, Gradzik Tomasz: *Metody digitalizacji dokumentów*, „IT w Administracji" 12/2010

Jankowska Marlena: *Autorstwo „zbiorowe" na przykładzie Wikipedii,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 110/2010

Jankowski Grzegorz: *Dostęp do informacji publicznej*, „In Gremio" 5/2010

Janowski Jacek: *Aktualna rola informatyki prawniczej w powiązaniu z informatyką administracyjną* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Januszko Wojciech: *Społeczeństwo informacyjne - manipulacje, szansę, zagrożenia* [w:] Witold Chmielarz, Tomasz Parys, Jerzy Kisielnicki [red.:] *Informatyka w przyszłości*, Wydział Zarządzania Uniwersytetu Warszawskiego 2010

Jastrzębska Anna: *Organizacje zbiorowego zarządzania prawami autorskimi a Creative Commons,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 108/2010, s. 20-33

Jaworski Michał: *Zasady rządzące interoperacyjnością w dokumentach Unii Europejskiej*, „Czas Informacji" 1/2010

Jaworski Ryszard: *Bezczynność i nieporadność organów ścigania jako przyczyny korzystania przez pracodawców z badań poligraficznych* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Jeruzałski Tomasz: *Rola procedury zgodności w uzyskaniu jednolitych standardów systemu informatycznego w administracji publicznej przykład Ministerstwa Pracy i Polityki Społecznej* [w:] Witold Chmielarz, Tomasz Parys, Jerzy Kisielnicki [red.:] *Informatyka w przyszłości*, Wydział Zarządzania Uniwersytetu Warszawskiego 2010

Jesionek Robert: *Jakość administracyjnego biznesu*, „IT w Administracji" 7/2010

Jędrzejek Czesław, Bąk Jarosław, Fałkowski Maciej, Smoleński Maciej, Więckowski Jacek: *Stosowalność ontologii Modelu Minimalnego do analizy aktów oskarżenia spraw nielegalnego handlu paliwem* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Kaczaia Monika: *Sprzedaż ubezpieczeń przez Internet* [w:] Janusz Zawiła-Niedźwiedzki, Katarzyna Rostek, Artur Gąsiorkiewicz [red.:] *Informatyka gospodarcza. Tom 4*, C.H. Beck 2010

Kaczmarek Berenika: *Dokument elektroniczny dowodem w procesie cywilnym* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Kaczmarek-Templin Berenika, Goździaszek Łukasz: *Mechanizm rozpoznania sprawy w elektronicznym postępowaniu upominawczym - polemika*, „Monitor Prawniczy" 16/2010, s. 896-902

Kaczmarek-Templin Berenika: *Kilka uwag o elektronicznej postaci umowy o arbitraż w kontekście przepisów regulujących formę zapisu na sąd polubowny*, „ADR. Arbitraż i Mediacja" 3/2009, s. 17-30

Kaczorek Grzegorz: *Handel elektroniczny* [w:] Janusz Zawiła-Niedźwiedzki, Katarzyna Rostek, Artur Gąsiorkiewicz [red.:] *Informatyka gospodarcza. Tom 4*, C.H. Beck 2010

Kaliński Wojciech: *Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne - część IV*, „Czas Informacji" 4/2010

Kaliński Wojciech: *Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne - część III*, „Czas Informacji" 3/2010

Kaliński Wojciech: *Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne - część II*, „Czas Informacji" 2/2010

Kaliński Wojciech: *Prawne aspekty rekomendacji Urzędu Zamówień Publicznych dotyczących udzielania zamówień na systemy informatyczne - część I*, „Czas Informacji" 2/2010

Kamiński Andrzej: *Zintegrowane systemy informatyczne zarządzania* [w:] Janusz Zawiła-Niedźwiedzki, Katarzyna Rostek, Artur Gąsiorkiewicz [red.:] *Informatyka gospodarcza. Tom 4*, C.H. Beck 2010

Kamiński Ireneusz C.: *Europejskie standardy dotyczące swobody wypowiedzi komercyjnej,* „Europejski Przegląd Sądowy" 6/2010, s.28-35

Kamiński Ireneusz C.: *Swoboda wypowiedzi w orzecznictwie ETPCz w 2009 r.*, „Europejski Przegląd Sądowy" 1/2011, s. 33-44

Kamiński Krzysztof, Zalesińska Anna: *Scenariusz postępowania hybrydowego* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Kamiński Krzysztof: *W sądowym e-wymiarze*, „IT w Administracji" 2/2010

Kamiński Mateusz: *Bez wychodzenia z domu*, „IT w Administracji" 5/2010

Kamiński Mateusz: *Czy nadal liczy się każdy e-mail*, „IT w Administracji" 6/2010

Kamiński Mateusz: *Kto straci na informatyzacji*, „IT w Administracji" 5/2010

Kamiński Mateusz: *Norma Polskiej Normy*, „IT w Administracji" 2/2010

Kamiński Mateusz: *Sygnowanie pism procesowych podpisem elektronicznym w świetle orzecznictwa sądów polskich* [w:] Jacek Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej,* C.H. Beck 2010

Kamiński Mateusz: *Zaufaj profilowi*, „IT w Administracji" 4/2010

Karczewska Joanna: *Jak zostać audytorem*, „IT w Administracji" 9/2010

Karczewska Joanna: *Metodyka audytów systemów IT*, „IT w Administracji" 9/2010

Karlik Piotr: *Grooming,* „Edukacja Prawnicza" 1/2010, s. 34-35

Karlińska Maria: *Rozwój usług telemedycznych dostępnych dla mieszkańców powiatu* [w:] Jerzy Gołuchowski, Aldona Frączkiewicz-Wronka [red.:] *Technologie wiedzy w zarządzaniu publicznym*, Uniwersytet Ekonomiczny w Katowicach 2010

Kasprzak Magdalena: *Badania wariograficzne w opinii pracodawców i pracowników* [w:] Zbigniew Góral [red.:] *Kontrola pracownika możliwości techniczne i dylematy prawne,* Wolters Kluwer 2010

Kaszubski Remigiusz W.: *Wpływ konstrukcji prawnej tajemnicy bankowej na wymianę informacji gospodarczej* [w:] Krzysztof Markowski, Marek Wierzbowski [red.:] *Prawne uwarunkowania wymiany informacji – nowe wyzwania,* Stowarzyszenie Absolwentów WPiA UW 2009 [pozycja ukazała się jesienią 2010], s. 89-118

Kautz Maciej: *Prawo do prywatności osób powszechnie znanych i jego ochrona w polskim systemie prawnym (część II),* „Edukacja Prawnicza" 12/2010, s. 20-22

Kawka Inga: *Wpływ orzeczeń Trybunału Sprawiedliwości Unii Europejskiej na polskie prawo telekomunikacyjne* [w:] Biernat Stanisław, Dudzik Sławomir [red.:] *Doświadczenia prawne pierwszych lat członkostwa Polski w Unii Europejskiej,* Wolters Kluwer 2010, s. 391-404

Zamówienie prenumeraty kwartalnika

„Czas informacji”

WYŚLIJ FAKSEM 22 871 85 56 lub 22 870 69 95

PRENUMERATA NA ROK 2011

Zamawiamy prenumeratę kwartalnika „**Czas Informacji**”

okres trwania prenumeraty (ilość egzemplarzy)	ilość zamawianych prenumerat	**cena**
prenumerata roczna 2011 od numeru 1/2011 - 4 kolejne numery		340 zł +5% VAT
prenumerata półroczna numer 1/2011 i 2/2011		200 zł +5% VAT

Prenumeratę prosimy przesłać do niżej wymienionego adresata

PRENUMERATOR		FIRMA	
imię		nazwa	
nazwisko		NIP	
stanowisko		ulica	
nr telefonu		kod, miasto	
nr faksu		nr telefonu	
e-mail		nr faksu; e-mail	

Wyrażam zgodę/ Nie wyrażam zgody na wykorzystywanie przez Centrum Promocji Informatyki sp. z o. o., Warszawa, ul. Międzyborska 50, moich danych (w tym adresu poczty elektronicznej), pod warunkiem przestrzegania przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. jedn. Dz. U. z 2002 r. Nr 101, poz. 926), w zakresie prowadzonej przez CPI działalności gospodarczej (a w szczególności działalności marketingowej i na przekazywanie danych uczestnika firmom biorącym udział w opracowaniu programów szkoleń). Mam świadomość prawa do wglądu, poprawiania lub usunięcia swoich danych w bazie danych osobowych CPI oraz dobrowolności ich podania. W związku z obowiązkiem wynikającym z ustawy z dnia 18 lipca 2002 r. (Dz. U. nr 144, poz. 1204) o świadczeniu usług drogą elektroniczną wyrażam zgodę na

Oznaczoną należność z tytułu kosztów prenumeraty w wysokości _____zł wpłacę w terminie 14 dni od daty otrzymania faktury.

Należy wypełnić i odesłać faksem na numer
22 871 85 56 lub 22 870 69 95

.....
pieczęć i podpis osoby upoważnionej

redaktor naczelny:	Wiesław Paluszyński wieslaw.paluszynski@czasinformacji.pl	Reklama:	Karolina Popek reklama@czasinformacji.pl
kolegium redakcyjne:	Izabela Adamska, Krzysztof Głomb, Xawery Konarski Tomasz Kulisiewicz, Marcin Maruta, dr Grzegorz Sibiga Piotr Waglowski, dr Wojciech Wiewiórowski	projekty graficzne:	Mikołaj Ostaszewski mikolaj.ostaszewski@zsrr.pl
sekretarz redakcji:	Monika Handzelewicz redakcja@czasinformacji.pl	skład i łamanie:	Michał Nowosielski michal@nowosielscy.com.pl
redakcja:	Centrum Promocji Informatyki sp. z o. o. ul. Międzyborska 50, 04-041 Warszawa tel. 22 870 69 78, 22 871 85 51 fax 22 870 69 95, 22 871 85 56 info@czasinformacji.pl www.czasinformacji.pl	nakład:	400 egz.
		prenumerata:	prenumerata@czasinformacji.pl www.czasinformacji.pl/prenumerata
			Zamówienia prenumeraty również u kolporterów.

Redakcja nie zwraca materiałów niezamówionych oraz zastrzega sobie prawo do ich redagowania i skracania.

wydawca:

Centrum Promocji Informatyki sp. z o. o.
www.cpi.com.pl

rada naukowa:

prof. dr hab. Jacek Gołaczyński
prof. dr hab. Remigiusz Kaszubski
prof. dr hab. Mirosław Kutyłowski
dr hab. Artur Nowak-Far
prof. dr hab. Ewa Nowińska
prof. dr hab. Witold M. Orłowski
dr hab. Grażyna Szpor

W części naukowej kwartalnika umieszczane są prace naukowe publikowane w języku polskim (ze streszczeniem), które podlegają recenzjom rady.

Czas informacji

Kwartalnik „**Czas Informacji**" jest scaloną formą czasopism „elektroniczna Administracja" i „Prawo Nowych Technologii", które Centrum Promocji Informatyki wydawało do 2009 roku. Pismo adresowane jest do przedstawicieli administracji oraz środowisk prawniczych.

Zapraszamy do składania zamówień na prenumeratę na 2011 rok.

www.czasinformacji.pl/prenumerata.php

cpi
centrum promocji informatyki
www.cpi.com.pl