Raport Instytutu Sobieskiego

Nr 26/2007

Czy PESEL2 jest potrzebny?

Robert Kępczyński, Krzysztof Komorowski,
Piotr Kociński, Tadeusz Chełkowski

TWORZYMY IDEE DLA POLSKI

INSTYTUT SOBIESKIEGO

Instytut Sobieskiego
ul. Nowy Świat 27, 00-029 Warszawa
tel./fax: (022) 826 67 47
tel.: (022) 211 12 75
fax: (022) 211 12 76

e-mail: sobieski@sobieski.org.pl
http://www.sobieski.org.pl

Volkswagen Bank Polska S.A.
45 2130 0004 2001 0340 1999 0001

Robert Kępczyński[1], Krzysztof Komorowski[2], Piotr Kociński[3], Tadeusz Chełkowski[4]
krzysztof.komorowski@sobieski.org.pl

Czy PESEL2 jest potrzebny?

Marzec 2007

Spis treści:

[1] Robert Kępczyński – absolwent wydziału Matematyki UW, konsultant w dziedzinie bezpieczeństwa systemów i zarządzania ryzykiem, CISSP, pracuje w międzynarodowej firmie informatycznej, współpracuje z Instytutem Sobieskiego.
[2] Krzysztof Komorowski – absolwent Wydziału Matematyki i Fizyki UMCS, konsultant w dziedzinie strategii informatycznych, pracuje w międzynarodowej firmie informatycznej, ekspert Instytutu Sobieskiego.
[3] Piotr Kociński – dr fizyki , OpenGroup Master IT Architect, pracuje w dziale usług technologicznych międzynarodowej firmy informatycznej, kieruje zespołem konsultantów i projektantów IT, współpracuje z Instytutem Sobieskiego.
[4] Tadeusz Chełkowski – absolwent wydziału Ekonometrii i Informatyki Akademii Ekonomicznej w Szczecinie, OpenGroup Master IT Architect, odpowiada za rozwój międzynarodowej firmy specjalizującej się w tworzeniu oprogramowania w Polsce i krajach bałtyckich, współpracuje z Instytutem Sobieskiego.

1. Wprowadzenie

Od ponad roku w MSWiA trwają prace nad systemem PESEL2. Udostępnione informacje na ten temat są mało precyzyjne. Wyłaniający się obraz systemu, choć fragmentaryczny, budzi wiele poważnych wątpliwości. Deklarowane cele, którym ma służyć PESEL2 są nieprecyzyjne i szeroko zakrojone. Co więcej, związek między samą koncepcją systemu PESEL2 a jego deklarowanymi celami jest bardzo luźny, co w przypadku tak wielkiego przedsięwzięcia musi budzić niepokój. W żadnym z opublikowanych dokumentów autorzy koncepcji nie odnieśli się do wielu istotnych problemów bezpieczeństwa, typowych dla takich systemów.

Dyskusja na temat PESEL2, jak dotąd, toczy się w wąskim gronie specjalistów i dotyczy przede wszystkim problemów technicznych. Tworzy to błędne wrażenie, że wizja informatyzacji państwa, którą kierują się autorzy koncepcji systemu PESEL2 jest powszechnie akceptowana.

Raport ma na celu ożywienie dyskusji na temat systemu PESEL2 i poszerzenie jej zakresu w dwóch wymiarach. Chcemy objąć dyskusją również faktyczne cele polityczne systemu i społeczne konsekwencje ich realizacji. Zależy nam także na poszerzeniu kręgu debaty o osoby spoza branży IT, które do tej pory nie włączyły się do dyskusji o PESEL2 z powodu mylnego przekonania, że jest to przedsięwzięcie czysto inżynierskie. Stąd też w raporcie staramy się używać języka zrozumiałego dla szerokiego kręgu odbiorców.

2. Informatyka, procesy administracyjne i polityka

Informatyka to nauka o przetwarzaniu informacji. Przetwarzanie informacji to ich tworzenie, przesyłanie z miejsca na miejsce, składowanie, analizowanie a także wnioskowanie w oparciu o zebrane informacje. Informacje mogą dotyczyć osób, przedmiotów czy zdarzeń. „Informacja" to *news* dostępny na portalu, wyciąg z konta bankowego, faktura z TP S.A., zestawienie danych o kliencie w sieci handlowej. Systemy komputerowe stały się najważniejszym narzędziem przetwarzania informacji. Informatyka to również wiedza o tym jak wspomagać, organizować i kontrolować pracę złożonych instytucji przy wykorzystaniu systemów komputerowych.

W informatyce bardzo ważnym pojęciem jest *proces*, proces biznesowy bądź *administracyjny*. Proces to szereg wzajemnie powiązanych *czynności* wykonywanych za każdym razem w ten sam sposób w celu uzyskania określonego rezultatu. Z każdą czynnością procesu związane jest pewne kwantum przetwarzanych informacji. Komputery i programy wspomagają wykonywanie tych czynności, a ostatnio umożliwiają również automatyczny nadzór nad ogółem procesów realizowanych w danym systemie.

Tworzenie *złożonego systemu informatycznego* (czyli zbioru wielu wyspecjalizowanych i współpracujących ze sobą programów komputerowych) powinno być poprzedzone definicją procesów administracyjnych, które ten system ma wspomagać. Jeśli procesy nie są zdefiniowane i opisane, to rozpoczynanie projektu informatycznego nie ma sensu. Bez zdefiniowanych procesów budowa systemu informatycznego przypomina wznoszenie budynku bez zdefiniowania celów, jakim będzie on służył: czy będzie biurowcem, halą sportową czy fabryką. Tworząc system informatyczny należy najpierw wskazać precyzyjnie cele, które system ma realizować, następnie zdefiniować procesy, które będą „narzędziami" do realizacji tych celów i dopiero na końcu zaprojektować programy komputerowe służące do wspomagania tych procesów.

Naturalną skłonnością rządzących jest gromadzenie informacji o rządzonych. Od stuleci tworzono lokalne i centralne kartoteki z danymi osobowymi. Poprzez analizę zgromadzonych informacji władza mogła realizować różne cele polityczne.

W latach dwudziestych ubiegłego wieku bolszewicy dostrzegli, że analiza danych zebranych w centralnych kartotekach z danymi osobowymi, ułatwia planowanie działań represyjnych na masową skalę. Najpierw robili to bolszewicy a później naziści. Co ciekawe takie specyficzne działania analityczne podjął demokratycznie wybrany rząd szwedzki, który realizował program eugeniczny opierając się na analizie obywateli na podstawie skatalogowanych zdjęć twarzy.

Po wprowadzeniu maszyn cyfrowych możliwości takich działań niepomiernie wzrosły. Odtąd kartoteki i akta zaczynają być przekształcane w bazy danych (nazywanych w tym dokumencie również rejestrami jeśli są w nich zgromadzone dane osobowe).

W Polsce w latach 70-tych wdrożono system PESEL, w ramach którego jako pierwszy został uruchomiony podsystem MAGISTER, który wedle oficjalnych oświadczeń miał *„obejmować osoby z wyższym wykształceniem”* oraz *„służyć potrzebom gospodarowania kadrami i planowania gospodarczego oraz usprawniania procesów administracyjnych”*. System PESEL był ściśle związany z koncepcją *meldunku*, czyli powszechnego obowiązku rejestracji aktualnego adresu zamieszkania. Pojawia się pytanie, jakie faktyczne cele polityczne realizowano w oparciu o bazę danych PESEL i jakie de facto cele mogą być realizowane przez system PESEL2.

Cele wskazane w akcie założycielskim PESEL są na tyle ogólne, że nie sposób sprawdzić czy zostały osiągnięte. Jeśli przyjąć, że PESEL został tak naprawdę założony po to, by poprzez centralną identyfikację obywateli powiązaną z obowiązkiem meldunkowym, uzyskać lepszą kontrolę państwa nad społeczeństwem, to wiele wskazuje, że taki cel został częściowo osiągnięty. To, że nie został osiągnięty w pełni, wynikało nie tyle z niedoskonałości narzędzi komputerowych, ale przede wszystkim z powodu *niskiej jakości* procesów administracyjnych. Nie znajdujemy w dokumentach, udostępnianych przez MSWA informacji o nowych procesach administracyjnych bądź zmianie starych, wypada się więc zadać pytanie czy PESEL2 jest potrzebny, a jeśli tak, to jak powinien być skonstruowany i jakim celom ma służyć.

3. PESEL2 według założeń MSWiA

MSWIA udostępniło do konsultacji społecznych dokument *„Podstawowy Dokument Programu PESEL2. Przebudowa i integracja rejestrów państwowych”*. Według autorów tego dokumentu poniższe stwierdzenia są uzasadnieniem dla budowy PESEL2:

„4.1 Cel operacyjny (bezpośredni).

Umożliwienie przedsiębiorcom oraz obywatelom korzystania z usług administracyjnych on-line oferowanych przez administracje różnych szczebli i rodzajów”

„4.2 Cel strategiczny (długookresowy).

Długookresowy cel strategiczny dla systemu ZSI PESEL2 wynika z faktu, że stanowił on będzie komponent infrastruktury informacyjnej państwa zdefiniowanej w Programie reformy infrastruktury informacyjnej państwa i strategii informatyzacji sektora publicznego.”

Autorzy dokumentu programowego na samym wstępie wskazali szereg teoretycznych korzyści wynikających z wprowadzenia systemu. Przykładowo, po wdrożeniu PESEL2 zmniejszona zostanie bliżej nieokreślona liczba zaświadczeń, poświadczeń i odpisów, które aktualnie są wymagane przez urzędy. Obywatel zostanie też „odmiejscowiony”, co oznacza, że cześć czynności administracyjnych związanych z obsługą np. dowodów osobistych będzie możliwa w dowolnym urzędzie gminnym, a nie tylko we właściwym dla miejsca zamieszkania. Autorzy dokumentu wskazali także, że budowa gigantycznego systemu zbierania i dystrybucji informacji osobowych jest jedynym sposobem uzyskania tych korzyści.

System PESEL2 w planach MSWiA ma być referencyjnym rejestrem ludności całej Polski. Każdemu obywatelowi zostanie przypisany uniwersalny identyfikator (czyli numer PESEL), nadrzędny wobec dotychczas używanych identyfikatorów (NIP, ZUS, KRUS, etc), które formalnie staną się identyfikatorami wewnętrznymi w swoich dziedzinowych rejestrach. Dane w rejestrze referencyjnym PESEL2 będą traktowane jako jedyne autentyczne źródło danych o obywatelach, a ekstrakt danych z PESEL2 pobrany przez urząd będzie miał status dokumentu urzędowego. Numer identyfikacyjny PESEL będzie musiał być stosowany w niezmienionej postaci w rejestrach państwowych urzędów i firm prywatnych (czyli potencjalnie we wszystkich bazach danych zarejestrowanych w GIODO). Potencjalne zagrożenia wynikające z tego ostatniego pomysłu zostaną omówione w rozdziale 7.

Aktualizacja danych o obywatelach w PESEL2 będzie wykonywana tylko poprzez urzędy pierwszego kontaktu na szczeblu gminy (USC, wydziały ewidencji ludności i dowodów osobistych).

Jeśli jednostka organizacyjna sektora państwowego chciałaby stworzyć swój własny rejestr, to będzie on musiał bazować na danych osobowych rejestru referencyjnego PESEL2. Zatem inne rejestry ludności będą pobierały podstawowe dane osobowe nie bezpośrednio od obywateli, ale z rejestru referencyjnego PESEL2 za pomocą sieci komputerowej. Zatem wszystkie bazy danych zawierające informacje o obywatelu, które są także przechowywane w bazie PESEL2 miałyby być bazami pochodnymi i podrzędnymi w stosunku do niej. Urzędy

pracujące na rejestrach pochodnych będą miały zakaz żądania informacji od obywateli, jeśli te informacje już znajdują się w PESEL2.

W dokumencie MSWiA nie znajdujemy informacji, jakie procesy administracyjne zostaną zmienione, wprowadzone bądź zlikwidowane. Nie wyjaśniono, w jaki sposób PESEL2 ułatwi kontakty obywatela z administracją i usprawni działanie tej ostatniej. Autorzy dokumentu też nie wyjaśniają, w jaki sposób PESEL2 umożliwi przedsiębiorcom oraz obywatelom korzystanie z usług on-line (przez Internet) oferowanych przez administracje różnych szczebli i rodzajów.

Dokument programowy MSWiA zawiera też szereg propozycji technicznych, w luźny sposób związanych z planowanymi funkcjami systemu (a więc architektura techniczno-operacyjna wydaje się być niezależna od funkcjonalności planowanej bazy! – w analogii budowlanej odpowiada to sytuacji, gdyby konstrukcja budowli była niezależna od jej funkcji). Większość szczegółów dotyczących architektury i konstrukcji rejestru PESEL2 jest nieznana.

Planowane rozwiązania, na podstawie informacji udostępnionych przez MSWiA, można scharakteryzować w następujący sposób:

- PESEL2 to centralny system identyfikacji obywateli i rejestr meldunków (zakłada się istnienie obowiązku meldunkowego),
- rejestr PESEL2 przechowuje i udostępnia dane o różnych uprawnieniach obywateli (świadczeniach etc.),
- identyfikatory PESEL będą unikalnymi identyfikatorami obywateli we wszystkich bazach dziedzinowych (czyli zapewniają administracyjne powiązanie wszystkich danych osobowych konkretnego obywatela z różnych baz dziedzinowych),
- wiarygodność danych przechowywanych w PESEL2 jest zadekretowana przez prawo a nie wynika z jego konstrukcji i sposobu działania. PESEL2 będzie jedynym legalnym źródłem danych osobowych dla innych rejestrów państwowych.

4. Czy centralne bazy danych osobowych są potrzebne?

Sądzimy, że istnieją dwa istotne powody, dla których państwo powinno utworzyć centralny rejestr z danymi osobowymi o charakterze identyfikacyjnym. Pierwszy dotyczy potrzeby jednoznacznego rozróżniania osób. Drugi wynika z konieczności *udowadniania tożsamości* w różnych okolicznościach.

Są też inne funkcje (np. analizowanie stanu zdrowia społeczeństwa), które państwo chciałoby realizować za pomocą centralnych rejestrów danych osobowych.

Ponieważ samo istnienie centralnej bazy danych osobowych stwarza poważne zagrożenia dla bezpieczeństwa obywateli, to uważamy, że plany realizacji tych innych funkcji za pomocą centralnego rejestru muszą być poprzedzone szczegółową analizą zysków i strat zarówno dla Państwa jak i dla obywateli a jej wyniki upublicznione.

Warto mieć świadomość, że realizacja innych funkcji za pomocą centralnej bazy wiąże się z koniecznością przechowywania w niej danych osobowych nie związanych z potrzebą identyfikacji osób.

Identyfikacja osób i *udowadnianie swojej tożsamości* są niezbędne, aby normalnie funkcjonować w świecie biznesu i w świecie instytucji publicznych. Począwszy od wyegzekwowania prawa do zniżki na bilet, składania wniosku w urzędzie, zakładania konta w banku a skończywszy na zakupie telefonu komórkowego, mamy do czynienia z sytuacjami, gdzie zmuszeni jesteśmy do udowadniania swojej tożsamości. Dlatego *baza danych osobowych*, rozumiana jako mechanizm ułatwiający identyfikację osoby, jest *niezbędna*. Zwróćmy uwagę, że sposób dowodzenia tożsamości zależy od okoliczności: inne informacje są potrzebne do identyfikacji osoby w banku, a inne, gdy student pokazuje kontrolerowi zniżkowy bilet. Mówimy, zatem o *tożsamości kontekstowej*, czyli tożsamości, której tylko część cech ma istotne znaczenie w danym kontekście.

Zatem konieczne jest tworzenie *dziedzinowych* baz danych identyfikacyjnych wspomagających proces dowodzenia tożsamości kontekstowej. Dowiedzenie tożsamości kontekstowej jest warunkiem koniecznym egzekwowania dziedzinowych uprawnień (typu zniżka na bilet, usługa medyczna etc). W przypadku rejestrów dziedzinowych musi być zachowana zasada *proporcjonalności* tj. zakres danych identyfikacyjnych w takim rejestrze nie może być większy niż wynika to z potrzeby identyfikacji konkretnej tożsamości kontekstowej.

Tożsamość udowadniamy okazując określony dokument, bądź używając indywidualnej karty elektronicznej. Ciężar dowodu własnej tożsamości spoczywa na obywatelu. Dokumenty służące do udowadniania swojej tożsamości kontekstowej (czyli np. legitymacja studencka) są wystawiane dopiero po udowodnieniu tożsamości poprzez dowód osobisty lub paszport. Instytucja wydająca dowody osobiste, które są głównymi dokumentami identyfikacyjnymi jest szczególnie odpowiedzialna za właściwą identyfikację obywateli. Aby dobrze wywiązać się ze swojej roli musi posiadać rejestr unikalnych identyfikatorów osób (czyli np. numery PESEL) oraz niezbędne minimum danych

osobowych, które pozwalają rozróżniać obywateli w danej zbiorowości.

Naszym zdaniem w Polsce potrzebny jest zarówno centralny państwowy rejestr danych osobowych do wydawania dowodów jak i niezależne rejestry dziedzinowe do identyfikacji tożsamości kontekstowej. Każdy z tych rejestrów musi spełniać *zasadę proporcjonalności*, według której zakres danych identyfikacyjnych w rejestrze powinien być ściśle dostosowany do jego funkcji identyfikacyjnej i ograniczony tylko do niej.

Aby rejestry dziedzinowe mogły właściwie pełnić swoje funkcje muszą być niezależne. MSWiA ma inne zdanie na ten temat i zamierza wymusić na innych państwowych rejestrach dziedzinowych ograniczenia dotyczące pobierania danych źródłowych od obywateli. Cytat z dokumentu MSWiA:

„Zostanie wprowadzony obowiązek wymiany informacji między jednostkami organizacyjnymi administracji publicznej o osobach fizycznych w celu minimalizacji pierwotnego zbierania informacji od obywateli oraz zakaz żądania informacji od obywateli, jeżeli informacja istnieje w systemie ZSI PESEL2."

Sądzimy, że właściciel (dysponent) danego uprawnienia i towarzyszący mu dziedzinowy rejestr identyfikacyjny, w którym te uprawnienia są zapisane, musi mieć swobodę kształtowania procesu sprawdzania tożsamości osób uprawnionych. Oferowany przez państwo system weryfikacji tożsamości powinien mieć tylko rolę pomocniczą dla właścicieli dziedzinowych rejestrów autoryzacyjnych. Nie można im zabronić pobierania od obywateli danych już istniejących w PESEL2, ponieważ konsekwencje oszukańczych wyłudzeń świadczeń uderzają bezpośrednio w budżety właścicieli dziedzinowych rejestrów autoryzacyjnych i podatników, a nie w MSWiA.

MSWiA chce zmusić obywateli i instytucje do ufania danym z PESEL2 a jednocześnie nie ufania danym z rejestrów już istniejących. Z obecnej praktyki wynika, że instytucje komercyjne mają ograniczone zaufanie do rejestrów państwowych. Nie można kupić telefonu komórkowego w promocji jeśli swoją tożsamość udowadnia się tylko za pomocą dowodu osobistego. Istnieją istotne powody, dla których zaufanie do państwowych rejestrów jest ograniczone i powody te nie znikną z chwilą wprowadzenia systemu PESEL2. Bazując na doświadczeniach innych krajów należy wątpić czy polepszenie jakości pracy i poprawa procesów w instytucji prowadzącej rejestr coś tu istotnie zmieni. Różne firmy będą uznawały wiarygodność różnych baz danych osobowych na podstawie swojego doświadczenia, a nie na podstawie prawnego nakazu.

Postulowana przez nas *niezależność* systemów dziedzinowych od centralnego rejestru nie oznacza, że wykluczamy możliwość przepływu danych pomiędzy rejestrami dziedzinowymi. Stwierdzamy jedynie, że brak precyzyjnie zdefiniowanych celów i procesów nie daje w tej chwili możliwości na wskazanie jak taki przepływ danych pomiędzy systemami dziedzinowymi miałby wyglądać i czemu miałby służyć.

W rozważaniach dotyczących centralnej bazy danych osobowych nie można pominąć kwestii jej struktury i zakresu informacji w niej przechowywanych. Społecznie akceptowalny limit ilości informacji przechowy-

wanych w centralnej bazie zależy od czynników kulturowych: porządku prawnego, wielkości populacji, tradycji panującej w danym kraju, poziomu zagrożenia kradzieżą tożsamości itd. Planowanego przez MSWiA zakresu danych w PESEL2 możemy się jedynie domyślać analizując stwierdzenia typu:

„W systemie ZSI PESEL2 powinny być gromadzone podstawowe cechy klasyfikacyjne i identyfikacyjne o osobie fizycznej występujące w ogólnokrajowych systemach informacyjnych, często wykorzystywane przez jednostki sektora publicznego, np. informacja o tym, czy osoba jest ubezpieczona w systemie ubezpieczenia zdrowotnego lub ubezpieczenia społecznego".

Zatem koncepcja MSWiA zmierza do stworzenia wielkiej bazy danych osobowych, zawierającej *nieproporcjonalny w stosunku do celów* zakres danych osobowych.

Sądzimy, że do skutecznego dowodzenia tożsamości, jak i z powodu zobowiązań międzynarodowych (np. paszport biometryczny), centralny rejestr danych osobowych powinien być zbiorem unikalnych identyfikatorów oraz powinien zawierać tylko taką ilość danych identyfikacyjnych, która jest konieczna do rozróżniania obywateli. Należy zaakceptować fakt, że w różnych instytucjach będą istniały rejestry danych osobowych, zawierające dane już istniejące w rejestrze centralnym, oraz że dla wielu instytucji i obywateli to nie rejestr centralny będzie wiarygodnym źródłem tych danych. Prawidłowo stosowana koncepcja rejestrów bazowych *nie wymaga nadrzędności danych w jednych bazach nad tymi samymi danymi w innych bazach, a identyfikator PESEL nie powinien stać się w żadnym wypadku unikalnym identyfikatorem osoby we wszystkich systemach dziedzinowych.*

5. Odnajdywanie obywateli, a obowiązek meldunkowy

W poprzednim rozdziale wskazaliśmy, że niezbędna jest centralna baza danych osobowych i unikalnych identyfikatorów osób. Wskazaliśmy także, że pożądane i naturalne jest istnienie wielu *niezależnych* dziedzinowych systemów z danymi osobowymi, dzięki którym możemy wybrać optymalny sposób dowodzenia kontekstowej tożsamości.

Poza udowadnianiem tożsamości potrzebny jest także skuteczny sposób *odnajdywania* osoby. Cecha ta wydaje się niezbędna w przypadku niektórych systemów dziedzinowych utrzymywanych przez banki, NFZ, czy operatorów telekomunikacyjnych. Każda z tych instytucji w określonej sytuacji (np. niespłacenie kredytu, informacja o zakażeniu, niepłacenie za usługę telekomunikacyjną) będzie musiała odnaleźć konkretną osobę. Jest oczywiste, że przy podpisywaniu umowy takie instytucje próbują ustalić prawdziwy adres klienta i zapisać go w swojej bazie danych. Banki, firmy telekomunikacyjne i inne instytucje nie zadawalają się oświadczeniem danej osoby o jej adresie, ale starają się podawane informacje zweryfikować zanim dokonają wpisu do bazy danych.

Upowszechnianie się tej praktyki, jak i wydarzenia z 11 września 2001 roku spowodowały, że w wielu krajach zaczęto rozważać pomysł utworzenia centralnej bazy danych z danymi identyfikacyjnymi obywateli, w tym danymi adresowymi. Dodać należy, że istotna część opinii społecznej w krajach anglosaskich kwestionuje ideę takiej bazy widząc w niej poważne zagrożenie dla swobód obywatelskich. W różnym stopniu, w różnych krajach plany te jednak są wprowadzane w życie. Jednak tam, gdzie już istnieją centralne bazy danych kontrolowane przez Państwo, nie stają się one jedynym, wiarygodnym źródłem danych adresowych dla innych instytucji!

Ponadto okazuje się, że zupełnie inne dokumenty identyfikacyjne, związane z innymi rejestrami osobowymi, często komercyjnymi, są traktowane jako bardziej wiarygodne od państwowych!

Potrzeba odnajdywania osób w oparciu o centralną bazę adresów zdaje się być pretekstem do utrzymywania obowiązku meldunkowego i w konsekwencji konieczności przechowywania informacji meldunkowej w bazie PESEL2. Urzędnicy uzasadniają obowiązek meldunkowy potrzebą odnajdywania obywateli. Sto lat temu obowiązek meldunkowy doskonale spełniał swoją rolę. Dzisiaj, kiedy mamy tysiące elektronicznych rejestrów zawierających adresy, nie jest już optymalnym narzędziem.

MSWiA zdaje się dostrzegać potrzebę usunięcia informacji meldunkowej z dowodu osobistego. *„Wprowadzone zostaną zmiany związane z formą dowodu osobistego. Rozważona zostanie możliwość usunięcia z dowodu adresu zameldowania powodująca konieczność jego każdorazowej wymiany przy zmianie danych adresowych."* Wydaje się, że MSWiA nie dostrzega, że prawdziwym problemem jest utrzymywanie zapisu o meldunku w bazie PESEL2. Upierając się przy utrzymaniu informacji meldunkowej w bazie PESEL2, MSWiA rozstrzyga jednym pocią-

gnięciem ciągle dyskutowaną w innych krajach Zachodu kwestię, czy państwo powinno w jednym centralnym miejscu posiadać wiedzę o miejscu zamieszkania jego obywateli. Czy MSWiA rozstrzygnęło słusznie i czy w ogóle ma prawo do takich rozstrzygnięć? Zwłaszcza, że w praktyce okazuje się, że dzisiejszy system oparty na obowiązku meldunkowym nie gwarantuje urzędowi państwowemu (np. sądowi) dotarcia do każdego obywatela. Tymczasem mała firma detektywistyczna, korzystająca w sprytny sposób z różnych komercyjnych rejestrów nie ma z tym problemu. Ponadto poza Polską stale przebywa ponad milion polskich obywateli.

Proponujemy rozważyć rezygnację z utrzymywania informacji adresowej w centralnej bazie danych osobowych, gdyż jest to zbędne we współczesnym zinformatyzowanym świecie, o ile Państwo nie ma ciągot totalitarnych. W związku z tym warto zastanowić się nad rezygnacją z instytucji obowiązkowego meldunku. W wielu państwach Zachodu nie istnieje obowiązek meldunkowy. Co więcej, nie we wszystkich państwach (np. USA, Wielka Brytania) wprowadzono nawet powszechny obowiązek posiadania dokumentu tożsamości ze zdjęciem (paszport takim dokumentem nie jest, ponieważ jest potrzebny wyłącznie osobom wyjeżdżających za granicę).

Warto zdać sobie sprawę z tego, co oznacza brak obowiązku meldunkowego. Jest to prawo obywatela do nieinformowania władz publicznych o każdorazowej zmianie miejsca zamieszkania. Jakie są konsekwencje niewypełnienia obowiązku meldunkowego w takim kraju jak Polska? Obywatel bez stałego zameldowania nie ma praw obywatelskich. Nie może leczyć siebie ani swojego dziecka. Nie może się zatrudnić. Nie może kupić mieszkania, telefonu komórkowego, wyjechać za granicę (ponieważ nie dostanie paszportu !). Nie może się nawet zameldować na pobyt stały, gdyż do tego jest potrzebne… uprzednie wymeldowanie!

Bez informacji adresowych PESEL2 mógłby się stać wiarygodną bazą, pomocną do rozróżniania i udowodnienia tożsamości osób, i jest to jedyna rola, którą, bez zdefiniowanych procesów, system typu PESEL2 mógłby pełnić. Tysiące innych niezależnych rejestrów mogłoby być powiązane z PESEL2 w sposób zapewniający ochronę prywatności obywateli, tworząc jednocześnie warunki dla znacznie skuteczniejszych sposobów udowadniania tożsamości i odszukiwania obywateli.

6. Do czego służy referencyjna baza danych?

W Polsce formalnie zarejestrowano już ponad 50 tysięcy rejestrów z danymi osobowymi. Baza danych klientów operatora sieci telefonicznej, baza danych klientów gazowni, baza danych z aktami urodzenia, baza danych ZUS, to przykłady typowych rejestrów.

Wiarygodność i użyteczność rejestrów można porównywać poprzez kombinację dwóch parametrów: procentu błędnych rekordów i łatwości podrobienia dokumentu reprezentującego rekord w rejestrze (zwykle pojedynczy zapis w rejestrze istnieje na zewnątrz rejestru w postaci dokumentu). Im mniejszy procent nieprawdziwych danych w rejestrze, tym jego wiarygodność jest większa. Im trudniej podrobić dokument odzwierciedlający zapis w rejestrze, tym rejestr jest bardziej użyteczny.

Każde przedsiębiorstwo, które masowo weryfikuje kontekstową tożsamość klientów, stara się wybierać rejestry najbardziej wiarygodne lub korzysta z wielu rejestrów jednocześnie. Operator sieci komórkowej sprzedający telefony po złotówce z roczną umową abonamentową oczekuje, że klient okaże dwa różne dokumenty ze zdjęciem, np. dowód osobisty i paszport oraz inne dokumenty dodatkowo potwierdzające jego tożsamość, np. fakturę z opłatą za elektryczność i zaświadczenie o zatrudnieniu. Innymi słowy operator komórkowy korzysta z danych z czterech rejestrów.

Dodajmy, że różne urzędy państwowe mają swoje rejestry, a za przepływ danych pomiędzy nimi odpowiedzialny jest sam obywatel! Niedopełnienie obowiązku powiadomienia urzędów o zmianie meldunku jest nie tylko potencjalnym utrudnieniem w następnej interakcji z tymi urzędami, ale może wiązać się z odpowiedzialnością karną! W celu likwidacji tej niedogodności MSWiA zaprojektowało nową organizację dla już istniejących rejestrów państwowych z danymi adresowymi, z PESEL2 w roli głównej. Istnienie wielu niezależnych rejestrów dziedzinowych z adresami jest faktem i MSWiA tego nie podważa, tylko dokonuje arbitralnego zróżnicowania rejestrów na wiarygodny PESEL2 i pozostałe „urzędowo" niewiarygodne.

Uzasadnieniem teoretycznym tego pomysłu jest koncepcja tzw. plików referencyjnych w teorii baz danych. Otóż w bazach danych gromadzimy dwa rodzaje danych: *dane same w sobie*, oraz informacje o formacie, czyli sposobie zapisu, w jakim te dane przechowujemy, czyli tzw. *metadane*. Jeśli na przykład mamy bazę danych osobowych w banku to danymi samymi w sobie są m.in. nazwiska klientów, stany ich kont, wykupione produkty, a metadanymi są w tym przypadku informacje, że miejsce w bazie, gdzie przechowujemy nazwisko klienta nie będzie dłuższe niż 100 znaków, a miejsce gdzie przechowujemy informację o stanie konta ma maksymalnie 20 cyfr, itp. W złożonym systemie, składającym się z wielu baz danych, informacja o nazwisku znajdzie się w więcej niż jednej bazie. Naturalnie można sobie wyobrazić sytuację, że każda z baz składowych złożonego systemu ma swoje metadane, czyli własny format zapisu nazwiska. Zwykle dąży się do narzucenia jednego wzorca zapisu danych w systemach złożonych z wielu baz, czyli wydziela się

jedno miejsce gdzie zapisane są *metadane* wspólne dla wszystkich baz. Miejsce to zwykło się nazywać właśnie bazą referencyjną czy też rejestrem referencyjnym.

Projekt MSWiA przewiduje, że PESEL2 stanie się bazą referencyjną, tyle, że w odróżnieniu od typowego zastosowania teorii opisanego wyżej, baza referencyjna będzie zawierała nie tylko metadane, ale przede wszystkim dane same w sobie! W przypadku systemu proponowanego przez MSWiA, traktowanie PESEL2 jako *jedynego wiarygodnego źródła danych nie jest żadną konsekwencją stosowania spójnej teorii informatycznej, a tylko administracyjnie narzuconą, naszym zdaniem niepotrzebnie, regułą!*

Optymalne rozwiązanie to wiele różnych i niezależnych rejestrów, których wiarygodność kształtuje rynek i zbiorowe doświadczenie obywateli. Pojęcie referencyjności dla danych osobowych nie powinno być stosowane.

7. Niepożądana funkcjonalność systemu PESEL2

W oparciu o informacje udostępnione przez MSWiA na temat projektowanego systemu PESEL2 można przypuszczać, że system stworzy wiele zagrożeń, takich jak:

- zapewni dziesiątkom tysięcy urzędników państwowych nieograniczony i niekontrolowany dostęp do informacji o życiu i zdrowiu wszystkich obywateli oraz wielu innych rodzajów danych osobowych zebranych z różnych rejestrów dziedzinowych,
- utrudni proces weryfikacji tożsamości i obniży jego skuteczność,
- ułatwi dokonywanie przestępstw za pomocą fałszywych dokumentów tożsamości i kradzionych danych identyfikacyjnych,
- w bardzo szerokim zakresie umożliwi państwu *profilowanie* zachowań i gustów wszystkich obywateli,
- ułatwi wyłudzanie usług i świadczeń od instytucji państwowych.

Niepożądane skutki uboczne, które powstaną wraz z uruchomieniem PESEL2 są w dużej mierze związane z jego planowaną wielkością. Z każdym dużym centralnym rejestrem występują podobne problemy. Zilustrujmy je na przykładzie hipotetycznego rejestru dowodów osobistych. Rejestr z dowodami osobistymi jest reprezentowany na zewnątrz przez dowód osobisty (a, na przykład, rejestr klientów gazowni jest reprezentowany przez imienną fakturę za dostawę gazu itp). Około 20 milionów obywateli posiada dowód osobisty. Każdy dowód musi być wymieniony raz na dziesięć lat. Musi być wymieniony również z powodu zmiany adresu zameldowania i zmiany nazwiska. Ponadto nowy dowód jest wydawany z powodu zgubienia starego, a taki przypadek obejmuje, co najmniej 5% obywateli rocznie. Zatem co roku wydaje się trzy miliony dowodów osobistych. Główne problemy bezpieczeństwa związane z dowodami osobistymi i rejestrem dowodów to:

- wydanie dowodu na dane osoby fikcyjnej,
- wydanie dowodu na dane innej osoby i bez jej wiedzy,
- wydanie dowodu wielokrotnie tej samej osobie (w celu późniejszego przerobienia tożsamości),
- podrobienie dowodu.

Jeśli przekupimy pracownika w urzędzie lub w innym miejscu skomplikowanego procesu wydawania dowodu, wówczas dokonanie jednego z powyższych oszustw będzie stosunkowo proste. A jeśli umiemy podrobić dokumenty źródłowe, które służą do wydania zagubionego dowodu osobistego, to wówczas też istnieje spora szansa na sukces.

Przy masowym wydawaniu dowodów musimy zachować równowagę między poziomem zabezpieczeń samego *dowodu osobistego*, a poziomem odporności *procesu wydawania dowodu* na oszustwa. Zatem, jeśli podrobienie dowodu będzie bardzo trudne, wtedy przestępcy skoncentrują się na oszustwach w obrębie procesu wydawania dowodów. Jeśli z kolei dowód będzie można łatwo pod-

robić, to nie warto poświęcać zbyt dużo środków na poprawę szczelności samego procesu. Nie ma prostej zależności między stopniem odporności na oszustwa procesu wydawania dowodów a ilością środków zainwestowanych w zabezpieczenie samego procesu. Na dodatek przy pewnym pułapie dalsze inwestycje w zabezpieczenie procesu nie przyniosą zauważalnego rezultatu. Wymóg zachowania równowagi pomiędzy poziomem zabezpieczenia dokumentu a poziomem zabezpieczenia procesu prowadzi do konkluzji, że poziom wiarygodności dowodu osobistego, poza pewną granicą, nie może już znacząco wzrosnąć.

Nielegalny dowód osobisty może być użyty do dokonania przestępstwa określanego terminem *kradzież tożsamości*. Przestępca też dokonuje kradzieży tożsamości jeśli używa tylko danych identyfikacyjnych innej osoby do wyłudzania usług, produktów i pieniędzy.

Kiedy ktoś posługuje się cudzym imieniem, nazwiskiem i numerem karty kredytowej w sklepie internetowym lub otwiera konto w banku internetowym na dane innej osoby – wtedy mamy do czynienia z kradzieżą tożsamości. W USA jest to ogromna plaga - tylko w roku 2005 zgłoszono 685 tysięcy przypadków,

Powyższa dyskusja wykazuje jak bardzo trudne i kosztowne jest zbudowanie centralnego rejestru danych osobowych, którego jakość i bezpieczeństwo będzie znacząco większa od innych profesjonalnie prowadzonych rejestrów. Zaprezentowany przez MSWiA projekt systemu PESEL2 jest bardzo dużą bazą danych osobowych, której decyzją administracyjną zostaną przypisane pewne funkcje i cechy, nie wynikające z jej konstrukcji. Wydaje się też, że nie ma planów zmiany procesów administracyjnych związanych z obsługą tej bazy, a bez tego poprawa jakości nie jest możliwa. Problemy związane z kradzieżą tożsamości nie są konsekwencją wyboru tej czy innej technologii użytej do budowy PESEL2, ale wynikają z samego faktu gromadzenia w jednym miejscu olbrzymiej ilości danych osobowych. Należy to uwzględnić i różnymi sposobami ograniczyć ryzyko kradzieży tożsamości na masową skalę, czego niestety koncepcja MSWiA nie przewiduje. W rozdziale 8 pokażemy konstrukcję systemu, który skutecznie ogranicza takie ryzyko.

Jeśli urząd państwowy pod jakimś pretekstem wymusi na właścicielach rejestrów dziedzinowych wyszukanie i dostarczenie wszystkich rekordów związanych z konkretnym numerem PESEL, to uzyska niewyobrażalną ilość danych o tej osobie. Ten administracyjny sposób zbierania informacji o obywatelu jest możliwy z powodu powszechnego, a w koncepcji MSWiA przymusowego, używania numeru PESEL jako identyfikatora osoby w publicznych i komercyjnych bazach danych. Dodać należy, że MSWiA planuje połączyć poprzez sieć system PESEL2 z innym do tej pory niezależnymi rejestrami publicznymi. Umożliwi to regularne przeszukiwanie baz danych pod kątem konkretnych cech lub zdarzeń, wyłonienie grup o specyficznych upodobaniach, czy o specyficznych zachowaniach, które będą interesowały urzędników. W wyniku takiego przeszukiwania otrzymamy populację podzieloną na łatwo rozróżnialne segmenty. Jest to tzw. *profilowanie*. Tego typu

analizy często wykonują firmy komercyjne w oparciu o własne bazy danych. Firma może podzielić całą *populację swoich klientów* na grupy o różnych preferencjach. Coraz częściej się zdarza, że firmy dzielą się danymi o klientach między sobą, co pozwala na jeszcze efektywniejsze profilowanie. Profilowanie daje ogromną przewagę jednej stronie. Jedna strona wie o drugiej znacznie więcej, co powoduje, że we wzajemnych relacjach jedna strona jest bardziej podmiotem, a druga przedmiotem.

W przypadku wprowadzenia PESEL2 stworzymy techniczną możliwość pełnego *profilowania całej populacji!* Pamiętajmy, że w bazie PESEL2 mają być również zapisane adresy. Oznacza to, że będzie możliwe spełnienie marzenia każdej totalitarnej władzy o technicznej możliwości regularnej identyfikacji grup *podejrzanych ze względu na jakieś kryterium* i wskazaniu gdzie podejrzani mieszkają!

Czy w imię oficjalnie deklarowanego, a nie wynikającego z logiki konstrukcji PESEL2, hipotetycznego polepszenia komunikacji obywatela z urzędem społeczeństwo ma zaakceptować stworzenie systemów, które umożliwią taką kontrolę nad sobą samym?

Jeśli we wszystkich rejestrach dziedzinowych stosowanoby *różne i nie powiązane ze sobą identyfikatory tego samego obywatela*, to wykonanie segmentacji na tych wszystkich bazach danych byłoby bardzo utrudnione i w konsekwencji uniemożliwiałoby profilowanie (właśnie taką koncepcję pokażemy w rozdziale 8). Niestety koncepcja MSWiA nie tylko nie chroni nas przed profilowaniem, ale stwarza dodatkowe ułatwienia dla tego procederu!

8. Bezpieczny rejestr danych osobowych

W tym rozdziale przedstawiamy rozwiązanie systemowe dla rejestrów państwowych i komercyjnych, które stworzy warunki dla prostej i skutecznej identyfikacji osób oraz zapewni właściwą równowagę między interesami państwa i interesami obywateli. Prezentowana koncepcja zawiera bardzo szczegółowy opis rozwiązań technicznych, choć zdajemy sobie sprawę, że niektóre elementy mogą nie być w pełni zrozumiałe dla wszystkich Czytelników. Jednak chcemy przedstawić opis szczegółów technicznych, gdyż zależy nam na przekonaniu wszystkich zainteresowanych tematem PESEL2, że można zbudować prosty system, który będzie skutecznie realizował tradycyjne cele centralnego rejestru identyfikacyjnego ludności i jednocześnie będzie wolny od wad koncepcji MSWiA.

Systemowe rozwiązanie dla elektronicznych rejestrów jest zbudowane na następujących założeniach:

- każdemu obywatelowi zostanie przypisany na całe życie unikalny identyfikator pierwotny (tak jak w PESEL),
- rola centralnego rejestru ludności jest ograniczona tylko i wyłącznie do funkcji identyfikacji tożsamości,
- centralny rejestr zawiera tylko te dane osobowe, które w ciągu życia są stałe lub zmieniają się bardzo rzadko. Centralny rejestr nie zawiera danych adresowych,
- każdy obywatel ma zapewnioną możliwość prostego i skutecznego sprawdzania tożsamości innych osób w oparciu o dowód osobisty,
- w każdym rejestrze autoryzacyjnym (czyli rejestrze dziedzinowym, który poza danymi identyfikacyjnymi zawiera również informacje o uprawnieniach do świadczeń lub usług) obywatel, jest reprezentowany przez identyfikator wtórny powiązany w sposób niejawny z identyfikatorem pierwotnym. Sposób powiązania identyfikatorów jest znany tylko osobie, do której te identyfikatory zostały przypisane,
- w rejestrach zawierających dużo informacji prywatnych i osobistych (np. NFZ) tożsamość obywatela jest reprezentowana tylko przez identyfikator wtórny i niezbędne minimum innych danych identyfikacyjnych. Główny Inspektor Ochrony Danych Osobowych (GIODO) miałby uprawnienia do decydowania czy konkretny rejestr państwowy lub prywatny musiałby spełniać ten wymóg. GIODO określałby również maksymalny zakres danych osobowych służących do identyfikacji osoby,
- właściciele państwowych rejestrów autoryzacyjnych mieliby pełną niezależność w kształtowaniu procesu sprawdzania tożsamości uprawnionych obywateli. Innymi słowy sami ustalaliby źródło i zakres informacji identyfikacyjnych potrzebnych do sprawdzenia tożsamości osób uprawnionych,
- obowiązywałby zakaz wymiany danych pomiędzy systemami dziedzinowymi je-

śli nie zdefiniowano precyzyjnie celów wymiany, procesów administracyjnych z tym związanych i nie przeprowadzono analizy ryzyka.

Rozwiązanie musi również zapewnić mechanizmy bezpieczeństwa, które wyeliminują lub ograniczą typowe zagrożenia występujące w centralnych rejestrach ludności. W szczególności, systemowe rozwiązanie dla rejestrów powinno:

- uniemożliwić urzędnikom państwowym nieograniczony i niekontrolowany dostęp do informacji zgromadzonych w rejestrach o życiu i zdrowiu obywateli,
- utrudnić dokonywanie przestępstw za pomocą fałszywych dokumentów tożsamości i kradzionych danych identyfikacyjnych,
- stworzyć techniczne bariery dla profilowania zachowań i gustów obywateli.

Rozwiązanie systemowe dla rejestrów, które spełni powyższe założenia, można zbudować za pomocą odpowiednio skonstruowanych elementów składowych:

- systemu identyfikatorów,
- bezadresowego Rejestru Identyfikacyjnego Obywateli (RIO),
- Elektronicznego dowodu osobistego,
- nowych regulacji prawnych dla rejestrów.

Zanim przedstawimy szczegóły koncepcji oraz sposobu weryfikacji tożsamości w oparciu o dowód osobisty i rejestr RIO, omówimy kluczowe pojęcie techniczne, niezbędne do zrozumienia sposobu weryfikacji.

W kryptografii powszechnie korzysta się z jednokierunkowej funkcji skrótu (ang. hash), która przekształca dowolny ciąg bitów (w świecie cyfrowym każda informacja to ciąg bitów) na inny ciąg bitów o stałej długości, nazywany w skrócie „hasz". Możemy przekształcać różne obiekty cyfrowe na ich *hasze*: zdjęcia, dokumenty, filmy DVD, etc. W systemach bezpieczeństwa powiązanie między haszem i obiektem cyfrowym jest używane do podobnych celów co powiązanie między osobą a jej odciskami palców. Jednokierunkowa funkcja skrótu ma następujące własności:

Działa tylko w jedną stronę tj. nie umiemy z hasza odtworzyć pierwotnego obiektu

Dla hasza otrzymanego z danego ciągu bitów jest praktycznie niemożliwe znalezienie innego ciągu bitów, który dawałby ten sam hasz

Te własności hasza będą wykorzystane do sprawdzania dokumentów tożsamości bez naruszania prywatności ich właścicieli.

Teraz przedstawimy *koncepcję proponowanego przez nas systemu identyfikatorów* i zasady ich stosowania, które byłyby obowiązujące dla wszystkich rejestrów z danymi osobowymi. Następnie, na przykładzie rejestru NFZ, przedstawimy szczegółowy przykład zastosowania naszej koncepcji.

System identyfikatorów.

W rejestrach wolno byłoby stosować tylko trzy typy identyfikatorów: pierwotny, wtórny i lokalny. Każdy obywatel miałby formalnie przypisany unikalny identyfikator pierwotny. Identyfikatory pierwotne występowałyby tylko w jednym rejestrze (patrz

dalej rejestr RIO). Wszystkie inne identyfikatory dotyczące tego samego obywatela byłyby wtórne lub lokalne. Identyfikator pierwotny byłby przypisywany osobie w trakcie procedury przygotowywania aktu urodzenia i unieważniany w trakcie procedury przygotowywania aktu zgonu. W proponowanej koncepcji identyfikatorem pierwotnym mógłby być dotychczasowy numer PESEL.

Identyfikatory wtórne byłyby pochodnymi identyfikatora pierwotnego, a więc nie byłyby z nim tożsame. Jeden identyfikator wtórny mógłby być użyty tylko w jednym rejestrze. Powiązanie identyfikatorów polegałoby na jednokierunkowym przekształceniu identyfikatora pierwotnego w główną część identyfikatora wtórnego. Przekształcenie byłoby wykonywane poprzez policzenie hasza dla identyfikatora pierwotnego i jednej liczby wybranej z 50 losowych liczb przechowywanych w Elektronicznym dowodzie osobistym. Niejawność powiązania wynikałaby z faktu, że wartości liczb losowych z dowodu osobistego byłyby znane tylko właścicielowi dowodu.

Identyfikator wtórny składałby się z *hasza* i dołączonego do niego numeru wykorzystanej liczby losowej z dowodu osobistego. Numer liczby wybranej do policzenia *hasz*a byłby jawny, aby zwolnić obywatela z obowiązku pamiętania, która liczba z dowodu została użyta do policzenia identyfikatora wtórnego. Zwróćmy uwagę, że w różnych dziedzinowych bazach danych identyfikatory wtórne byłyby różne a wiedza o sposobie ich powiązania nie byłaby dostępna urzędnikom. Brak wiedzy o sposobie powiązania różnych identyfikatorów tej samej osoby uniemożliwiałby (a w każdym razie bardzo utrudniałby) *profilowanie* obejmujące wiele baz, o którym mówiliśmy w rozdziale 7.

Używanie liczb losowych z dowodu osobistego do celów innych, niż generowanie identyfikatorów wtórnych powinno być prawnie zabronione. Można sobie wyobrazić, że niektóre rejestry komercyjne projektowałyby systemy autoryzacji z użyciem tych liczb jako haseł. Groziłoby to wzrostem ryzyka kradzieży dowodu osobistego.

Identyfikator lokalny byłby stosowany według tych samych zasad co identyfikator wtórny. Jedną różnicą między identyfikatorem wtórnym i lokalnym byłby brak powiązania tego drugiego z identyfikatorem pierwotnym.

Rejestr Identyfikacyjny Obywateli (RIO).

Kluczowym składnikiem systemu byłby Rejestr Identyfikacyjny Obywateli będący centralną bazą z danymi do wydawania dowodów osobistych i sprawdzania tożsamości obywateli Polski. W rejestrze byłyby przechowywane rekordy z danymi osobowymi i identyfikacyjnymi, które w ciągu życia są stałe lub zmieniają się bardzo rzadko. Uważamy, że w tak ważnej kwestii jak kontrolowany przez Państwo centralny rejestr danych identyfikacyjnych należy precyzyjnie wskazać zakres gromadzonych danych, czego niestety zabrakło w materiałach udostępnionych przez MSWiA.

Pojedynczy rekord w rejestrze RIO zawierałby 12 pól:

1. Identyfikator pierwotny (D).
2. Imię i nazwisko.

3. Data i miejsce urodzenia.
4. Płeć.
5. Imię i nazwisko panieńskie matki.
6. Data urodzenia matki.
7. Dwie cyfry oznaczające numer aktualnego dowodu osobistego. Pełen numer dowodu osobistego składałby się z części niezmiennej: identyfikatora pierwotnego i części zmiennej: dwóch cyfr reprezentujących aktualny dowód. Dowód osobisty mógłby być zmieniany 99 razy w ciągu życia (D).
8. Hasz cyfrowego zdjęcia twarzy (D).
9. Hasz ciągu alfanumerycznych danych osobowych tj. danych z pól 1,2,3,4,5,6,7 (D).
10. Zdjęcie cyfrowe twarzy wykonane w roku wydania dowodu.
11. W zaszyfrowanej postaci 50 ponumerowanych liczb sześciocyfrowych wygenerowanych losowo. Każda osoba miałaby przydzielane te liczby tylko raz w życiu.
12. Hasz wszystkich liczb z pola 11 (D).

Rejestr RIO zawierałby też listę numerów dowodów osobistych unieważnionych, sfałszowanych i zagubionych. Rejestr nie zawierałby żadnych danych autoryzacyjnych, czyli danych umożliwiających egzekucję uprawnień przez obywatela.

Ponieważ większość państw przechodzi na paszport biometryczny, którego część biometryczna musi zwierać, co najmniej zdjęcie twarzy, dlatego warto w rejestrze danych identyfikacyjnych przechowywać cyfrowe zdjęcie twarzy i jego hasz. Ułatwi to eliminowanie niektórych oszustw dotyczących tożsamości bez naruszenia prywatności.

Elektroniczny dowód osobisty.

Integralną częścią systemu identyfikacyjnego byłby Elektroniczny dowód osobisty. Elektroniczny dowód wizualnie byłby podobny do aktualnie używanych dowodów. Dodatkowo miałby wmontowany komponent elektroniczny, w którym byłyby zapisane wszystkie dane właściciela z rekordu z RIO. Na komponencie elektronicznym dane byłyby zapisywane tylko raz w trakcie jego personalizacji, a zmiana zapisu wymagałaby użycia nowego blankietu dowodu. Na dowodzie byłyby wydrukowane dane z rekordu w RIO: pola od 1 do 7 oraz zdjęcie cyfrowe z pola 10.

W komponencie elektronicznym byłyby zapisane wszystkie dane z rekordu w RIO z jednym wyjątkiem: liczby losowe z pola 11 byłyby jawne. Dodatkowo w komponencie elektronicznym mógłby być umieszczany podpis elektroniczny (wykonany kluczem prywatnym MSWiA) danych z pól od 1 do 8 i 12 rekordu RIO. Weryfikacja dowodu z pomocą podpisu elektronicznego byłaby stosowana głównie w momentach przeładowania sieci lub niedostępności rejestru RIO. Podpis elektroniczny byłby także dodatkowym zabezpieczeniem przed podrobieniem dowodu.

Pełen numer dowodu osobistego składałby się z części niezmiennej: identyfikatora pierwotnego i części zmiennej: dwóch cyfr reprezentujących aktualny dowód. Dowód byłby zmieniany raz na 10 lat. W przypadku utraty dowodu wszystkie dane identyfika-

cyjne zostałyby otworzone z rejestru RIO. A po odszyfrowaniu pola 11, także 50 liczb losowych.

Weryfikacja tożsamości w oparciu o RIO.

W oparciu o tak skonstruowany system możemy przedstawić skuteczny sposób weryfikacji tożsamości. Część danych z rejestru RIO byłaby powszechnie dostępna dla wszystkich obywateli poprzez różne kanały komunikacyjne (np. przez Internet, SMS-y). Każdy obywatel miałby dostęp do pól rekordów RIO zaznaczonych przez literę D. Mimo tego ograniczenia jest to wystarczająca ilość informacji do sprawdzenia wszystkich danych z dowodu osobistego.

Zdalny dostęp do RIO umożliwiałby *weryfikację dowodów osobistych i danych na nich zawartych* przy zachowaniu poufności danych osobowych.

Weryfikacja dowodu byłaby możliwa przez Internet. Jeśli na stronie WWW udostępnionej w Internecie przez MSWiA wprowadzi się dane z pól od 1 do 7 i po chwili dostanie odpowiedź, że hasz policzony z danych wprowadzonych z dowodu ma tę samą wartość, co w polu 9 rekordu w RIO, to oznacza, że dowód jest ważny, dane na nim są prawdziwe oraz nikt do tej pory nie zgłosił żadnego oszustwa dokonanego za jego pomocą. Pewność sposobu sprawdzania wynika z tego, że jest bardzo trudno znaleźć drugi zestaw wartości pól od 1 do 7, który dawałby ten sam hasz.

Dostępność rejestru RIO przez Internet w wersji angielskojęzycznej byłaby pomocna w likwidacji coraz bardziej masowego procederu używania polskich dowodów osobistych przez cudzoziemców poza Polską. Nielegalni emigranci w UE są w stanie sporo zapłacić za polskie dokumenty tożsamości, które umożliwiają im legalną pracę. Duża skala tego procederu pozwala przestępcom zainwestować dużo środków w produkcję wysokiej jakości podróbek (patrz pozycja 6. w załączonej bibliografii). Jeśli urzędnicy z innych krajów mieliby możliwość prostego i szybkiego sprawdzenia polskiego dowodu, to na pewno by to robili i tym samym obniżyli „atrakcyjność" polskich dowodów dla przestępców krajowych i zagranicznych

Do sprawdzenia dowodu mógłby być użyty również telefon komórkowy. Wtedy do rejestru RIO trzeba wysłać SMS-a z pełnym numerem dowodu osobistego a w odpowiedzi otrzymalibyśmy wartość hasza z pola 9. Jeśli hasz dla danych wziętych z dowodu tj. z pola od 1 do 7 i policzony lokalnie na PC lub innym urządzeniu będzie taki sam jak hasz otrzymany SMS-em z RIO, to takie sprawdzenie byłoby tak samo dobre jak sprawdzenie przez stronę WWW. Możemy w podobny sposób sprawdzić autentyczność zdjęcia cyfrowego na dowodzie osobistym poprzez wysłanie numeru dowodu osobistego z prośbą o odesłania hasza tego zdjęcia.

Wdrożeniu rejestru RIO powinno towarzyszyć szereg zmian prawnych. Najważniejsze z nich to:

- regulacje gwarantujące właścicielom rejestrów autoryzacyjnych niezależność w kształtowaniu procesu weryfikacji tożsamości (patrz dyskusja w rozdziale 4); przypomnijmy, że w tym względzie propozycje MSWiA są zupełnie inne,

- regulacje chroniące obywatela przez przed profilowaniem (patrz dyskusja w rozdziale 7),
- zakaz przechowywania identyfikatorów pierwotnych w rejestrach i bazach danych, z wyjątkiem rejestru RIO. W rejestrach sektora publicznego byłyby stosowane identyfikatory wtórne a w rejestrach sektora prywatnego identyfikatory lokalne lub wtórne. Ponadto identyfikator wtórny lub lokalny wykorzystywany w jednym rejestrze nie mógłby być przechowywany jako informacja identyfikacyjna w innym rejestrze,
- regulacje dotyczące maksymalnego zakresu danych identyfikacyjnych w rejestrach ze szczególną potrzebą ochrony prywatności.

Postulujemy także, by wyposażyć GIODO w mechanizmy prawne eliminujące stosowanie nadmiernego zakresu danych identyfikacyjnych we rejestrach z wrażliwymi danymi osobowymi. W trakcie projektowania rejestru autoryzacyjnego lub w trakcie rejestracji bazy z danymi osobowymi, GIODO miałby prawo do klasyfikowania rejestrów pod względem wrażliwości danych osobowych i prawo do określania maksymalnego zakresu danych identyfikacyjnych.

Na przykład operator telefonii komórkowej mógłby używać tylko czterech parametrów identyfikujących swoich klientów: identyfikator wtórny, imię, nazwisko i adres.

9. Przykład zastosowania koncepcji: Rejestr NFZ

W rozdziale 4 pokazaliśmy, że potrzebne są centralne bazy danych, z których jedna byłaby centralnym rejestrem identyfikacyjnym obywateli. Wskazaliśmy, że naturalnym uzupełnieniem centralnej baz danych identyfikacyjnych są rejestry dziedzinowe. Aby lepiej zrozumieć naszą koncepcję w tym rozdziale przedstawimy konkretny rejestr dziedzinowy, wskażemy jego funkcje i określimy maksymalny zakres danych osobowych, które są konieczne do realizacji tych funkcji. Jako przykład wybraliśmy rejestr usług medycznych, gdyż jest to najbardziej wrażliwy rejestr dziedzinowy z punktu widzenia danych osobowych.

Na początku obywatel uprawniony do korzystania z usług medycznych NFZ zgłasza się do punktu rejestracji w celu wyrobienia karty pacjenta. Pracownik punktu rejestrującego sprawdza Elektroniczny dowód osobisty. Jeśli ma wątpliwości to wchodzi na stronę serwera MSWiA i dokonuje sprawdzenia dowodu w oparciu o dane w rejestrze RIO według wcześniej opisanego sposobu. Następnie weryfikuje dokumenty, które uprawniają do usług medycznych NFZ. Jeśli wszystko się zgadza, to wykonuje następne kroki:

- generuje identyfikator wtórny na podstawie identyfikatora pierwotnego (który jest wydrukowany na dowodzie i przechowywany w RIO), wartości wybranej liczby z dowodu (z pięćdziesięciu liczb losowych) i numeru liczby losowej,
- zapisuje identyfikator wtórny do rejestru NFZ i zakłada rekord pacjenta,
- przygotowuje wniosek o wydanie karty pacjenta i przesyła go do centrum personalizacji kart w NFZ. Wniosek zawiera imię i nazwisko, identyfikator wtórny w rejestrze NFZ, wiek, adres oraz zdjęcie,
- wyznacza termin odbioru karty pacjenta.

Po wyprodukowaniu karty, centrum personalizacji kart NFZ niszczy dane pacjenta i odsyła kartę do punkty rejestracji.

Na karcie pacjenta jest wydrukowane jego imię i nazwisko. Osoba uprawniona do usług medycznych we wszystkich kontaktach ze służbą zdrowia posługuje się kartą pacjenta i dodatkowo dowodem osobistym jeśli zajdzie taka potrzeba. Zatem w każdej bezpośredniej interakcji personel medyczny zna imię i nazwisko pacjenta. Lekarz może też wprowadzić te dane do komputera w celu wypisania skierowania lub innego dokumentu. Ale z mocy prawa systemy komputerowe w służbie zdrowia nie mogą zapisywać tych danych do swoich baz. Czyli po sporządzeniu i wydrukowaniu skierowania dane identyfikacyjne pacjenta, których przechowywanie jest zabronione są automatycznie usuwane z pamięci komputera.

Tak jak każdy inny rejestr, rejestr NFZ musi spełniać zasadę *proporcjonalności*, czyli funkcje realizowane poprzez ten rejestr muszą być proporcjonalne do jego przeznaczenia.

Rejestr NFZ powinien:

- umożliwić jednoznaczną identyfikację osób uprawnionych,
- umożliwić prowadzenie badań i analiz statystycznych,
- zapewnić możliwość kontaktowania się z pacjentami poprzez pocztę,
- zapewnić skuteczną ochronę danych osobowych.

Do jednoznacznej identyfikacji danej osoby wśród całej grupy osób uprawnionych wystarczy jego *identyfikator wtórny*.

Aby różnicować populację dla celów analiz i statystyk medycznych, które są potrzebne do planowania rozwoju usług i profilaktyki, wystarczą dane osobowe obejmujące *wiek* pacjenta, *płeć* i kod (z *adresu zamieszkania)*

NFZ powinien też mieć możliwość wysyłania listów do poszczególnych osób np. w przypadku epidemii. Do tego celu wystarczy *adres* i *identyfikator wtórny*.

Największym problemem jest zapewnienie skutecznej ochrony danych osobowych pacjentów. W przyszłości w rejestrze NFZ będą umieszczone szczegółowe dane o naszym zdrowiu, chorobach psychicznych, alergiach i wielu innych sprawach. Zatem rejestr NFZ musi mieć niezawodne mechanizmy ochrony danych o chorobach pacjentów. W szczególności system ochrony prywatności musi uwzględniać brak dobrej woli i należytej staranności personelu służby zdrowia.

Najskuteczniejszym mechanizmem bezpieczeństwa w systemie ochrony danych osobowych jest duży poziom anonimowości danych o pacjentach. Pożądaną anonimizację danych o pacjentach uzyska się poprzez zakaz używania w bazach medycznych i rejestrze NFZ innych danych identyfikacyjnych pacjentów niż: identyfikator wtórny, płeć, wiek (wiek jako ilość lat a nie data urodzenia) i adres.

Zaproponowany dla rejestru NFZ zakres danych identyfikacyjnych osób uprawnionych do usług medycznych jest proporcjonalny w stosunku do funkcji tego rejestru i jednocześnie zapewnia skuteczną ochronę danych osobowych pacjentów.

10. Podsumowanie

W niniejszym raporcie staraliśmy się wykazać, że różne typy rejestrów danych osobowych są niezbędne dla sprawnego funkcjonowania gospodarki i urzędów państwowych. Pokazaliśmy również do jak groźnych celów mogą być wykorzystywane centralne bazy danych osobowych oraz jakie zagrożenia stwarza sam fakt istnienia takich baz.

MSWiA tworząc koncepcję systemu PESEL2 nie określiło precyzyjnie jego funkcji, nie zdefiniowało procesów administracyjnych, które system miałby wspomagać i nie odniosło się do problemu zagrożeń. Uważamy, że sama konstrukcja PESEL2 jest wadliwa, planowany zakres danych osobowych jest nadmiarowy, oraz, że nie da się przeciwdziałać zagrożeniom związanym z PESEL2 przez dodanie nawet najbardziej wyszukanych mechanizmów bezpieczeństwa. Konieczna jest zmiana samej koncepcji. Stąd też zaproponowaliśmy rozwiązanie alternatywne.

Przedstawiliśmy jak powinien wyglądać kontrolowany przez państwo centralny rejestr danych identyfikacyjnych, jak powinny wyglądać rejestry dziedzinowe oraz pokazaliśmy jakie funkcje powinny być realizowane przez te rejestry. Pokazaliśmy również jak proponowany przez nas system identyfikatorów przeciwdziała realnym zagrożeniom związanym z masowym gromadzeniem danych osobowych w wielu różnych bazach.

Ze względu na brak zdefiniowanych celów i procesów administracyjnych wokół PESEL2 nie jest możliwa ani analiza samej potrzeby przepływów danych pomiędzy systemami dziedzinowymi ani zagrożeń z tym związanych.

Mamy nadzieję, że ten raport przyczyni się do ożywienia dyskusji o PESEL2.

Wybrana bibliografia

1. „Podstawowy Dokument Programu PESEL2. Przebudowa i integracja rejestrów państwowych", MSWiA, sierpień, 2006.
2. Ewidencje i Rejestry w Administracji Publicznej". Marzec 2005. http://www.e-administracja.org.pl/baza_wiedzy/pliki/Pietrzyk_Gustaw_Seminarium_integracji_rejestrow.pdf
3. Identity Theft Statistics - http://idtheft.about.com/od/dataandstat1/a/ID_Theft_Stats.htm
4. The identity project, Report, Version 1.09 June 27, 2005, London School of Economics and Political Sciences.
5. The demeaning of identity and personhood in national identification systems, Richard Sobel , Harvard Journal of Law & Technology, Volume 15, Number 2 Spring 2002.
6. Relacja z programu „Panorama" nadanego w telewizji BBC o fałszowaniu paszportów: http://news.bbc.co.uk/2/hi/uk_news/6169678.stm