



LIPIEC — WRZESIEŃ

2016 nr 42



REDAKTOR NACZELNY (EDITOR IN CHIEF)

Jerzy Banaś

SEKRETARZ REDAKCJI (EDITORIAL OFFICE SECRETARY)

Danuta Juwko

OPRACOWANIE GRAFICZNE I TECHNICZNE (GRAPHIC & TECHNICAL DESIGN)

Anna Luścińska-Jagiello

PROJEKT GRAFICZNY (GRAPHIC DESIGN)

Justyna Kopecka

ZESPÓŁ REDAKCYJNY (EDITORIAL STAFF)

Joanna Gurtowska

Ewelina Jakielaszek

WSPÓŁPRACOWNICY (CONTRIBUTING EDITORS)

Agnieszka Dziewulska, Tomasz Goliński, Hubert Kwinta

RADA REDAKCJI (EDITORIAL COUNCIL)

Piotr Woyciechowski (przewodniczący) (chief)

prof. dr hab. Hubert Kolečki (UAM)

prof. dr hab. Tadeusz Tomaszewski (UW)

prof. dr hab. Tadeusz Widła (UŚ)

dr Rafał Cieśla (UWr)

dr Mieczysław Goc (PTK)

Aleksandra Gryniewicz

Ewa Leszczyńska-Ambroziewicz

Grażyna Rafalska

Szymon Ruman

Piotr Wojcieszek

FOTOGRAFIE (PHOTOGRAPHS)

Artur Tkaczyk, Dorota Zielińska

archiwa autorów publikacji

OKŁADKA (COVER)

Projekt okładki – Dorota Zielińska (str. 1)

GALERIA CiD

Znaczki pocztowe nagrodzone na Konferencji GPSPA 2016 w Berlinie: polski znaczek ZABYTKOWE ORGANY w POISCE (str. 2), francuskie znaczki z serii Le salon du Timbre (str. 3)

Redakcja (Editorial Office)

ul. Rybaki 35 p. 5, 00-221 Warszawa, Poland

tel. +48 22 235-23-43

fax +48 22 235-42-98

Sekretarz Redakcji (Editorial Office Secretary)

tel. +48 22 235-21-66

e-mail: redakcjacid@pwpw.pl

www.czlowiekidokumenty.pl

Druk i oprawa (Printing House)

Polska Wytwórnia Papierów Wartościowych S.A.

Nakład 2500 egz.

ISSN 1895-7552

Egzemplarz bezpłatny (free copy)

Od Redakcji str. 5

Nowości i wydarzenia str. 6

Szymon Ruman

e-Dowód, państwo usługowe i cyfrowa suwerenność str. 9

Remigiusz Lewandowski

Dokument w smartfonie – nowoczesność czy niebezpieczna ekstrawagancja? str. 15

Krzysztof Izak

Czy smartfon może zastąpić dowód osobisty? str. 21

Michał Kraszewski-Cąkała, Tomasz Goliński, Piotr Życki, Mieczysław Szustakowski

Biometria mobilna – nowoczesna kontrola graniczna str. 31

Daniel Mierzejewski, Monika Rogalska, Marek Rosiak

Papiery zabezpieczone i specjalne produkowane w PWPW str. 39

Wspólny sukces Poczty Polskiej i Polskiej Wytwórni Papierów Wartościowych str. 46

Anna Zalesińska

e-Rewolucja w dokumentach sądowych str. 47

Remigiusz Lewandowski

O potrzebie regulacji sfery dokumentów publicznych str. 53

Krzysztof Izak

Dokument i tożsamość jako element dżihadu str. 59

Tadeusz Tomaszewski

Jeszcze o tym, czy warto badać kopie i inne wtórne odwzorowania pisma ręcznego str. 75

Monika Krucińska

Iran – z Lechistanu do Persji str. 85

Monika Olbryś-Zegarowska, Tomasz Turek

Walka o wolność i honor... Walka o ojczyznę str. 95

Joanna Gurtowska

Przegląd prasy zagranicznej str. 99

Jerzy Banaś

Światowe życie ekspertów str. 100

Editorial p. 5

News and events p. 6

Szymon Ruman

e-ID, service state and digital sovereignty p. 9

Leaving the management of building an e-country to corporations may not properly secure the interests of the Republic of Poland or its citizens.

Remigiusz Lewandowski

Documents in smartphones – modernity or dangerous extravagance? p. 15

The diligence, dynamics, and determination of the Ministry of Digitisation to improve the low computerisation of Poland are really welcome. However, the enthusiasm accompanying these activities should not make us blind to the flaws in some of the solutions proposed.

Krzysztof Izak

Can smartphones replace personal IDs? p. 21

It is possible that our documents, including but not limited to personal IDs, driving licences, or payment cards may soon be available on the screens of our mobile phones.

Michał Kraszewski-Cąkała, Tomasz Goliński, Piotr Życki, Mieczysław Szustakowski

Mobile biometry – modern border control p. 31

Daniel Mierzejewski, Monika Rogalska, Marek Rosiak

Security and special papers manufactured at the Polish Security Printing Works (PWPW) p. 39

Polish postage stamp received an award in Berlin p. 46

Anna Zalesińska

e-Revolution in court documents p. 47

Remigiusz Lewandowski

On the need to regulate the domain of public documents p. 53

There can be no doubt that public documents and currency play an important role in socio-economic relations of all countries, and in particular in the field of state security, especially economic and public.

Krzysztof Izak

Document and identity as elements of jihad p. 59

In the months that followed the terrorist attacks in Paris (13 November 2015 and 14 July 2016), Brussels (22 March 2016), and the series of July attacks in Germany no significant changes were observed in the way that the EU authorities view the threat of Muslim immigrants arriving in Europe.

Tadeusz Tomaszewski

Is it worth analysing copies and other secondary tracing of handwriting p. 75

Another article in the “Experiences of document experts” series.

Monika Krucińska

Iran – from Lechia to Persia p. 85

Another article in the “Passports of the world” series.

Monika Olbryś-Zegarowska, Tomasz Turek

From PWPW history – Fighting for freedom and honour... fighting for the motherland p. 95

The dramatic fights for the PWPW redoubt during the Warsaw Uprising of 1944 led to massive casualties and damage to buildings. However, the insurgents proved that it is worth sacrificing one's life for the ideal of freedom.

Joanna Gurtowska

Foreign press review p. 99

Jerzy Banaś

High life of experts – conferences, fairs and exhibitions p. 100

Szanowni Czytelnicy,

„konia z rzędem” temu, kto dziś powie, kiedy wreszcie doczekamy się rewolucji w naszych dokumentach identyfikacyjnych i wprowadzenia nowych e-dowodów osobistych (ostatnio mówi się o roku 2018). Wielką niewiadomą jest też to, jak będą one wyglądały, i jaka będzie ich funkcjonalność i przede wszystkim kto je dla nas wykona. A drugiego „konia” temu, kto odpowie na pytanie, kiedy doczekamy się cyfrowej rewolucji we wszystkich dokumentach – jaką zapowiada i zapowiada Ministerstwo Cyfryzacji. Muszę przyznać, że działalność tego ministerstwa budzi we mnie ambiwalentne refleksje. Z jednej strony cieszy jego dynamiczna aktywność i pewnego rodzaju determinacja w poszukiwaniu najlepszych rozwiązań w informatyzacji administracji państwowej i cyfryzacji dokumentów, bo daje to nadzieje na konkretne sukcesy w tych dziedzinach. Z drugiej zaś strony obawiam się zrealizowania wszystkich, nawet tych najbardziej futurystycznych zapowiedzi: że już niebawem, może za rok, nasze najważniejsze dokumenty zostaną zdematerializowane, znajdą się na ekranach urządzeń mobilnych i będą istniały wyłącznie w sferze wirtualnej. Podobne nadzieje i obawy podzielają Szymon Ruman, Remigiusz Lewandowski i Krzysztof Izak, autorzy artykułów otwierających to wydanie.

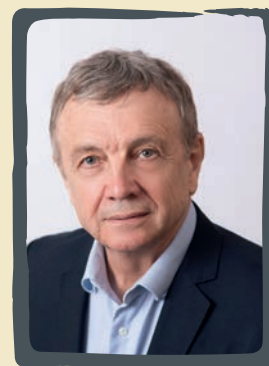
Aktualnie najnowocześniejsze dokumenty to te, które w warstwie cyfrowej zawierają dane biometryczne ich właścicieli; wymagają one jednak równie nowoczesnych urządzeń i systemów do ich kontroli. Ponadto ciągle rosnący przepływ ludzi między krajami i kontynentami wymusza konieczność elastycznego dostosowywania możliwości kontroli dokumentów do natężenia ruchu na przejściach granicznych. W poszukiwaniu rozwiązań umożliwiających zwiększenie sprawności kontroli granicznych, powołany został w 2014 roku w Warszawie projekt BIOMET z udziałem m.in. WAT i PWPW S.A. Celem tego projektu jest stworzenie prototypu dla mobilnej kontroli granicznej, czyli przenośnego systemu do weryfikacji osób przekraczających zewnętrzną granicę UE i ich dokumentów. Zaangażowane przy realizacji projektu konsorcjum naukowo-przemysłowe dokonało już pierwszych prób prototypów i przewiduje, że w październiku br. nastąpi zakończenie prac. O jego szczegółach można dowiedzieć się więcej z artykułu, którego autorami są uczestnicy projektu.

Cyfryzacja nieco wolniej, ale dosięga także wymiaru sprawiedliwości – na ten temat pisze Anna Zalesińska. Pozostając w kręgu prawa, w artykule Remigiusza Lewandowskiego przedstawiamy kolejne argumenty na to, że sfera dokumentów publicznych wymaga pilnych i nowoczesnych ustawowych regulacji. Natomiast Krzysztof Izak kontynuuje analizę zagrożeń związanych z nieustającą falą imigrantów przybywających codziennie do Europy. Jest już tradycją, że w wydaniu z tego kwartału roku wracamy do tematu powstania warszawskiego i Twierdzy PWPW, tym razem w artykule Moniki Olbryś-Zegarowskiej i Tomasza Turka.

Jak zawsze serdecznie namawiam do przeczytania całości tego wydania. Bardzo dziękuję za przesłane nam listy i maile. Proszę nas nadal czytać, także na www.czlowiekidokumenty.pl, polecać innym, pisać do nas (redakcjacid@pwpw.pl), dzwonić, jak również odwiedzać Redakcję.

Zapraszam i serdecznie pozdrawiam.

Jerzy Banaś
Redaktor Naczelny



JERZY BANAŚ – absolwent Wydziału Filozoficzno-Historycznego UAM w Poznaniu. Ukończył też Doktoranckie Studia Zarządzania i Finansów oraz podyplomowe studium konsultingu gospodarczego w Szkole Głównej Handlowej w Warszawie. Publicysta, menadżer.

PWPW S.A. NA XXVI FORUM EKONOMICZNYM W KRYNICY

W dniach 6–8 września br. Polska Wytwórnia Papierów Wartościowych zaprezentowała swoją ofertę podczas XXVI FORUM EKONOMICZNEGO w Krynicy. Stoisko znajdowało się w namiocie Polskiej Fundacji Narodowej wśród stoisk innych spółek Skarbu Państwa. Pokazane zostały dokumenty, papier i druki zabezpieczone, karty oraz systemy i rozwiązania IT, zaprezentowano m.in. dokumenty identyfikacyjne, w tym elektroniczny dowód osobisty dla obywateli Armenii, i nowy polski banknot 500 złotych z wizerunkiem Jana III Sobieskiego.

W ekspozycji znalazł się także okolicznościowy zabezpieczony druk promocyjny poświęcony akcji płk. Ignacego Matuszewskiego, który wraz z mjr. Henrykiem Floyar-Rajchmanem we wrześniu 1939 roku zorganizowali i przeprowadzili ewakuację 75 ton złota z rezerw Banku Polskiego przez Rumunię, Turcję i Syrię do Francji, gdzie zostało ono przekazane Rządowi Rzeczypospolitej. Ciekawostką jest to, że druk ów zawiera ukryty rysunek, widoczny tylko w świetle UV, który ukazuje całą trasę ewakuacji rezerw złota z Warszawy do Marsylii.

Inną atrakcją stoiska PWPW były wirtualne prezentacje wspomnianych wyżej



Fot. 1. Premier RP Beata Szydło w towarzystwie ministra skarbu państwa Dawida Jackiewicza z wizytą na stoisku PWPW S.A.

banknotów i dokumentów. Można było je obejrzeć i przestudiować ich szczegóły dzięki zastosowaniu specjalnej technologii multimedialnej, choć fizycznie produkty te nie były obecne w gablotach.

Stoisko PWPW odwiedzili m.in. premier RP Beata Szydło, wicepremier Mateusz Morawiecki i minister skarbu państwa Dawid Jackiewicz.

PWPW S.A. STAWIA NA NOWE TECHNOLOGIE

Sukcesem zakończył się proces certyfikacyjny i w dniu 16 sierpnia br. Polska Wytwórnia Papierów Wartościowych S.A. jako jedyna polska firma uzyskała certyfikat Common Criteria poświadczający bezpieczeństwo pomieszczeń oraz procedur wytwarzania apletów SmartApp podlegających certyfikacji. Poświadczenia takie są wystawiane na dwa lata, na podstawie wyników bardzo restrykcyjnego procesu ewaluacji. Tym samym PWPW po raz kolejny udowodniła, że spełnia najwyższe międzynarodowe wymogi bezpieczeństwa i jakości wytwarzanego oprogramowania informatycznego.

Certyfikat jest kolejnym krokiem przybliżającym PWPW do realizacji zadań umożliwiających wprowadzenie w Polsce dowodów osobistych z warstwą elektroniczną. Jednym z kluczowych elementów certyfikacji bezpieczeństwa produktu jest potwierdzenie, że powstaje on w bezpiecznym środowisku, w gronie kompetentnych, wysoko wykwalifikowanych pracowników i zgodnie z określoną metodyką, gwarantującą odpowiednią kontrolę nad procesem i jakością wytwarzania bezpiecznych produktów IT. Uzyskany przez PWPW S.A. certyfikat SMARTAPP DEVELOPMENT SITE poświadcza spełnienie wszystkich tych wymogów. Uzyskanie certyfikatu wiązało się z poddaniem PWPW złożonej procedurze oceny, m.in. w obszarach takich jak: bezpieczeństwo fizyczne pomieszczeń, system monitoringu, procedury reagowa-



Fot. 2. Ekspozycja druku promocyjnego poświęconego plk. Ignacemu Matuszewskiemu

nia ochrony na incydenty, zabezpieczenia logiczne sprzętu komputerowego, procedury zarządzania sprzętem i oprogramowaniem, metodyka zarządzania wytwarzaniem oprogramowania, procedury testowania wytworzonych produktów czy procedury przekazywania wytworzonych produktów i ich dokumentacji.

PWPW we wszystkich obowiązujących testach Common Criteria, wypadła pozytywnie i bez zastrzeżeń. Ujednolicone kryteria oceny bezpieczeństwa przy certyfikacji Common Criteria, ze względu na swoją porównywalność, prowadzą do wyników rozpoznawalnych na rynku międzynarodowym. Dzięki temu produkty PWPW S.A. mogą być oferowane nie tylko na rynku krajowym, ale i na rynkach zagranicznych i tam z powodzeniem służyć obywatelom. Aktualnie trwają ostatnie przygotowania do ewaluacji kolejnych wersji produktów SmartApp-SIGN i SmartApp-ID, wykorzystywanych w nowoczesnych dokumentach podróży i e-dowodach. Dzięki poświad-

czeniu SMARTAPP DEVELOPMENT SITE aplety te będą mogły znacznie szybciej uzyskać certyfikat umożliwiający wprowadzenie ich do bezpiecznego obiegu.

EKSPORT Z PWPW S.A.

W ostatnim czasie PWPW S.A. zawarła dwie umowy na produkcję oraz dostawę

drugiego. Pierwszy kontrakt dla Gwatemali był realizowany w latach 2013–2014. Wynegocjowanie kolejnego zamówienia jest elementem strategii umacniania pozycji spółki w krajach Ameryki Łacińskiej. Liczne kontrakty handlowe potwierdzają międzynarodową wartość jej marki oraz stanowią istotną część działalności biznesowej.



Fot. 3. Banknoty wyprodukowane dla Gwatemali przez PWPW S.A.

paszportów dla Republiki Armenii. Umowy obejmują wyprodukowanie kilkudziesięciu tysięcy paszportów biometrycznych, a także produkcję i dostawę łącznie 1 mln paszportów niebiometrycznych, tzw. starego typu. Kolejne zamówienie dla Republiki Armenii jest wynikiem dobrej współpracy z klientem oraz potwierdzeniem wysokiej jakości usług świadczonych przez firmę. W lipcu br. PWPW pozyskała zamówienie na dostawę 40 mln banknotów dla Banku Gwatemali. Banknoty o nominale 10 quetzali będą produkowane w Polsce po raz

Polska Wytwórnia Papierów Wartościowych jest nowoczesną firmą o prawie stuletniej tradycji i doświadczeniu oraz o ugruntowanej pozycji na światowym rynku producentów banknotów i dokumentów. Stale podnosi kompetencje w zakresie rozbudowy nowoczesnego parku maszynowego oraz rozwoju nowoczesnych, często własnych i chronionych patentami technologii i zabezpieczeń. Wysoka jakość oferowanych produktów i usług jest najlepszą wizytówką Wytwórni.

Źródła: Centrum Prasowe PAP, PWPW S.A.

Szymon Ruman

E-DOWÓD, PAŃSTWO USŁUGOWE I CYFROWA SUWERENNOŚĆ

Oddanie kierowania budową e-państwa w ręce firm komercyjnych może spowodować, że realizacja tego zadania nie będzie zabezpieczała w odpowiedni sposób interesów Rzeczypospolitej i jej obywateli.



Wprowadzenie w Polsce dowodów elektronicznych czy też e-dowodów zapowiedział po raz pierwszy rząd PO, bodaj w 2008 r. Polacy korzystają jednak nadal z tradycyjnych plastikowych dowodów osobistych, podczas gdy obywatele innych państw UE cieszą się od lat e-dowodami z szeroką gamą funkcjonalności. Krokiem w dobrym kierunku jest ogłoszone na początku lipca br. porozumienie zawarte przez trzy ministerstwa – Cyfryzacji, Spraw Wewnętrznych i Administracji oraz Zdrowia – którego efektem ma być wypracowanie harmonogramu wprowadzenia e-dowodu, jak również odpowiedź na pytanie, co ma się na nim znaleźć. Zawarcie porozumienia poprzedziła burza pomysłów dotyczących e-dowodu oraz elektronicznej Karty Ubezpieczenia Zdrowotnego (e-KUZ). Pojawiały się takie koncepcje jak połączenie e-dowodu lub e-KUZ z kartami płatniczymi wydawanymi przez banki lub zaprojektowanie dowodu jako aplikacji mobilnej. Pomijając fakt, że takie rozwiązanie byłoby bardzo korzystne dla samych banków, gdyż mogłoby spowodować, że 100% obywateli RP otrzymałoby karty bankowe – budziło ono spore kontrowersje ze względów bezpieczeństwa. Poza tym, dane osobowe Polaków, e-tożsamość i dostęp do danych zdrowotnych to kwestie zbyt wrażliwe, aby

podlegały outsourcingowi. A ich przechowywanie, zabezpieczenie i udostępnianie to kwestia cyfrowej suwerenności państwa i jego obywateli.

Powracające jak bumerang pomysły, by stosować bankowe systemy teleinformatyczne na potrzeby uwierzytelniania obywateli w związku z korzystaniem przez nich z usług typu e-government, oznaczają istotne rozszczelnienie systemu identyfikacji elektronicznej i uwierzytelniania oraz de facto rezygnację państwa z własnego monopolu na identyfikację i uwierzytelnianie obywateli. Taki stan rzeczy rodzi szereg zagrożeń naruszających istotny interes bezpieczeństwa państwa. W szczególności rozwiązanie takie charakteryzuje się następującymi słabymi stronami:

1. Wykorzystanie wyłudzonych rachunków bankowych lub wykorzystywanie nieautoryzowanego dostępu do istniejących rachunków bankowych w celu tworzenia fałszywej tożsamości i dokonywanie na tej podstawie innych, wtórnych przestępstw.

Eksperci zajmujący się zwalczaniem przestępczości zwracają uwagę, że wykorzystywanie sektora bankowego w działalności przestępczej odbywa się m.in. poprzez:

- uzyskiwanie nieautoryzowanego dostępu do istniejących rachunków bankowych,

SZYMON RUMAN – prawnik, legislator, menedżer. Założyciel Instytutu Druckiego-Lubeckiego. Były podsekretarz stanu w Ministerstwie Cyfryzacji. Pełnił także funkcję doradcy Zarządu PWPW S.A.

- zakładanie na podstawie fałszywych danych rachunków bankowych wykorzystywanych następnie w nielegalnym procederze,
- wykorzystanie tzw. słupów do zakładania rachunków służących do transferowania środków pochodzących z przestępstwa¹.

W tym zakresie szczególne zagrożenie generowane jest w cyberprzestrzeni z wykorzystaniem bankowości elektronicznej (np. penetracja zasobów informatycznych banku, phishing, pharming, skimming). W omawianym przypadku może mieć zatem miejsce sytuacja, w której na podstawie wyłudzonego rachunku lub nieautoryzowanego dostępu do niego przestępca zostanie pozytywnie zweryfikowany (uwierzytelniony) w ramach systemu bankowego i uzyska otwarty dostęp do świadczeń (w tym finansowych) i e-usług (związanych np. z wydawaniem dokumentów i tworzeniem tożsamości) oferowanych przez państwo. W konsekwencji otwarcie bankowego kanału uwierzytelniania obywateli na potrzeby korzystania z usług e-government może wywołać falę przestępstw uderzających bezpośrednio w interes państwa i jego bezpieczeństwa. Już obecnie bowiem skala przestępczości opartej na nieautoryzowanym lub wyłudżonym dostępie do bankowości elektronicznej jest poważna.

2. Bankowe systemy teleinformatyczne nie posiadają ustandaryzowanych systemów bezpieczeństwa IT, w tym scertyfikowanych w zakresie Common Criteria. Należy podkreślić, że międzynarodowe normy dotyczące bezpieczeństwa teleinformatycznego oraz stosowana praktyka wskazują na konieczność certyfikowania produktów IT pod kątem bezpieczeństwa. Typowym przykładem są dokumenty elektroniczne (paszport

biometryczny) oraz podpis elektroniczny, które zgodnie z obowiązującymi w Polsce przepisami – w związku z ich rolą w systemie identyfikacji i uwierzytelniania – muszą być scertyfikowane na zgodność z Common Criteria.

3. Otwarcie kanału uwierzytelniania poprzez systemy bankowe może prowadzić do przejęcia przez banki wrażliwych danych obywateli. Faktycznie już dziś nie jest jasne, czy państwo posiada jakąkolwiek kontrolę nad pozyskiwaniem przez banki danych osobowych w ramach projektu 500+.
4. Obecnie brak jest wystarczających doświadczeń innych państw w zakresie wykorzystywania systemów bankowych do uwierzytelniania obywateli na potrzeby korzystania z e-usług.

W państwach członkowskich UE dominującym narzędziem uwierzytelniania pozostaje elektroniczny dowód osobisty wraz z certyfikatem, który należy uznać za optymalny instrument – z punktu widzenia bezpieczeństwa państwa oraz wygody obywateli. Elektroniczny dowód osobisty jest stosowany w: Belgii, Cyprze, Estonii, Finlandii, Hiszpanii, Litwie, Luksemburgu, Łotwie, Malcie, Niemczech, Portugalii, Słowacji, Włoszech. Dodatkowo wdrożenie elektronicznego dowodu osobistego jest planowane w Bułgarii, a w Austrii uwierzytelnianie odbywa się poprzez elektroniczną kartę ubezpieczenia społecznego. Tymczasem systemy bankowości elektronicznej stosowane są tylko w czterech państwach, jako narzędzia subsydiarne względem podstawowych – elektronicznego dowodu osobistego lub certyfikatu. Warto zwrócić uwagę także na przypadek Estonii jako państwa najbardziej zaawansowanego pod względem informatyzacji. W Estonii stosowane są dwa narzędzia uwierzytelniania: elektro-

niczny dowód osobisty oraz tzw. mobilne ID, z tym że zasadnicza część logowań (ponad 70%) odbywa się poprzez elektroniczny dowód osobisty. Wydaje się, że zastosowane przez rząd estoński rozwiązanie, nie wykorzystujące systemów bankowych do uwierzytelniania, wynika z odpowiedniej troski o bezpieczeństwo i finanse państwa.

5. Należy oczekiwać, że zaangażowanie banków w system uwierzytelniania nie będzie bezpłatne i wiązać się będzie z koniecznością poniesienia przez Skarb Państwa dodatkowych kosztów. Takie dodatkowe obciążenie finansowe państwa nie wydaje się racjonalne w związku z planowanym wprowadzeniem elektronicznego dowodu osobistego, który powinien stać się (podobnie jak w innych państwach) podstawowym i powszechnym narzędziem uwierzytelniania. W takiej sytuacji dublowanie wydatków państwa na dwa alternatywne względem siebie instrumenty uwierzytelnienia nie jest racjonalne.

Powyższe przesłanki przemawiają za niewykorzystywaniem systemów bankowych do uwierzytelniania. Wyjątkiem od tej zasady może być – mające już miejsce – zaangażowanie banków na potrzeby programu 500+. Z uwagi jednak na przedstawione argumenty powinno to mieć charakter przejściowy – do czasu wdrożenia elektronicznego dowodu osobistego.

Zgodnie z ostatnimi deklaracjami, prace rządowe zmierzają do wprowadzenia e-dowodu zawierającego cyfrowo zapisane dane obywatela, a także umożliwiającego dostęp do danych zgromadzonych w bazach służby zdrowia. Rozważana jest także opcja, by e-dowód zawierał podstawową wersję podpisu elektronicznego. Takie e-dowody produkowałby narodowy wytwórca dokumentów kontrolowany w pełni przez państwo.

Kluczowa wydaje się jednak odpowiedź na pytanie: po co nam e-dowód? Informatyzacja państwa jest źródłem wielu problemów już od ponad 20 lat. Projekty informatyczne pochłaniają ogromne sumy i nie przynoszą spodziewanych korzyści. Czy projekt, który kosztować będzie, jak się szacuje, 1,5 mld złotych przyniesie realne korzyści dla obywateli?

Aktualnie najwięcej propozycji dotyczących e-państwa (w tym e-tożsamości) wychodzi z Ministerstwa Cyfryzacji. Tematykę tę ma koordynować Komitet Rady Ministrów ds. Cyfryzacji, a konkretne działania mają zostać przydzielone Ministerstwu Rozwoju, Ministerstwu Finansów, Ministerstwu Zdrowia oraz Kancelarii Prezesa Rady Ministrów. W tym miejscu zdziwienie budzi fakt, iż w pracach koncepcyjnych nie są reprezentowane w należyty sposób MSWiA, MON czy MS, mimo poruszania tak ważnych kwestii, jak e-tożsamość, cyberbezpieczeństwo oraz e-sądy. Zakłada się za to szeroki udział ekspertów rynkowych. I czasem nie wiadomo, czy budową naszego e-państwa kieruje jeszcze rząd, czy już wyłącznie lobbysci dużych międzynarodowych korporacji.

Powyższy opis sytuacji jest istotny z punktu widzenia zabezpieczenia interesów państwa polskiego w planowanych działaniach. Takie kwestie jak e-tożsamość (eID), e-zdrowie, schemat krajowy karty płatniczej dotyczą w sposób ścisły zadań, które na rzecz państwa realizuje PWPW S.A. Tym bardziej, że pojawiają się w debacie takie koncepcje, jak np. mobilne ID, zwane dowodem osobistym w telefonie komórkowym. Takie rozwiązanie stawia pod znakiem pytania wdrożenie w Polsce dowodu osobistego z warstwą elektroniczną, jaki funkcjonuje w prawie wszystkich państwach UE. Ponadto „dowód w komórce” to rozwiązanie, które nie ma możliwości zastosowania w strefie Schengen, jest więc jedynie iluzją dokumentu tożsamości. Nie gwarantuje także żadnego

poziomu wiarygodności czy bezpieczeństwa dokumentu.

Należy uznać, że informatyzacja stała się i będzie w najbliższych latach jednym z kluczowych obszarów działania państwa. Punktem wyjścia jest przyjęcie modelu państwa usługowego, czyli takiego, którego celem jest świadczenie usług, to jest dostarczanie konkretnej, mierzalnej wartości dla obywateli i innych podmiotów (organizacji społecznych, przedsiębiorców). W tym nowym ujęciu, które wprowadził do debaty publicznej Nikodem Bończa Tomaszewski, operacyjnymi priorytetami informatyzacji państwa powinny być: udostępnienie w postaci cyfrowej jak największej liczby usług publicznych projektowanych w oparciu o realne potrzeby i z udziałem obywateli; udostępnianie danych i zbiorów w postaci cyfrowej, co daje łatwy, równy dostęp do wiedzy, stymuluje gospodarkę i buduje potencjał narodowy; rozwój społeczeństwa obywatelskiego poprzez dostarczenie narzędzi, które bezpośrednio angażują obywateli w sferę publiczną (konsultacje, partycypowanie w decyzjach); zapewnienie suwerenności państwa w sferze cyfrowej względem lobbingu i presji zewnętrznej.

Tak zdefiniowane cele budowy państwa usługowego dają nam już pojęcie, jak cennym narzędziem w ręku obywatela może być e-dowód.

Z punktu widzenia obywatela podniesienie poziomu bezpieczeństwa dokumentu poprzez wprowadzenie warstwy elektronicznej to korzyść wysoce abstrakcyjna. Jednak możliwość dostępu do usług e-administracji i łatwego załatwiania spraw w ZUS, US czy urzędzie gminy online są już znacznie bardziej namacalne. Gdyby jeszcze obok lub zamiast trudno dziś dostępnego narzędzia, jakim jest Profil Zaufany, na e-dowodzie znalazł się podpis elektroniczny, każdy mógłby uwierzytelnić się nim nie tylko w kontaktach z pań-

stwem, ale także w codziennych transakcjach. Przykładowo ułatwiłoby to jeszcze bardziej korzystanie z usług bankowych bądź zawieranie umów. Mowa tu nie tylko o umowach cywilnoprawnych, ale również umowach o pracę, które można by zawierać online po przeprowadzonych na odległość negocjacjach. Ogromnym ułatwieniem byłby z pewnością dostęp do danych zdrowotnych i załatwianie, przy pomocy e-dowodu, spraw związanych z ochroną zdrowia. Korzyści będą oczywiście zależeć od pomyślnego wdrożenia systemu gromadzącego dane o zdarzeniach medycznych czy takich rozwiązań jak e-zwolnienie i e-recepta. Jednak cyfryzacja relacji lekarz–pacjent byłaby ogromną zmianą jakościową, przyniosłaby także państwu liczone w setkach milionów złotych rocznie oszczędności wynikające z uszczelnienia systemu.

Na koniec warto przypomnieć, zdefiniowane trafnie również przez Bończa Tomaszewskiego, sześć warunków cyfrowej suwerenności państwa:

1. Potrzebne są kompetencje cyfrowe budowane w oparciu o własne kadry. Chodzi tu zarówno o kompetencje czysto techniczne, jak i o zdolność do budowania rozwiązań zgodnych z potrzebami tych, dla których powstają. Potrzebne jest więc sprawne operowanie obszarem interakcji ludzi i maszyn.
2. Sprzęt informatyczny i telekomunikacyjny oraz systemy i programy komputerowe stanowią materialną tkankę internetu. Całkowity outsourcing w tej dziedzinie to nic innego jak powierzenie własnej niezależności stronie trzeciej. Administracja potrzebuje własnych operacyjnych kadr IT, pełnej kontroli nad systemami i własnej, chronionej infrastruktury teleinformatycznej.
3. Dane gromadzone w państwowych systemach. W cyberprzestrzeni to dane są walutą obiegową. Są, niczym su-

rowce naturalne, substratem przekuwanym na produkty i pieniądze. Jeśli spojrzymy na współcześnie oferowane „darmowe” usługi w sieci, to zobaczymy, że zazwyczaj płacimy ich dostawcy informacjami na nasz temat. Państwo, które nie potrafi twardo regulować rynku handlu danymi, efektywnie ograniczać nadużyć i chronić informacji o swoich obywatelach, przypomina w swej bezradności to z początków rewolucji przemysłowej. Na marginesie – rolę takiego regulatora mogłaby efektywnie sprawować Krajowa Rada Radiofonii i Telewizji rozbudowana o kompetencje i zasoby obecnego Urzędu Komunikacji Elektronicznej.

4. Realne mechanizmy działania, które możemy nazwać e-usługami. Suwerenna cyfrowo organizacja nie tylko porządkuje i przyspiesza własną pracę za pomocą narzędzi IT, ale przede wszystkim używa rozwiązań cyfrowych, by dostarczać najlepsze usługi swoim odbiorcom. To jednak wymaga głębokiego rozpoznania ich potrzeb, czyli umiejętności o wiele większych niż sprawność techniczna.
5. Cyberprzestrzeń, tak jak każde terytorium, musi być chroniona. Jeśli przenosimy działalność państwa do sieci cyfrowych, to ich ochrona jest tak samo oczywista jak ochrona dróg, mostów czy sieci energetycznej w świecie materialnym. Cyberbezpieczeństwo to także ochrona obywateli w internecie, bezpieczny obrót gospodarczy, działania militarne w sieci itp.
6. Państwo suwerenne w cyberprzestrzeni musi mieć oparcie w rozwiniętym obszarze narodowej gospodarki, któremu będzie zapewniać stałe wsparcie. Polska potrzebuje ekosystemu rodzimych prywatnych firm osadzonych w krajowym rynku i zdolnych do brania udziału w grze w skali globalnej. Dlatego

niezwykle ważne jest ustalenie czytelnych reguł współpracy z dostawcami, szerokie finansowanie przez państwo prac badawczo-rozwojowych, działania na rzecz innowacyjności polskiego przemysłu informatycznego, a także wykorzystanie jego dotychczasowego dorobku oraz infrastruktury. Sektor IT nie będzie się prawidłowo rozwijał bez wsparcia uczelni i instytucji naukowych, które powinny zapewniać stały dopływ specjalistów, nowych pomysłów i technologii².

Do tych sześciu warunków dodałbym jeszcze jeden: dobry rząd, który będzie chciał działać, by spełniać sześć powyższych warunków i budować cyfrową suwerenność.

Oddanie kierowania budową e-państwa w ręce firm komercyjnych może spowodować, że realizacja tego zadania nie będzie zabezpieczała w odpowiedni sposób interesów Rzeczypospolitej i jej obywateli. Ponadto cyfryzacja państwa w oparciu o duże banki może wykluczyć polskie firmy z tego procesu i oprócz błędnych założeń spowodować, że ewentualne zyski popłyną do w większości zagranicznych korporacji. Nie można na to pozwolić, zwłaszcza mając na uwadze fakt, iż nasz kraj dysponuje tak wyspecjalizowanym podmiotem jak Polska Wytwórnia Papierów Wartościowych – firma z prawie stuletnią tradycją, a jednocześnie innowacyjna i przygotowana do budowania e-państwa.

Organizatorzy konferencji PAŃSTWO USŁUGOWE, która odbyła się prawie rok temu (14–15 października 2015 r. w siedzibie NInA w Warszawie), przybliżyli swoją koncepcję w następujący sposób: *Wyobraź sobie, że pismo, które dostajesz z urzędu, jest przyjazne i zrozumiałe, a przez telefon miły urzędnik wskazuje najkorzystniejszy sposób postępowania. Składasz wniosek przez internet, bez pięciu załączników, bo urzędnik sam sprawdził wszystko w swojej bazie. Na koniec ważny dokument odbierasz*

w urzędzie, który masz po drodze, a nie 50 km od miejsca zamieszkania.

Czy ta wizja pozostanie marzeniem, utopią – to będzie zależało od zdolności państwa do przestawienia się na myślenie i funkcjonowanie usługowe, a także od zdolności dostarczania przyjaznych użytkownikom e-usług w miejsce uciążli-

wych procedur. Jeżeli takie e-usługi przestaną być wyjątkami potwierdzającymi regułę nieudolnej e-administracji, to e-dowód stanie się kluczem do przyjaznego e-państwa, a rząd, który go wprowadzi oraz polskie firmy budujące e-państwo staną się motorem kolejnej rewolucji technologicznej.

W artykule wykorzystałem fragmenty mojego tekstu zatytułowanego E-DOWÓD, CYFROWA DOBRA ZMIANA, który ukazał się w „Rzeczpospolitej” 12 lipca br., oraz oficjalne stanowiska PWPW S.A. kierowane do rządu w trakcie prac legislacyjnych.

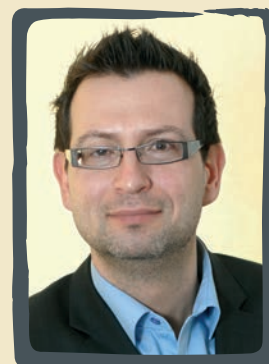
¹Raport o stanie bezpieczeństwa w Polsce w 2014 roku, Ministerstwo Spraw Wewnętrznych, Warszawa 2015, s. 199–200.

²N. Bończa Tomaszewski, *Sześć warunków niepodległości w cyberprzestrzeni*, <http://www.rp.pl/Rzecz-o-polityce/306079883-Szesc-warunkow-niepodleglosci-w-cyberprzestrzeni.html#ap-1>.

Remigiusz Lewandowski

DOKUMENT W SMARTFONIE – NOWOCZESNOŚĆ CZY NIEBEZPIECZNA EKSTRAWAGANCJA?

Aktywność, dynamika i determinacja Ministerstwa Cyfryzacji zmierzające do poprawy niskiego stopnia informatyzacji Polski niezwykle cieszą. Entuzjazm towarzyszący tym działaniom nie powinien jednak przesłonić niedoskonałości niektórych z proponowanych rozwiązań.



W literaturze przedmiotu oraz w mediach bardzo często podnosi się zagadnienie niskiego stopnia informatyzacji państwa w naszym kraju. Podkreślenia wymaga fakt, że zgodnie z indeksem DESI Komisji Europejskiej z 2016 r. (the Digital Economy and Society Index) Polska pozostaje na 22. miejscu wśród państw członkowskich Unii Europejskiej pod względem zaawansowania w budowie gospodarki cyfrowej i społeczeństwa cyfrowego. Autorzy raportu poświęconego DESI 2016 zwracają uwagę, że *Polska spada do grupy państw pozostających w tyle, gdyż tempo nadrobiania przez nią zaległości jest niższe w porównaniu z wynikiem DESI między 2014 a 2015 r. Szczegóły indeksu za 2016 r.*¹ przedstawia ryc. 1.

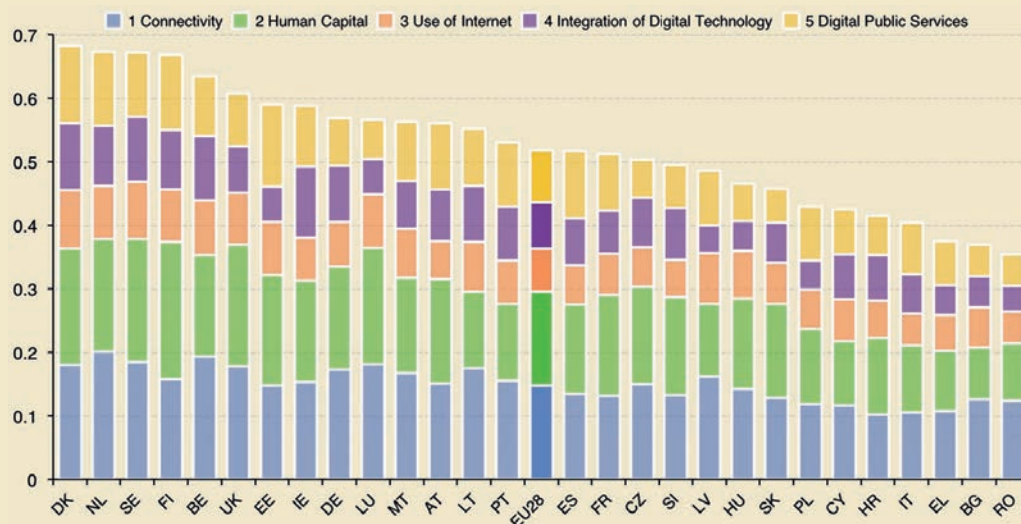
Spośród badanych w ramach indeksu obszarów – w relacji do średniej UE – dość nisko ocenione zostały przez unijnych ekspertów: kapitał ludzki (w odniesieniu do umiejętności korzystania z IT i internetu), integracja technologii cyfrowych oraz dostęp do łączności internetowej. Co ciekawe, obszar cyfrowych usług publicznych kształtuje się na poziomie zbliżonym do średniej UE, niemniej jednak eksperci zwracają uwagę, że *aktywne wykorzystanie e-administracji utrzymuje się na stosunkowo niskim poziomie i zaledwie 22%*

*użytkowników internetu składa formularze elektroniczne (21 miejsce w UE)*². Ta konstatacja pozostaje zgodna z – jak się wydaje – powszechnym odczuciem w tym zakresie, tj. z niezadowoleniem z wąskiego katalogu dostępnych elektronicznie usług publicznych oraz z narzędzi służących do dostępu do nich.

Z tych względów niezwykle cieszą aktywność, dynamika i determinacja Ministerstwa Cyfryzacji zmierzające do poprawy zobrazowanego powyżej stanu rzeczy. Zaprezentowany przez minister cyfryzacji, Annę Streżyńską, i przekazany do konsultacji społecznych PROGRAM ZINTEGROWANEJ INFORMATYZACJI PAŃSTWA³ wraz ze STRATEGIĄ INFORMATYZACJI PAŃSTWA – PLANEM DZIAŁAŃ MINISTRA CYFRYZACJI⁴ stanowią w dużym stopniu odpowiedź na zdiagnozowane m.in. przez Komisję Europejską i odczuwalne dość boleśnie przez Polaków słabe strony i deficyty informatyzacji państwa.

Entuzjazm towarzyszący wskazanym wyżej działaniom nie powinien jednak przesłonić niedoskonałości niektórych z proponowanych rozwiązań, a w szczególności nie powinien ograniczyć zdrowego rozsądku, jakiego oczekuje się przy realizacji każdej inicjatywy publicznej. W ramach niniejszego artykułu chciałbym skupić się na jednym zagadnieniu: usytuowaniu informatyzacji w obszarze dokumentów publicznych.

REMIGIUSZ LEWANDOWSKI – dr nauk ekonomicznych, Wydział Nauk Ekonomicznych i Zarządzania UMK w Toruniu, członek Rady Przemysłowo-Programowej Wydziału Elektroniki WAT w Warszawie.



Ryc. 1. Indeks DESI 2016

1. Connectivity – jakość sieci połączeń;
 2. Human Capital – kapitał ludzki;
 3. Use of Internet – korzystanie z internetu;
 4. Integration of Digital Technology – integracja technologii cyfrowej;
 5. Digital Public Services – cyfrowe usługi publiczne.
 Źródło: <https://ec.europa.eu/digital-single-market/desi>.

We współczesnym świecie nikt nie neguje potrzeby wykorzystania rozwiązań informatycznych w sferze dokumentów publicznych, w tym także w sferze związanej z zarządzaniem tożsamością. Zasadniczym pytaniem jest jednak, czy rozwiązania informatyczne powinny pełnić funkcję subsydiarną w odniesieniu do dokumentów publicznych i zarządzania tożsamością, czy też powinny (docelowo) zastąpić dokumenty „analogowe”. Nie jest to zagadnienie ani błahe, ani czysto teoretyczne, albowiem takie pytania stawiane są w aktualnej debacie publicznej, która towarzyszy zapowiadanym przez Ministerstwo Cyfryzacji działaniom.

Przed podjęciem próby udzielenia odpowiedzi na powyższe pytania należy jednak doprecyzować zakres rozważań podjętych w niniejszym artykule. Obejmuje on:

1. dokumenty publiczne i ich potencjalną transformację w dokument cyfrowy,
2. narzędzia dostępu do elektronicznych usług publicznych, a w szczególności po-

tencjalne wykorzystanie dokumentów publicznych jako tego rodzaju narzędzia.

W ramach niniejszego artykułu dokument publiczny definiuję jako odpowiednio zabezpieczony dokument urzędowy, wytwarzany według określonego wzoru w seriach lub w znacznej liczbie, gotowy w całości lub jako blankiet wymagający indywidualizacji bądź personalizacji, a służący do identyfikacji osób, rzeczy lub potwierdzający stan prawny albo prawa osób posługujących się takim dokumentem. Dokumentami publicznymi w szczególności są:

1. dowód osobisty,
2. paszport,
3. dokumenty ubezpieczenia zdrowotnego,
4. dokumenty tożsamości cudzoziemca: polski dokument tożsamości cudzoziemca, tymczasowe zaświadczenie tożsamości cudzoziemca,
5. dokumenty podróży dla cudzoziemców: dokument podróży dla cudzoziemca

zgodny z **KONWENCJĄ GENEWSKĄ**, polski dokument podróży dla cudzoziemca, tymczasowy polski dokument podróży dla cudzoziemca, naklejka wizowa, zezwolenie na przekraczanie granicy w ramach Małego Ruchu Granicznego,

6. dokumenty dotyczące pobytu: karta pobytu, dokument potwierdzający prawo stałego pobytu, zgoda na pobyt tolerowany, karta pobytu członka rodziny obywatela UE, karta stałego pobytu członka rodziny obywatela UE, oświadczenia o zamiarze powierzenia pracy cudzoziemcowi,
7. dokumenty komunikacyjne: prawo jazdy, dowód rejestracyjny, karta pojazdu,
8. odpisy aktów stanu cywilnego i zaświadczenia USC,
9. wypisy aktów notarialnych,
10. znaki akcyzy,
11. legitymacje funkcjonariusza Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Służby Kontrwywiadu Wojskowego, Straży Granicznej,
12. legitymacje funkcjonariuszy i pracowników innych organów administracji centralnej,
13. świadectwa i dyplomy ukończenia szkół,
14. sądowe tytuły wykonawcze,
15. wyroki sądowe oraz zaświadczenia o niekaralności,
16. książeczki wojskowe,
17. dokumenty związane z posiadaniem broni palnej,
18. inne druki, w tym zaświadczenia, licencje, patenty, świadectwa kwalifikacji, dokumenty poświadczające określony stan prawny itp., mające znaczenie dla bezpieczeństwa państwa, bezpieczeństwa obrotu prawnego i gospodarczego.

Czy zatem warto podjąć prace nad transformacją przedstawionych wyżej enumeratywnie dokumentów w dokumenty cyfrowe? Przed udzieleniem odpowiedzi nasuwa się kolejne pytanie: czymże miałyby być owe

„dokumenty cyfrowe”? Tu otwiera się olbrzymie pole do dywagacji i projekcji, które jednak zawężę do luźnej koncepcji zaprezentowanej przez minister Annę Streżyńską w tygodniku WPROST⁵:

- *Smartfon zastąpi dowód osobisty?*
- *To mój cel! Za cztery lata, wychodząc z tego ministerstwa, chcę mieć na telefonie wszystko, co tylko da się zakodować na takim urządzeniu elektronicznym: dowód osobisty, kartę płatniczą, biblioteczną, dowód rejestracyjny, prawo jazdy... I akt odwołania.*

Dokument publiczny, a w szczególności dokumenty potwierdzające tożsamość osoby (dowód osobisty) lub określone uprawnienia (np. prawo jazdy) albo szczególne uprawnienia (np. legitymacje funkcjonariuszy Policji i służb specjalnych) – w postaci aplikacji na telefon komórkowy budzą poważne wątpliwości. Należy zwrócić uwagę, że forma dokumentu publicznego (w tym sposób jego zabezpieczenia) powinna zapewniać:

1. szybką i jednoznaczną weryfikację tego, czy dokument jest prawdziwy,
2. szybką i jednoznaczną weryfikację tego, czy dane osobowe i wizerunek zapisane w dokumencie odpowiadają tożsamości osoby legitymującej się danym dokumentem,
3. ochronę przed przerabianiem i podrobieniem dokumentu,
4. ochronę tożsamości obywateli przed kradzieżą,
5. możliwość weryfikacji, o której mowa w pkt 1 i 2, w odniesieniu do wybranych dokumentów (np. prawa jazdy) również przez funkcjonariuszy służb zagranicznych.

Dokument w telefonie komórkowym nie wypełnia tych warunków koniecznych. W odróżnieniu od dokumentu w formie materialnej, „dokument – aplikacja” jest możliwy do okazania jedynie tak długo, na ile pozwala bateria w telefonie oraz na ile łączność internetowa udostępnia komunikację z rejestrami państwo-

wymi. A zatem tego rodzaju „dokument” posiadałby cechę nietrwałości i nieciągłości działania, co negatywnie weryfikuje dwa pierwsze warunki konieczne wskazane powyżej. W sytuacji wymagającej kontroli tożsamości lub uprawnień taka weryfikacja mogłaby się okazać niemożliwa do przeprowadzenia (bo np. bateria się rozładowała lub brak jest zasięgu sieci GSM).

Druga słabość omawianych rozwiązań to podatność na ataki hakerów. Na całym świecie tego rodzaju ataki trwają praktycznie bez przerwy. Dotyczą one także naszego państwa. Choćby ostatnio – odnotowany w lipcu br. atak na serwery Netii, w efekcie którego ujawniono dane personalne klientów i historie przeprowadzanych przez nich transakcji⁶, czy też atak z sierpnia br. na serwery międzynarodowej korporacji IT, Opera Software AS, w wyniku którego najprawdopodobniej doszło do wycieku danych i haseł 1,7 mln klientów Opera Sync⁷. Działalność sprofesjonalizowanych międzynarodowych grup hakerskich to bardzo poważne zagrożenie dla bezpieczeństwa państwa. Dokument tożsamości w formie aplikacji telefonicznej wydaje się doskonałym narzędziem z punktu widzenia hakerów zainteresowanych przejęciem cudzej tożsamości w różnych celach, w szczególności terrorystycznych lub związanych z przestępczością gospodarczą. Jak wskazano w RAPORCIE O STANIE BEZPIECZEŃSTWA W POLSCE W 2014 ROKU: *Cyberprzestrzeń pozostaje obszarem działania zarówno indywidualnych przestępców, jak i zorganizowanych grup przestępczych oraz środowisk ekstremistycznych i organizacji terrorystycznych. Upowszechnienie dostępu do Internetu, w kontekście globalnego charakteru cyberprzestrzeni, przy jednocześnie stosunkowo dużej możliwości zachowania anonimowości i popełniania przestępstw na terenie jednego państwa z obszaru innego, sprzyja występowaniu różnego rodzaju zagrożeń, zarówno dotyczących bezpieczeństwa sys-*

temów informatycznych, jak i o charakterze stricte przestępczym (przestępczość o charakterze ekonomicznym, kryminalnym i narkotykowym). Istotne jest również, że cyberzagrożenia mają charakter elastyczny i bezpośrednio zależny od kierunków rozwoju nowoczesnych technologii. Sprawy przestępstw coraz częściej wykorzystują dedykowane oprogramowanie umożliwiające kamuflowanie miejsca, z którego działają, korzystają z sieci anonimizujących, m.in. TOR czy wirtualnych systemów dokonywania płatności w Internecie, np. bitcoin, pozostając poza jakąkolwiek kontrolą instytucji finansowych⁸.

RAPORT jako jedną z podstawowych kategorii przestępstw popełnianych w cyberprzestrzeni wskazuje phishing, polegający na pozyskiwaniu za pośrednictwem internetu danych wrażliwych, takich jak hasła, loginy itd., a także kampanie cyberspieszowskie wymierzone w poszczególne państwa. To realne zagrożenie dla dokumentów identyfikacyjnych i dokumentów potwierdzających określone uprawnienia – po umieszczeniu ich w cyberprzestrzeni. Zagrożenie to jest szczególnie jaskrawe w dobie globalnego terroryzmu.

W tym kontekście trudno jest znaleźć uzasadnienie dla konceptu tworzenia „wirtualnych” dokumentów publicznych, zwłaszcza że dokumenty fizyczne dobrze spełniają swoje funkcje i zapewniają bezpieczeństwo identyfikacyjne. Co więcej, współczesne technologie polegające na współistnieniu warstwy fizycznej dokumentu z warstwą elektroniczną (mikroprocesorem wraz z odpowiednimi danymi, np. biometrycznymi, kwalifikowanym podpisem elektronicznym itd.) znacząco podnoszą bezpieczeństwo. Ponadto brak możliwości zastosowania owych elektronicznych „dokumentów” poza granicami kraju (np. prawa jazdy lub dowodu osobistego jako dokumentu umożliwiającego podróżowanie w strefie Schengen) oraz

dodatkowe koszty, jakie poniósłby Skarb Państwa z tego tytułu zdają się przemawiać za tym, że pomysł „dokumentów” elektronicznych to raczej ekstrawagancja o poważnych, negatywnych skutkach dla bezpieczeństwa narodowego.

Drugim z rozpatrywanych w niniejszym artykule zagadnień jest kwestia narzędzi używanych do korzystania z e-usług publicznych. Wydaje się, że podstawową przyczyną znikomego funkcjonowania w praktyce e-usług w Polsce są słabe narzędzia dostępu. Obecnie korzystając można z dwu podstawowych narzędzi: kwalifikowanego podpisu elektronicznego (narzędzie płatne o marginalnym zastosowaniu w odniesieniu do korzystania z e-usług) oraz profilu zaufanego, o którym minister Anna Streżyńska mówi, że *jest to rzecz, która na tyle jest odstrasżająca dla klientów, że zaledwie 300 tys. osób w Polsce korzysta z profilu zaufanego jako środka komunikacji i potwierdzania swojej woli w kontaktach z administracją. Można powiedzieć, że są to pasjonaci, ponieważ profil zaufany jest powiązany bezpośrednio z serwisem ePUAP, który został zbudowany za ponad 150 mln zł i niestety jest wysoce awaryjnym produktem*⁹.

Instrumenty dostępu do e-usług publicznych muszą zapewniać gwarancję prawidłowej weryfikacji tożsamości osoby pragnącej skorzystać z tego rodzaju usług. A zatem narzędzie to zapewnia odpowiednie uwierzytelnienie dające dostęp do e-usług. Obecnie Ministerstwo Cyfryzacji rozważa jako tzw. dostawców tożsamości: narodowego dostawcę tożsamości, banki, operatorów telekomunikacyjnych i operatorów pocztowych¹⁰. Ryzykowne wydaje się powierzenie wskazanej wyżej roli tak szerokiemu gronu podmiotów. Raz jeszcze podkreślenia wymaga relatywna słabość funkcjonujących obecnie komercyjnych systemów teleinformatycznych. Przestępczość internetowa, a w szczegól-

ności phishing, w tym kontekście generuje realne ryzyko naruszające bezpieczeństwo identyfikacyjne obywateli. Zagadnienie to podjąłem zresztą również w artykule *O POTRZEBIE REGULACJI SFERY DOKUMENTÓW PUBLICZNYCH*. Warto zatem raz jeszcze podkreślić, że w związku z planami emisji dowodu elektronicznego wyposażonego w mikroprocesor to właśnie ten rodzaj dokumentu powinien być naturalnym instrumentem uwierzytelniającym obywatela online. Alternatywne pomysły, np. wykorzystanie bankowości elektronicznej, obarczone są szeregiem bardzo poważnych słabości (np. phishing, brak certyfikacji, luki w systemach, przypadki włamań do systemów e-bankowości, przypadki infiltracji prywatnych podmiotów przez zagraniczne służby specjalne, ryzyko wynikające z braku nadzoru kapitałowego państwa itp.), a praktyka stosowana przez kraje najbardziej zaawansowane w informatyzacji państwa to potwierdza. Szczególnie dobry jest tu przykład Estonii, gdzie ok. 70% logowań do Portalu e-Usług Państwowych odbywa się poprzez elektroniczny dowód osobisty¹¹, który stanowi powszechny instrument identyfikacji każdego obywatela. Jedynie ok. 30% logowań odbywa się poprzez mobilne ID (Mobiil ID), które wymaga jednak dodatkowej umowy z operatorem telefonii komórkowej i wymiany karty SIM. Czy jest zatem sens wyważać otwarte już drzwi i dodatkowo ponosić koszty z tego tytułu? Czy jest sens tworzyć nowe, kosztowne i niezapewniające wymaganego bezpieczeństwa narzędzia uwierzytelniania w sytuacji przygotowań do emisji elektronicznego dowodu osobistego wyposażonego w mikroprocesor? Czy jest sens dublować wydatki publiczne na alternatywne narzędzia dla wąskiej grupy osób? Myślę, że w obliczu przedstawionych faktów pomysły te także uznać należy za bardziej ekstrawaganckie aniżeli racjonalne.

¹Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2016 r. Profil krajowy Polska, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14161.

²Tamże.

³<https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/program-zintegrowanej-informatyzacji-panstwa>.

⁴<https://mc.gov.pl/konsultacje/program-zintegrowanej-informatyzacji-panstwa/zalacznik-1-strategia-informatyzacji-panstwa-plan-dzialan-ministra-cyfryzacji>.

⁵C. Bielakowski, A. Grabek, Dowód, karta płatnicza i prawo jazdy na telefonie? Streżyńska: To mój cel, <https://www.wprost.pl/tylko-u-nas/535894/Dowod-karta-platnicza-i-prawo-jazdy-na-telefonie-Strezyńska-To-moj-cel.html>.

⁶D. Kosiński, Netia zaatakowana! Dane klientów zostały wykradzione i ujawnione, <http://www.spidersweb.pl/2016/07/netia-atak-2016.html>.

⁷Ł. Kotkowski, Korzystasz z Opery na kilku urządzeniach? Koniecznie zmień hasło!, <http://www.spidersweb.pl/2016/08/opera-sync-atak.html>.

⁸Raport o stanie bezpieczeństwa w Polsce w 2014 r., <http://isp.policja.pl/isp/aktualnosci/7789,Raport-o-stanie-bezpieczenstwa-w-Polsce-w-2014-r.html>.

⁹K.G., Anna Streżyńska: w Polsce zaledwie 300 tys. osób korzysta z Profilu Zaufanego jako środka komunikacji, <http://www.rdc.pl/informacje/anna-strezyńska-w-polsce-zaledwie-300-tys-osob-korzysta-z-profilu-zaufanego-jako-srodka-komunikacji-posluchaj/>.

¹⁰Załącznik nr 2 do SIP: opis docelowego modelu eID. Krajowy Schemat Identyfikacji Elektronicznej (eID) w Polsce z uwzględnieniem budowy państwowego brokera eID i wykorzystaniem usług zaufania, https://mc.gov.pl/files/zalacznik_nr_2_do_sip.pdf.

¹¹Dane za estońską fundacją e-Governance Academy.



Krzysztof Izak

CZY SMARTFON MOŻE ZASTĄPIĆ DOWÓD OSOBISTY?

W czerwcu 2016 r. minister cyfryzacji Anna Streżyńska zapowiedziała początek prawdziwej rewolucji cyfrowej w Polsce. Możliwe, że już niebawem nasze dokumenty, m.in. dowody osobiste, prawa jazdy, dowody rejestracyjne czy karty płatnicze będą dostępne na ekranach telefonów komórkowych¹.



Po głosach apologetów wspomnianej wyżej inicjatywy czas na głębszą refleksję. Zdaniem optymistów już w 2017 r. wymienione dokumenty mają być dostępne jako specjalna aplikacja w smartfonie. W wersji elektronicznej wydawane będą także legitymacje, karty biblioteczne, bilety miesięczne itp. To zapowiada początek prawdziwej rewolucji cyfrowej w Polsce. W tej wersji dokumenty dostępne są już w Austrii i Estonii. W tym drugim państwie e-dowody osobiste funkcjonują od prawie dziesięciu lat i są potwierdzeniem posiadania przez właściciela ubezpieczenia zdrowotnego, pozwalają na uzyskanie e-recepty oraz identyfikację użytkownika podczas logowania do systemu internetowych usług bankowych. Jeśli pójdziemy w tym kierunku co Austria i Estonia, portfele z naszymi plastikowymi kartami pozostaną w domu. Dla wielu ludzi, zwłaszcza młodszych, wśród których nowinki cyfrowe są oczekiwane i pożądane, nowy system może być bardzo wygodny. W Polsce jest ok. 19 mln smartfonów, a więc używa ich co drugi mieszkaniec naszego kraju (a trzeba też brać pod uwagę osoby, które posiadają więcej niż jedno takie urządzenie lub tablet). Pozostali mają „stare” komórki lub nie korzystają w ogóle z telefonów mobilnych. Jak zatem będzie wyglądać ich życie po 2017 r.? Czy będą zmuszeni do nabycia nowych urządzeń i nauczania się ich

obsługi? Dla wielu z nich już nawet mID, czyli mobilny dowód tożsamości, może być rzeczą trudną do opanowania, nie mówiąc o pozostałych dokumentach i „udogodnieniach”. Pani minister zapowiedziała, że nowy system będzie dostępny tylko dla tych osób, które wyrażą chęć korzystania z niego. W ten sposób już na początku będziemy mieli do czynienia z dwoma równoległymi systemami legitymowania: tradycyjnym i elektronicznym, co stworzy pewien chaos i może prowadzić do problemów, bowiem jedne instytucje będą wymagać dokumentów w formie tradycyjnej, a inne w elektronicznej. Upłynie dużo czasu i kosztować to może wiele nerwów, zanim przekona się społeczeństwo do cyfryzacji posiadanych dokumentów. Chyba że cała operacja nabierze charakteru odgórnego, rządowego nakazu. Ale wówczas o żadnej dobrowolności nie może być mowy. Pozostaje też pytanie, kto przenosić będzie nasze dokumenty do cyberprzestrzeni i kto będzie sprawował kontrolę nad ich zasobem i jego bezpieczeństwem? Problem z kolejnym ograniczaniem naszej prywatności staje się w tym przypadku bardzo aktualny.

Zgodnie z dyrektywą unijną Polska musi wprowadzić e-dowody do 2019 r., aby nie utracić wielomilionowej dotacji. Dokumenty takie miały trafiać do polskich obywateli już w 2010 r., ale skandal korupcyjny pokrzyżował te plany. Od tego czasu do chwili obecnej

KRZYSZTOF IZAK – były funkcjonariusz ABW. Zajmował się problematyką terroryzmu oraz ekstremizmów religijnych i politycznych.

pojawiło się już kilka wzorów tradycyjnych dowodów osobistych. W najnowszej wersji na dokumencie brak jest adresu zameldowania właściciela i jego podpisu. Nie ma również warstwy elektronicznej w postaci czipa zawierającego zakodowane informacje dodatkowe na temat użytkownika dokumentu, co zakładano w projekcie i co jest niezbędne, aby dowód osobisty stał się e-dowodem. W praktyce okazało się, że chip pozostałby „niewypełniony”, a tym samym bezużyteczny, wobec czego z niego zrezygnowano. Jednak politycy i urzędnicy zreflektowali się i przystąpili do prac w ramach Zespołu ds. wprowadzenia warstwy elektronicznej w dowodzie osobistym. Miejmy nadzieję, że tym razem z powodzeniem, ponieważ Polska Wytwórnia Papierów Wartościowych gotowa jest do produkcji takich dokumentów, co pokazuje przykład dowodów osobistych dla cudzoziemców. Nie ma się zatem czego wstydić i pora podjąć odpowiednie decyzje, aby nadrobić kilkuletnią zwłokę. Skoro trwają prace nad e-dowodem, to jaki jest sens wprowadzania mID, rozpraszania wysiłków i środków? Trudno mi się wypowiadać w tej kwestii, ponieważ nie znam szczegółów relacji między PWPW a jego organem właścicielskim, czyli Ministerstwem Skarbu Państwa oraz pomiędzy nimi a Ministerstwem Cyfryzacji. Jednak realizacja projektu mID może osłabić pozycję dotychczasowego producenta naszych dokumentów i częściowo wejść w kompetencje MSW. Z drugiej strony, skoro w niedalekich planach są dokumenty mID, to może nie ma większego sensu kontynuowanie badań i doświadczeń nad zabezpieczaniem tradycyjnych, plastikowych dokumentów? W przekonaniu wielu osób wystarczy bowiem dokonać cyfrowego odwzorowania tych dokumentów, które znajdują się w naszym posiadaniu i bezpieczeństwo będzie zapewnione...

Otóż – tak nie jest. Zdaje sobie z tego sprawę również Ministerstwo Cyfryzacji, bowiem np. wszelkie czynności notarialne będą mogły być wykonywane jedynie dla obywa-

teli legitymujących się tradycyjnymi dowodami osobistymi. Czyżby chodziło o brak zaufania do cyfrowych dokumentów? Zapowiedź wprowadzenia mID stanowi element tzw. rewolucji cyfrowej. Ma to być zupełnie nowy system zbudowany na fundamencie świata cyfrowego i osiągnięć trzeciej rewolucji przemysłowej, która jest dla nas podstawową infrastrukturą. A więc będzie to czwarta rewolucja przemysłowa, podczas gdy duża część mieszkańców kuli ziemskiej, zwłaszcza w Afryce i Azji, nie przeszła jeszcze drugiej rewolucji przemysłowej.

ZA I PRZECIW

Wymienione wyżej wątpliwości oraz opinie i oceny wysuwane w dalszej części tekstu nie były dotąd dostrzegane w medialnej dyskusji na temat zalet i wad pomysłu pani minister Anny Streżyńskiej. W doniesieniach dziennikarskich zdecydowanie przeważały zalety nowego systemu, w którym będzie można realizować różnorodne usługi, takie jak np:

- płatności podatkowe
- e-policja – zgłoszenie przestępstwa
- realizowanie recept
- zakupy online
- potwierdzenie wieku (zakup alkoholu, social media)
- usługi pocztowe
- karta parkingowa
- e-ZUS
- rejestr obecności dzieci w szkole
- bilet komunikacji miejskiej
- usługi zdrowotne
- karnety na basen, do kina, teatru².

Wszystko to brzmi pięknie, ale co się stanie, gdy nasz smartfon przestanie działać, ponieważ wyładuje się bateria, a nie będziemy mieć dostępu do zasilania? Panią przy kasie będziemy musieli poprosić o dostęp do gniazdka elektrycznego i kilka minut przerwy? Wątpię jednak w cierpliwość jej i klientów stojących za nami w kolejce. Po prostu oprócz dowodu w komórce będziemy również nosić ze sobą plastikowy do-



Ryc. 1. „Tradycyjny” dowód osobisty

Źródło: <http://www.isanok.pl/aktualnosc/id15133,od-1-marca-nowy-dowod-osobisty-co-sie-zmieni> (dostęp: 7.08.2016).

kument. Tak dla pewności i spokoju ducha. Ale to może być dopiero początek naszych rozterek. Michał Zych, przedstawiciel znanej firmy doradczej Ernst & Young, zwrócił uwagę, że jedyny moment krytyczny, z jakim będą musieli się zmierzyć posiadacze mID, to uwierzytelnienie się. Jeżeli już to zrobimy – podobnie jak w bankach, instytucjach, gdzie jesteśmy już zarejestrowani, wykorzystanie e-usług będzie tak szerokie, jak tylko możemy sobie wyobrazić. Według eksperta przykłady innych państw, w szczególności Estonii, pokazują, że zarówno karty biblioteczne, jak i prawo jazdy oraz wszystkie podstawowe dokumenty mogą być sprawdzane elektronicznie. Wcześniej użytkownik musiałby kupić czytnik, żeby zakodować tam odpowiednie informacje i uwierzytelić się, czyli potwierdzić swoją tożsamość. Obecnie te informacje są już zakodowane na kartach telefonów komórkowych, w związku z czym ten proces jest dużo prostszy. Istnieje odpowiednia aplikacja na telefon, a uwierzytelniać się będzie można za pomocą PIN-u. Estończycy zaczęli od kart ze specjalnymi czipami, a teraz przeszli na smartfony. Dla specjalisty z EY смартфон jest bezpieczniejszy niż „tradycyjny” dowód osobisty. Teraz, gdy zgubimy dowód w postaci plastikowej karty lub ktoś nam go ukradnie, to od razu może go użyć. Telefon komórkowy ma więcej zabezpieczeń. Rozwiązania tego typu nie przechowują naszych danych na telefonach komórkowych, tylko będą korzystały z tych

informacji dopiero w wyniku zasilenia urządzenia odpowiednimi danymi, kiedy będziemy chcieli ich użyć. Obecnie, jeśli zgubimy dowód, musimy zgłosić ten fakt na policji, w banku itp., natomiast Biuro Informacji Kredytowej udostępnia darmową usługę, dzięki której można za pomocą smartfona zastrzec w bankach utracony dowód osobisty. W przypadku telefonu komórkowego mamy dostęp do centrali przez 24 godziny na dobę, możemy szybciej zgłosić, że ktoś nam ten smartfon z dowodem ukradł³.

Ale w przypadku utraty dowodu osobistego też taka procedura istnieje. Ponadto nie zgadzam się ze stwierdzeniem, że na smartfonach nasze dowody osobiste będą bezpieczniejsze. Dostęp do nich będą mieli chociażby operatorzy systemów komórkowych⁴. Umieszczone w cyberprzestrzeni dokumenty mimo haseł i zabezpieczeń nie będą miały stuprocentowej gwarancji bezpieczeństwa przed dostaniem się w niepowołane ręce. Zagrożenia dla urządzeń mobilnych są analogiczne jak w przypadku komputerów. Tak samo należy mieć na uwadze: włamania do urządzenia, infekcje złośliwymi kodami, kradzieże, awarie lub zablokowanie, podsłuchy sieciowe, włamania do infrastruktury, z której korzystają urządzenia (Wi-Fi, VPN itp.) i ataki socjotechniczne. Wrażliwość urządzeń mobilnych jest także podobna do komputerów, ale ich wielkość jest już różna. W przypadku błędów systemu operacyjnego smartfony i tablety wypadają znacznie gorzej niż komputery. Większość komputerów na świecie korzysta z systemu operacyjnego Microsoft Windows. Działy IT w firmach wiedzą, w jaki sposób zapewnić komputerom z tym systemem regularną aktualizację, często dysponują narzędziami do centralnej instalacji i aktualizacji oprogramowania i co ważne – mają świadomość konieczności wykonywania tych czynności. Urządzenia mobilne wykorzystują zaś wiele różnych platform i systemów operacyjnych, m.in. Apple iOS, Google Android OS, Nokia

Symbian OS, Microsoft Windows Mobile/Phone, BlackBerry OS itd. Praktyka pokazuje, że urządzenia mobilne w wielu firmach nie są regularnie aktualizowane, co znacząco zwiększa ryzyko naruszenia ich bezpieczeństwa, nie mówiąc już o urządzeniach pozostających w posiadaniu indywidualnych użytkowników. Biorąc pod uwagę zagrożenia dla urządzeń mobilnych, podkreślić należy również niską świadomość i ostrożność użytkowników tych urządzeń. W przypadku komputerów ludzie zwykle zdają sobie sprawę z niebezpieczeństw, na jakie są narażeni i starają się przestrzegać znanych im zasad bezpieczeństwa (np. chronią komputer hasłem, nie klikają w linki umieszczone w wiadomościach e-mail, nie otwierają załączników od nieznanych nadawców itp.). Z kolei w czasie korzystania ze smartfonów ostrożność użytkowników często jest wyłączona. Wynika to z wieloletniego przyzwyczajenia do beztroskiego korzystania z telefonów, gdzie w zakresie bezpieczeństwa nic szczególnego nie mogło się wydarzyć. Dlatego należy pamiętać, że smartfony to komputery, a nie telefony⁵.



Ryc. 2. Mobilny dowód osobisty (mID)

Źródło: <http://tarnow.in/nadciaga-e-rewolucja-juz-w-przyszlym-roku-dowod-osobisty-zapiszemy-w-smartfonie/> (dostęp: 7.08.2016).

Istotne dla bezpieczeństwa jest też inne zagrożenie. Otóż smartfony mogą zostać zhakowane podczas ładowania ich przy użyciu standardowego przewodu USB podłączonego do komputera. Gdy podłączamy telefon do publicznej stacji ładowania (np. na lotnisku, w pociągu, w kawiarni, galerii handlowej itp.), raczej nie zastanawiamy się, czy

ma to wpływ na bezpieczeństwo naszego urządzenia i przechowywanych w nim danych. W 2014 r. podczas konferencji BLACK HAT przedstawiono koncepcję, zakładającą że telefon komórkowy może zostać zainfekowany szkodliwym oprogramowaniem w wyniku podłączenia go do fałszywej stacji ładowania. Teraz, po dwóch latach od ogłoszenia tej koncepcji, eksperci z firmy Kaspersky Lab odtworzyli eksperyment bez korzystania ze specjalistycznej wiedzy czy narzędzi. Przy użyciu jedynie zwykłego komputera PC oraz standardowego kabla USB i wyposażeni w zestaw poleceń (dostępnych w Internecie) zdołali ukradkiem zainstalować w smartfonie aplikację. Oznacza to włamanie się do smartfona bez wykorzystania do tego celu szkodliwego oprogramowania. Eksperyment badaczy z Kaspersky Lab w 2016 r. dotyczył bezpieczeństwa danych i prywatności posiadaczy smartfonów. W ramach doświadczenia eksperci przetestowali wiele tych urządzeń działających pod różnymi wersjami systemów Android oraz iOS, aby dowiedzieć się, jakie dane urządzenie przesyła na zewnątrz, kiedy jest podłączone do komputera PC lub Mac w celu naładowania baterii. Wyniki testów pokazały, że urządzenia mobilne ujawniają komputerowi cały zestaw danych podczas tzw. uścisku dłoni (procesu „przywitania się” pomiędzy urządzeniem a komputerem PC/Mac, do którego jest podłączone) obejmujących: nazwę urządzenia, dane producenta, typ, numer seryjny, informacje dotyczące oprogramowania układowego (tzw. firmware), systemu operacyjnego, systemu plików, listę plików oraz identyfikator procesora. Ilość danych wysłanych podczas „uścisku dłoni” różni się w zależności od urządzenia mobilnego oraz komputera, ale każdy smartfon przesyła ten sam podstawowy zestaw informacji, łącznie z nazwą urządzenia, producenta, numerem seryjnym itd. Obecnie, gdy smartfony niemal nieustannie towarzyszą swoim właścicielom, urządzenia te pełnią funkcję unikatowego identyfikatora dla każdej osoby postronnej,

która może być zainteresowana gromadzeniem i późniejszym wykorzystaniem takich danych. Nie byłoby żadnego problemu, gdyby z telefonu podłączonego do nieznanego komputera lub urządzenia ładującego osoba atakująca mogła zebrać jedynie kilka unikatowych identyfikatorów. Należy podkreślić, że incydenty, w których dokonano kradzieży danych z urządzeń mobilnych podłączonych do komputera zostały odnotowane już w 2013 r., w ramach kampanii cyberszpiegowskiej pod kryptonimem CZERWONY PAŹDZIERNIK. Również ugrupowanie Hacking Team wykorzystало połączenie z komputerem w celu zainfekowania urządzeń mobilnych szkodliwym oprogramowaniem. Grupy cyberprzestępcze znalazły więc sposób, aby wykorzystać rzekomo bezpieczną wymianę danych pomiędzy smartfonem a komputerem PC, do którego był on podłączony. Sprawdzając dane identyfikacyjne uzyskane z podłączonego urządzenia, atakujący zdołali zidentyfikować, jaki model urządzenia wykorzystywała ofiara, oraz przeprowadzić swój atak przy użyciu określonego szkodliwego kodu. Nie byłoby to tak łatwe do wykonania, gdyby smartfony nie wymieniały automatycznie danych z komputerem PC po połączeniu się z portem USB⁶. Zagrożenie jest więc oczywiste. Regularny użytkownik smartfona może być śledzony za pośrednictwem identyfikatora urządzenia, na którym ukradkiem zainstalowano różne szkodliwe programy.

Warto przypomnieć, że większość ludzi przechowuje na swoich urządzeniach mobilnych ważne poufne informacje, łącznie z hasłami, zdjęciami, kontaktami, plikami i innymi danymi. W wielu przypadkach jest to jedyna kopia tych informacji. Jeden na czterech użytkowników twierdzi, że na jego smartfonie znajdują się informacje, których nigdy nie powinien zobaczyć nikt inny. Co więcej, Europejczycy nie rozstają się ze swoimi smartfonami i korzystają z nich niemal wszędzie: w pracy (50%), w samochodzie (38%), w transporcie publicznym (45%), w łóżku

(55%), a nawet w łazience (30%). Poza domem urządzenia te są narażone na szereg zagrożeń, takich jak uszkodzenie mechaniczne, zgubienie lub kradzież. Mogą one także paść ofiarą szkodliwych programów, przy użyciu których cyberprzestępcy kradną dane, a nawet szpiegują użytkowników za pośrednictwem wbudowanej kamery i mikrofonu. Szczególnie zagrożone są urządzenia wykorzystywane do uzyskiwania dostępu do Internetu poprzez otwarte sieci Wi-Fi. Niestety, niewielu użytkowników wykonuje jakiegokolwiek kroki, by zmniejszyć ryzyko. Zaledwie 18% Europejczyków dostosowuje swoje zachowanie online do faktu, że korzysta z niechronionej, publicznej sieci Wi-Fi, mimo że komunikacja może zostać przechwycona przez cyberprzestępców. Co więcej, tylko 45% użytkowników korzysta z funkcji bezpieczeństwa wbudowanych w smartfony, takich jak zdalne blokowanie i odnajdywanie. Skutki pozostawiania urządzeń mobilnych bez ochrony mogą być bardzo poważne. Zgodnie z wynikami badania jedna czwarta osób, których smartfon został zgubiony lub skradziony, potwierdza, że doszło do wycieku ich poufnych informacji. Podczas przebywania w domu użytkownicy są narażeni na inny rodzaj zagrożeń, szczególnie w takich miejscach jak sypialnie i łazienki. W rękach cyberprzestępcy zhakowany smartfon może zamienić się w urządzenie szpiegowskie, a wbudowana kamera i mikrofon mogą pozwolić na podglądanie i podsłuchiwanie nieświadomego całej sytuacji użytkownika. Ignorancja lub nadmierne zaufanie, jakimi użytkownicy obdarzają swoje urządzenia mobilne, mogą prowadzić do zaniedbań w zakresie bezpieczeństwa. Trudno sobie wyobrazić, że telefon, który prawie bez przerwy mamy przy sobie i którego używamy przez większość dnia do rozmaitych zadań, może stać się jakimkolwiek zagrożeniem. Niestety, cyfrowy przyjaciel może zostać cyfrowym wrogiem. Niedostrzeżenie potencjalnych zagrożeń oraz potrzeby stosowania ochrony

sprzętu i danych niejednokrotnie prowadzi do utraty poufnych informacji, pieniędzy, a nawet do kradzieży tożsamości. Kamera smartfona, której używamy do uwieczniania naszych wspomnień, może stać się narzędziem służącym do szpiegowania nas⁷.

Dlatego też specjaliści od bezpieczeństwa publikują statystyki, które mają wyculić nas na zagrożenia. Firma Symantec opublikowała raport, z którego wynika, że 27% Polaków (37% Europejczyków) nie potrafiłaby rozstać się ze swoim smartfonem. Jest on oknem na świat, ale też łakomym kąskiem dla cyberprzestępców, którym zależy na danych – nie tylko naszych. Ośmiu na dziesięciu posiadaczy smartfonów z Polski zadeklarowało, że na urządzeniu ma dostęp do poufnych informacji lub nawet zapisuje je na nim. 32% ankietowanych nie stosuje hasła do zabezpieczenia smartfona, więc złodziej może spokojnie przeglądać pocztę i logować się na konta w różnych serwisach (18% ankietowanych przechowuje hasła na urządzeniu) oraz dzwonić do naszych znajomych. Kradzieże sprzętu nie są czymś niespotykanym. W Polsce smartfona lub tablet straciło tak lub zgubiło 27% biorących udział w badaniu (w raporcie nie było danych na temat negatywnych konsekwencji tych kradzieży wynikających z przejęcia umieszczonych na urządzeniach informacji). Wiadomo jednak, czego najbardziej boją się Polacy – wysokich rachunków (56%). Niepożądanego kontaktu z osobami z książki telefonicznej obawia się 35% Polaków, tyle samo, co utraty pieniędzy (na przykład wydanych na zakupy w sieci). Warto tu zaznaczyć, że obywatele naszego kraju entuzjastycznie podchodzą do robienia zakupów ze smartfonu – bezpiecznie czuje się z tym 13% Niemców i 15% Rosjan, ale aż 32% Polaków. Udostępnienie raportu zbiegło się w czasie z publikacją komentarza Wojciecha Wiewiórowskiego, do 2014 r. generalnego inspektora ochrony danych osobowych (obecnie zastępcy europejskiego inspektora ochrony danych), w sprawie danych osobowych przechowywanych właśnie na różnych urządzeniach mobilnych. Przestrzegął on: *Nieodpowiedzial-*

ne korzystanie ze smartfonów i tabletów niesie za sobą zagrożenie dla przechowywanych tam danych osobowych – nie tylko samego właściciela urządzenia, ale także wszystkich osób, o których informacje są zapisane np. w książce adresowej. Oficjalnie „darmowe” aplikacje też często służą pozyskaniu informacji z telefonu. Zdaniem W. Wiewiórowskiego za aplikacje bardzo często płacimy walutą, jaką stanowią informacje, gdyż internauci nie czytają warunków użytkowania i w pośpiechu zgadzają się na przekazywanie danych osobowych. Podobnie ma się sprawa w przypadku synchronizacji danych z chmurą – do dostawcy trafiają kontakty, dokumenty, hasła. Inspektor podał ciekawy przykład tego, jak można łatwo przekazać dane osobowe w niepowołane ręce: Chcąc zsynchronizować muzykę, do której mamy dostęp przy pomocy iPada, z komputerem samochodowym, jednocześnie dajemy dostęp do naszego kalendarza, zbioru naszych adresów kontaktowych, a także adresów naszych klientów i informacji o nich. Informacje te uzyska każdy serwisant firmy, od której kupiliśmy samochód. Przy pomocy tego samego łącza będzie mieć dostęp do informacji, która jest przekazywana przez komputer na temat samochodu, ale i informacji z naszego iPada⁸. Aż strach sobie wyobrazić, co się stanie, gdy w smartfonie znajdą się nasze dokumenty osobiste.

Wykonywanie połączeń telefonicznych jest tylko jedną z wielu funkcji smartfonów. Pod względem bezpieczeństwa wymagają one stosowania przez użytkowników zasad ochrony analogicznie jak komputery – i to może być kolejny czynnik przemawiający przeciw odzworowaniu cyfrowemu naszych dokumentów osobistych w smartfonach. W tym miejscu docieramy do problematyki dochodzeniowo-śledczej i prawnej. W projekcie proponowanym przez Ministerstwo Cyfryzacji będziemy mieli do czynienia z dokumentem wirtualnym, a nie elektronicznym, bo te zostały już opracowane przez PWPW. Zawierają czipy lub inne nośniki informacji zwane popularnie biometrią. Falszerze trudnią się podrabianiem i takich dokumentów, ze względu na niewielkie wykorzystanie czytni-

ków biometrycznych, które w Polsce znajdują się przede wszystkim w posiadaniu Straży Granicznej na lotniskach. Inna sprawa, że urzędnicy w wielu instytucjach nie podchodzą z należytą uwagą do okazywanych im przez właścicieli dowodów osobistych. Weryfikacja odnosi się najczęściej do porównania wizerunku na zdjęciu z twarzą posiadacza dokumentu. Kontrola ta jest niekiedy tak pobieżna, że urzędnik nie zwraca większej uwagi na fakt, że legitymująca się osoba na zdjęciu posiada bujny zarost, a w rzeczywistości go nie ma lub odwrotnie (sam tego doświadczyłem). Często samym ubiorem i określonym zachowaniem można wzbudzić zaufanie weryfikującego tożsamość i sprawić, aby uwierzytelnienie naszej osoby stało się pobieżne. Na nic się więc nie zdadzą najlepsze zabezpieczenia dokumentu i używanie najnowszych technik laserowych w tej dziedzinie, skoro najsłabszym ogniwem w procedurze sprawdzenia tożsamości oraz weryfikacji oryginalności dokumentu i tak pozostaje człowiek. Sytuacja pod tym względem może stać się jeszcze bardziej ryzykowna w przypadku mID. Dotąd najwięcej fałszywych dokumentów podczas rutynowej kontroli ich właścicieli wykrywa Straż Graniczna, zarówno paszportów, jak i dowodów osobistych, krajowych i zagranicznych. Na drugim miejscu jest Policja (dowody osobiste, prawa jazdy, dowody rejestracyjne pojazdów). Mimo stosowania przez fałszerzy skomplikowanych metod, funkcjonariusze obu

służb są w stanie wykryć fałszyfikaty, a wątpliwości rozwiewają laboratoria kryminalistyczne. Nie będzie to już takie proste w przypadku dokumentów cyfrowych.

W reklamach, ogłoszeniach i ofertach można przeczytać, że smartfon jest uniwersalnym narzędziem wymiany informacji, które możemy na bieżąco wykorzystywać w codziennym życiu. Wzrasta również jego znaczenie jako urządzenia służącego identyfikacji jego posiadacza oraz dokonywania codziennych transakcji, natomiast technologie wspomagające bezpieczeństwo mID są już pewne, niezawodne i dostępne. Co więcej, mobilny identyfikator zapewnia najwyższy poziom ochrony prywatności. Mobilna technologia wprowadzić nas ma na wyższy poziom życia. Zapewnić nowy poziom kontaktu władz z obywatelami. Jeżeli tak, to również kontroli. Przed wprowadzeniem mobile-ID w Estonii przeprowadzona została analiza bezpieczeństwa pod kątem prawnym, behawioralnym i technicznym (np. awaria komponentów). Wniosek był dla mnie zaskakujący. Ryzyko związane z mID jest takie samo jak ryzyko wykorzystania plastikowego dowodu osobistego. Musi to być zatem kraj uczciwych obywateli, którzy nie fałszują dokumentów, nie starają się podszywać pod cudzą tożsamość i nie dokonują ataków hackerskich. Duże zaufanie do mobilnych technologii identyfikacji wykazują Brytyjczycy i Amerykanie. Brytyjska firma De La Rue, największa na świecie wytwórnia zajmująca się drukiem oficjalnych dokumentów, dokumentów specjalnych oraz papieru z zabezpieczeniami, ogłosiła, że przygotowuje się do odejścia od klasycznych, „papierowych” paszportów i wkrótce zamierza przenieść je na smartfony. Przedstawiciele firmy przyznali, że pomysł jest jeszcze na wczesnym etapie realizacji, a prace nad stworzeniem technologii, która pozwoli na bezpieczne przechowywanie danych na urządzeniach mobilnych dopiero się rozpoczynają. Innowacyjne dokumenty będą również pełnić funkcję elektronicznych kart pokładowych. Z kolei w 2015 roku niektóre porty lotnicze w USA ogłosiły, że będą honorować



Ryc. 3. Skanowanie paszportu przez jego właściciela na lotnisku w Minneapolis w marcu 2012. Dokument został wprowadzony do cyfrowego systemu tożsamości
Źródło: <http://rwelab.forbes.pl/smartfon-zamiast-paszportu-prace-trwaja,artykuly,204640,1,1,1.html> (dostęp: 7.08.2016).

aplikację paszportową na równi z papierowym dokumentem. Osoby, które chciały posługiwać się tą technologiczną nowinką, musiały posiadać ważny – klasyczny – paszport i pobrać aplikację. Prym za oceanem wiecie port lotniczy w Miami, który już przed dwoma laty wprowadził specjalne kioski do mobilnej odprawy paszportowej. Z urządzeniami mobilnymi coraz ściślej współpracują również same lotniska. To w Miami jest pierwszym na świecie, które połączyło swoje terminale ze smartfonami podróżnych. Po ściągnięciu specjalnej aplikacji pasażerowie mogą zapoznać się m.in. z nowymi ofertami lokali gastronomicznych, sklepów czy uzyskać informacje o lotach⁹. Brak jest niestety informacji na temat stopnia niezawodności i bezpieczeństwa tych systemów, a w dobie współczesnych zagrożeń terrorystycznych i migracji ludności z krajów podwyższonego ryzyka jest to niezwykle istotne.

ZAGROŻENIA

Dotychczasowa praktyka dochodzeniowo-sledcza nie pokrywa się z przepisami prawa, w których brakuje jednoznacznej definicji terminu „dokument”, co jest przyczyną nieporozumień i błędnej interpretacji prawa. Sprzyja to fałszerzom i grupom przestępczym. Polskie Towarzystwo Kryminalistyczne podjęło się próby stworzenia jednolitego aktu prawnego o randze ustawy, wnosząc do niego szereg przepisów, których brak jest w obecnym systemie prawnym, w tym m.in. odnoszących się do hierarchii dokumentów oraz technik ich wytwarzania i sposobów zabezpieczania, dystrybucji, przechowywania oraz kontroli ich autentyczności i wiarygodności. Praca ta jest niezwykle pożądana i na czasie. Miałem nadzieję, że po spotkaniu przedstawicieli MSW, PTK i PWPW szybko zostaną sfinalizowane prace nad kompleksową ustawą dotyczącą dokumentów¹⁰.

Tymczasem może być tak, iż inicjatywa Ministerstwa Cyfryzacji zdoła zdystansować, zarówno w sferze legislacyjnej, jak i w kwestii pojawienia się nowego produktu, prace legisla-

cyjne nad „tradycyjnymi” dokumentami. Tylko czy mID na pewno będzie dokumentem w ujęciu semantyki i prawa? Otóż wydaje się, że nie, bowiem dokument cyfrowy (elektroniczny) określić można jako „logicznie spójną porcję informacji przetwarzanej w systemie komputerowym”. Dla karnomaterialnej kwalifikacji tych informacji jako dokumentu konieczne jest, aby stanowiły one dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne. Z punktu widzenia ochrony prawnej udzielanej dokumentowi przez przepisy **KODEKSU KARNEGO** istotne jest jej zapewnienie na każdym etapie: zarówno tworzenia, przechowywania, przesyłania, jak i odbierania. Dokument cyfrowy, będący fizycznie zbiorem bajtów, czyli wartości zerojedynkowych, powinien zatem, tak jak dokument tradycyjny, doznawać ochrony prawnej. Jednak tak nie jest. Ponadto brakuje podstaw do wskazania ratio legis motywującego rozróżnienie dokumentów „tradycyjnych” od cyfrowych. W przypadku „tradycyjnych” nośników informacji zarówno przesyłanie, jak i przechowywanie zmaterializowanych elementów znajduje swoją ochronę. W przypadku nośników elektronicznych nie jest to już takie oczywiste. Trudno jest przy tym znaleźć powód odmiennego traktowania tych dwóch kategorii dokumentów, jako że ryzyko naruszenia autentyczności i integralności dokumentu cyfrowego jest wysokie. Tak więc w przypadku sfalszowania tego ostatniego lub jakiegokolwiek ingerencji w jego treść czyn ten nie będzie mógł być traktowany jako fałsz materialny dokumentu (art. 270 § 1 k.k.), a jedynie jako czynienie szkody w bazie danych (art. 268a k.k.), bądź ewentualnie jako sabotaż komputerowy (art. 269 k.k.). Do takiego wniosku prowadzi bowiem konieczność uznania danych na niezapisanym nośniku informacji tylko jako informacji, co powoduje niespójność w obrębie regulacji prawnej, a także stawia pod znakiem zapytania konieczność rozróżnienia pomiędzy „informacją” a „dokumentem”¹¹.

Moim zdaniem potencjalni fałszerze i oszuści mogą otrzymać nowy instrument do swej przestępczej działalności, a zwalczanie oszustw

tożsamości przy jednoczesnym przestrzeganiu krajowych przepisów rejestracyjnych dowodów osobistych będzie nowym wyzwaniem dla operatorów sieci komórkowej. Do ich obowiązków będą należały m.in. weryfikacja dokumentu tożsamości (autentyczności dokumentu), uwierzytelnianie klienta, czyli uwierzytelnianie posiadacza dokumentu jako jego prawowitego właściciela oraz ocena ryzyka. Problemem już teraz są zmiany przepisów telekomunikacyjnych na całym świecie – coraz częściej operatorzy sieci komórkowych muszą być w stanie określić, kim są ich klienci. Dane użytkowników są rejestrowane przy zakupie nowej karty SIM lub gdy zostaje dodana dodatkowa funkcjonalność do konta bądź urządzenia. Co prawda firma Morpho, reklamująca się jako światowy lider biometrii, oferuje instrumenty do biometrycznej weryfikacji klienta oraz rozwiązywania rejestracyjne i dotyczące tożsamości mobilnej, które umożliwiają rejestrację klientów operatorów sieci komórkowych w celu weryfikacji ich tożsamości, ale – jak każda inna firma – nie jest w stanie zapewnić, że jej produkty są w pełni bezpieczne przed ingerencją z zewnątrz.

Hakerzy mogą tworzyć i rozpowszechniać złośliwe aplikacje, a my nie będziemy w stanie wysledzić ich źródła. Mogą dodawać konie trojańskie i złośliwe kody do istniejących legalnych aplikacji, a następnie ponownie podpisać zaktualizowaną wersję z anonimowym lub fałszywym świadectwem i rozprowadzać je. Pół biedy, gdy są to pojedynczy hackerzy, ale gdy mamy do czynienia z operacjami w cyberprzestrzeni dokonywanymi przez służby specjalne i prowadzeniem w sieci operacji szpiegowskich, sytuacja może być groźna dla bezpieczeństwa państwa i jego obywateli. Grupy cyberszpiegowskie wykorzystywały wcześniej legalne, otwarte narzędzia służące do testów penetracyjnych w połączeniu z własnym szkodliwym oprogramowaniem lub bez niego. Różnica w porównaniu z obecną sytuacją polega na tym, że coraz więcej grup stosuje rozwiązanie Browser Exploitation Framework (BeEF) jako atrakcyjną i skuteczną alternatywę. Należy zastanowić się nad

konsekwencjami ewentualnej ingerencji w system mobilnych dokumentów przez obce służby specjalne. Szkody mogą być poważne, a koszty jeszcze większe, nie mówiąc o spadku zaufania obywateli do państwa. Przykładów mamy już wiele. Najbardziej znaczący – z lipca 2016 r. w USA, kiedy tuż przed konwencją wyborczą demokratów w Filadelfii, gdzie Hillary Clinton została oficjalnie potwierdzona jako kandydatka partii na prezydenta, słynny portal Wikileaks opublikował ok. 20 tysięcy e-maili Partii Demokratycznej. Przecieki wywołały wielkie poruszenie wśród wyborców, ponieważ opublikowane dokumenty miały świadczyć o nieuczciwie prowadzonej kampanii Hillary Clinton i o nagiñaniu zasad na potrzeby zwycięstwa wyborczego. Celem ujawnienia tych dokumentów było uderzenie w kandydatkę demokratów i doprowadzenie do podziału w partii. Okazało się, że e-maile zostały wykradzione przez rosyjskich hackerów, którzy niespecjalnie starali się ukryć swoje pochodzenie, pozostawiając wyraźne ślady jednoznacznie wskazujące na to, że źródłem ataku jest grupa powiązana z rosyjską służbą wywiadu wojskowego (GRU)¹². Ten ostatni cyberatak, wpływający na politykę USA, był wydarzeniem bez precedensu, zwiększającym szanse wyborcze Donalda Trumpa, faworyta Moskwy. Nietrudno wyobrazić sobie w przyszłości skutki takiego cyberataku na aplikacje z mobilnymi dokumentami i próby wprowadzania w nich zmian tożsamości wybranych lub przypadkowych osób.

Nowoczesne technologie skutecznie wykorzystują również terroryści. Można powiedzieć, że nie byłoby Państwa Islamskiego, gdyby nie high technology. Postęp techniczny i globalizacja naznaczyły również sam islam, który stara się zwalczać współczesnych „niewiernych” nie tylko tradycyjnymi metodami walki, takimi jak zamachy terrorystyczne na szeroką skalę czy ataki w wykonaniu „samotnych wilków”, ale także własną bronią Zachodu – technologią i mediami. Spór islamu z Zachodem wyzwolił wiele sił destrukcyjnych i wyposażył je w możliwości operacyjne i techniczne niezbędne

do podjęcia walki. Państwo Islamskie i inne organizacje ekstremistyczne sprawnie posługują się siecią nowoczesnych środków komunikacji i wykorzystują je jako narzędzie do pozyskiwania rzesz zwolenników oraz rekrutacji wojowników poza jakąkolwiek kontrolą. Większość ludzi, zwłaszcza młodych, ulega tym samym dominującym trendom w modzie i fascynuje się tą samą światową technologią. Dlatego też każda nowinka technologiczna jest przez fachowców ulokowanych w środowiskach islamskich ekstremistów (a wielu z nich to niezwykle utalentowani absolwenci najlepszych uczelni na świecie) skrzętnie badana i analizowana pod kątem możliwości jej wykorzystania w starciu z niewiernymi. Zgodnie z zasadą, że wszystkie formy walki, włączając w to oszustwa i fałszerstwa, są dopuszczalne, wręcz konieczne dla zwycięstwa islamu.

Z tego powodu trudno założyć, że cyfryzacja dokumentów nie pociągnie za sobą poważnego ryzyka i prób przejmowania dokumentów

ze smartfonów. Potem już wystarczy taki dokument wykorzystać, sfalszować, wykonać z niego „oryginał” na karcie plastikowej lub dokonać jego cyfryzacji. Zastosowanie przez dżihadystów w toczącej się walce z „niewiernymi” nowoczesnej broni, technologii i posługiwanie się zachodnią myślą technologiczną przynosi i przyniesie jeszcze wiele szkód i strat, a jej przebieg będzie dla nas bardzo bolesny. Trzeba bowiem pamiętać, że etap obecnej walki to bitwy, starcia i potyczki oraz akty barbarzyńskie, pełne okrucieństwa, aby celowo sparaliżować przeciwnika strachem. Jednak główny atak jest cichy. Islamskie Państwo Kalifatu to nie tylko polityczny twór ujęty w granicach części Syrii i Iraku, ale także idea i stan ducha radykalizowanych muzułmanów, które przetrwają w ich świadomości nawet po odbiciu zajmowanych przez nich terytoriów. Wielu z nich oraz ich jawnych i ukrytych sympatyków jest obywatelami różnych państw Europy, dla których cyfrowe dokumenty mogą być cennym narzędziem prowadzącym ich do celu.

¹[IAR, awi] Anna Streżyńska: e-dowody w komórkach w przyszłym roku, <http://www.polskieradio.pl/42/273/Artykul/1632448,Anna-Strezynska-edowody-w-komorkach-w-przyszlym-roku> (dostęp: 4.08.2016).

²M. Tomaszewicz, Dowód osobisty będzie aplikacją na smartfona, <http://www.antyradio.pl/Technologia/Mobile/Dowod-osobisty-bedzie-aplikacja-na-smartfona-9214> (dostęp: 4.08.2016).

³S. Zadrozna, Czekaj nas e-rewolucja. Dowód osobisty zapiszemy w smartfonie, <http://www.polskieradio.pl/42/273/Artykul/1634138,Czekaj-nas-erewolucja-Dowod-osobisty-zapiszemy-w-smartfonie> (dostęp: 4.08.2016).

⁴W dniu 28 lipca 2016 r. weszły w życie przepisy ustawy antyterrorystycznej, zgodnie z którymi karty SIM prepaid na telefony komórkowe będzie można kupić legitymując się dowodem osobistym, a w przypadku cudzoziemców spoza Unii Europejskiej – paszportem lub kartą pobytu. Operatorzy usług komórkowych będą weryfikować tożsamość kupujących.

⁵M. Stawowski, Bezpieczeństwo: (Nie)bezpieczne smartfony – czy technologia zabezpieczeń jest gotowa na nowe zagrożenia?, http://www.alebank.pl/index.php?option=com_content&view=article&id=15407:bezpieczenstwo-niebezpieczne-smartfony-czy-technologia-zabezpiecze-jest-gotowa-na-nowe-zagrozenia&catid=573:bank-201205&Itemid=265&Itemid=105&Itemid=105 (dostęp: 4.08.2016).

⁶[Interia Mobtech], Podczas ładowania telefonu przestępcy mogą wykraść nasze dane, <http://mobtech.interia.pl/porady/news-podczas-ladowania-telefonu-przestepcy-moga-wykrasc-nasze-dane,nld,2209486> (dostęp: 4.08.2016).

⁷[Kaspersky Lab], Od cyfrowego przyjaciela do wroga: użytkownicy nie mogą się rozstać ze swoimi smartfonami, <http://www.kaspersky.pl/nawosci/wiadomosci-prasowe/2578/od-cyfrowego-przyjaciela-do-wrogaciela-uzytkownicy-nie-moga-sie-rozstac-ze-swoimi-smartfonami> (dostęp: 4.08.2016).

⁸[Newseria], GIDODO: smartfony i tablety stwarzają zagrożenie dla bezpieczeństwa danych osobowych, http://www.info.newseria.pl/news/gidodo_smartfony_i_tablety,p820197614 (dostęp: 4.08.2016).

⁹[tt], Smartfon zamiast paszportu? Prace trwają, <http://rwelab.forbes.pl/smartfon-zamiast-paszportu-prace-trwaja,artykuly,204640,1,1.html> (dostęp: 4.08.2016).

¹⁰Osoby zainteresowane tą problematyką odsyłam do artykułu dr hab. Mieczysława Goca pt. Ustawa o dokumentach potrzebna od zaraz, „Człowiek i Dokumenty” 2016, nr 41.

¹¹P. Ochman, Spór o pojęcie dokumentu w prawie karnym, <http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2009/01/Zochman.pdf> (dostęp: 4.08.2016).

¹²O. Górzyński, Hillary Clinton na celowniku Rosjan. Kreml dąży do prezydentury dla Trumpa, <http://wiadomosci.wp.pl/kat,1356,title,Hillary-Clinton-na-celowniku-Rosjan-Kreml-dazy-do-prezydentury-dla-Trumpawid,18440544,wiadomosc.html> (dostęp: 4.08.2016).

Michał Kraszewski-Cąkała, Tomasz Goliński, Piotr Życki,
Mieczysław Szustakowski

BIOMETRIA MOBILNA – NOWOCZESNA KONTROLA GRANICZNA

Rosnący przepływ ludzi pomiędzy krajami wymusza konieczność elastycznego dostosowywania możliwości kontroli dokumentów do natężenia ruchu na przejściu granicznym. Nowoczesnym rozwiązaniem umożliwiającym takie połączenie jest zaprojektowany w Polsce system BIOMET.



Przejścia graniczne to wyznaczone miejsca na granicy państwa przeznaczone do jej przekroczenia na podstawie paszportów oraz innych uprawniających do tego dokumentów. Przekraczanie granicy wiąże się nieodwrotnie z przeprowadzaniem kontroli granicznej. Biorąc pod uwagę rosnącą z roku na rok liczbę osób przekraczających granicę, zrozumiałe jest, że obciążenia punktów kontrolnych stają się coraz większe. Wyjątkowymi przypadkami wśród przejść granicznych są punkty kontroli drogowej oraz kolejowej. Są one szczególnie wrażliwe na zachwianie przepustowości z uwagi na nagły wzrost natężenia przepływu podróżnych. Niesie to za sobą ryzyko niezachowania bezpiecznej drożności przejścia granicznego. Bezpiecznej – to znaczy takiej, która gwarantuje skuteczną kontrolę pojazdów, towarów i przede wszystkim podróżnych, przy zachowaniu rozsądnego czasu kontroli. Tylko w takim przypadku przejście graniczne wraz z przeprowadzanymi kontrolami granicznymi skutecznie spełnia swoją funkcję w całym systemie związanym z ochroną i bezpieczeństwem granic.

ICAO I STRATEGIA TRIP

Zapewnienie bezpieczeństwa podróży międzynarodowych w dużym stopniu zależy od właściwego zarządzania identyfikacją podróżnych. Już jakiś czas temu zwróciła na to uwagę Organizacja Międzynarodowe-

go Lotnictwa Cywilnego (International Civil Aviation Organisation, ICAO) wyznaczająca w skali globalnej standardy i rekomendacje w zakresie bezpieczeństwa lotnictwa cywilnego. Znalazło to odzwierciedlenie w jej podejściu do dokumentów podróży. Od lat 80. XX w. ICAO zalecała stosowanie czytanych maszynowo dokumentów podróży (Machine Readable Travel Documents, MRTDs) co wpłynęło także na standaryzację i podniesienie poziomu zabezpieczenia paszportów. Opracowywano dla nich kolejne wersje specyfikacji, co ostatecznie zaowocowało wprowadzeniem paszportów biometrycznych. Od 2013 roku ICAO nie mówi już jednak tylko o samym zabezpieczeniu dokumentów podróży, lecz o stosowaniu holistycznego podejścia do całości procesu zarządzania identyfikacją podróżnych, tzw. strategii TRIP (Travellers Identification Programme)¹. Podejście to zostało zilustrowane na ryc. 1.

Potrzeba skoncentrowania się nie tylko na dokumentach podróży, lecz na bezpieczeństwie całego procesu identyfikacji podróżnego pojawiła się m.in. w wyniku stałego wzrostu intensywności ruchu lotniczego i liczby przewożonych pasażerów – przy konieczności zapewnienia nie mniej efektywnej kontroli granicznej. Jednocześnie trzeba wziąć pod uwagę, że podróżni zawsze oczekują szybkiej i sprawnej kontroli prowadzonej w humanitarnych warunkach, przestępcy zaś, wobec wysokiego stopnia

MICHAŁ KRASZEWSKI-CĄKAŁA – absolwent Politechniki Warszawskiej. Ukończył studia magistersko-inżynierskie na wydziale inżynierii produkcji a następnie studia podyplomowe o specjalności Informatyczne Systemy Zarządzania w Szkole Głównej Handlowej oraz studia podyplomowe na Politechnice Warszawskiej w zakresie Prowadzenia Projektów IT. W PWPW od 13 lat, obecnie w zakresie jego kompetencji leży nadzór i prowadzenie projektów.



Ryc. 1. Holistyczne zarządzanie identyfikacją podróżnych
Źródło: Proposal for an ICAO Traveller Identification Programme (ICAO TRIP) Strategy, materiał roboczy A-38-WP/11 EX/6 17/05/13 na 38. sesję Zgromadzenia ICAO, 2013.

zabezpieczenia dokumentów podróży, zaczęli szukać innych słabych punktów w całym procesie identyfikacji, których wykorzystanie umożliwiłoby nielegalne przekroczenie granicy. Trzeba pamiętać, że to przestępstwo jest często związane z innymi, np. terroryzmem, nielegalną migracją, handlem ludźmi i wykorzystywaniem nieletnich.

Według ICAO proces identyfikacji podróżnych opiera się na pięciu elementach. Są to:

1. dowodzenie tożsamości (Evidence of Identity),
2. maszynowo czytane dokumenty podróży (MRTD),
3. wydawanie dokumentów i kontrola tego podprocesu (Document Issuance and Control),
4. systemy i narzędzia inspekcyjne (Inspection systems and tools),
5. interoperacyjne aplikacje (Interoperable applications).

Z punktu widzenia niniejszego artykułu najbardziej interesującym elementem są systemy i narzędzia inspekcyjne, które służą do bezpiecznego i efektywnego odczytu oraz weryfikacji maszynowo czytanych dokumentów podróży i danych biometrycznych. Jest

oczywiste, że samo, nawet najlepsze, zabezpieczenie dokumentów nic nie da, jeżeli osoby weryfikujące ich autentyczność nie będą posiadały odpowiedniej wiedzy oraz systemów i narzędzi umożliwiających im prawidłowe wykonanie tego zadania.

PRZEKRACZANIE GRANICY LĄDOWEJ NA PRZYKŁADZIE POLSKIEGO ODCINKA GRANICY UE

Warto zauważyć, iż pomimo tego, że ICAO zajmuje się podróżami lotniczymi, to jej podejście do identyfikacji podróżnych można zastosować we wszystkich rodzajach podróży. Odpowiednim wyposażeniem powinni dysponować funkcjonariusze nie tylko na lotniskach, ale na wszystkich granicach – także lądowych. W przypadku Polski mają one bardzo duże znaczenie, gdyż znaczna część jej granicy (963 km) stanowi zewnętrzną granicę lądową Unii Europejskiej. Ze zrozumiałych względów musi ona być bardzo dobrze chroniona, a jednocześnie przekraczana jest przez bardzo dużą liczbę podróżnych. W trzecim kwartale 2015 roku liczba przekroczeń granicy Polski (76,7mln)² – czyli w ciągu trzech miesięcy przeprowadzono prawie 10 mln kontroli.

Granica lądowa może być przekraczana w różny sposób: pieszo, samochodem, motocyklem, rowerem, autokarem bądź koleją. Praktycznie we wszystkich tych przypadkach funkcjonariusz Straży Granicznej dokonujący odprawy musi być mobilny i stąd konieczność wyposażenia go w mobilne środki łączności i przenośne czytniki, które umożliwią wszechstronną weryfikację dokumentów. Problem staje się jeszcze bardziej złożony, jeżeli funkcjonariusz ma wykorzystywać cały potencjał biometrycznych dokumentów podróży i dokonać ich pełnej weryfikacji, włączając w to odczyt i kontrolę warstwy elektronicznej oraz odczyt danych biometrycznych podróżnego. Jest to nie lada wyzwanie – w mobilnym wyposażeniu trzeba zmieścić większość funkcji bramki ABC do automa-

tycznej kontroli granicznej. Waga sprzętu powinna być akceptowalna dla funkcjonariusza a zasilanie musi pozwalać na autonomiczną pracę przez długi czas. Urządzenie powinno także mieć zdalny dostęp do baz danych i certyfikatów podpisu elektronicznego wymaganych przy weryfikacji dokumentów biometrycznych.

PROJEKT BIOMET

Chociaż zarysowane wyżej zadanie nie jest łatwe, konsorcjum naukowo-przemysłowe w składzie: Wojskowa Akademia Techniczna w Warszawie (WAT), reprezentowana przez prof. dr. hab. inż. Mieczysława Szustakowskiego, jako lider projektu, Przedsiębiorstwo Badawczo-Produkcyjne OPTEL sp. z o.o., MLabs sp. z o.o. oraz Polska Wytwórnia Papierów Wartościowych S.A. w Warszawie (PWPW) rozpoczęło w 2014 roku projekt badawczo-rozwojowy pod nazwą BIOMET. Projekt jest w większości finansowany ze środków Narodowego Centrum Badań i Rozwoju w Warszawie, a jego celem jest stworzenie prototypu rozwiązania dla mobilnej kontroli granicznej, tj. przenośnego systemu do weryfikacji osób przekraczających zewnętrzną granicę Unii Europejskiej i ich dokumentów. Pokłosiem tego projektu będzie możliwość zastosowania nowoczesnego systemu do przeprowadzania kontroli mobilnej na granicach europejskich oraz w innych częściach świata.

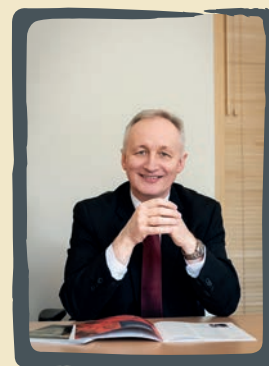
PWPW jest w Polsce jedynym podmiotem produkującym blankiety dowodów osobistych i paszportów biometrycznych. Na potrzeby dostarczanych produktów PWPW realizuje także projekty IT wspierające systemy paszportowo-dowodowe. W tym przypadku rozwiązania zastosowane w projekcie przez PWPW, a także dostarczone oraz wdrożone przez pozostałych konsorcjantów naturalnie wpisują się w strategię wprowadzania na rynek innowacyjnych produktów. We wszystkich obszarach produkty PWPW cechują się najwyższą jakością, zastosowaniem naj-

lepszych na rynku zabezpieczeń, innowacyjnością rozwiązań opracowanych przez doświadczonych ekspertów przy wykorzystaniu zaplecza badawczo-rozwojowego. Paszporty biometryczne produkowane przez PWPW S.A. należą do najnowocześniejszych tego typu dokumentów na świecie. Poza tradycyjnymi zabezpieczeniami użytymi podczas produkcji dokumenty dostosowane są do elektronicznego zapisu, przechowywania i odczytu pierwszej oraz drugiej cechy biometrycznej, tj. zdjęcia i odcisków palców osoby, na którą wystawiony jest paszport. System BIOMET pozwala na pełne wykorzystanie potencjału paszportu biometrycznego w warunkach mobilnych.

Projekt BIOMET obejmuje wykonanie demonstratora, tj. działającego prototypu systemu przy jednoczesnym założeniu pewnych ograniczeń. PWPW, będąc naturalnym partnerem przy realizacji projektów dotyczących dokumentów tożsamości i podróży, aktywnie uczestniczy w projekcie. Za jego realizację odpowiadają również pozostałe podmioty w konsorcjum: wyższa uczelnia techniczna – WAT jako lider oraz dwie polskie firmy komercyjne – MLabs i OPTEL. Wynik projektu umożliwia mobilne wykonanie pełnej odprawy granicznej, np. w przedziale pociągu, w autobusie lub na zielonej granicy. To rozwiązanie znacząco poprawia możliwości wykonania pracy w nietypowych warunkach przez Straż Graniczną, która pełni rolę gestora w projekcie.

Projekt realizowany jest etapowo, jego poszczególne fazy przedstawiają się następująco:

- Etap I – koncepcja i zaprojektowanie całego rozwiązania
- Etap II – implementacja i testy w warunkach laboratoryjnych
- Etap III (obecnie realizowany) – uwzględnienie uwag wynikających z testów laboratoryjnych i przeprowadzenie docelowych testów w warunkach rzeczywistych (tj. na przejściach granicznych), przeprowadzenie szkoleń użytkowników oraz przygotowanie dokumentacji. W tym eta-

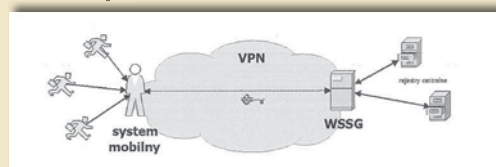


TOMASZ GOLIŃSKI – absolwent Wydziału Elektroniki Politechniki Warszawskiej oraz studiów MBA Uniwersytetu Gdańskiego. W PWPW S.A. pracował w latach 1990–2016 na różnych stanowiskach związanych głównie z badaniami i rozwojem. Jest członkiem Komitetu Ekspertów Federacji INTERGRAF.

pie PWPW odgrywa wiodącą rolę w zakresie przeprowadzenia testów z udziałem konsorcjantów. Przeprowadza testy integracyjne polegające m.in. na sprawdzeniu współpracy wszystkich elementów oraz przygotowuje dokumentację, w tym scenariusze testów. Dodatkowo każdy konsorcjant dostosowuje i sprawdza poszczególne elementy systemu, za które jest odpowiedzialny.

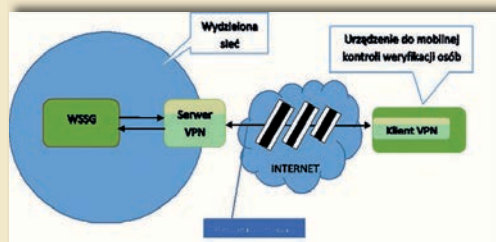
Przewidywana data zakończenia przypadku na III kwartał 2016 roku.

Cała infrastruktura systemu BIOMET (ryc. 2) składa się z:



Ryc. 2. Schemat poglądowy całego rozwiązania projektu BIOMET

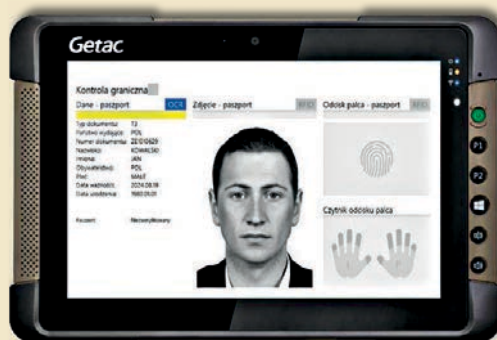
1. mobilnego zestawu, w którego skład wchodzi m.in. moduł integracyjny, tablet stanowiący interfejs graficzny dla operatora wraz z urządzeniami biometrycznymi oraz peryferyjnymi,
2. Wzorcowego Systemu Straży Granicznej (WSSG) zaprojektowanego i wykonanego przez PWPW, który stanowi element centralny (tzw. serce systemu) spełniający głównie funkcje serwera podpisu na potrzeby odczytu drugiej cechy biometrycznej z paszportu oraz interfejsu do systemów zewnętrznych. Dodatkowo pełni on funkcję administracyjno-zarządczą dla całego systemu (zarządzanie certyfikatami, baza danych),



Ryc. 3. Schemat poglądowy obrazujący bezpieczną łączność w systemie BIOMET

3. modułów zapewnienia bezpiecznej szyfrowanej łączności pomiędzy powyższymi elementami wraz z dedykowanymi kartami mikroprocesorowymi (ryc. 3).

Elementem systemu, z którym operator ma bezpośredni oraz najczęstszy kontakt podczas kontroli, jest tablet (ryc. 4), który



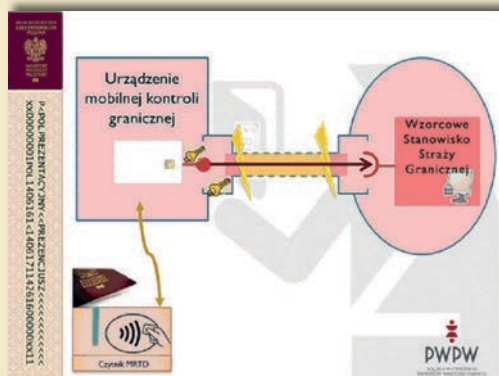
Ryc. 4. Ekran tabletu widoczny dla operatora (dostarczony przez firmę MLabs)

z kolei jest zintegrowany z pozostałymi urządzeniami wchodzącymi w skład zestawu mobilnego. Na wszystkich tych urządzeniach zainstalowane jest dedykowane oprogramowanie³ sterujące całym zestawem i realizujące komunikację z poszczególnymi elementami. W skład zestawu oprócz tabletu wchodzi m.in.:

- czytnik dokumentów do pobierania danych z pola odczytu maszynowego (MRZ) z paszportu oraz odczytania zawartości mikroprocesora paszportowego,
- czytnik odcisków palców do pobrania na żywo odcisków od osoby przekraczającej granicę,
- układ zasilania o wysokiej efektywności energetycznej,
- moduł centralny integrujący wszystkie elementy zestawu mobilnego⁴.

Zestaw mobilny wykorzystuje dodatkowo zaimplementowanego klienta VPN, tj. oprogramowanie do zestawienia oraz utrzymania bezpiecznej, szyfrowanej łączności z WSSG (ryc. 5).

Niewątpliwie ogromną zaletą systemu mobilnego jest możliwość ciągłej pracy przez około 8 godzin. Gwarantuje to układ zasilania o wysokiej efektywności energetycznej,



Ryc. 5. Schemat ilustrujący koncepcję zabezpieczeń w systemie BIOMET

do którego podłączony jest tablet wraz z pozostałymi urządzeniami mobilnymi. Dodatkowo stworzono oraz zaimplementowano algorytm optymalnego zarządzania energią. Układ dostosowany jest do prac w różnych warunkach atmosferycznych.

Proces biznesowy dla systemu BIOMET obejmuje następujące etapy:

1. przyjęcie dokumentu paszportowego od osoby przekraczającej granicę,
2. odczytanie pola MRZ dokumentu paszportowego i odczyt zawartości mikroprocesora,
3. pobranie odcisku palca tej osoby w celu weryfikacji zgodności biometrycznej,
4. przekazanie odczytanych danych poprzez system bezpiecznej łączności do serwera WSSG,
5. odpytanie przez WSSG zewnętrznych rejestrów o informacje na temat osoby, której dotyczy zapytanie wysłane z systemu mobilnego,
6. odesłanie przez WSSG odpowiedzi do zestawu mobilnego,
7. interpretacja danych przez zestaw mobilny (pozwolenie na przejście danej osoby lub jej zatrzymanie).

Nowoczesność systemu wynika z wykorzystania innowacyjnych rozwiązań oraz zalet związanych z bezpośrednim użytkowaniem, tj.:

- możliwości odczytu z paszportów drugiej cechy biometrycznej, zgodnie z me-



Ryc. 6. Karta SmartApp-CRYPTO 3.0 produkcji PWPW S.A.

chanizmem EAC, oraz jej weryfikacji w warunkach mobilnych,

- zastosowania mobilnego czytnika odcisków palców,
- zapewnienia bezpiecznej szyfrowanej łączności bezprzewodowej pomiędzy urządzeniem mobilnym a WSSG (z użyciem certyfikatów X.509),
- komfortu użytkowania dla operatora – waga kamizelki to tylko około 6 kg,
- energooszczędności – ponad 8 godzin autonomicznej pracy,
- zastosowania nowoczesnych kart mikroprocesorowych SmartApp-CRYPTO 3.0 produkcji PWPW, zgodnych ze standardem GIDS.

PWPW opracowała własne aplety – PWPW SmartApp®. Produkty te są wykorzystywane w kartach i dokumentach elektronicznych, takich jak paszporty biometryczne, elektroniczne dowody osobiste, legitymacje oraz karty kryptograficzne. Rozwiązania PWPW SmartApp® składają się ze specjalistycznego oprogramowania (tzw. apletu) opracowanego przez programistów PWPW, systemu operacyjnego oraz specjalnego mikroprocesora dedykowanego dla zastosowań wymagających dużego poziomu bezpieczeństwa.

Jednym z produktów z rodziny PWPW SmartApp® jest SmartApp-CRYPTO przeznaczony do zastosowań kryptograficznych, takich jak podpis elektroniczny, szyfrowanie danych oraz uwierzytelnienie w systemach informatycznych. Produkty te mogą być



PIOTR ŻYCKI – absolwent Uniwersytetu Gdańskiego, Akademii Wychowania Fizycznego i Sportu w Gdańsku oraz Akademii Leona Koźmińskiego w Warszawie. Przez ponad 6 lat związany z branżą weryfikacyjną jako Dyrektor odpowiedzialny za realizację kontraktów w Polsce, Europie Wschodniej oraz Azji. Obecnie Product Manager w PWPW.

wykorzystane w kartach kryptograficznych, legitymacjach i kartach korporacyjnych. Najnowszy produkt PWPW SmartApp-CRYPTO 3.0 poza wymienionymi funkcjonalnościami pozwala również na bezpieczne przechowywanie danych użytkownika w specjalnym systemie plików oraz obsługuje technologię MIFARE, dedykowaną dla kart miejskich oraz kart dostępowych.

KARTY PWPW SMARTAPP-CRYPTO 3.0

Karty płynnie integrują się z systemem operacyjnym Windows i są od razu widoczne po włożeniu ich do czytnika. Nie jest wymagana żadna pośrednia biblioteka ani dodatkowe oprogramowanie zewnętrzne, tzw. middleware. Priorytet: wygoda użytkownika.

Kluczowe funkcjonalności:

- podpis elektroniczny,
- szyfrowanie danych,
- szyfrowanie i podpisywanie poczty elektronicznej,
- uwierzytelnienie użytkownika w serwisach internetowych SSL/TLS,
- logowanie do domeny Windows na podstawie certyfikatów X.509,
- bezpieczne przechowywanie danych na karcie.

Zastosowania:

- legitymacje służbowe,
- karty kryptograficzne,
- karty dostępowe do systemów IT,
- przechowywanie danych (obiekty danych na karcie).

Dostępne interfejsy:

- stykowy (contact) – ISO 7816,
- bezstykowy (contactless) – ISO 14443 1-4, MIFARE,
- dualny (dual) – stykowy + bezstykowy.

Więcej o produktach PWPW SmartApp® dowiedzą się Państwo z artykułu Pawła Śniecikowskiego zamieszczonego w naszym czasopiśmie CiD nr 36/2015.

Ogromną wartością dodaną projektu BIOMET jest jego uniwersalność. Umożliwi to wprowadzenie na rynek nowoczesnego mobilnego systemu do przeprowadzania kontroli na granicach nie tylko europejskich, ale również w innych częściach świata. Jego funkcjonalność pozwoli na szerokie zastosowanie. Poza Strażą Graniczną odbiorcami docelowego systemu mogą być jednostki policji, wojska czy żandarmerii wojskowej. BIOMET stworzy nowe możliwości funkcjonariuszom służb mundurowych,



Ryc. 7. Zestaw mobilny z kamizelką (wykonany przez firmę MLabs) wraz z czytnikiem dokumentów oraz kartą mikroprocesorową (wyprodukowaną i dostarczoną przez PWPW S.A.) – wygląd rzeczywisty



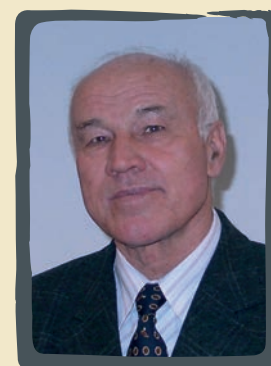
Ryc. 8. Zestaw mobilny z kamizelką (wykonany przez firmę MLabs) wraz z czytnikiem dokumentów (wybrany przez PWPW S.A.) – wygląd rzeczywisty



Ryc. 9. Zastosowany w projekcie czytnik mobilny firmy Vicomp do odczytu warstwy elektronicznej paszportów



Ryc. 10. Zastosowany w projekcie czytnik mobilny firmy Vicomp do odczytu warstwy elektronicznej paszportów



MIECZYSLAW SZUSTAKOWSKI – profesor zwyczajny w Instytucie Optoelektroniki Wojskowej Akademii Technicznej. Specjalizuje się w tematyce systemów bezpieczeństwa, technik biometrycznych, detekcji zagrożeń, techniki terahercowej, czujników światłowodowych, obrazowania multispektralnego i rozszerzonej rzeczywistości.



Ryc. 11. Wersja mobilna prototypu czytnika ultradźwiękowego firmy OPTEL

mających uprawnienia do kontroli osób i ich dokumentów.

Rozwiązania zastosowane w systemie rozszerzają (w stosunku do stacjonarnej bramki ABC) możliwości prowadzenia pełnej kontroli dokumentów biometrycznych na:

- obszary przygraniczne, w tym odcinki trudnodostępne dla ruchu kołowego, np. teren górzasty, gęsty las, plaże,
- transport kolejowy oraz autobusowy – możliwość kontroli podróżnych bezpośrednio w środku transportu,

- jednostki pływające, np. kutry, łodzie motorowe, promy,
- imprezy masowe.

Należy podkreślić, iż koszty przeprowadzenia projektu, a także zakupu systemu przez przyszłego użytkownika mogą być oceniane jako niewspółmiernie niskie w porównaniu do efektów. Pełna mobilna kontrola graniczna w sytuacji niekontrolowanego ruchu granicznego, jak ma to miejsce obecnie np. w Europie (przepływ setek tysięcy uchodźców z Syrii, kraju objętego wojną do-

mowa) czy w krajach, gdzie szerzą się terroryzm, przemyt narkotyków i handel ludźmi, pozwoli na zdecydowaną poprawę bezpieczeństwa i ogromne oszczędności dla budżetów państw.

PODSUMOWANIE

Biometria mobilna, w tym przede wszystkim projekt BIOMET, jest nowoczesną odpowiedzią na wymagania związane ze wzrostem liczby osób przekraczających granice oraz potrzebą koncentracji uwagi nie tylko na dokumentach podróży, lecz na bezpieczeństwie całego procesu identyfikacji podróżnych. Jest nowoczesnym wsparciem systemów i narzędzi inspekcyjnych, które wg ICAO są jednym z pięciu elementów procesu zarządzania identyfikacją podróżnych.

Od Redakcji:

Dziękujemy konsorcjantom projektu: Wojskowej Akademii Technicznej, firmie MLabs sp. z o.o. w osobie Pana dr. inż. Mikołaja Sobczaka oraz Przedsiębiorstwu Badawczo-Produkcyjnemu OPTEL sp. z o.o. w osobie Pani Agnieszki Bicz za materiały oraz aktywne wsparcie przy tworzeniu tego atykułu.

Projekt jest w większości finansowany ze środków Narodowego Centrum Badań i Rozwoju w Warszawie (nr projektu DOBR-BIO4/057/13245/2013).

Bezsprzecznymi zaletami systemu BIOMET są jego mobilność oraz możliwość pracy bez podłączonego zewnętrznego zasilania przez około 8 godzin. Dodatkowo system wspiera funkcjonalności, które charakteryzują stacjonarne przejście graniczne, dzięki czemu przeprowadzenie kontroli granicznej osób na zielonej granicy, w transporcie kolejowym i autobusowym lub w celu rozładowania korków na przejściach pieszych nie jest już technicznym problemem. Rozwiązanie to stwarza możliwości do tej pory niedostępne dla funkcjonariuszy Straży Granicznej.

Zaawansowanie technologiczne oraz mobilność systemu BIOMET sprzyjają skuteczniejszej ochronie granic w Europie oraz na całym świecie, a co za tym idzie – wzrostowi bezpieczeństwa obywateli.

¹Proposal for an ICAO Traveller Identification Programme (ICAO TRIP) Strategy, materiał roboczy A-38-WP/11, EX/6, 17/05/13, na 38. sesję Zgromadzenia ICAO, 2013.

²Ruch graniczny oraz wydatki cudzoziemców w Polsce i Polaków za granicą w III kwartale 2015 roku, Informacja sygnałna, Wyniki Badań GUS, Warszawa–Rzeszów, grudzień 2015 r., <http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualno->

[sci/5466/13/6/1/ruch_oraz_wydatki_iii_kwartal_2015.pdf](http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualno-sci/5466/13/6/1/ruch_oraz_wydatki_iii_kwartal_2015.pdf), dostęp 24.03.2016.

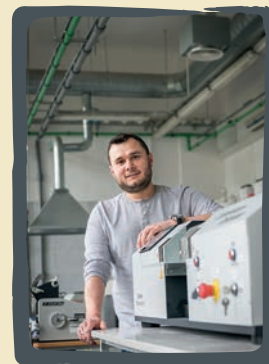
³Dedykowane oprogramowanie zostało stworzone przez firmę MLabs.

⁴Układ zasilania wraz z algorytmem optymalnego zarządzania energią oraz moduł centralny są autorskimi rozwiązaniami zaprojektowanymi i dostarczonymi przez firmę MLabs.

Daniel Mierzejewski, Monika Rogalska, Marek Rosiak

PAPIERY ZABEZPIECZONE I SPECJALNE PRODUKOWANE W PWPW

PWPW oferuje szeroką gamę papierów własnej produkcji – zarówno standardowe papiery zabezpieczone, jak i papiery specjalne opracowane według specyficznych, indywidualnych potrzeb i wymagań klientów.



Na początek nieco historii, która dla Polskiej Wytwórni Papierów Wartościowych (PWPW), rozpoczęła się w 1919 roku. Wtedy to utworzone zostały Państwowe Zakłady Graficzne. W ich skład weszło kilka warszawskich drukarni oraz papiernia, która w roku 1920 rozpoczęła produkcję papierów wartościowych ze znakami wodnymi. Do tego celu wyposażono ją wówczas w okrągłositową maszynę papierniczą szwajcarskiej firmy Escher Wyss, na której produkowano papier banknotowy z umiejscowionym wielotonowym znakiem wodnym. Przeznaczony on był do druku nowych polskich banknotów z datą emisji 1924 r. oraz szeregu papierów ze znakami wodnymi przeznaczonymi dla emitentów akcji, obligacji, listów zastawnych, czeków, weksli i innych druków wartościowych. W czasie II wojny światowej (1939–1945) zarówno papiernia jak i drukarnie były wykorzystywane przez niemieckiego okupanta Polski do czasu powstania warszawskiego w 1944 roku i wówczas zrujnowane. Po wojennych zniszczeniach papiernia wznowiła pracę pod koniec 1947 roku.

Na przestrzeni lat wielokrotnie dokonywano modernizacji oraz unowocześnienia posiadanego parku maszynowego. W 1987 roku wdrożono zakupioną w firmie Security Printing technologię produkcji papierów zabezpieczonych wraz z uruchomieniem nowych ciągów technologicznych do produkcji płaszczy sitowych, masy papierniczej, produkcji i konfekcjonowa-

nia papieru. Ważną zmianą w obszarze papierni było uruchomienie w roku 2005 nowej maszyny papierniczej MP-3 oraz instalacja w 2013 r. nowoczesnej linii konfekcjonowania papierów wartościowych.

Papiernia PWPW może pochwalić się blisko stuletnim doświadczeniem w produkcji wysoko zabezpieczonych papierów wartościowych. Wysoki poziom technologii, ciągłe doskonalenie parku maszynowego oraz wysokiej klasy specjaliści pozwalają lokować ją, w gronie znanych i cenionych papierni funkcjonujących na globalnym rynku.

STANDARDOWE PAPIERY ZABEZPIECZONE

PWPW oferuje papiery zabezpieczone produkowane przez w pełni wyposażoną własną papiernię. Podstawowy asortyment stanowią:

1. papiery banknotowe,
2. papiery paszportowe,
3. papier samoprzylepny na naklejki wizowe,
4. papiery na druki zabezpieczone,

PAPIER BANKNOTOWY

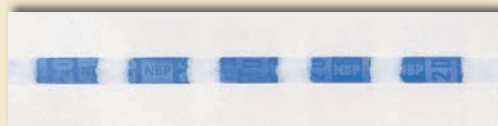
Produkowane przez PWPW papiery banknotowe wykorzystywane są zarówno do druku wszystkich nominałów banknotów polskich, jak i na potrzeby klientów zagranicznych. Dysponujemy pełną gamą zabezpieczeń funkcjonujących w tego rodzaju papierach. Do najczęściej stosowanych należą: wielotonowe znaki wodne, filigranowe znaki wodne, nitki zabezpieczające,

DANIEL MIERZEJEWSKI — absolwent Wydziału Rolnictwa i Biologii SGGW w Warszawie. W PWPW pracuje od 2004 roku, obecnie na stanowisku Specjalisty ds. Zabezpieczeń.

włókna zabezpieczające oraz zabezpieczenia specjalne trzeciego poziomu.

Znaki wodne w papierach banknotowych zazwyczaj mają formę umiejscowionych, wielotonowych znaków portretowych realizowanych według indywidualnych projektów klientów. W formie filigranu – jednotonowego jasnego i bardzo kontrastowego znaku wodnego – najczęściej przedstawiany jest nominał banknotu lub skrót nazwy banku narodowego danego kraju. Znak wodny jest zabezpieczeniem trudnym do podrobienia a jednocześnie łatwym do zweryfikowania. Ocena jego autentyczności jest możliwa w świetle przechodzącym bez stosowania jakichkolwiek urządzeń.

Nitki zabezpieczające mogą zawierać mikroteksty, wykazywać zmienność optyczną oraz aktywność w świetle UV. Nitki mogą być zatapiane w strukturze papieru lub wprowadzane w formie okienek. Zatopione nitki zabezpieczające bardzo często wykazują dodatkowe właściwości, np. przewodność elektryczną czy magnetyzm, pozwalające na odczyt maszynowy. W przypadku nitek okienkowych najlepsze efekty wizualne uzyskuje się dla nitek szerokich, około 4 mm. W dotychczasowej produkcji stosowaliśmy



Fot. 1. Papier na polski banknot kolekcjonerski emitowany w kwietniu 2016 r. o nominale 20 zł z nitką Active



Fot. 2. Papier na polski banknot o nominale 200 zł z nitką RollingCube



Fot. 3. Papier testowy z nitką okienkową Rapid

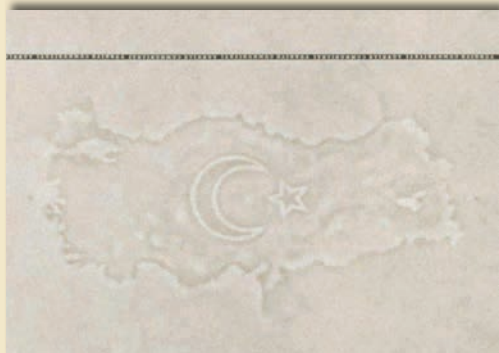
bardzo różne typy nitek, w tym najnowsze dostępne na rynku rozwiązania, takie jak RollingStar, RollingCube, Active, Rapid (fot. 1–3).

Włókna zabezpieczające dostępne w różnych kolorach mogą być widoczne w świetle dziennym oraz aktywne w świetle UV. Dobór włókien zabezpieczających zależy od indywidualnych preferencji klientów.

Określone w specyfikacji technicznej parametry papieru banknotowego są kontrolowane w trakcie całego procesu produkcyjnego zarówno on-line, poprzez zainstalowane czujniki oraz automatyczne systemy kontroli jakości, jak i podczas badań laboratoryjnych. Dysponujemy kompletnie wyposażonym laboratorium, w którym prowadzone są testy produkowanego papieru oraz kontrole wejściowe materiałów stosowanych w procesie produkcyjnym. Dla każdej partii wyprodukowanego papieru przygotowywany jest certyfikat jakości zawierający wyniki przeprowadzonych testów i potwierdzający jakość produktu.

PAPIER PASZPORTOWY

Polska Wytwórnia Papierów Wartościowych ma długoletnie doświadczenie w produkcji papierów paszportowych na rynek polski oraz na eksport. Dostarczamy papier na paszporty m.in. dla Bangladeszu, Ekwadoru, Litwy, Słowacji i Turcji (fot. 4). W swojej ofercie posiadamy wszystkie rodzaje papieru



Fot. 4. Papier na paszporty tureckie z wielotonowym znakiem wodnym przedstawiającym mapę kraju oraz znakami filigranowymi przedstawiającymi symbole Turcji

wykorzystywanego do produkcji książeczek paszportowej, tzn. papiery na strony wizowe, personalizowane oraz wyklejkę.

Do zabezpieczeń najczęściej implementowanych w papierach paszportowych należy zaliczyć wielotonowe znaki wodne, znaki filigranowe, zabezpieczenia chemiczne papieru oraz włókna i nitki zabezpieczające.

Na stronach wizowych i personalizowanych stosowane są głównie wielotonowe, umiejscowione znaki wodne przedstawiające godło państwa lub inny element symbolizujący dany kraj (fot. 5). Z uwagi na układ i wymagane pola książeczki paszportowej

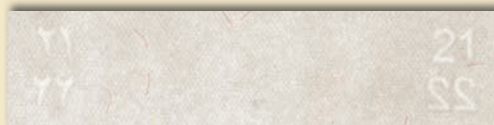


Fot. 5. Papier na strony wizowe paszportu polskiego z umiejscowionym wielotonowym znakiem wodnym oraz pozytywno-negatywową nitką zabezpieczającą

oraz bezpieczeństwo dokumentu, na stronach wizowych i personalizowanych zazwyczaj stosuje się różne wzory znaków. Projekty stron wizowych bardzo często pozwalają na umieszczenie znaków wodnych o większych wymiarach, dzięki temu charakteryzują się one dużą szczegółowością projektu. PWPW posiada własną pracownię projektową i produkuje sita eguterowe, co pozwala na oferowanie klientom przygotowania znaku wodnego według dostarczonego projektu lub opracowanie własnych wzorów.

Papier wyklejki po zadrukowaniu jest przyklejany do okładki paszportu, z tego powodu papiery te najczęściej nie są zabezpieczane znakami wodnymi.

Znaki wodne filigranowe w książeczkach paszportowych wykorzystywane są głównie do numeracji stron – wpływa to na zwiększenie bezpieczeństwa dokumentu i chroni przed zamianą stron przez fałszerzy. Numerację stron możemy wykonać w każdym systemie liczbowym stosowanym w danym kraju. W produkowanych przez nas papierach niekiedy strony paszportu numerowane są jednocześnie w dwóch różnych systemach liczbowych, np. cyfry arabskie oraz indyjsko-arabskie (fot. 6).



Fot. 6. Papier paszportowy zawierający numerację w znakach filigranowych wykonaną w dwóch różnych systemach liczbowych

W paszportach stosowane są przede wszystkim zatopione nitki zabezpieczające zawierające mikroteksty i rysunek flagi danego kraju, aktywne w świetle UV w jednym lub kilku kolorach (fot. 7).



Fot. 7. Papier na stronę personalizowaną paszportu polskiego z pozytywno-negatywową nitką zabezpieczającą

Bardzo ważnym elementem zabezpieczającym papiery paszportowe są zabezpieczenia chemiczne, które chronią przed próbami wywabiania umieszczonych danych poprzez działanie różnymi odczynnikami chemicznymi. W papierach produkowanych w PWPW stosujemy zabezpieczenia reagujące na bardzo szeroką gamę odczynników chemicznych, w tym: rozpuszczalniki polarne i niepolarne, utleniacze, substancje redukujące, korektory, kwasy, zasady.



MONIKA ROGALSKA – absolwentka Wydziału Chemicznego Politechniki Łódzkiej, specjalizacja: technologia celulozy, papieru i poligrafii. Kierownik Działu Technologicznego i Przygotowania Produkcji Papieru w PWPW.

W papierach paszportowych powszechnie stosowane są różnokolorowe włókna zabezpieczające widoczne w świetle dziennym, aktywne w świetle UV oraz widoczne jednocześnie w obu zakresach fal świetlnych. Na stronach personalizowanych rekomenduje się stosowanie włókien widocznych w świetle dziennym, o mało kontrastowych kolorach, aby uniknąć zakłóceń w obszarach zdjęć twarzy. Coraz częściej stosowane są także włókna papierowe wielokolorowe, aktywne w świetle UV. W tym przypadku każde włókno posiada odcinki w różnych zdefiniowanych kolorach, np. włókno dwukolorowe – żółto-niebieskie, włókno trzykolorowe – żółto-czerwono-zielone itp. W niektórych produktach, w zależności od preferencji klientów, stosowane są także zabezpieczenia w postaci różnokolorowych, bardzo drobnych cząstek aktywnych w świetle UV, rozmieszczonych równomiernie w strukturze papieru. Jest to tzw. gwiazdny pył (Star Dust).

Analogicznie jak w przypadku innych papierów produkowanych w PWPW, zdefiniowane w specyfikacji technicznej parametry papierów paszportowych kontrolowane są on-line w trakcie całego procesu produkcyjnego poprzez automatyczne systemy kontroli jakości oraz podczas badań laboratoryjnych. Wszystkie partie wyprodukowanego papieru otrzymują certyfikat jakości zawierający wyniki przeprowadzonych testów i potwierdzający jakość produktu.

PAPIERY SAMOPRZYLEPNE NA NAKLEJKI WIZOWE

PWPW posiada w swoim parku maszynowym także powlekarkę, co umożliwia produkcję papieru zabezpieczonego z warstwą samoprzylepną m.in. na naklejki wizowe.

Papier samoprzylepny, tzw. sandwich składa się z trzech warstw:

- warstwy wierzchniej, którą stanowi papier zabezpieczony,
- warstwy klejowej,
- podłoża silikonowanego chroniącego warstwę klejową.

Zarówno warstwa wierzchnia papieru zabezpieczonego, jak i papier samoprzylepny produkowane są w papierni PWPW. W zależności od potrzeb klientów papiery na naklejki wizowe mogą posiadać różnego typu zabezpieczenia, m.in. włókna zabezpieczające czy zabezpieczenia chemiczne, a także dedykowany kolor papieru. W papierach tego rodzaju nie stosuje się znaków wodnych, ponieważ nie ma możliwości ich weryfikacji w świetle przechodzącym.

Kleje stosowane do wytworzenia warstwy samoprzylepnej w naszej technologii oparte są na bazie wodnej.

Zarówno w procesie produkcji podłoża zabezpieczonego, jak i papieru samoprzylepnego jakość produktu kontrolowana jest on-line przez wykorzystanie istniejących automatycznych systemów kontrolnych oraz czujników, a także w trakcie badań laboratoryjnych. Papiery samoprzylepne badane są zgodnie z normami FINAT, które pozwalają określić m.in. gramaturę aplikowanego kleju, przyczepność warstwy klejowej, odporność na starzenie i inne parametry.

Podłoże silikonowe stanowiące warstwę spodnią sandwicha może zawierać nadrukowane wzory według projektu klienta lub PWPW. Poza funkcją marketingową pozwala to w prosty sposób identyfikować strony papieru samoprzylepnego w procesach konfekcjonowania oraz druku.

Większość papieru samoprzylepnego produkowanego w PWPW stanowi papier na zunifikowane naklejki wizowe strefy Schengen, produkowany na potrzeby wiz polskich oraz innych krajów Unii Europejskiej.

PAPIERY NA DRUKI ZABEZPIECZONE

Do grupy tej zaliczamy szeroki asortyment papierów wykorzystywanych do produkcji banderol akcyzowych, certyfikatów, świadectw szkolnych, bonów, biletów, legitymacji, czeków itp.

Wszystkie wymienione produkty wykonywane są na papierach zabezpieczonych

znakami wodnymi, które mogą być umiejscowione w ściśle określonym miejscu na dokumencie, bieżąco-umiejscowione lub bieżące, tzn. pokrywające całą powierzchnię papieru. Projekty znaków wodnych mogą być dostarczane przez klienta lub opracowane przez grafików w pracowni projektowej PWPW i dostosowane do indywidualnych potrzeb nabywcy oraz przeznaczenia dokumentu, np. wielkości użytku. Innymi stosowanymi zabezpieczeniami są kolorowe włókna zabezpieczające widoczne w świetle dziennym i promieniach UV, a także zabezpieczenia chemiczne chroniące przed próbami usuwania lub zmiany naniesionych wpisów albo potwierdzenia autentyczności dokumentu.

PAPIERY SPECJALNE

Oprócz standardowych papierów zabezpieczonych PWPW posiada w swojej ofercie produkty specjalne opracowane według specyficznych wymagań klientów. Papiery te są odpowiedzią na zapytania ofertowe bądź indywidualne potrzeby poszczególnych rynków produktów zabezpieczonych.

Można tu wymienić między innymi papier o właściwościach antybakteryjnych i antygrzybiczych. Produkt opracowany został w PWPW w roku 2012, a jego skuteczność potwierdzono poprzez badania w certyfikowanym laboratorium Instytutu Biochemicznego ISEGA w Niemczech. Papier spełnia rygorystyczne wymogi normy AATCC 100. Technologia ta dedykowana jest szczególnie do banknotów emitowanych w krajach, w których warunki klimatyczne sprzyjają rozwojowi mikroorganizmów. Są to kraje, gdzie występuje połączenie dużej wilgotności i nierzadko bardzo wysokich temperatur. Cała produkcja papierów banknotowych o właściwościach antymikrobiologicznych została sprawdzona na każdym etapie procesów wytwarzania papieru oraz druku banknotów i w związku z uzyskaniem pozytywnych rezultatów – trafiła do szerokiego portfolio firmy.

Kolejnym produktem oferowanym dla klientów specjalnych jest papier z powłoką chro-



Fot. 8. Pranie w palce – banknot testowy z powłoką

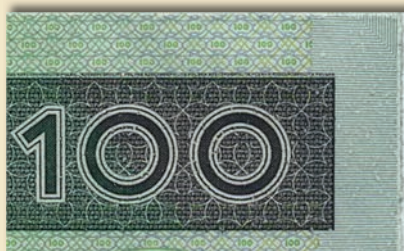


Fot. 9. Pranie w palce – banknot testowy bez powłoki

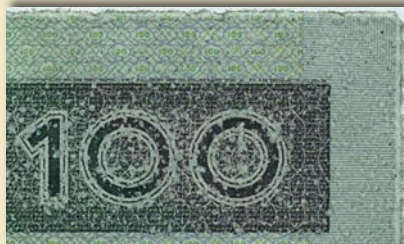
niącą przed zabrudzeniami oraz mechanicznymi uszkodzeniami powierzchni (fot. 8–11). W czasie opracowywania tego rozwiązania wykonywano testy odporności na zabrudzenia, jak również testy mechanicznego i chemicznego niszczenia powierzchni papieru oraz odporności zadruku, zgodnie z wymaganiami dla banknotów euro. W oparciu o wyniki badań oszacowano podniesienie odporności na zabrudzenia o około 30% w stosunku do papieru banknotowego zawierającego w roztworze powlekającym jedynie alkohol poliwinylowy. Co raz częściej w postępowaniach przetargowych



MAREK ROSIAK – absolwent Wydziału Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego oraz Szkoły Głównej Handlowej w Warszawie. Specjalista ds. Promocji i PR w PWPW.



Fot. 10. Ścieranie kulkami – banknot testowy z powłoką



Fot. 11. Ścieranie kulkami – banknot testowy bez powłoki

pojawiają się zapytania odnośnie do tego typu papierów z uwagi na to, iż charakteryzują się one znacznie dłuższym cyklem życia w stosunku do papierów standardowych.

Innym z projektów PWPW zakończonych z sukcesem jest opracowanie rozwiązania pozwalającego na poprawę jakości i trwałości personalizacji dokumentów na drukarkach atramentowych. Odbywa się to poprzez dodanie do powleczenia papieru odpowiednich substancji chemicznych. Przeprowadzone dotychczas próby dały bardzo dobre wyniki.

Ciekawym i niezwykle użytecznym rozwiązaniem jest papier posiadający cechę umożliwiającą grawerowanie laserowe. Jako pierwsze grawerowane były jedynie dokumenty poliwęglanowe, a później (jak w przypadku polskiego paszportu) laminaty papieru z poliwęglanem. Jednakże konstrukcja laminatu tworzywa i papieru jest narażona na pewne zabiegi fałszerskie, których można uniknąć, gdy rezygnuje się z jednej z tych warstw (np. folii). W PWPW opracowany został nowy, specjalny skład masy papierniczej oraz roztworu powlekającego, pozwalający uzyskać w podłożu papierowym wyraźny, czytelny obraz wykonywany metodą grawerowania laserowego, bez konieczności laminowania papieru z folią tworzywową. Papier ten został nazwany skrótowcem LEAP®, od określenia: Laser Engravable Anticounterfeiting Paper. Właściwości tego papieru pozwalają na zastosowanie go do personalizacji dokumentów za pomocą różnych technik – zarówno samego grawerowania, jak i personalizacji kolorowej przy użyciu drukarek. Można więc nanieść kolorową fotografię użytkownika dokumentu wykonaną metodą inkjetową, natomiast dane alfanumeryczne oraz powtórzone zdjęcie w postaci tzw. ducha wygrawerować laserem. Zastosowanie papieru LEAP® jako podłoża dokumentu pozwala zabezpieczyć go chemicznie, co uniemożliwia przerobienie danych zawartych w dokumencie przy użyciu dostępnych na rynku substancji. Ma to szczególnie duże

znaczenie przy stosowaniu personalizacji inkjetowej. Dzięki specjalnie opracowanemu składowi papieru ślad grawerowania pozostaje nie tylko na powierzchni dokumentu, ale również w samej strukturze papieru, co daje ciekawy efekt wzmocnienia obrazu obserwowanego w prześwicie (fot. 12–14).



Fot. 12. Wygrawerowany w papierze kod 2D



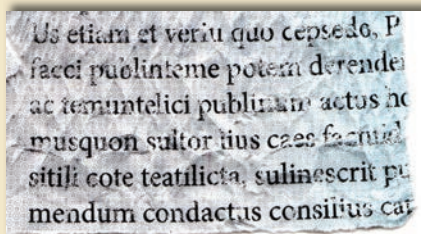
Fot. 13. Wygrawerowany w papierze element graficzny



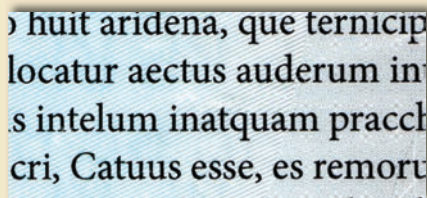
Fot. 14. Wygrawerowany w papierze wizerunek Demeter

W dzisiejszych czasach oprócz bezpieczeństwa dokumentów zwraca się również uwagę na ich funkcjonalność. Dbłość o środowisko oraz przesłanki ekonomiczne nakładają na producentów konieczność wydłużenia czasu użytkowania poszczególnych druków. Wychodząc naprzeciw tym wymogom, PWPW wprowadziła do swojej oferty również papier z powłoką zwiększającą adhezję druku laserowego. Pozwala to podnieść trwałość tonera laserowego i jego odporność na warunki standardowego użytkowania. Druki ze specjalną powłoką zachowują nienaruszony wzór wydrukowany za pomocą drukarki laserowej również w przypadku zginania arkusza papieru czy pocierania jego powierzchni różnymi twardymi materiałami (fot. 15–18).

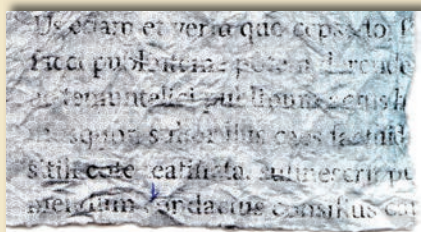
Należąca do parku maszynowego PWPW powlekarka umożliwia wykonywanie papierów zabezpieczonych z warstwą klejową.



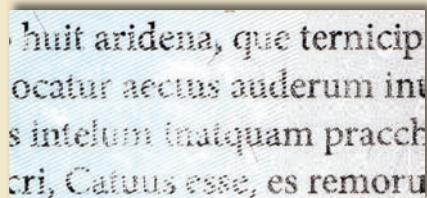
Fot. 15. Papier z powłoką poprawiającą druk laserowy – CRUMPLING



Fot. 17. Papier z powłoką poprawiającą druk laserowy – test taśmą TESA



Fot. 16. Papier bez powłoki poprawiającej druk laserowy – CRUMPLING



Fot. 18. Papier bez powłoki poprawiającej druk laserowy – test taśmą TESA

Oprócz standardowych papierów wizowych od ubiegłego roku rozpoczęliśmy produkcję papierów na samoprzylepne znaki akcyzy. Charakteryzują się one warstwą adhezyjną dostosowaną do tzw. podłoży trudnych i można je stosować zarówno na powierzchniach z plastiku, szkła czy metalu, jak również na lakierowanych puszkach.

Pośród szerokiej gamy produktów PWPW na uwagę zasługuje również specjalny papier zawierający w swoim składzie, oprócz włókien celulozowych, włókna syntetyczne. Pa-

pier jest dodatkowo powlekany specjalnym roztworem zaklejającym, dzięki czemu charakteryzuje się wysoką odpornością na wodę, właściwą chłonnością dla stempli olejowych i rozpuszczalnikowych oraz ma specyficzną strukturę łatwo wyczuwalną w dotyku. Papier ten stosowany jest przy produkcji polskich dowodów rejestracyjnych, a jego cechy powodują, że dokument ten, mimo ponad dziesięcioletniego użytkowania, wciąż jest jednym z najbezpieczniejszych polskich druków.

WSPÓLNY SUKCES POCZTY POLSKIEJ I POLSKIEJ WYTWÓRNI PAPIERÓW WARTOŚCIOWYCH

*Znaczek pocztowy ZABYTKOWE ORGANY W POLSCE został nagrodzony
na wrześniowej konferencji w Berlinie.*

Podczas trwającej w Berlinie w dniach 5–7 września 2016 r. KONFERENCJI GPSPA (GOVERNMENTAL POSTAGE STAMP PRINTERS' ASSOCIATION) Polska Wytwórnia Papierów Wartościowych znalazła się w gronie firm wyróżnionych w cyklicznym konkursie filatelistycznym. Nagrodę w kategorii „techniki kombinowane” zdobył znaczek o nazwie ZABYTKOWE ORGANY W POLSCE. Jest to sukces, który udało się osiągnąć dzięki współpracy Poczty Polskiej S.A. i Polskiej Wytwórni Papierów Wartościowych S.A. Na znaczku zaprezentowane zostały barokowe organy z kościoła klasztorne-go Archiopactwa Cysterskiego w Jędrzejowie. Jest to jeden z najcenniejszych zabytków tego typu w Europie. Unikalne są zarówno brzmienie instrumentu, zastosowane w jego budowie rozwiązania techniczne, jak i kunszt artystyczny wykonania, w tym dekoracje i bogate zdobienia. Ponoć to właśnie organy jędrzejowskie miały być pierwowzorem dla słynnych organów znajdujących się w katedrze oliwskiej w Trójmieście.

Znaczek ilustruje ciekawą konstrukcję instrumentu. Bryłę organów przedstawiono symbolicznie i wkomponowano w tło architektury kościoła. Efektowne są misterne oddanie szczegółów architektonicznych, jak również harmonijna kolorystyka znaczka. Autorem projektu jest Marzanna Dąbrowska a autorem rytu – Przemysław Krajewski. Znaczek o wymiarach 51 x 39,5 mm został wpro-



Fot. 1. Statuetka za nagrodzony znaczek ZABYTKOWE ORGANY W POLSCE

wadzony do obiegu 30 lipca 2015 r. Znaczek w pełnej okazałości prezentujemy na 2. stronie okładki tego wydania.

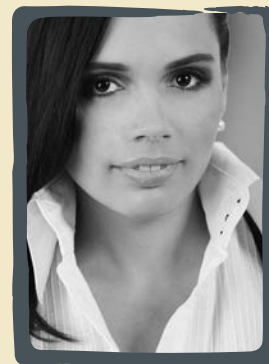
Obecnie PWPW produkuje zarówno znaczki obiegowe w wielomilionowych powtarzalnych nakładach, jak i znaczki okolicznościowe, niskonakładowe. Znaczki produkowane przez Wytwórnię wielokrotnie były nagradzane w konkursach filatelistycznych, m.in. w MIĘDZYNARODOWYM KONKURSIE SZTUKI FILATELISTYCZNEJ w Asiago we Włoszech.

Źródła: Centrum Prasowe PAP, PWPW S.A.

Anna Zalesińska

e-REWOLUCJA W DOKUMENTACH SĄDOWYCH

Od 2010 roku, kiedy w KODEKSIE POSTĘPOWANIA CYWILNEGO pojawił się protokół elektroniczny, a wraz z nim transkrypcja¹, dotychczasowe klasyczne podejście do dokumentu sądowego uległo rewolucyjnej zmianie.



ANNA ZALESIŃSKA – doktor nauk prawnych, Radca Prawny w Centrum Kompetencji i Informatyzacji Sądownictwa Sądu Apelacyjnego we Wrocławiu.

Wzorem procedury cywilnej² analogiczne zmiany pojawiły się w postępowaniu w sprawach o wykroczenia³ oraz w postępowaniu karnym⁴. Kolejnym etapem było wdrożenie, podobnie jak ma to miejsce w innych państwach europejskich, ustnych uzasadnień do postępowań sądowych. I wreszcie 10 lipca 2015 r. zostały uchwalone przepisy umożliwiające kompleksową obsługę w pełni elektronicznej, dwustronnej komunikacji z sądem w sprawach cywilnych, a co za tym idzie – ustawodawca dopuścił wykorzystanie formy elektronicznej oraz formy dokumentowej w celu utrwalania dokumentów sądowych w toku postępowania cywilnego. Ta przełomowa zmiana wprowadza wreszcie polskie sądownictwo w XXI wiek. Warto przy tej okazji dokonać pewnej rewizji pojęcia dokumentu sądowego w kontekście ewolucji dotychczasowych oraz pojawienia się nowych instytucji procesowych w szeroko rozumianych postępowaniach sądowych. W pierwszej części artykułu umówione zostaną zagadnienia związane z protokołem elektronicznym oraz ustnym uzasadnieniem. Kolejna część natomiast poświęcona zostanie dokumentom sądowym, które wraz z wdrożeniem Elektronicznego Biura Podawczego w sądach powszechnych będą wytwarzane pierwotnie w postaci elektronicznej.

PROTOKÓŁ ELEKTRONICZNY

Pierwszym zwiastunem zmian w postępowaniach sądowych, które przez ostatnie

dekady tylko w minimalnym zakresie dopuszczały korzystanie z nowoczesnych rozwiązań technologicznych (możliwość przeprowadzania dowodu na odległość przy wykorzystaniu wideokonferencji), było pojawienie się protokołu elektronicznego⁵. Formalnie ustawodawca nie posługuje się terminem „protokół elektroniczny”, tylko odwołuje się do postaci, w jakiej jest on utrwalany. Przepis mówi wprost o protokole sporządzanym za pomocą urządzeń utrwalających dźwięk albo obraz i dźwięk. Stanowi to konsekwencję koncepcji ustawodawcy, który odszedł od sztucznego tworzenia nowych bytów prawnych (czego przykładem jest Elektroniczne postępowanie upominawcze) w kierunku tworzenia spójnej koncepcji systemu prawnego bazującego na funkcji, jaką pełni dana instytucja prawna, a nie na sposobie jej utrwalenia. W przypadku przyjęcia odmiennej koncepcji konieczne byłoby tworzenie niejako lustrzanego odbicia przepisów – tylko dlatego, że do utrwalenia doszło w postaci elektronicznej. I tak, ustawodawca na etapie tworzenia przepisów dotyczących protokołów utrwalonych w postaci zapisu audio lub audio-wideo zdeterminował dalszy kierunek informatyzacji, gdzie nie ma już miejsca dla takich sztucznych konstrukcji słownych jak pozew elektroniczny, wyrok elektroniczny czy też elektroniczny tytuł wykonawczy. Zarówno nowelizacja, która wprowadziła protokół elektroniczny, jak

i ustne uzasadnienie oraz Elektroniczne Biuro Podawcze systemowo bazują na dotychczasowej terminologii, akcentując jedynie postać utrwalenia. W przypadku protokołu elektronicznego nie ma znaczenia, jak został sporządzony (pismem odręcznym, komputerowym, w postaci cyfrowej etc.), bowiem w każdym przypadku jego funkcja, polegająca na wiernym odtworzeniu przebiegu postępowania, zostaje spełniona. Od chwili podpisania protokołu zyskuje szczególną moc dokumentu urzędowego⁶. Jako dokument urzędowy korzysta on z wynikających z art. 244 k.p.c. domniemań prawdziwości oraz prawidłowości zawartych w nim stwierdzeń i oświadczeń⁷. Dotyczy to nie tylko postępowania cywilnego, ale także analogicznie postępowania w sprawach o wykroczenia⁸ oraz postępowania karnego⁹.

W **KODEKSIE POSTĘPOWANIA CYWILNEGO** oraz **KODEKSIE POSTĘPOWANIA W SPRAWACH O WYKROCZENIA** ustawodawca przyjął jednolity model konstrukcji nowej postaci protokołu elektronicznego. Zasadą jest, że sporządza się protokół w postaci zapisu obrazu i dźwięku albo samego dźwięku. Decyzja w tym zakresie należy do przewodniczącego. Tylko w wyjątkowych sytuacjach, gdy ze względów technicznych utrwalenie przebiegu posiedzenia za pomocą urządzenia rejestrującego dźwięk albo obraz i dźwięk nie jest możliwe, protokół jest sporządzany wyłącznie pisemnie. Dopuszczenie możliwości odstąpienia od sporządzenia protokołu elektronicznego w przypadku niespełnienia warunków technicznych stanowi bezpośrednią konsekwencję etapowości wdrożenia systemu, które trwa od 2011 r., a ma zakończyć się dopiero w 2020 r. Ponadto w trakcie eksploatacji systemu mogą się pojawić problemy natury technologicznej, stąd konieczne stało się zapewnienie możliwości powrotu do pisemnej postaci protokołu sądowego. Zgodnie z art. 158 k.p.c. i odpowiednio art. 37 k.k.w. protokół elektroniczny składa się z dwóch komponentów, tj. zapisu dźwięku lub obrazu

i dźwięku oraz części pisemnej, zwanej protokołem skróconym. Pojawia się zatem nowa postać dokumentu sądowego, który pierwotnie ma postać elektroniczną. Część doktryny opowiedziała się do kwalifikacji tego typu dokumentów jako utrwalonych w formie ustnej w jej kwalifikowanej postaci elektronicznej¹⁰. Jednak koncepcja ta nie spotkała się z szeroką akceptacją. Za dominujące należy uznać stanowisko, że wraz z pojawianiem się protokołów elektronicznych doszło do wyróżnienia elektronicznej formy czynności¹¹. Na gruncie **KODEKSU POSTĘPOWANIA KARNEGO** ustawodawca przyjął założenia odmienne od przedstawionych powyżej. Zgodnie z art. 147 k.p.c. przebieg czynności protokołowanych może być utrwalony ponadto za pomocą urządzenia rejestrującego dźwięk albo obraz i dźwięk. Tylko w pewnych wyjątkowych sytuacjach utrwalenie przesłuchania za pomocą urządzenia rejestrującego obraz i dźwięk jest obligatoryjne, na przykład gdy zachodzi niebezpieczeństwo, że przesłuchanie danej osoby nie będzie możliwe w dalszym postępowaniu. Zapisy dźwięku albo obrazu i dźwięku stają się załącznikami do protokołu. Ustawodawca odstąpił zatem od nadania zapisowi cyfrowemu charakteru protokołu sądowego, a jedynie nadał mu walor załącznika, przyznając pierwszeństwo protokołowi pisemnemu.

Wraz z protokołem elektronicznym pojawiła się transkrypcja, zwana – w postępowaniu w sprawach o wykroczenia oraz w postępowaniu karnym – przekładem. W **KODEKSIE POSTĘPOWANIA CYWILNEGO** ustawodawca przyjął, że jeżeli jest to niezbędne dla zapewnienia prawidłowego orzekania w sprawie, przewodniczący może zarządzić sporządzenie transkrypcji odpowiedniej części protokołu sporządzonego za pomocą urządzenia rejestrującego dźwięk albo obraz i dźwięk. Zgodnie natomiast z art. 37 § 6 k.k.w., jeżeli jest to niezbędne dla zapewnienia prawidłowego orzekania w sprawie, prezes sądu może zarządzić sporządzenie przekładu odpowied-

niej części protokołu elektronicznego. Przekład stanowi załącznik do protokołu. W obu przypadkach ustawodawca celowo posłużył się klauzulą generalną, pozostawiając otwarty katalog sytuacji, kiedy konieczne może być sporządzenie transkrypcji (przekładu). Czynności związane z transkrypcją są wykonywane przez pracowników sądów zwanych transkrybentami. Za prawidłowe i terminowe wykonanie transkrypcji przez transkrybentów odpowiada osoba kierująca czynnościami związanymi z transkrypcją. Transkrypcję należy sporządzać zgodnie z zasadami określonymi w załączniku nr 1 do INSTRUKCJI KANCELARYJNEJ¹². Transkrypcja nie jest podpisywana. W **KODEKSIE POSTĘPOWANIA KARNEGO** przyjęte natomiast zostało, że przekład jest sporządzany obligatoryjnie. Tak sporządzony przekład ma status załącznika do protokołu sądowego.

W przypadku transkrypcji (przekładu) mamy do czynienia z nową instytucją procesową, która znacznie odbiega od klasycznych dokumentów sądowych. Po pierwsze, transkrypcja nie stanowi części protokołu, którym jest zapis elektroniczny wraz z pisemnym protokołem¹³. Sporządzenie transkrypcji jest czynnością materialno-techniczną, a pod jej treścią nie podpisuje się ani przewodniczący, ani transkrybent. Niewątpliwie jednak sama transkrypcja pozostaje dokumentem sądowym, tyle że sporządzonym w postaci elektronicznej. Brak podpisu uniemożliwia kwalifikację tej instytucji do formy elektronicznej. Konieczne staje się zatem na gruncie proceduralnym, wzorem prawa materialnego¹⁴, wyróżnienie formy dokumentowej. W efekcie pojawienie się transkrypcji (przekładu) umożliwiło wyłonienie nowej kategorii dokumentów sądowych utrwalonych w formie dokumentowej.

Pojawienie się protokołu elektronicznego i transkrypcji (przekładu) stało się bezpośrednim impulsem do prowadzenia dalszych prac legislacyjnych, których celem było zwiększenie wykorzystania nowoczesnych środków

komunikacji elektronicznej w postępowaniu sądowym. Prace te zaowocowały pojawieniem się tzw. ustnych uzasadnień.

USTNE UZASADNIENIA

Pojawienie się ustnych uzasadnień w procedurze cywilnej zrewolucjonizowało dotychczasowe podejście do dokumentu sądowego, chyba nawet bardziej niż protokół elektroniczny. Tradycyjny sposób utrwalania uzasadnienia na piśmie zastąpiony został możliwością rejestracji ustnej wypowiedzi sędziego. Ustne uzasadnienia stanowią kolejny etap informatyzacji postępowania cywilnego. Informatyzacja w tym wypadku dotknęła w znaczący sposób najbardziej istotnego etapu postępowania sądowego – wyrokowania. Pomimo tego, że w procedurze cywilnej i wykroczeniowej ustne uzasadnienia funkcjonują już od kilku lat, to wciąż budzą kontrowersje, zarówno wśród teoretyków, jak i praktyków.

Zgodnie z dotychczasowymi przepisami (art. 326 **K.P.C.**) ogłoszenie wyroku następuje na posiedzeniu, na którym zamknięto rozprawę. W sprawie zawilej sąd może jednak odroczyć ogłoszenie wyroku, tylko jeden raz, na czas do dwóch tygodni. Ocena, czy sprawa jest zawila należy do składu orzekającego. Przepis dotyczący możliwości odroczenia ma charakter instrukcyjny i jego naruszenie nie pociąga za sobą negatywnych skutków. Ogłoszenie wyroku następuje przez odczytanie sentencji. Po ogłoszeniu sentencji orzeczenia przewodniczący lub sędzia sprawozdawca podaje ustnie zasadnicze powody rozstrzygnięcia. Powinny one być zgodne z pisemnym uzasadnieniem.

Jeżeli jednak przebieg posiedzenia jest utrwalany za pomocą urządzenia rejestrującego dźwięk albo obraz i dźwięk, ustawodawca wprowadził alternatywę¹⁵: uzasadnienie może być wygłoszone po ogłoszeniu sentencji wyroku i utrwalone za pomocą tego urządzenia¹⁶. W przypadku gdy wygłaszane jest ustne uzasadnienie, nie podaje się ustnie mo-

tywów rozstrzygnięcia. Ustne uzasadnienie jest wygłaszane bezpośrednio po odczytaniu sentencji, o czym jednak należy uprzedzić strony i uczestników postępowania przed jego wygłoszeniem. Jednakże wygłoszenie ustnego uzasadnienia jest możliwe tylko wtedy, kiedy przebieg posiedzenia był utrwalany przy wykorzystaniu protokołu elektronicznego. Dotyczy to co najmniej posiedzenia, na którym jest wygłaszane ustne uzasadnienie. Ustne uzasadnienie musi odpowiadać wymogom przewidzianym w art. 328 § 2 k.p.c., powinno więc zawierać wskazanie podstawy faktycznej rozstrzygnięcia oraz wyjaśnienie podstawy prawnej wyroku z przytoczeniem przepisów prawa. Ponadto uzasadnienie powinno w sposób pełny, logiczny i jak najbardziej adekwatny przedstawiać motywy rozstrzygnięcia i argumenty, jakie posłużyły sądowi orzekającemu do przyjęcia stanowiska zajętego w sentencji wyroku. Członkowie składu orzekającego nie podpisują ustnego uzasadnienia, bowiem jest ono częścią protokołu elektronicznego i w tym zakresie zastosowanie znajduje art. 158 § 3 k.p.c.

W przypadku zgłoszenia wniosku o doręczenie wyroku wraz z uzasadnieniem lub – gdy wniosek taki nie był zgłoszony – zaskarżenia wyroku bądź wniesienia skargi o stwierdzenie niezgodności z prawem prawomocnego orzeczenia, transkrypcję wygłoszonego uzasadnienia należy sporządzić w terminie dwóch tygodni liczonych odpowiednio od dnia zgłoszenia wniosku lub zaskarżenia wyroku bądź wniesienia skargi. Termin ten ma charakter terminu instrukcyjnego, a jego uchybienie nie powoduje negatywnych konsekwencji procesowych. W przypadku uzasadnień, które zostały wygłoszone, brak jest możliwości przedłużenia tego terminu. Wynika to z tego, że uzasadnienie zostało już w praktyce sporządzone, a termin dwóch tygodni jest wystarczający na wykonanie czynności technicznej przekładu na tekst (transkrypcji).

Transkrypcja ustnego uzasadnienia sporządzana jest, analogicznie jak w przypadku protokołów elektronicznych, przez wyspecjalizowane zespoły transkrybentów pod nadzorem osób kierujących czynnościami związanymi z transkrypcją. Transkrypcje ustnych uzasadnień są dokonywane zgodnie z zasadami określonymi w załączniku nr 1 do INSTRUKCJI KANCELARYJNEJ. Transkrypcja ustnego uzasadnienia nie podlega autoryzacji przez przewodniczącego ani skład orzekający. Nie jest również przez nikogo podpisywana. W razie braków lub nieścisłości jej treści pierwszeństwo ma zapis ustnego uzasadnienia utrwalony w protokole elektronicznym.

W przypadku gdy zapis ustnego uzasadnienia jest w całości lub części nieczytelny ze względów technicznych, konieczne jest zastosowanie odpowiednio przepisów regulujących postępowanie w razie zaginięcia lub zniszczenia akt (art. 716 k.p.c. i n.). Postępowanie takie może zostać wszczęte na wniosek lub z urzędu. Zgodnie natomiast z art. 725 k.p.c. oraz 726 k.p.c. na potrzeby odtworzenia akt istnieje możliwość odwołania się do różnych źródeł informacji, w tym również do oświadczeń stron, prywatnych pism i notatek, a także samodzielnie utrwalonego przez strony zapisu dźwięku, zgodnie z art. 1611 k.p.c.

Transkrypcja ustnego uzasadnienia podlega sprostowaniu lub uzupełnieniu. Aczkolwiek należy odróżnić sytuację, gdy omyłka nastąpiła po stronie transkrybenta, który dokonał zapisu słownego w sposób niezgodny z wypowiedzią, od takich okoliczności, kiedy to do błędu doszło po stronie przewodniczącego w trakcie wygłaszania uzasadnienia. W pierwszej sytuacji to zespół transkrybentów dokonuje sprostowania transkrypcji, natomiast w drugiej zachodzi konieczność sprostowania uzasadnienia orzeczenia sądowego (ustnego uzasadnienia, które zostało nagrane i tzw. protokołu skróconego sporządzanego obok nagrania). W postępowaniu cywilnym zastosowanie znajdują odpowiednio art. 350–353 k.p.c.

Co do zasady stronie, która zgłosiła wniosek o doręczenie wyroku z uzasadnieniem, doręcza się na piśmie odpis wyroku wraz z uzasadnieniem. Analogicznie jest w przypadku ustnego uzasadnienia. Ustawodawca jednak, z uwagi na zapewnienie realizacji konstytucyjnej zasady wymiaru sprawiedliwości w postaci zagwarantowania równości, w § 2 wskazał, że doręczeniu podlega ponadto transkrypcja ustnego uzasadnienia. Pewne wątpliwości można mieć co do sformułowania użytego w treści art. 331 § 1 k.p.c., które zdaje się sugerować, że doręczeniu podlega wyłącznie wyrok wraz z transkrypcją, a nie informatyczny nośnik danych zawierający zapis wygłoszonego uzasadnienia. Należy się zgodzić ze stanowiskiem K. Flagi-Gieruszyńskiej i A. Klich, że na gruncie prawa procesowego cywilnego doszło do wyróżnienia dwóch odrębnych instytucji w postaci ustnego uzasadnienia wyroku i jego transkrypcji, o czym przesądza redakcja art. 329 k.p.c. Instytucję transkrypcji należy odnieść do działalności organizacyjnej sądu, a nie judykacyjnej. Utożsamianie ustnego uzasadnienia z jego transkrypcją prowadziłoby do sytuacji, w której osoba niewykwalifikowana i pozbawiona statusu sędziego, mająca decydującą rolę w kształcie transkrypcji, wywierałaby wpływ na merytoryczne rozstrzygnięcie sprawy. W przypadku błędów w treści transkrypcji brak równoczesnego doręczenia zapisu ustnego uzasadnienia mógłby spowodować negatywne konsekwencje dla odwołującego się. Tym samym w przypadku sporządzenia ustnego uzasadnienia strona powinna otrzymać odpis wyroku, zapis ustnego uzasadnienia na informatycznym nośniku danych oraz jego transkrypcję. Pominięcie któregośkolwiek z elementów skutkować może pozbawieniem strony postępowania prawa do należytej obrony. Transkrypcja bowiem nie jest stanowiskiem sądu, a jedynie jego technicznym odzwierciedleniem¹⁷.

Strona postępowania wnosząca o doręczenia wyroku wraz z uzasadnieniem nie

powinna być obciążona opłatą 15 zł, którą – zgodnie z art. 77 ust. 1a **USTAWY Z DNIA 28 LIPCA 2005 R. O KOSZTACH SĄDOWYCH W SPRAWACH CYWILNYCH** – pobiera się od wniosku o wydanie na podstawie akt sprawy zapisu dźwięku albo obrazu i dźwięku z przebiegu posiedzenia. Obowiązek uiszczenia opłaty dotyczy wyłącznie protokołu elektronicznego.

Doręczenie wyroku z transkrypcją uzasadnienia jest równoznaczne z doręczeniem wyroku z uzasadnieniem. Od tego momentu liczone są terminy na wniesienie środków zaskarżenia, zgodnie z **KODEKSEM POSTĘPOWANIA CYWILNEGO**.

Jako dokument urzędowy ustne uzasadnienie korzysta z wynikających z art. 244 k.p.c. domniemań prawdziwości oraz prawidłowości zawartych w nim stwierdzeń i oświadczeń¹⁸. Zgodnie z art. 308 k.p.c. w przypadku dowodów i innych dokumentów niż zawierające tekst (art. 2431 k.p.c.), w szczególności zawierających zapis obrazu, dźwięku albo obrazu i dźwięku, sąd przeprowadza dowód, stosując odpowiednio przepisy o dowodzie z oględzin oraz o dowodzie z dokumentów. Dowód z dokumentu zawierającego zarówno tekst, jak i dźwięk albo obraz i dźwięk będzie zatem przeprowadzany na podstawie art. 244 k.p.c. i następnych (w zakresie treści stanowiącej tekst) i art. 308 k.p.c. (w pozostałym zakresie)¹⁹. Znowelizowany art. 308 k.p.c. stanowi procesową konsekwencję wprowadzonej do prawa materialnego **USTAWĄ Z DNIA 10 LIPCA 2015 R. DO KODEKSU CYWILNEGO**²⁰ definicji dokumentu jako nośnika informacji umożliwiającego zapoznanie się z jej treścią (art. 773 k.c.). Regulacja ta zakończyła dotychczasowy spór w doktrynie o to, w jaki sposób przeprowadzać dowód z protokołu elektronicznego, a co za tym idzie – dowód z ustnego uzasadnienia utrwalonego w postaci zapisu cyfrowego²¹. Zgodnie z nowymi przepisami dowody z innych dokumentów niż zawierających tekst (wymienione w art. 2431 k.p.c.), w szczególności zawierających

zapis obrazu, dźwięku albo obrazu i dźwięku, sąd przeprowadza, stosując odpowiednio przepisy o dowodzie z oględzin oraz o dowodzie z dokumentów.

Na prawdziwą rewolucję trzeba było jednak czekać do 2015 roku, kiedy to została

uchwalona nowelizacja **KODEKSU CYWILNEGO** oraz **KODEKSU POSTĘPOWANIA CYWILNEGO**²², która zmieniła sposób postrzegania dokumentu i jego formy w obszarze prawa materialnego, a do prawa procesowego wprowadziła Elektroniczne Biuro Podawcze.

¹Pisałam o tym w artykułach: *Elektroniczny protokół sądowy*, „Człowiek i Dokumenty” 2010, nr 18, s. 25–29 oraz *Elektroniczny protokół sądowy a transkrypcja*, „Człowiek i Dokumenty” 2012, nr 25, s. 31–34.

²Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz. U. z 2014 r., poz. 101 ze zm.), dalej „k.p.c.”.

³Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (t.j. Dz. U. z 2013 r., poz. 395 ze zm.), dalej „k.p.w.”.

⁴Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89, poz. 555 ze zm.), dalej „k.p.k.”.

⁵Ustawa z dnia 29 kwietnia 2010 r. o zmianie ustawy – Kodeks postępowania cywilnego (Dz. U. z 2010 r. Nr 108, poz. 684).

⁶Por. K. Kołakowski [w:] *Kodeks postępowania cywilnego*, t. I, *Komentarz do art. 1–50514*, red. K. Piasecki, Warszawa 2006, s. 656 i 657; postanowienie Sądu Najwyższego z dnia 9 kwietnia 2010 r., sygn. akt III CSK 178/09.

⁷Por. Postanowienie Sądu Najwyższego z dnia 21 stycznia 2005 r., sygn. akt I CK 4/05, www.sn.pl.

⁸Do postępowania w sprawach o wykroczenia protokół elektroniczny został wprowadzony ustawą z dnia 4 kwietnia 2014 r. o zmianie ustawy – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2014 r., poz. 579).

⁹Do postępowania karnego protokół elektroniczny został wprowadzony ustawą z dnia 10 lipca 2015 r. o zmianie ustawy – Kodeks postępowania karnego (Dz. U. z 2015 r., poz. 1334).

¹⁰Por. S. Cieślak, *Forma czynności w procesie cywilnym – stan obecny i perspektywy rozwoju*, [w:] *Postępowanie rozpoznawcze w przyszłym Kodeksie postępowania cywilnego*, red. K. Markiewicz, A. Torbus, Warszawa 2014, s. 155–172.

¹¹Por. A. Kościółek, *Elektroniczne czynności procesowe w sądowym postępowaniu cywilnym*, Warszawa 2012, s. 178–179 oraz 187 i n.; A.K. Bieliński, *Elektroniczne czynności procesowe z uwzględnieniem orzeczeń sądowych*, [w:] Ł. Błaszczak (red.), *Wokół problematyki orzeczeń*, Toruń 2007, s. 125–133; J. Gołaczyński, *Elektroniczne czynności procesowe*, „Prawo Mediów

Elektronicznych”, dodatek do „Monitora Prawniczego” 2004, nr 4, s. 3 i n.; A. Zalesińska, *Wpływ informatyzacji na założenia konstrukcyjne procesu cywilnego*, Warszawa 2016 r. [w druku].

¹²Zarządzenie Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej (Dz. Urz. MS Nr 5, poz. 22 ze zm.), dalej „Instrukcja kancelaryjna”.

¹³Por. Uzasadnienie, druk sejmowy Sejmu VII kadencji nr 2131, www.sejm.gov.pl.

¹⁴W Kodeksie cywilnym przywoływana już nowelizacja z dnia 10 lipca 2015 r. wprowadziła definicję dokumentu oraz nową formę czynności prawnych – formę dokumentową.

¹⁵Ustawa z dnia 29 sierpnia 2014 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz ustawy o kosztach sądowych w sprawach cywilnych (Dz. U. z 2014 r., poz. 1296).

¹⁶Identyczne rozwiązanie przewidziane zostało w Kodeksie postępowania w sprawach o wykroczenia ustawą z dnia 4 kwietnia 2014 r. o zmianie ustawy – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2014 r., poz. 579). Przedstawione na gruncie procedury cywilnej rozważania pozostają aktualne również w kontekście postępowania w sprawach o wykroczenia.

¹⁷Por. K. Flaga-Gieruszyńska, A. Klich, *Nowy model uzasadnienia wyroku w procesie cywilnym*, „Prawo Mediów Elektronicznych” 2015, nr 1, s. 8–17.

¹⁸Por. Postanowienie Sądu Najwyższego z dnia 21 stycznia 2005 r., sygn. akt I CK 4/05, www.sn.pl.

¹⁹Por. Uzasadnienie do druku Sejmu VII kadencji nr 2678, www.sejm.gov.pl.

²⁰Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2014 r., poz. 121, ze zm.), dalej „k.c.”.

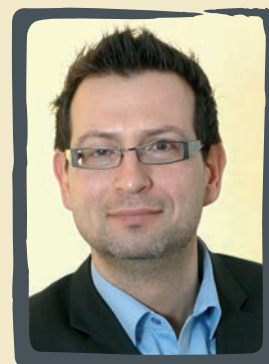
²¹Szerzej na ten temat: B. Kaczmarek-Templin, *Dowód z dokumentu elektronicznego w procesie cywilnym*, Warszawa 2012.

²²Ustawa z dnia 10 lipca 2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz. U. z 2015 r., poz. 1311 ze zm.).

Remigiusz Lewandowski

O POTRZEBIE REGULACJI SFERY DOKUMENTÓW PUBLICZNYCH

Nie ulega wątpliwości, że dokumenty publiczne oraz znaki pieniężne odgrywają znaczącą rolę w relacjach gospodarczych i społecznych każdego państwa. Zwłaszcza w dziedzinie bezpieczeństwa państwa, głównie bezpieczeństwa ekonomicznego oraz publicznego.



Zarówno dokumenty publiczne, jak i banknoty stanowią ważny element systemu bezpieczeństwa państwa. Dotyczy to w szczególności dwóch dziedzin bezpieczeństwa państwa, a mianowicie bezpieczeństwa ekonomicznego oraz publicznego. Z uwagi na istniejący związek pomiędzy dokumentami publicznymi (i banknotami) a wskazanymi dziedzinami bezpieczeństwa państwa zasadne wydaje się objęcie regulacją ustawową pełnego procesu zarządzania cyklem życia dokumentów, począwszy od etapu projektowania dokumentu i doboru adekwatnych zabezpieczeń, przez etap produkcji blankietu, akwizycji danych osobowych i personalizacji, aż po etap zarządzania dokumentami, których ważność wygasa. Szczątkowe elementy przepisów regulujących omawiane kwestie można co prawda znaleźć w ustawach dotyczących wybranych kategorii dokumentów (m.in. w **USTAWIE Z DNIA 6 SIERPNIA 2010 R. O DOWODACH OSOBISTYCH**, **USTAWIE Z DNIA 13 LIPCA 2006 R. O DOKUMENTACH PASZPORTOWYCH**), jednak brak jest aktu prawnego, który nie tylko objąłby wszystkie wymagające tego dokumenty publiczne, ale równocześnie regulowałby kompleksowo całość zagadnień związanych z ich cyklem życia.

Praktyka ostatnich lat wskazuje, że tego rodzaju regulacja jest niezwykle potrzebna. Obecnie bowiem mamy do czynienia

z sytuacją, w której szereg dokumentów publicznych pozbawionych jest zabezpieczeń adekwatnych do pełnionych przez nie funkcji i ryzyka, jakie może generować dla państwa i obywateli ich podrobienie lub fałszowanie. Przykładem mogą być choćby wypisy aktów notarialnych, pozwolenia na broń, legitymacje pracowników niektórych urzędów centralnych, sądowe tytuły wykonawcze, zaświadczenia o niekaralności itp. Przypomnieć także należy sprawę elektronicznej karty ubezpieczenia zdrowotnego, której projekt w 2015 r. budził szereg poważnych wątpliwości i zastrzeżeń, m.in. w zakresie proponowanych zabezpieczeń fizycznych i informatycznych¹. Sprawa ta uwypukliła słabość regulacji państwa w odniesieniu do sfery projektowania wzorów dokumentów. Każdy minister może bowiem – na podstawie odpowiedniej delegacji ustawowej – wprowadzać nowe wzory dokumentów w zakresie posiadanych przez siebie kompetencji dotyczących kierowania odpowiednim działem administracji rządowej. Zwykle wzory takich dokumentów określone są na poziomie rozporządzeń wykonawczych. Trudno jednak oczekiwać profesjonalnej wiedzy na temat projektowania dokumentów od urzędników nie zajmujących się na co dzień tego rodzaju dziedziną. Innym przykładem obrazującym niedoskonałość obowiązujących regulacji prawnych

REMIGIUSZ LEWANDOWSKI – dr nauk ekonomicznych, Wydział Nauk Ekonomicznych i Zarządzania UMK w Toruniu, członek Rady Przemysłowo-Programowej Wydziału Elektroniki WAT w Warszawie.

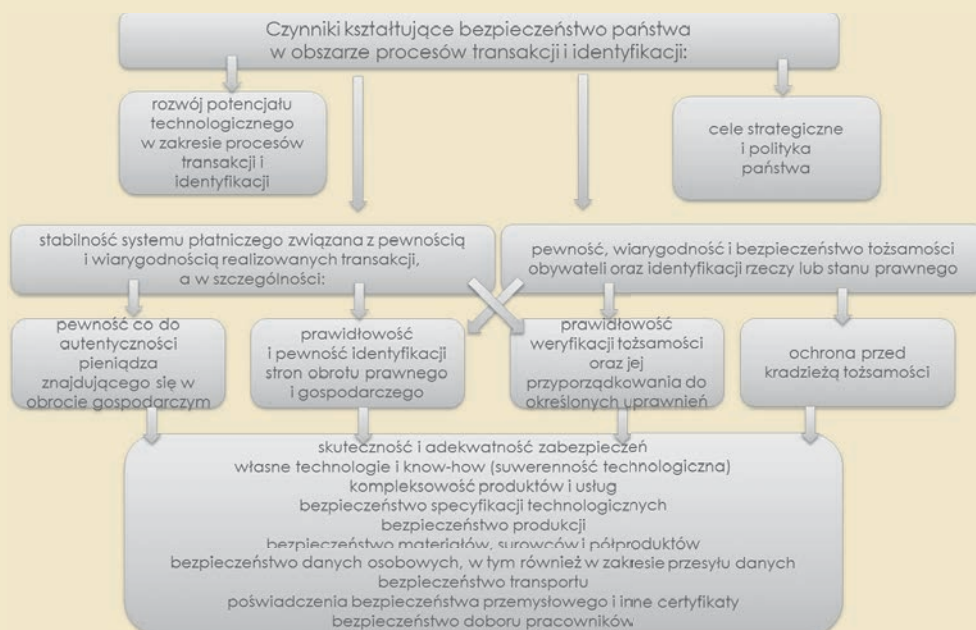
może być sprawa projektu elektronicznego dowodu osobistego z 2011 r. (projekt PL.ID), kiedy to Agencja Bezpieczeństwa Wewnętrznego podzieliła się z premierem swoimi istotnymi zastrzeżeniami i obawami dotyczącymi rozpisania otwartego postępowania przetargowego na produkcję e-dowodu, co generowało ryzyko przejęcia strategicznych informacji państwowych przez obce podmioty (a także obce służby specjalne)². Sprawa ta unaoczniała problem braku legalnego monopolu państwowego wytwórcy dokumentów w odniesieniu do produkcji i personalizacji strategicznych dokumentów publicznych. Warto przypomnieć, że monopol taki nie należy do rzadkości w dużych państwach Unii Europejskiej.

Nie ulega zatem wątpliwości, że dokumenty publiczne pełnią istotną funkcję w systemie bezpieczeństwa narodowego, a relacja ta wymaga uregulowania prawnego. Wskazany związek przyczynowo-skutkowy ujęto na ryc. 1. Związek ten był już szczegółowo przedstawiony na łamach CZŁOWIEKA I DOKUMENTÓW³.

Na tym tle przyjąć można, że dokumenty odgrywają szczególną rolę w kształtowaniu tak zwanego bezpieczeństwa identyfikacyjnego, to jest stanu niezakłóconego funkcjonowania państwa w obszarze obejmującym:

1. prawidłową weryfikację deklarowanej tożsamości osób,
2. prawidłową identyfikację rzeczy (np. przedmiotu oznaczonego znakiem akcyzy),
3. weryfikację prawidłowości przyporządkowania danej osoby i jej tożsamości do określonych uprawnień wynikających z dokumentu, jakim się ona posługuje,
4. potwierdzenie stanu prawnego (np. na podstawie wypisu aktu notarialnego),
5. obrót prawny i gospodarczy związany z użyciem dokumentów potwierdzających tożsamość,
6. ochronę obywateli przed kradzieżą tożsamości⁴.

Państwo, poprzez przepisy prawa, władztwo w zakresie emisji dokumentów i zna-



Ryc. 1. Czynniki kształtujące bezpieczeństwo państwa w obszarze procesów transakcji i identyfikacji
Źródło: opracowanie własne.

ków pieniężnych oraz politykę właścicielską wobec kontrolowanych kapitałowo spółek (np. PWPW S.A.), może kształtować bezpieczeństwo identyfikacyjne oraz bezpieczeństwo związane z obrotem znakami pieniężnymi. W tym obszarze, jak się wydaje, istnieją znaczące możliwości poprawy bezpieczeństwa Polski i Polaków. Warto zatem powrócić do inicjatywy Polskiego Towarzystwa Kryminalistycznego z 2008 r., kiedy to opracowano projekt ustawy o dokumentach publicznych, która miała regulować sferę dokumentów publicznych⁵. Z uwagi na upływ czasu projekt należałoby dostosować do aktualnych realiów i wymogów związanych z bezpieczeństwem państwa. Ustawa powinna objąć następujące zagadnienia:

1. zdefiniowanie dokumentu publicznego wraz z enumeratywnym wskazaniem dokumentów poddanych regulacji,
2. klasyfikację stosowanych w dokumentach zabezpieczeń pod względem ich weryfikacji oraz pod względem wymaganego poziomu bezpieczeństwa,
3. zdefiniowanie narodowego wytwórcy dokumentów, jego zadań i statusu,
4. utworzenie państwowego organu odpowiedzialnego za nadzór nad całokształtem spraw związanych z projektowaniem, produkcją, emisją dokumentów oraz zarządzaniem dokumentami wygasłymi.

Proponowaną definicję dokumentu publicznego i szczegółowy wykaz takich dokumentów zawarłem w artykule *DOKUMENT W SMARTFONIE – NOWOCZESNOŚĆ CZY NIEBEZPIECZNA EKSTRAWAGANCJA?* na str. 16–17 niniejszego wydania.

Osobne zagadnienie stanowią banknoty, których jednak raczej nie należy regulować przedmiotowymi przepisami z uwagi na niezależność banku centralnego.

Przepisy regulujące funkcjonowanie dokumentów publicznych powinny odnosić się także do dokumentów elektronicznych (z warstwą elektroniczną) oraz do informatycznych narzędzi uwierzytelniania obywatela w teleinformatycznych systemach administracji rządowej.

Przy tej okazji warto zwrócić uwagę na pojawiające się niekiedy pomysły zastępowania dokumentów publicznych, w szczególności identyfikacyjnych oraz potwierdzających określone uprawnienia (jak np. prawo jazdy), aplikacjami na telefony komórkowe. Takie koncepty świadczą o niskim poziomie wiedzy i świadomości dotyczącej bezpieczeństwa identyfikacyjnego, bowiem tylko zabezpieczony przed fałszowaniem dokument w zmaterializowanej formie odpowiada na występujące w codziennym życiu wyzwania związane z identyfikacją. „Dokument” w formie aplikacji telefonicznej, którego zdolność do identyfikacji lub potwierdzenia stanu prawnego zależy od żywotności baterii w telefonie oraz odporności oprogramowania na ataki hakerów, nie jest dokumentem wystarczającym do potwierdzenia wynikających z niego treści na akceptowalnym poziomie pewności i wiarygodności. Co więcej, admiratorzy dokumentów w postaci aplikacji telefonicznych nie zdają sobie najwyraźniej sprawy z konieczności – w przypadku Polski – wymiany dominującej części kart SIM w telefonach, aby móc wdrożyć postulowane przez nich rozwiązania. Wiąże się to nie tylko z dodatkowymi kosztami (kto miałby je ponieść?), ale również z niedogodnością dla obywateli. W konsekwencji rozwiązanie niezwykle kosztowne, a przy tym niezapewniające wymaganego poziomu bezpieczeństwa identyfikacyjnego, zapewne okazałoby się marginalne z punktu widzenia powszechności użycia. Oczywiście, zmaterializowana forma dokumentu nie wyklucza zastosowania w jego ramach rozwiązań informatyczno-elektronicznych, jak choćby zapisu danych (w tym danych biometrycznych) na mikroprocesorze czy też danych do składania bezpiecznego podpisu elektronicznego, weryfikowanych za pomocą certyfikatu kwalifikowanego. Podobne refleksje nasuwają się przy analizie potencjalnych narzędzi uwierzytelniania obywatela w systemach teleinformatycznych typu e-government. Naturalnym rozwiązaniem jest oczywiście elektroniczny dowód osobisty. Alternatywne pomysły, np. wykorzystanie bankowości elektronicznej,

obarczone są szeregiem bardzo poważnych słabości (np. phishing, brak certyfikacji, luki w systemach, przypadki włamań do systemów e-bankowości, przypadki infiltracji prywatnych podmiotów przez zagraniczne służby specjalne, ryzyko wynikające z braku nadzoru kapitałowego państwa etc.), co potwierdza praktyka stosowana przez kraje najbardziej zaawansowane w informatyzacji państwa.

Klasyfikacja zabezpieczeń stosowanych w dokumentach publicznych pod względem sposobu weryfikacji może przyjąć następującą formę:

1. zabezpieczenia weryfikowane w sposób wizualny i organoleptyczny (bez użycia urządzeń pomocniczych – np. znak wodny, nitka zabezpieczająca, staloryt, OVI, CLI/MLI, elementy wypukłe itp.),
2. zabezpieczenia weryfikowane poprzez zastosowanie prostych, ogólnodostępnych przyrządów (np. mikrodruki pozytywowo-negatywowe, nadruki i włókna aktywne w świetle UV weryfikowane przy użyciu lupy, lampy emitującej promieniowanie UV w zakresie 365 nm itp.),
3. zabezpieczenia weryfikowane przy użyciu specjalistycznych urządzeń (np. meta-meria, znaczniki czasowe, NIR itp.),
4. zabezpieczenia weryfikowane maszynowo (automatycznie),
5. zabezpieczenia niejawne.

Z kolei wymagany poziom bezpieczeństwa dokumentów publicznych (poziom zabezpieczeń) mógłby przyjąć trzystopniową skalę: od poziomu niskiego, przez średni, do wysokiego. Zabezpieczenia dokumentu publicznego powinny być adekwatne do:

1. ryzyka naruszenia bezpieczeństwa państwa w związku z przerabianiem lub podrabianiem danego typu dokumentu,
2. ryzyka naruszenia bezpieczeństwa obywateli RP w związku z przerabianiem lub podrabianiem danego typu dokumentu,
3. funkcji, jakie dany dokument pełni w obrocie prawnym lub gospodarczym.

Na ryc. 2 przyporządkowano, według subiektywnej opinii autora, wymagany minimalny poziom bezpieczeństwa do różnych typów dokumentów. Za określonym poziomem bezpieczeństwa danego dokumentu powinny stać indywidualnie dopasowane do niego zabezpieczenia. Rodzaj i liczba zabezpieczeń powinny być skorelowane z daną klasą zabezpieczeń (niską, średnią, wysoką) i odpowiednio dobrane przez ekspertów. Świadomie nie wskazano niskiego poziomu bezpieczeństwa w odniesieniu do żadnego z ujętych typów dokumentów. W opinii autora bowiem wpływ wskazanych dokumentów na bezpieczeństwo narodowe wymaga zastosowania zabezpieczeń chroniących je w lepszy sposób przed podrabianiem lub przerabianiem. Niski poziom zabezpieczeń może być adekwatny w przypadku różnego rodzaju zaświadczeń i druków, które nie mają istotnego wpływu na bezpieczeństwo identyfikacyjne.

Kolejną istotną kwestią wymagającą unormowania jest zdefiniowanie statusu narodowego wytwórcy dokumentów publicznych, zadań realizowanych przez ten podmiot oraz zasad, na podstawie których owe zadania są realizowane. Pod pojęciem narodowego wytwórcy dokumentów należy rozumieć producenta dokumentów publicznych, o których mowa w postulowanej ustawie. Wykonywanie działalności gospodarczej narodowego wytwórcy dokumentów publicznych powinno wiązać się z wymogiem uzyskania odpowiedniej koncesji. Koncesjonowanie (reglamentacja działalności gospodarczej) zasługuje na szczególne znaczenie spośród instrumentów regulacji państwa. Za jedną z najważniejszych przesłanek uznaje się bowiem bezpieczeństwo państwa, w tym ochronę interesów obywateli oraz ochronę interesów gospodarczych państwa⁶. Co więcej, zgodnie z praktyką obowiązującą w wielu innych państwach członkowskich Unii Europejskiej, ustawa powinna wyłączać zamówienia na wskazane dokumenty z **PRAWA ZAMÓWIEŃ PUBLICZNYCH**⁷. Status narodowe-

go wytwórcy dokumentów powinien wiązać się z określonymi wymogami względem takiego podmiotu. Powinny one dotyczyć zarówno potencjału ekonomicznego, jak i technologicznego oraz gwarantować bezpieczeństwo w zakresie produkcji strategicznych dla państwa wyrobów. Dlatego narodowy wytwórca dokumentów powinien mieć formę organizacyjno-prawną spółki akcyjnej o kapitale zakładowym nie niższym niż 50 mln zł, z siedzibą na terenie Rzeczypospolitej Polskiej. Skarb Państwa w takim podmiocie powinien dysponować bezpośrednio większością głosów na walnym zgromadzeniu. Kontrola kapitałowa Skarbu Państwa nad omawianym typem przedsiębiorstwa jest bezdyskusyjna i stanowi składową systemu bezpieczeństwa narodowego⁸. Ponadto od narodowego wytwórcy należałoby oczekiwać świadectwa bezpieczeństwa przemysłowego pierwszego stopnia, udokumentowanego posiadania niezbędnego parku maszynowego koniecznego do wytwarzania dokumentów publicznych oraz usytuowania zakładu produkcyjnego (lub zakładów produkcyjnych), w których odbywa się produkcja dokumentów publicznych, na terenie Rzeczypospolitej Polskiej.

W tym miejscu warto również podnieść kwestię – pojawiających się niekiedy w przekazach medialnych dotyczących wyłączenia z zakresu zadań państwa – funkcji nadzoru nad obszarem identyfikacji obywateli oraz emisji (a nie produkcji) wybranych kategorii dokumentów publicznych⁹. W szczególności pomysły te koncentrują się wokół przekazania tych zadań np. do banków. To bardzo niebezpieczne koncepcje, gdyż mogą one prowadzić do budowy alternatywnych względem struktur państwa prywatnych superpodmiotów dysponujących ogromną siłą zarówno w wymiarze kapitałowym, jak i zakresie informacji na temat obywateli i ich danych. Funkcje nadzoru nad zagadnieniem identyfikacji obywateli, zarządzania tożsamością oraz emisji dokumentów publicz-

nych powinny być objęte wyłącznym monopolem państwa.

Bezwzględnie konieczne wydaje się powołanie odpowiedniej jednostki państwowej odpowiedzialnej za kompleksowy nadzór nad sferą dokumentów publicznych. Aktualna atomizacja odpowiedzialności w tym zakresie, w połączeniu z pozbawionymi odpowiednich regulacji elementami cyklu życia dokumentów, przynosi fatalne skutki, jak przytoczone wcześniej projekty elektronicznej karty ubezpieczenia zdrowotnego lub sprawa otwartego postępowania na elektroniczny dowód osobisty. Stąd zasadne jest powołanie do życia wskazanej instytucji, np. w strukturach Agencji Bezpieczeństwa Wewnętrznego. Do zadań takiej jednostki powinny w szczególności należeć:

1. stały nadzór nad prawidłowością funkcjonowania dokumentów publicznych w obrocie prawnym i gospodarczym,
2. inicjowanie ewentualnych zmian w zabezpieczeniach stosowanych w dokumentach publicznych,
3. ostateczne zatwierdzanie wzorów dokumentów publicznych oraz ostateczny dobór i zatwierdzanie zabezpieczeń zastosowanych w dokumentach publicznych,

Dokument / poziom bezpieczeństwa	Minimalny poziom zabezpieczeń		
	niski	średni	wysoki
Dowód osobisty			•
Paszport			•
Dokumenty ubezpieczenia zdrowotnego			•
Dokumenty tożsamości cudzoziemca			•
Dokumenty podróży dla cudzoziemców			•
Dokumenty dotyczące pobytu			•
Dokumenty komunikacyjne			•
Ódpisy aktu stanu cywilnego i zaświadczenia USC		•	
Wypisy aktów notarialnych		•	
Znaki akcyzy			•
Legitymacje funkcjonariuszy Policji, ABW, AW, SKW, SSW, SG			•
Legitymacje funkcjonariuszy i pracowników innych centralnych organów administracji centralnej			•
Świadectwa i dyplomy ukończenia szkół		•	
Sądowe tytuły wykonawcze		•	
Wyroki sądowe oraz zaświadczenia o niekaralności		•	
Książeczki wojskowe			•
Dokumenty związane z posiadaniem broni palnej			•

Ryc. 2. Dokumenty publiczne wraz z przyporządkowanym poziomem ich minimalnego zabezpieczenia

Źródło: opracowanie własne.

4. przyporządkowanie stopnia zabezpieczeń do określonych dokumentów,
5. nadzór nad przestrzeganiem warunków licencjonowanej działalności narodowego wytwórcy dokumentów,
6. prowadzenie Rejestru Dokumentów Publicznych.

Wskazany wyżej nadzór nad prawidłowością funkcjonowania dokumentów publicznych powinien obejmować pełen cykl życia dokumentów, tj.: analizę zagrożeń, projektowanie dokumentów (w tym szczególnie w zakresie zabezpieczeń), produkcję blakietów, przechowywanie blakietów u producenta i w miejscu personalizacji, akwizycję i przetwarzanie danych, personalizację, aktywację warstwy elektronicznej dokumentów (jeżeli jest zintegrowana w dokumencie), wydawanie dokumentów, wydawanie duplikatów, użytkowanie dokumentu (ze zwróceniem uwagi na prawną odpowiedzialność posiadacza za właściwe użytkowanie), weryfikowanie autentyczności dokumentów, wygaśnięcie ważności dokumentu, wycofanie dokumentu, unieważnienie dokumentu. Instytucja odpowiedzialna za nadzór nad wyżej wskazanymi dziedzinami powinna opracowywać odpowiednie zalecenia dotyczące bezpieczeństwa dla podmiotów odpowiedzialnych za realizację poszczególnych etapów cyklu życia dokumentów.

Rejestr Dokumentów Publicznych powinien być z kolei bazą danych dokumentów

publicznych, a jego obiektem powinny być dokumenty publiczne. W bazie danych Rejestru należałoby gromadzić dane o produkcji, wydawaniu, fałszowaniu i ochronie technologicznej dokumentów publicznych.

Ważna pozostaje także kwestia zapewnienia dystrybucji wzorów dokumentów publicznych wśród uprawnionych podmiotów zajmujących się szkoleniami w zakresie bezpieczeństwa dokumentów.

Jednym z podstawowych warunków prawidłowego funkcjonowania państwa, zabezpieczenia rzetelności obrotu gospodarczego oraz bezpieczeństwa obywateli jest zaufanie do wiarygodności dokumentów. Mimo niewątpliwego postępu technicznego i coraz skuteczniejszych metod zabezpieczenia dokumentów przed fałszerstwami, odnotowujemy nadal wysoką dynamikę przestępczości związanej z dokumentami, które stanowią dziś podstawowe narzędzie popełniania wielu rodzajów przestępstw powodujących milionowe straty Skarbu Państwa. Główne powody powyższego stanu rzeczy to brak aktu prawnego (ustawy), który w sposób kompleksowy regulowałby kwestie związane z wytwarzaniem i emisją dokumentów publicznych oraz regulowałby nadzór państwa nad tą dziedziną, a także niedostateczny poziom zabezpieczeń wybranych kategorii dokumentów. Najwyższy czas zmienić ten stan.

¹R. Lewandowski, *Elektroniczna karta ubezpieczenia zdrowotnego – słabe i mocne strony projektowanego rozwiązania*, „Człowiek i Dokumenty” 2015, nr 37, s. 17–26.

²R. Lewandowski, *W kierunku partnerstwa strategicznego państwa i PWPW S.A.*, „Człowiek i Dokumenty” 2013, nr 28, s. 15.

³R. Lewandowski, *Rola PWPW S.A. w systemie bezpieczeństwa państwa. Część II*, „Człowiek i Dokumenty” 2013, nr 30, s. 23–26.

⁴Na podstawie: R. Lewandowski, T. Goliński, *Nielegalna migracja a bezpieczeństwo identyfikacyjne*, [w:] M. Tomaszewska-Michalak, T. Tomaszewski (red.), *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, SAWPiA UW, Warszawa 2015, s. 112.

⁵Projekt ustawy o dokumentach publicznych, „Człowiek i Dokumenty” 2006, nr 3, s. 7.

⁶C. Kosikowski, *Publiczne prawo gospodarcze Polski i Unii Europejskiej*, LexisNexis, Warszawa 2007, s. 187.

⁷R. Lewandowski, *Rola narodowego wytwórcy banknotów, dokumentów i towarzyszących im systemów IT w systemie bezpieczeństwa obrotu gospodarczego i prawnego*, [w:] K. Raczkowski, *Bezpieczeństwo ekonomiczne obrotu gospodarczego*, Wolters Kluwer, Warszawa 2014, s. 240–242.

⁸R. Lewandowski, *Gospodarka a bezpieczeństwo narodowe i rola państwa*, „Człowiek i Dokumenty” 2016, nr 40, s. 35.

⁹Zob. np. K. Klinger, M. Janczura, *Do lekarza jak do bankomatu*, „Dziennik Gazeta Prawna” z 18 kwietnia 2016 r., s. A2.

Krzysztof Izak

DOKUMENT I TOŻSAMOŚĆ JAKO ELEMENT DŻIHADU

Miesiące, które upłynęły od zamachów terrorystycznych w Paryżu (13 listopada 2015 r. i 14 lipca 2016 r.), Brukseli (22 marca 2016 r.) oraz serii lipcowych ataków w Niemczech nie spowodowały widocznych zmian w sposobie postrzegania przez władze UE zagrożenia związanego z przybywającymi do Europy muzułmańskimi imigrantami.



Wyprowadzanie na ulice europejskich miast coraz większej liczby policjantów i żołnierzy nie uchroni obywateli Europy przed kolejnymi atakami, najwyżej przesunie je w czasie. Tymczasem z tygodnia na tydzień wzrasta liczba nielegalnych imigrantów przybywających do Europy z krajów muzułmańskich, którym pomocy w dotarciu na nasz kontynent udzielają władze poszczególnych państw, instytucje pozarządowe i siły morskie UE operujące na Morzu Śródziemnym.

Jeśli klasa polityczna wciąż będzie unikać zdefiniowania zagrożenia, to przeciwdziałanie mu będzie niemożliwe. Pozostanie jedynie usuwanie skutków zamachów i likwidowanie kolejnych komórek terrorystycznych cieszących się poparciem lub sympatią społeczności muzułmańskich. Niewątpliwie spowoduje to radykalizację nastrojów społecznych oraz wzrost siły i aktywności organizacji skrajnie prawicowych, antyimigracyjnych. Co przy działaniach tzw. lewicowców, wspierających imigrantów i dopatrujących się w nich źródła potrzebnej Europie – ich zdaniem – „nowej krwi” w celu wprowadzenia zróżnicowania etnicznego i kulturowego wywoła akty wzajemnej agresji i przemocy, które już mają miejsce w Niemczech, Austrii, Szwecji czy we Francji. Mimo tego zagrożenia rząd niemiecki kontynuuje politykę nastawioną na przyjmowanie imigrantów z krajów podwyższonego ryzyka

(pod osłoną nocy przyjmowane są na niemieckich lotniskach specjalne transfery imigrantów z Turcji i Grecji), przechodząc od epoki oblędu czystej rasy do szaleństwa pomieszania ras, prowadząc Europę w kierunku kryzysu wartości i tożsamości oraz kulturowego i cywilizacyjnego upadku, którego świadkiem będą kolejne pokolenia, a może już nasze dzieci i wnuki.

W przemówieniu transmitowanym na żywo przez telewizję w marcu 2016 r. turecki prezydent Recep Tayyip Erdoğan, który chce uczynić z Turcji drugie Imperium Otomańskie, a siebie chętnie widziałby jako nowego sułtana, podkreślił, że Ankara nie będzie słuchać krytyki z zewnątrz na temat przestrzegania praw¹. Wypowiadał się w czasie, gdy w Brukseli trwało spotkanie premiera Turcji Ahmeta Davutoglu z szefem Rady Europejskiej Donaldem Tuskiem i przewodniczącym KE Jean-Claude'em Junckerem. Erdoğan powiedział m.in.: *W czasie, gdy Turcja gości trzy miliony migrantów, ci, którzy nie mogą znaleźć miejsca dla garstki uchodźców, i ci, którzy w samym środku Europy przetrzymują tych niewinnych ludzi w haniebnych warunkach, najpierw muszą spojrzeć na siebie.* Gdyby UE właściwie i rzetelnie zdefiniowała, kim są tzw. uchodźcy i nie bała się nazwać ich muzułmanami, którzy w Europie skutecznie zawłaszczają naszą przestrzeń, i konsekwentnie piętnowała antyludzki charakter

KRZYSZTOF IZAK – były funkcjonariusz ABW. Zajmował się problematyką terroryzmu oraz ekstremizmów religijnych i politycznych.



Ryc. 1. Strona personalizacyjna fałszywego paszportu terrorysty Ahmada Almohammada

Žródło: <http://freeglobe.parlamentnilisty.cz/Articles/14789-srbska-policie-zadrzela-muze-se-stejnym-pasem-jaky-se-nasel-u-teroristy-v-parizi-foto-.aspx> (dostęp 24.05.2016).

ich religii, traktującej innowierców jako ludzi drugiej kategorii, Erdoğan nie wypowiedziałby tych słów, bowiem gości u siebie właśnie muzułmanów – braci i siostry w wierze. Nie należy również zapominać, iż prezydent Turcji konsekwentnie realizuje idee międzynarodowego ruchu Braci Muzułmanów, których celem jest panowanie islamu nad światem i wywodzi się z niego cały szereg islamskich organizacji terrorystycznych².

FAŁSZYWE DOKUMENTY – FAŁSZYWA TOŻSAMOŚĆ

W dniu 26 marca 2016 r. specjalny oddział włoskiej policji zatrzymał w Belizzi koło Salerno, na południu kraju, Dżamala ed-Dine Ouali'ego, obywatela Algierii, który był poszukiwany europejskim nakazem aresztowania wydanym przez władze Belgii. Miał on sfabrykować i dostarczyć dżihadystom³ z Bliskiego Wschodu fałszywe dokumenty umożliwiające uzyskanie statusu uchodźcy w UE. Nazwisko Algierczyka znajdowało się na dokumentach znalezionych w październiku 2015 r. podczas przeszukania mieszkania w pobliżu Brukseli. Odkryto tam również dokumenty z fotografiami niektórych terrorystów zaangażowanych w zamachy w Paryżu z 13 listopada 2015 r. i w Brukseli z 22 marca 2016 r. Należy w tym miejscu przypomnieć, iż dwóch z ośmiu terrorystów wjechało do Europy, posługując się sfalszowanymi paszportami syryjskimi. Przy

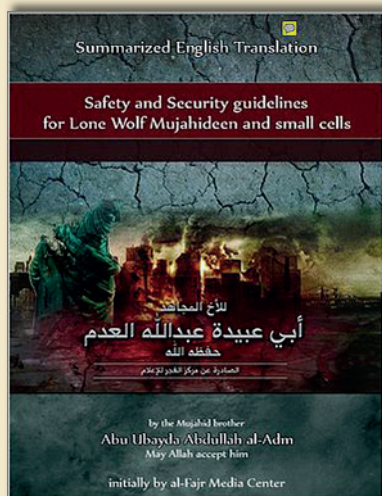
zwłokach jednego z nich, Ahmada Almo-hammada, znaleziono taki właśnie paszport. Innym przykładem jest Szwed syryjskiego pochodzenia podejrzewany o członkostwo w grupie terrorystycznej, która przygotowywała ataki w Paryżu i Brukseli. Osobą tą jest Osama Krajem, który w 2005 r. wystąpił w propagandowym filmie dokumentalnym pt. BEZ GRANIC – FILM O SPORCIE I INTEGRACJI, przedstawiającym, oczywiście na wyrost, integrację w Malmö przez pryzmat sportu. Krajem, wówczas jedenastoletni chłopiec, opowiadał w nim, jak drużyna piłkarska pomogła mu odnaleźć się w szwedzkim społeczeństwie. Osiem lat później bohater filmu został zatrudniony jako stażysta w dziale zarządzania rady miejskiej Malmö. Niedługo potem zaczął ubierać się w tradycyjny strój muzułmański (długa, luźna szata) i zapuścił brodę. W 2014 r. zniknął bez słowa, a rok później można go było zobaczyć na fotografiach dżihadystów w Syrii. Z powrotem przedostał się do Europy jako uchodźca, posługując się fałszywym syryjskim paszportem. We wrześniu 2015 r. został zarejestrowany na greckiej wyspie Leros. Następnie dotarł do Niemiec, gdzie w Ulm spotkał się z Salahem Abdeslamem, koordynatorem ataków w Paryżu. Osama Krajem został aresztowany 8 kwietnia 2016 r. Wiadomo, że kontaktował się z zamachowcem samobójcą z brukselskiego metra. Miał również przy sobie torbę z ładunkami wybuchowymi. Nie zdetonował ich i nie zostały one odnalezione. Krajem podczas przesłuchania nie ujawnił, co z nimi zrobił. Natomiast wspomniany Abdeslam jesienią 2015 r. przybył do jednego z niemieckich obozów dla uchodźców, skąd przywiózł trzech mężczyzn, którzy z fałszywymi syryjskimi paszportami dotarli do Europy przez grecką wyspę Leros. Dwóch z nich zostało zatrzymanych. Istniała obawa, iż trzeci wciąż mógł ukrywać się w Brukseli i posiadać torbę z ładunkami wybuchowymi, których nie zdetonował Osama Krajem w brukselskim metrze w dniu 22 marca 2016 r.

Fałszywe dokumenty umożliwiają podróż tzw. foreign fighters na front dżihadu oraz powrót z niego do Europy jako dezertersów, weteranów i potencjalnym terrorystom. Pod koniec 2015 r. Państwo Islamskie wysłało z Iraku do Europy ponad 40 osób, których tożsamość poznały służby specjalne państw UE. Mieli oni odgrywać rolę uśpionych komórek planujących przeprowadzenie zamachów terrorystycznych w Europie w okresie świąteczno-noworocznym. Wiadomo było, że wszystkie te osoby to Irakijczycy w wieku od 20 do 35 lat i że przybyli do Europy, ukrywając się w grupach nielegalnych imigrantów. Natomiast tym, co umknęło uwadze poszukujących ich służb, był fakt, iż prawdziwa tożsamość potencjalnych terrorystów niekoniecznie musiała pokrywać się z danymi personalnymi figurującymi w ich dokumentach, o ile w ogóle takie posiadali.

W 2015 r. Państwo Islamskie opublikowało w Internecie dwa przewodniki dla dżihadystów. Pierwszy, pt. *Hijrah to the Islamic State*, zawiera szczegółowe informacje na temat bezpiecznej podróży do Syrii i Iraku,

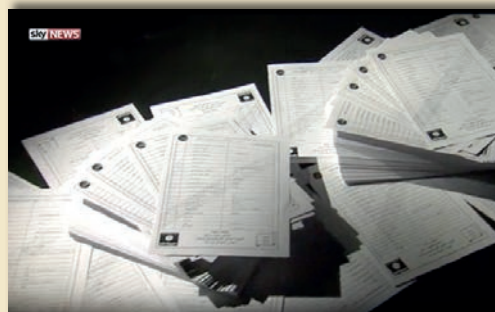
natomiast drugi, *How to survive in the West. A Mujahid Guide*, jest szczegółowym materiałem instruktażowym dla potencjalnych bojowników, co podkreślają tytuły kolejnych rozdziałów: 1. *Ukrywanie ekstremistycznej tożsamości*; 2. *Naruszenie lojalności*; 3. *Zarabianie pieniędzy*; 4. *Prywatność internetowa*; 5. *Szkolenie*; 6. *Prymitywna broń*; 7. *Broń nowoczesna*; 8. *Produkowanie bomb w domu*; 9. *Transport broni*; 10. *Co dzieje się, gdy jesteś szpiegowany i zostajesz napadnięty*; 11. *Zaczyna się dżihad*; 12. *Ucieczka w celu znalezienia bezpieczeństwa*. Materiał ten przygotowuje „prawdziwych” muzułmanów do wojny w sercu Europy. Walka zbrojna zastąpić ma działalność misyjną (dawa) określaną mianem dżihadu języka lub zaproszeniem do islamu, która mimo olbrzymich nakładów pracy nad ukazaniem, jak dobrymi obywatelami w społeczeństwie europejskim są muzułmanie, ponosi sromotną porażkę. Według autorów przewodnika niewierni przywódcy w państwach zachodnich kłamią w mediach i nazywają wszystkich muzułmanów terrorystami⁴, choć muzułmanie temu zaprzeczają, chcąc być pokojowo nastawionymi obywatelami. Jednak społeczności europejskie osaczyły – zdaniem autorów – muzułmanów i zmusiły ich do radykalizacji⁵, co będzie przyczyną porażki Zachodu i powodem podboju Rzymu.

W ostatnich dwóch akapitach umieszczonych we wstępie można przeczytać: *Niniejsza książka to przewodnik dla muzułmanów, którzy mieszkają na terenie w większości niemuzułmańskim lub w państwie, gdzie rządzący są surowi wobec wiernych. Niniejszy przewodnik wyjaśni wam różne scenariusze sytuacji, w których możecie się znaleźć oraz sposób reakcji. Nauczy was jak być tajnym agentem, który prowadzi podwójne życie, co muzułmanin będzie musiał zrobić, aby przetrwać w nadchodzących latach. Autor tej książki przez ponad 10 lat badał globalny dżihad, więc ma wiedzę na temat różnych typów grup dżihadu na świecie oraz tego, w jaki*



Ryc. 2. Strona tytułowa WYTYCZNYCH W SPRAWIE BEZPIECZEŃSTWA I OCHRONY DLA MUDŻAHEDINÓW SAMOTNYCH WILKÓW
Źródło: <http://www.critical-link.co.uk/#!Operation-Temperer-The-plan-to-deploy-military-personnel-to-support-Police-in-the-event-of-multiple-terrorists-attacks-and-to-guard-critical-infrastructure-targets/c6ke/55b786520cf228fd5ebac119> (dostęp 24.05.2016).

sposób te grupy doznały porażek i osiągnęły sukcesy. Mam nadzieję, że odniesiesz korzyści z tej książki i pamiętaj, że poza Allahem nie ma mocy ani schronienia, więc proś go, bo będziesz ich potrzebował. Z rozdziału pierwszego dowiadujemy się o konieczności zachowania w tajemnicy prawdziwej tożsamości, jej zmiany i posługiwania się pseudonimem. Na początku stycznia 2016 r. ukazał się w Internecie podręcznik Państwa Islamskiego dla „samotnych wilków”, również w języku angielskim, żeby niemówiący po arabsku bracia mogli go stosować w swoich błogosławionych operacjach, zatytułowany SAFETY AND SECURITY GUIDELINES FOR LONE WOLF MUJAHIDEN (WYTYCZNE W SPRAWIE BEZPIECZEŃSTWA I OCHRONY DLA MUDŽAHEDINÓW SAMOTNYCH WILKÓW). 58-stronicowa instrukcja terroryzmu, która na okładce pokazuje płonące wieżowce, zbudowane w stylu zachodnim, opisuje m.in. jak ważny jest element zaskoczenia w chwili zamachu i w jaki sposób można osiągnąć maksymalny efekt. Wyjaśnia, że kluby nocne, pełne głośniejszej muzyki i pijanych ludzi, to idealne miejsce na omówienie planów terrorystycznych bez zwracania uwagi i bycia zauważonym. Ideą podręcznika jest wskazanie, że koniecznością jest wkomponowanie się w zachodni styl życia i niewyglądanie na muzułmanina, aby pozostać poza zainteresowaniem zachodnich służb bezpieczeństwa. Czytamy: *Nie ulega wątpliwości, że dzisiaj, w dobie samotnych wilków, bracia z Zachodu, trzeba wiedzieć kilka ważnych rzeczy na temat bezpieczeństwa w celu zapewnienia sukcesu w działaniach. Mamy nadzieję, że wielu niemówiących po arabsku braci uzna ten podręcznik za interesujący i będzie go stosować do swoich operacji.* Autor kładzie duży nacisk na wtapianie się żyjących na zachodzie dżihadystów w tłum. Mają oni między innymi golić brodę, integrować się i udawać chrześcijan. Przydatne w tym ostatnim jest noszenie niewielkich krzyżyków. Powinni także stronić od muzułmańskich, bezalkoholowych perfum, a nawet od arabskiego je-



Ryc. 3. Wypełnione formularze zgłoszeniowe do Państwa Islamskiego
Źródło: <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12189582/Isil-leak-of-1736-top-secret-documents-names-16-British-terrorists.html> (dostęp 24.05.2016).

dzenia. To może bowiem stanowić trop dla wrogich służb specjalnych. Ubierać się mają na sposób zachodni i używać niereligijnych pozdrowień, z wykluczeniem na przykład zwrotu *salam alejkum*. Jednocześnie niezalecane są zbyt częste zmiany zachowania, gdyż także one mogą wzbudzać podejrzenia. Specjalne ostrzeżenia kierowane są pod adresem liderów, którzy założyli nowe komórki terrorystów. Po dokonaniu dzieła powinni oni udać się na front lub zakończyć życie w samobójczym zamachu. Dzięki temu zminimalizują ryzyko przedostania się informacji w niepowołane ręce.

O ile fałszywe dokumenty i zmiana tożsamości dżihadystów stanowią poważny problem dla służb specjalnych, to dokumenty wytwarzane przez Państwo Islamskie są doskonałym źródłem identyfikacji ekstremistów. Na początku marca 2016 r. stacja Sky News „otrzymała” od bliżej nieznanego mężczyzny, podającego się za Abu Hameda, kartę pamięci zawierającą dane 22 tysięcy dżihadystów z Państwa Islamskiego. Abu Hamed należał najpierw do Wolnej Armii Syryjskiej, a następnie wstąpił do Państwa Islamskiego. Kartę ukradł on szefowi osławionej służby wywiadu i bezpieczeństwa organizacji, Abu Lukmanowi as-Suriemu. Z łupem tym zbiegł następnie do Turcji. Karta pamięci zawiera formularze zgłoszeniowe z 23 pytaniami. Poza imieniem i nazwiskiem

kandydaci wpisywali tam m.in. swoje numery telefonów, a także informacje o własnej rodzinie, posiadanym wykształceniu i doświadczeniu bojowym oraz o zakresie swej wiedzy na temat *szariat*u. Podawali również, kto rekomendował ich do Państwa Islamskiego. W formularzu można było także zadeklarować gotowość wzięcia udziału w szkoleniu na zamachowca-samobójcę. Według Sky News niektóre z ujawnionych nazwisk były już wcześniej dobrze znane, ale nowe dokumenty mogą pomóc w zidentyfikowaniu ekstremistów, o których działalności władze ich krajów dotąd nie wiedziały. Formularze wypełnili ochotnicy z 51 państw, w tym Wielkiej Brytanii, kilku krajów Europy Północnej, USA, Kanady oraz państw Afryki Północnej i Bliskiego Wschodu. O przecieku tajnych danych personalnych Państwa Islamskiego poinformował SÜDDEUTSCHE ZEITUNG twierdząc, że wraz z niemieckimi regionalnymi telewizjami publicznymi NDR i WDR uzyskał wgląd w kilkadziesiąt formularzy z danymi na temat dżihadystów niemieckich. Formularze wypełniano przy wjeździe na opanowane przez IS tereny Syrii. Przedstawiciele niemieckich służb poinformowali, że pozyskane dokumenty dotyczą również znanych im obywateli Niemiec, którzy nie zostali osądzeni, ponieważ brak było dowodów na temat ich udziału w Państwie Islamskim. Od wybuchu wojny domowej w Syrii z Niemiec w rejon walk wyjechało ponad 800 radykałów. Około 130 z nich zginęło w walkach. Jedna trzecia powróciła do kraju. 70 osób zdobyło doświadczenia wojenne⁶.

Porozumienie Unii Europejskiej i Turcji z 18 marca 2016 r. dotyczące odsyłania z greckich wysp imigrantów, którym udało się tam dotrzeć nielegalnie przez Morze Egejskie spowodowało wyraźne ograniczenie liczby ludzi przerzucanych z wybrzeża Turcji. Przemysłownicy zamieścili na FACEBOOKU nową ofertę, zachwalając swoje usługi. Proponowali m.in. miejsce na statku płynącym z tureckiego portu Mersin do Włoch. Koszt transpor-

tu to 4 tys. USD od osoby, czyli cztery razy drożej niż tradycyjnym, dotychczasowym szlakiem przez Morze Egejskie na pobliskie wyspy należące do Grecji. Jedna z ofert była bardzo konkretna: *Rejs jest w sobotę, z Mersin do Włoch, na statku handlowym długości 110 metrów, zaopatrzonym w jedzenie, wodę, kamizelki ratunkowe i lekarstwa*. Inne oferty dotyczyły rejsu z Antalyi. Wszystkie mieściły się cenowo w granicach od 3 do 5 tys. USD. Numery telefonów komórkowych przemysłowników zamieszczone są na stronach społecznościowych. Można zatelefonować i „zarezerwować rejs”. Organizatorzy procederu, którzy nie dysponują własnymi statkami, przekupują załogi i lokują imigrantów pod pokładem jako pasażerów na gapę. Znacząco przymknięcie bram szlaku przerzutu ludzi do Grecji (zamiast od kilkuset do dwóch tysięcy imigrantów dziennie, w kwietniu i maju 2016 r. liczba imigrantów przybywających do Grecji została ograniczona od kilkudziesięciu do ok. 200, ale w czerwcu przybyło ich 1450 a w lipcu ponad 2000) spowodowało nie tylko wzrost kosztów tego procederu, ponieważ wydłużyło trasy, a przede wszystkim wywołało popyt na europejskie dokumenty umożliwiające wjazd do UE. Ponadto zamknięcie szlaku bałkańskiego uwięziło wielu imigrantów w pułapce na terenie Grecji. Dotyczy to zwłaszcza obywateli Afganistanu, których w 2015 r. dotarło do Europy ponad 250 tys. Poza Niemcami i krajami skandynawskimi nie mają oni większych szans na pozytywne przejście procedury uchodźczej. Stąd popyt na fałszywe syryjskie paszporty, które dają pewność uzyskania statusu uchodźcy. W 2015 r. na FACEBOOKU utworzony został arabskojęzyczny profil AZYL W NIEMCZACH, na którym znalazła się oferta sprzedaży syryjskich paszportów oraz informacje na temat miejsc, gdzie służby graniczne nie pobierają odcisków palców. Paszport można otrzymać przesyłką za pośrednictwem kurierów. Podano także turecki numer telefonu, na który należy złożyć zamówienie. O doku-

ment wystąpiło wiele osób przebywających w obozach dla uchodźców rozmieszczonych w południowej Turcji. Na tym samym profilu dostępny jest również cennik innych fałszywych dokumentów, w tym świadectw, zaświadczeń i legitymacji, oraz instruktaż, jak zachować się podczas przesłuchania przez służby imigracyjne, aby pozytywnie przejść przez procedurę azylową. Jednak w ostatnich miesiącach Afgańczycy legitymujący się syryjskimi paszportami coraz częściej nie przechodzą weryfikacji z prozaicznego powodu. Otóż służby w niektórych państwach podczas kontroli przeprowadzają wywiady z domniemanymi Syryjczykami, którzy – jak się okazuje – w ogóle nie mówią po arabsku, a jeśli już, to nie potrafią odpowiedzieć na proste pytania dotyczące „ich” kraju. Ci, którzy posiadają pieniądze, za 10 tys. euro mogą w Grecji kupić pakiet dla jednej osoby zawierający fałszywy paszport, pozwolenie na pobyt w Grecji i bilety lotnicze. Potencjalnym klientom umożliwia to bezproblemowe przedostanie się do Niemiec, Szwecji lub Wielkiej Brytanii. Według gazety DAILY MAIL, której informacji udzielił jeden z przemysłowców, w procedurze tym biorą udział setki osób przebywających na greckich wyspach⁷.

Dla Afgańczyków pozostających jeszcze w ojczyźnie istnieje „specjalna” oferta podróży do Europy okreśną drogą. Agenci

z biur turystycznych już mówią o potencjalnych kierunkach. Wzrasta zapotrzebowanie na loty do Indii, Indonezji, Tadżykistanu i Uzbekistanu. Afgańczycy, którzy dotrą do tych krajów, ubiegają się o status uchodźcy w biurach ONZ i liczą na korzystną relokację. Są i tacy, którzy mają nadzieję, że do Europy dotrą przez Rosję, Ukrainę, a nawet Białoruś i kupują przeloty do naszych wschodnich sąsiadów. Na zmiany błyskawicznie zareagował czarny rynek. W Kabulu pojawili się handlarze dokumentami – za „wizę Schengen” trzeba zapłacić 15–25 tys. dol. Według osób pośredniczących w organizowaniu tych dokumentów, pochodzą one wprost z europejskich ambasad, gdzie są wydawane przez urzędników w zamian za łapówki. Ta opcja jest jednak dostępna tylko dla wybrańców, bo nawet przy założeniu, że dana rodzina wyprzeda cały swój dobytek, nie będzie w stanie kupić tak drogiej wizy. Bez wątpienia najbardziej nietypowym kierunkiem podróży, który obierają mieszkańcy Afganistanu, jest Kuba. Od lutego 2016 r. rośnie liczba wniosków o wizy, bowiem wyspa ta jest traktowana jako przystanek w drodze do Stanów Zjednoczonych lub Kanady (przez Meksyk). Niektórzy wybierają kraje Ameryki Południowej, z której także chcą ruszyć na północ. Cały proces nie jest prosty, bo jeśli na przykład rodzina zdobędzie wizy do Ekwadoru, do którego nie da się dolecieć z Afganistanu, musi jeszcze zorganizować sobie pozwolenia na cały tranzyt. Wówczas przykładowy szlak lotniczy potrafi wieść z Afganistanu przez Pakistan, gdzie trzeba zdobyć wizę tranzytową do Brazylii, skąd dopiero można lecieć do Ekwadoru. A to przecież nie koniec podróży, bo dopiero stamtąd rozpoczynają się próby przedostania się do Ameryki Północnej⁸.

Z przedstawionych wyżej informacji, wynika, że nie wszyscy imigranci z krajów muzułmańskich chcą osiedlić się w Europie. Dla niektórych (przykład Afgańczyków) kierunkiem może być Ameryka Łacińska, ale i tak ostatecznym celem są Stany Zjednoczone

شهادة سواقة دولية

شهادة سواقة خاصة

@safi.alhalabi

شهادة سواقة خاصة

تأمين إقامة تركية

تصديق أوراق من الخارجية

الخدمة التي نقدمها

الخدمات التي نقدمها هي:

- 1- تصديق أوراق من الخارجية
- 2- تأمين إقامة تركية
- 3- شهادة سواقة خاصة
- 4- شهادة سواقة دولية
- 5- تصديق أوراق من الخارجية
- 6- تأمين إقامة تركية
- 7- شهادة سواقة خاصة
- 8- شهادة سواقة دولية
- 9- تصديق أوراق من الخارجية
- 10- تأمين إقامة تركية
- 11- شهادة سواقة خاصة
- 12- شهادة سواقة دولية
- 13- تصديق أوراق من الخارجية
- 14- تأمين إقامة تركية
- 15- شهادة سواقة خاصة
- 16- شهادة سواقة دولية
- 17- تصديق أوراق من الخارجية
- 18- تأمين إقامة تركية
- 19- شهادة سواقة خاصة
- 20- شهادة سواقة دولية

Album: Zdjeka na wsi casu

Genre: polski

Polizine

Obwiazki przeplatanej zdjęć

Posiada

Wzrostu post

Ryc. 4. Cennik fałszywych syryjskich dokumentów
Źródło: <http://krajwspanialy.pl/fałszywe-paszporty-imigranta-facebook/> (dostęp. 24.05.2016).

lub Kanada. Z drugiej strony nie wszystkich można posądzać o złe zamiary zbudowane na fundamencie idei dominacji islamu nad światem. Przykładem są ci, którzy za pieniądze są skłonni wrócić do ojczystego kraju. W 2015 r. Niemcy „deportowały” ok. 21 tys. osób, których wnioski o azyl zostały odrzucone. To kropla w morzu, jeżeli liczyć, że zobowiązanych do opuszczenia Niemiec jest obecnie 200 tys. imigrantów. Część z nich wyjedzie zapewne dobrowolnie, skuszona korzyściami materialnymi. Uczyniło to w 2015 r. ponad 37 tys. przybyszów, głównie z państw bałkańskich. Dostali nie tylko bilety w jedną stronę, ale także co najmniej kilkaset euro na wynajęcie mieszkania, a w uzasadnionych przypadkach nawet 3 tys. euro na uruchomienie własnego biznesu. Jest to suma równa dziewięciomiesięcznym średnim dochodom w Kosowie czy Bośni i Hercegowinie. W stosunku do imigrantów z innych krajów obowiązują odmienne zasady. Generalnie każdy wracający do swego kraju dorosły imigrant może liczyć na 200 euro plus bilet czy też 250 euro na benzynę, jeżeli wraca własnym samochodem. Na dzieci do 12 lat przypada premia 100 euro. Ale są też specjalne programy, które czynią z biednych imigrantów ludzi bogatych w kraju pochodzenia. Na przykład 21-letni Lauand Sadek w grudniu 2015 r. dał się skusić na powrót do rodzinnego Irbilu w irackim Kurdystanie za cenę biletu lotniczego, tysiąca euro do ręki i obietnicy pomo-

cy w uruchomieniu własnego sklepu spożywczego. W sumie miał otrzymać 6 tys. euro. Wszystko to opowiedział dziennikarzom WASHINGTON POST, będąc już w Irbilu. Jednak takie postępowanie sprawia, iż wielu imigrantów przybywa do Niemiec, licząc wyłącznie na tego rodzaju korzyści materialne⁹. Ponadto nie ma żadnej pewności, że ci, którzy wrócili do kraju pochodzenia, nie zechcą znowu wyruszyć do Europy, skoro tu dostają pieniądze „za powrót”. Osoby, które uzyskują prawo do pobytu w danym kraju, otrzymują opiekę socjalną i zasiłki. Część muzułmanów traktuje wypłacane im w państwach Unii Europejskiej zasiłki pieniężne jako należny im podatek pogłówny (*dżizja*) płacony w czasach kalifatu przez *zimmich* (chrześcijan i żydów zamieszkujących ziemie znajdujące się pod kontrolą islamu).

Z drugiej strony zbliża się nowe niebezpieczeństwo związane ze zniesieniem wiz dla obywateli Turcji. Procedura ta miała nastąpić już od 1 lipca br., jednak została oddalona w czasie, ponieważ Turcja nie zdołała spełnić warunków, od których UE uzależniała zawieszenie ruchu wizowego z Ankarą. Powodem był impas, w jakim pograżyły się prowadzone od 2013 r. turecko-unijne negocjacje. Pierwotnie zakładano, że rozmowy zakończą się do lipca br. Głównym punktem spornym okazała się turecka ustawa antyterrorystyczna, która zdaniem obrońców praw człowieka jest na tyle szeroka, że daje władzom pretekst do ścigania dysydentów politycznych i dziennikarzy. Turcja zapowiedziała, że nie zmieni ustawy pod naciskiem UE, tym bardziej, że zmaga się z poważnym zagrożeniem ze strony terrorystów. W ocenie Komisji Europejskiej Turcja spełniła większość z 72 kryteriów zniesienia wiz; pozostało jedynie pięć, w tym postulowana przez UE zmiana ustawy antyterrorystycznej. Ankara uważa, że spełniła wszystkie wymagania¹⁰. Bez dopełnienia pozostałych warunków UE nie zniesie wiz, co obiecała w ramach obowiązującej od 20 marca umowy o odsyłaniu



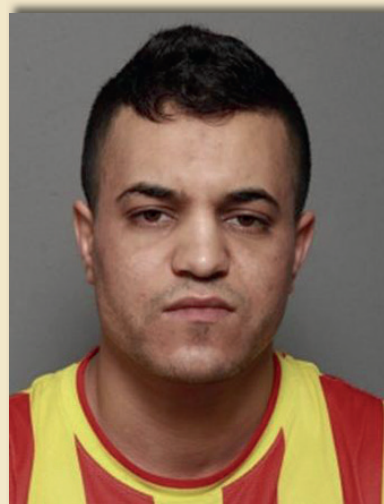
Ryc. 5. Paszport turecki

Źródło: <http://www.wykop.pl/link/3159427/zobacz-jak-latwo-uchodczy-kupia-falszywe-paszporty/> (dostęp 24.05.2016).

do Turcji nielegalnie przybywających do Unii migrantów. W dniu 20 maja br. szefowie MSZ państw UE wypracowali porozumienie, które umożliwi Unii szybsze i łatwiejsze zawieszanie ruchu bezwizowego z państwem trzecim w przypadku nadużyć albo ze względów bezpieczeństwa. To skutek obaw niektórych państw unijnych przed planowanym zniesieniem wiz dla obywateli Turcji, Kosowa oraz Ukrainy i Gruzji, zamieszkanym łącznie przez około 125 mln ludzi¹¹. Jednak nieudany pucz wojskowy w Turcji 15 lipca 2016 r. całkowicie zmienił sytuację. Zawieszono prawa człowieka, tysiące ludzi znalazło się w więzieniach, dziesiątki tysięcy straciło pracę, zapowiedziano wprowadzenie kary śmierci i zagrożono otwarciem szlaków dla imigrantów, jeśli najpóźniej w październiku UE nie zniesie wiz dla Turków, co w kontekście obecnej rzeczywistości w Turcji wydaje się nierealne.

Niezależnie od tego, czy i kiedy zniesione zostaną wizy dla posiadaczy tureckich paszportów, obok przyjeżdżających dotąd imigrantów legitymujących się fałszywymi paszportami syryjskimi pojawiają się tacy, którzy posługują się fałszywymi paszportami tureckimi. Na czarnym rynku w Stambule można je kupić już za 200 euro, co i tak podobno stanowi nieco wygórowaną cenę ze względu na nadpodaż tych dokumentów. Istnieje też prawdopodobieństwo, że prezydent Turcji, chcąc uchodzić za jeszcze bardziej bezkompromisowego i twardego polityka, odporne na naciski UE, i tym samym zyskać poparcie coraz większej części społeczeństwa dla swych autorytarnych rządów, wykorzysta odsunięcie w czasie zniesienia wiz dla obywateli Turcji do zawieszenia lub wycofania się z umowy zawartej w marcu z UE przez byłego już premiera Ahmetą Davutoğlu. Groziłoby to Europie nową falą migracyjną, być może jeszcze większą niż ta, która miała miejsce w 2015 r. Tak czy inaczej, obie opcje – Turcy lub Syryjczycy (a właściwie ci, którzy posługują się tu tureckimi i syryjskimi paszportami) – stawiają UE na przegranej pozycji,

a wszystko przez doprowadzone do absurdu prawa człowieka, polityczną poprawność, utopijną ideologię multikulturalizmu i krótkowzroczną, bezrefleksyjną politykę.



Ryc. 6. Tarek Belgacem

Źródło: <http://www.leparisien.fr/espace-premium/actu/l-et-range-portrait-de-l-assailant-du-commissariat-de-la-goutte-d-or-11-01-2016-5438287.php#xtref=https%3A%2F%2Fwww.google.pl> (dostęp 24.05.2016).

Tymczasem procedury rejestrowania uchodźców wciąż nie funkcjonują w sposób prawidłowy. Wielu migrantów rejestruje się więc pod różnymi nazwiskami i otrzymuje kilka dokumentów, dzięki którym mogą wyłudzać pomoc socjalną i niezauważenie przemieszczać się po Europie. Mężczyzna, który 7 stycznia 2016 r. zginął w Paryżu w wyniku operacji antyterrorystycznej policji, miał wiele nazwisk. We Francji nazywał się Hale Mohammed i pochodził rzekomo z Iraku. W Szwecji był Gruzinem o nazwisku Nika Khenchiasvili. W Luksemburgu znany był jako Mohammed Salah z Maroka. W Niemczech zaś jako Walid Salihi z Syrii lub Walid Esalihi z Maroka. Z kolei zamachowiec, który mieszkał w schronisku dla uchodźców w Recklinghausen w Nadrenii Północnej-Westfalii, podał w sumie dwadzieścia różnych tożsamości i sześć narodowości. W rzeczywistości nazywał się Tarek Belgacem, urodzony 28 marca 1991 roku w Ouled

Chamekh w Tunezji. W styczniu 2016 r. zaatakował za pomocą topora i atrapy bomby komisariat policji w paryskiej dzielnicy Goutte-d'Or, krzycząc: *Allahu akbar!* Został zastrzelony przez funkcjonariuszy. Belgacem bez trudu oszukiwał władze w całej Europie, podając fałszywą tożsamość i wykorzystywał do celów przestępczych słabe punkty w systemie azylowym. Nie mając szans na uzyskanie pozwolenia pozostania w Europie, przez pięć lat poruszał się swobodnie po krajach Unii Europejskiej i popełniał czyny karalne. Było to możliwe, ponieważ system rejestrowania uchodźców i wymiany informacji do dziś nie działa tak jak powinien, nawet w obrębie samych Niemiec. Postępowania wciąż toczą się niezależnie od siebie, z powodów technicznych i prawnych władze często nie są w stanie wymieniać się nawet najważniejszymi informacjami, a ponieważ poszczególne niemieckie landy pracują na zróżnicowanych systemach, imigranci mogą rejestrować się w wielu schroniskach pod innymi nazwiskami, wyrabiać sobie dokumenty z różną tożsamością i wielokrotnie pobierać pomoc finansową. Federalny Urząd do spraw Migracji i Uchodźców (Bundesamt für Migration und Flüchtlinge – BAMF) zamierza wprawdzie w ciągu bieżącego roku wprowadzić jednolite postępowanie i centralny bank danych, słabe punkty jednak pozostaną. W przypadku Belgacema pracownicy policji mieli okazję prześledzić rejestracyjny chaos od 31 stycznia 2011 roku. Tego dnia Tunezyjczyk złożył w Timișoarze w Rumunii wniosek o azyl. Zanim urzędnicy rozstrzygnęli sprawę, pojechał dalej, do Austrii, gdzie 8 kwietnia 2011 roku złożył podobny wniosek – tym razem jako Mohammad Ben Kalifa z Zuwary w Libii. Austriacy pobrali jego odciski palców i stwierdzili, że zarejestrował się już w Rumunii, odesłali go więc z powrotem do tego kraju. Tam jego wniosek o azyl został odrzucony i w lipcu 2011 r. mężczyznę wydano do Tunezji. Trzy miesiące później, w październiku 2011 roku, Belgacem przybył

statkiem do Trapani na Sycylii. W 2013 roku wyjechał do Szwecji, skąd został odesłany z powrotem do Włoch, a stamtąd przedostał się do Francji. W lipcu 2013 roku dokonał podobno napadu rabunkowego w Sainte-Maxime we Francji, a trzy miesiące później w Luksemburgu. Nie został jednak aresztowany i 10 grudnia 2013 roku pojechał do Niemiec. Policjanci zatrzymali go na dworcu głównym w Akwizgranie. Nie miał przy sobie żadnych dokumentów. Niemieccy urzędnicy pobrali mu odciski palców i zaczęli przeszukiwać europejski bank danych o uchodźcach EURODAC, który od 2011 roku gromadzi ślady daktyloskopijne. Aby jednak chronić dane osoby ubiegającej się o azyl, system nie podaje nazwisk, lecz jedynie płeć i datę wjazdu do kraju unijnego (sic!). Policjanci wykryli więc tylko, że mężczyzna, który podaje, że nazywa się Salihi, został już zarejestrowany w Rumunii, Austrii, Szwecji i we Włoszech. Nic ponadto. Nie mogli dowiedzieć się, że w Rumunii odmówiono mu azylu i wydano go do kraju pochodzenia. Nie wiedzieli też, że zarzuca się mu popełnienie poważnych przestępstw we Francji i w Luksemburgu. Aby uzyskać te informacje, musieliby mozolnie prosić urzędników w poszczególnych krajach o pomoc prawną. Tak więc Tarek Belgacem mógł pozostać w Niemczech i na nowo złożyć wniosek o azyl. Niemieccy urzędnicy sprawdzali w Rumunii czy Esalihi, jak się on teraz nazywał, ubiegał się tam o azyl. Na zwykłej drodze prawnej na odpowiedź czeka się wiele tygodni, a nawet miesięcy. W tym przypadku jednak Niemcy nie dowiedzieli się niczego, ponieważ od czasu deportacji w 2011 roku sprawa ta została uznana za załatwioną. Bukareszt sądził, że Esalihi alias Salihi alias Belgacem przebywa obecnie w Tunezji. On jednak mieszkał w Recklinghausen i znowu zwrócił na siebie uwagę władz. Policja podejrzewała go o dokonanie dwudziestu przestępstw, takich jak ciężkie uszkodzenie ciała, handel narkotykami, podróżowanie bez biletu, kradzieże ze sklepów,

znieważenie, stosowanie gróźb. Dnia 9 lutego 2014 r. podobno obmacywał kobiety w dyskotecie w Kolonii. Nigdy nie został zatrzymany, ale prokuratura prowadziła przeciwko niemu śledztwo. W marcu 2015 roku Belgacem umknął jednak niemieckim władzom, próbując jako Gruzin uzyskać azyl w Szwecji. Pozostał tam przez cztery miesiące, zanim Szwedzi nie zorientowali się, że taki wniosek złożył już w Niemczech i nie odesłali go do tego kraju. Tu trafił na kilka tygodni do więzienia. Po odzyskaniu wolności pozostał w Niemczech, potem zaś zdecydował się dokonać zamachu w Paryżu.



Ryc. 7. Niemiecka karta pobytu obcokrajowca
Źródło: http://deutsch-online.ru/dop_mat/articles/article_83 (dostęp 24.05.2016).

W Niemczech osobom starającym się o azyl bardzo łatwo jest uzyskać różne tożsamości, o czym świadczy kolejny przypadek. Dnia 19 stycznia, dwa tygodnie po śmierci Belgacema, czterystu policjantów wkroczyło do dwóch schronisk dla uchodźców w Ahlen w Westfalii, ponieważ te spokojne dotychczas miejsca zaczęły nagle zgłaszać przypadki poważnych naruszeń prawa: bijatyk, kradzieży, ekscesów alkoholowych. Krótco przedtem wprowadziło się tam 230 imigrantów z Afryki Północnej, głównie młodych mężczyzn. Większość z nowoprzybyłych po kilku dniach zniknęła, a ich miejsce pobytu jest nieznane. Następnie zaś pojawiło się kolejnych 138 imigrantów, z których 66 przedłożyło dokumenty z innymi nazwiskami niż te znalezione przez policję w kartotece zawierającej odciski palców. W przypadku czterech przeszukanych osób znaleziono również

dokumenty wystawione na co najmniej dwa różne nazwiska. Dokumenty te służą ubiegającym się o azyl w Niemczech jako zastępczy dowód osobisty. Zaświadczenia o zgłoszeniu się jako osoba wnioskująca o azyl z reguły wystawiane są w trakcie wstępnej rejestracji. Jest to kartka papieru ze zdjęciem i podanym nazwiskiem oraz krajem pochodzenia. To rozwiązanie przejściowe, do czasu aż w BAMF będzie mógł zostać złożony formalny wniosek o azyl, co trwa w tej chwili nawet kilka miesięcy. W Nadrenii Północnej-Westfalii podanie wymyślnego nazwiska jest niemal pozbawione ryzyka. Podczas wstępnej rejestracji w schroniskach dla uchodźców nie są bowiem pobierane odciski palców, które dałoby się sprawdzić w bazie danych. Można zatem podać wymyśloną tożsamość, a następnie udać się do innego schroniska i wyrobić dokument na inne nazwisko. Wiele osób starających się o azyl za pomocą kilku dokumentów wielokrotnie wyłudziło miesięczne kieszonkowe w wysokości 140 euro. Niektóre niemieckie landy podczas wstępnej rejestracji pobierają wprawdzie odciski palców, ale posługują się różnymi programami komputerowymi, które nie dają możliwości wymieniania się informacjami. Urzędnicy przeprowadzający wstępną rejestrację w poszczególnych landach nie mogą też porównać własnych danych ze zbiorem odcisków palców Federalnej Policji Kryminalnej czy EURODAC. Istniejące grupy przestępcze wykorzystują dziurawy system do własnych celów, a chodzi im nie o azyl w Niemczech, lecz o szybkie pieniądze. Policjanci w Stuttgarcie zatrzymali 21 podejrzanych, którzy, podobnie jak w Kolonii, podczas ostatniej nocy sylwestrowej obmacywali i okradali kobiety. Ukradli około trzydziestu telefonów komórkowych. Większość sprawców pochodzi z Afryki Północnej. Jeden z nich, Algierczyk, w schronisku dla uchodźców w Ellwangen sprzedał wiele z tych skradzionych komórek. Mężczyzna pięciokrotnie rejestrował się w różnych miejscach jako osoba ubiega-

jąca się o azyl, za każdym razem podając inne nazwisko. Z kolei celem akcji policyjnej w Ellwangen było ustalenie tożsamości sześćdziesięciu mężczyzn, którzy stale sprawiali tam problemy. Wielu z nich nie zgadzało się na pobranie odcisków palców ani na badania lekarskie. Kiedy pojawili się funkcjonariusze, jednej trzeciej z tych osób nie można było znaleźć. Dwudziestu zostało przeszukanych. W przypadku siedmiu mężczyzn policjanci odkryli, że posługują się oni wieloma tożsamościami, pięciu złożyło już wnioski o azyl w innych krajach Unii Europejskiej.

U niektórych samotnie przyjeżdżających do Niemiec mieszkańców Afryki Północnej obserwuje się duże skłonności przestępcze. Grupa śledcza „Silvester” ustaliła, że część tych mężczyzn podróżuje po Niemczech specjalnie po to, by wielokrotnie pobierać kieszonkowe lub wyruszać z kolejnych schronisk na bandyckie wyprawy. W grudniu 2015 r. niemiecki minister spraw wewnętrznych Thomas de Maizière zaprezentował projekt jednolitego dokumentu – dowodu przybycia, który ma zastąpić różnicowane systemy rejestracji i dotychczasowe zaświadczenia. Podczas wystawiania nowych dokumentów odciski palców i zdjęcia paszportowe będą gromadzone w centralnej kartotece Federalnego Urzędu do spraw Migracji i Uchodźców. Z tego banku danych będą mogły korzystać w przyszłości władze federalne, urzędnicy landów i gmin, by zapobiec podwójnemu rejestrowaniu się i nadużyciom. Nowy system testowany był w Berlinie, Heidelbergu, Herford, Zirndorf i Bielefeld, z pozytywnym rezultatem¹².

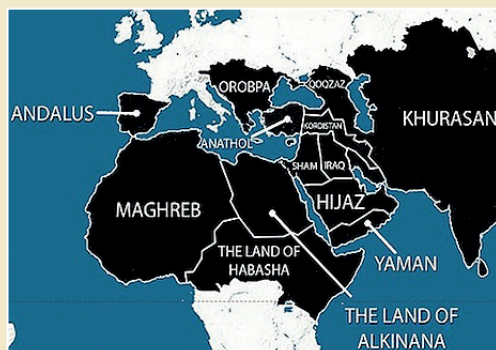
W całych Niemczech ma powstać około 1500 ośrodków rejestracyjnych wyposażonych w skanery linii papilarnych, kamery i urządzenia do kontroli paszportów. Federalny Urząd do spraw Migracji i Uchodźców zapewniał, że cały sprzęt zostanie dostarczony do końca czerwca 2016 r. Część ekspertów z poszczególnych landów nie wierzy jednak ani w to, że uda się to zrobić w tak krótkim czasie, ani w zapewnienia BAMF, iż

rejestracja jednego uchodźcy zajmie jedynie dziesięć minut. Praktycy uważają, że bardziej realne jest pół godziny. W nowym systemie konieczna będzie bowiem fotografia twarzy oraz około trzynastu zdjęć odcisków palców na jednego uchodźcę: dziesięć palców po kolei, skany czterech palców obu dłoni plus oba kciuki razem. Ponadto nazwiska będą musiały zostać zapisane jednolicie, nie obejdzie się więc bez pomocy tłumacza, a ośrodki przyjmujące imigrantów mają do czynienia z wieloma różnymi językami. Nawet jeśli niemiecki system rejestracyjny niedługo zacznie działać, pozostaną jeszcze problemy z EUODAC. Trzeba bowiem pilnie rozwiązać kwestie wymiany informacji w Europie, a przede wszystkim zdecydowanie i natychmiastowo usunąć absurdalny zakaz (patrz: prawa człowieka) umieszczania nazwisk i informacji o sytuacji prawnej w banku danych, bądź ustalić odpowiednie regulacje w tej dziedzinie odpowiadające obecnej sytuacji. Bezpieczeństwo obywateli krajów przyjmujących imigrantów z państw muzułmańskich powinno być ważniejsze od formalnych praw człowieka, których muzułmanie nie uznają albo w sposób zdecydowany i bezkompromisowy używają ich do własnych celów, aby zapewnić dominację wyznawanej przez siebie religii.

EUROPA DAR AL-HARB

Europa dla muzułmańskich radykałów stanowi terytorium wojny (*dar al-harb*), dżihadu języka i miecza, nieustannej walki toczonej dopóty, dopóki nie zostanie narzucony jej szariat. Już teraz Państwo Islamskie snuje plany odzyskania Półwyspu Iberyjskiego, czyli arabsko-berberyjskiej Andaluzji oraz Bałkanów z Węgrami, Austrią i Słowacją jako prowincji Orobra, z którą graniczyłaby Polska. To tylko na początek, bo w dalszej perspektywie cała część Europy zaznaczona na ryc. 8 kolorem białym powinna być zmieniona na czarny.

Na początku kwietnia 2016 r. Federalny Urząd Kryminalny (Bundeskriminalamt – BKA)



Ryc. 8. Przyszłe prowincje kalifatu (Państwa Islamskiego)
Źródło: <https://patricforyoh.wordpress.com/the-jihadists-terrorists-of-the-islamic-state-of-iraq-and-al-sham-isis-now-trying-to-rebrand-as-simply-the-islamic-state/> (dostęp 24.05.2016).



Ryc. 9. Fethullah Gülen
Źródło: <http://tr.zaman.co.at/news/fethullah-guelen-hocaefendi-buetuen-duenya-elinizden-gitse-gamlanmayin> (dostęp: 24.05.2016).

poinformował, że w Niemczech przebywa wciąż 400 tys. niezarejestrowanych imigrantów, spośród których wielu unika kontaktu z urzędami, obawiając się odrzucenia wniosku o azyl. Wielu imigrantów z krajów bałkańskich i Maghrebu weszło konflikt z prawem, natomiast Syryjczycy, Irakijczycy i Afgańczycy nie wyróżniali się w tej statystyce. Ponadto w Niemczech przebywać ma obecnie ok. 500 znanych służbom specjalnym ekstremistów stwarzających zagrożenie dla bezpieczeństwa kraju. Kierując się radykalną islamską ideologią, w każdej chwili mogą dokonać zamachu. W porównaniu do stycznia 2015 r. liczba takich osób uległa niemal podwojeniu. Ponadto kolejnych kilkaset osób, znanych z imienia i nazwiska, uważanych jest za sympatyków Państwa Islamskiego i potencjalnych pomocników terrorystów. Wielokrotnie wyższa jest liczba tego typu osób pozostających poza świadomością i ewidencją zachodnich instytucji. Według Federalnego Urzędu Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV, odpowiednika polskiej Agencji Bezpieczeństwa Wewnętrznego) w Niemczech aktywnie działa ok. 30 islamskich grup ekstremistycznych zrzeszających około 35 tys. członków, pragnących uczynić z Niemiec państwo islamskie oparte na szariacie. Około 4 tys. z nich stanowią salaficki dżihadysty. Są oni dynamicznie rozwijającą się

grupą islamską w Niemczech pośród 4,3 mln oficjalnie mieszkających tam muzułmanów. Nieoficjalne statystyki uwzględniające nielegalnych i niezarejestrowanych muzułmanów mówią o ponad 7 milionach.

Większość muzułmanów u naszych zachodnich sąsiadów stanowią obywatele Turcji oraz Niemcy tureckiego pochodzenia w drugim i trzecim pokoleniu – dzieci i wnuki przybyłych do Niemiec w latach 60. tureckich robotników. Wśród tej społeczności dużą sympatią od początku cieszy ruch Hizmet (Służba) założony przez znanego kaznodzieję Fethullaha Gülena. Międzynarodową misję szerzenia islamu w ideologii typowej dla Braci Muzułmanów realizował on pod hasłami: *Budujmy szkoły, nie meczety* oraz *Nasz dżihad to edukacja*. Działał w sposób stwarzający pozory wspierania dialogu międzyreligijnego i międzykulturowego, usypiając czujność władz. W Niemczech ruch działał po cichu, lecz skutecznie, tworząc specjalne szkoły, prywatne gimnazja i uczelnie wyższe, lokalne centra studiów nad KORANEM oraz tzw. latarnie (Lichthäuser), czyli męskie kolektywy, w których obowiązywały ścisła dyscyplina, całkowite posłuszeństwo, przymusowe czytanie KORANU i wspólne modlitwy pięć razy dziennie. Gülen dbał o kreowanie publicznego wizerunku ekumenicznego ruchu islamskiego zabiegającego o dialog mię-

dzynarodowy, ustanawiając w Niemczech 15 stowarzyszeń dialogu¹³. W Polsce założony został Dunaj Instytut Dialogu, oprócz tego w Krakowie istnieje związana z ruchem uczelnia „Vistula”. Zwolennicy Gülena nie przygotowywali się do zbrojnego dżihadu, lecz dżihadu języka. Ich działalność jest subtelna i wyrafinowana, aby uniknąć oskarżenia o szerzenie nienawiści religijnej i przemocy. Ma być to rozciągnięta w czasie misja krzewienia islamu, zgodnie z treścią kazania wygłoszonego kiedyś przez Gülena do uczniów: *Musicie poruszać się niezauważeni w arteriach systemu, dopóki nie dosięgnięcie wszystkich ośrodków władzy (...). Kontynuujcie, dopóki sytuacja nie dojrzeje. Jeśli zrobicie coś przedwcześnie, świat spadnie nam na głowy i muzułmanie całego świata będą cierpieć (...). Musicie czekać, aż nadejdzie czas, w którym w waszych rękach znajdzie się cała władza państwowa (...). Do tego czasu jakkolwiek krok będzie przedwczesny – będzie to jak rozbicie jajka bez czekania czterdziestu dni, aż wykluje się pisklę. Byłoby to jak zabicie pisklęcia w środku.*

Nie należy również zapominać, że Turcja jest po części odpowiedzialna za falę imigrantów przybywających do Europy w 2015 roku, ponieważ otwierała obozy dla uchodźców, wyposażała ich w telefony komórkowe, GPS, nowe ubrania i pieniądze. Wina spoczywa również po stronie kanclerz Niemiec, która zaprosiła imigrantów do swego kraju. Zapewnienia władz tureckich, iż zdolne są do kontroli własnych granic, należy traktować jako odpowiadające rzeczywistości, ale z zastrzeżeniem, że jedynie wtedy, jeżeli będzie to dla Ankarę opłacalne. Okazuje się zatem, że UE stała się zakładnikiem Turcji w kwestii imigrantów. Zgadza się przyjąć wygórowane warunki stawiane przez Ankarę, co świadczy o jej politycznej słabości i relatywizmie w kwestii praw człowieka, które w Turcji są notorycznie łamane, czego Bruksela starała się nie wytykać przymusowemu partnerowi, aby go nie urazić. Dopiero po nieudanym puczu z 15 lipca, dzięki któremu prezydent Recep Tayyip Erdoğan umocnił

swoją władzę, przejrzała na oczy, dostrzegła jego dyktatorskie zapędy i nowe zagrożenie.

Przed podobnym problemem z imigrantami jak Niemcy stoją obecnie Włochy. W kwietniu 2016 r. w kryzysowej sytuacji znalazła się Sycylia, gdzie na początku tegoż miesiąca przybysze zajęli główny plac stolicy wyspy – Cagliari, domagając się możliwości jej opuszczenia, ponieważ chcieliby przedostać się na północ Europy. Wielu z nich odmówiło przy tym udziału w procedurach identyfikacyjnych z obawy, że nie będą mogli liczyć na prawo legalnego pobytu w Europie. Sporo miast i miasteczek południa Włoch zostało zdominowanych przez imigrantów. Tymczasem ich napływ z wybrzeża libijskiego nie ustaje. Libia jako kraj upadły stała się teraz międzynarodowym centrum przerzutu ludzi, którzy trafiają tu m.in. przez Egipt, wraz Syryjczykami z obozów w Jordanii. Propagandowe działania UE polegające na ochronie jej południowych granic poprzez wysłanie okrętów na Morze Śródziemne w rzeczywistości są misją humanitarną, ponieważ napotkane na pełnym morzu łodzie i statki z imigrantami są co prawda zatrzymywane, ale ich „ładunek”, zamiast z powrotem do Libii, trafia w komfortowych warunkach prosto do obozów przejściowych we Włoszech, na Malcie lub Cyprze. Takie działanie UE to nic innego jak zalegalizowane pośrednictwo w przemyśle imigrantów z Libii do Europy i zwiększanie ich liczby. Jeden z bossów gangu przemytniczego działającego w Trypolisie w wywiadzie dla egipskiego portalu informacyjnego stwierdził, że od pewnego czasu zupełnie nie przejmuje się już stanem technicznym łodzi, na których wysyła ludzi na północ. Powiedział, że jeżeli któraś ze zdezelowanych łodzi odmówi posłuszeństwa na pełnym morzu albo nawet zacznie tonąć, to i tak Europejczycy ich znajdą i wyłowią, zabierając do siebie. Organizatorzy przerzutu doskonale wykorzystują bezradność, naiwność i polityczną poprawność europejskich instytucji i decydentów. Włosi porzucili przy tym plany relokacji imigrantów ze swego kraju

do innych państw UE, ponieważ nie są w stanie zweryfikować ich tożsamości, a podczas wizyty przedstawicieli polskiej Straży Granicznej odmówili bezpośredniego dostępu do kandydatów do relokacji.

Zagrożeń tych nie dostrzegają lub bagatelizują je unijni politycy. Także papież Franciszek, darzący wyraźną estymą muzułmanów, podczas wizyty na greckiej wyspie Lesbos zaprosił trzy rodziny syryjskich uchodźców (12 osób) do Watykanu. Na pytanie dziennikarzy, dlaczego uprzywilejował wyłącznie rodziny muzułmańskie, odpowiedział, że wybrane rodziny miały legalne dokumenty, co umożliwiło ich podróż to Watykanu. Oby rzeczywiście tak było, choć z drugiej strony trudno oprzeć się wrażeniu, że największy chrześcijański autorytet preferuje wyznawców wrogiej religii, zapominając o tym, że są oni sprawcami prześladowań społeczności chrześcijańskich na Bliskim Wschodzie. Interesujące jest też porównanie przez papieża Państwa Islamskiego do Chrystusa i jego uczniów¹⁴. Tymczasem imigranci z krajów muzułmańskich znajdują w Europie dogodne warunki do życia, ale na własnych zasadach, korzystają z różnych przywilejów i starają się egzekwować swoje prawa. Na przykład uchodźcy z Syrii pozwalają rządowi Danii i Inger Støjberg, minister imigracji tego kraju, za wydłużenie do trzech lat (dotąd obowiązywał jeden rok) procesu sprowadzania rodziny z kraju pochodzenia. Należy przy tym zwrócić uwagę, że procedura łączenia rodzin spada na kraj przyjmujący, on też ponosi jej koszty. Nie można też zapominać, że rodziny muzułmańskie są bardzo liczne, a trzeba im zapewnić zakwaterowanie, opiekę socjalną itp., więc koszty te będą wysokie, co może spowodować społeczne protesty. W Niemczech z kolei, gdzie imigranci dopuszczają się wielu przestępstw, Niemiecka Rada Prasy zaleciła dziennikarzom, by w swoich artykułach nadal unikali podawania narodowości lub

wyznania sprawców przestępstw. Po wydarzeniach w Kolonii w ostatnią noc sylwestrową media domagały się zmiany tej zasady. Jak widać, mniejszości muzułmańskie w Europie mogą liczyć na przychyłność wielu środowisk, niezależnie od tego, jaki stopień zagrożenia stwarzają. A jest on wysoki. Zamachowcy z Paryża i Brukseli nie mogliby organizować i przygotowywać swych procederów, gdyby nie pomoc i ukrywanie ich przez braci w wierze. Najlepszym przykładem tej antyzachodniej islamskiej solidarności jest fakt, że środowiska muzułmańskie nigdy nie przeprowadziły demonstracji potępiających zamachowców – podkreślam: zamachowców, a nie same akty terrorystyczne. Nie powstała też żadna inicjatywa antyterrorystyczna. Muzułmanie natomiast chętnie uczestniczą w zbiorowych aktach agresji, przemocy i ulicznych zamieszkach. Cieszą się, gdy w zamachach giną „niewierni”. Jeśli elity polityczne UE wciąż liczą na integrację mniejszości muzułmańskich w Europie, to wykazują się całkowitym brakiem zrozumienia problemu i narażają własne kraje na destabilizację i zagrożenie terrorystyczne. Świadczy o tym najlepiej wypowiedź jednego z muzułmańskich działaczy w stolicy Niemiec, który zapytany przez burmistrza niemieckiej dzielnicy Berlina – Neukölln, zdominowanej przez muzułmanów, o obowiązek integracji z niemieckim społeczeństwem, odpowiedział: *Jak się Niemcom nie podoba, jak my tu żyjemy, niech wynoszą się na Majorkę*.

W niedalekiej perspektywie z religijno-ideologiczną ofensywą wśród imigrantów w Europie ruszy Arabia Saudyjska, która, mimo iż nie przyjmuje do siebie uchodźców z krajów muzułmańskich, to już zapowiedziała, że w Niemczech wybuduje dwieście meczetów. Będzie w nich promowana najbardziej radykalna wersja islamu, jaką jest wahhabizm. Z kolei Turcja wysłała ponad 900 imamów, którzy, jak polecił

prezydent Erdoğan, mają zapobiec szybkiej integracji muzułmanów z resztą społeczeństwa. Można się spodziewać, iż Arabia Saudyjska zrealizuje swoje postanowienie, tak jak uczyniła to na Bałkanach, gdzie

za jej pieniądze odbudowano po wojnie setki meczetów, a kolejne postawiono od fundamentów.

Na tym tle sytuacja w Polsce wydaje się dużo korzystniejsza.

(Opinie zawarte w tym artykule opierają się na osobistych przemyśleniach i wiedzy autora. W żadnym wypadku nie odnoszą się do procedur i zadań realizowanych przez instytucje, z którymi był związany zawodowo).

¹W 2013 r., podczas wizyty w Niemczech Recep Tayyip Erdoğan, jeszcze jako premier Turcji, posiadającej drugą co do wielkości armię NATO, przestrzegał ponad trzymilionową mniejszość turecką przed integrowaniem się z Niemcami, gdyż islam zakazuje (zgodnie z doktryną) współżycia z „niewiernymi”. Z kolei podczas wizyty w Niemczech w 2015 r. w jednej z hal targowych w Karlsruhe, gdzie zgromadziło się blisko 14 tysięcy zwolenników tureckiego przywódcy, Erdoğan pytał zebranych: „Czy chcecie, abyśmy, zaczynając od Niemiec, rozpoczęli dzieło budowy nowej Turcji?”. W odpowiedzi usłyszał gromkie: „Tak!”. Erdoğan podkreślał wtedy, że panturecką tożsamość wspierają język oraz islam. Tłumaczył swoim rodakom: „Nie możecie się uczyć niemieckiego czy angielskiego, jeśli najpierw nie opanujecie dobrze tureckiego”. W czasie wystąpienia kilkanaście razy wzywał też imię Allaha i apelował, żeby wspólnoty tureckie w Niemczech działały na rzecz umacniania globalnych wpływów Turcji; <http://euroislam.pl/jak-turcja-kontroluje-islam-w-niemczech/>.

²Recep Tayyip Erdoğan (ur. 1954), z wykształcenia ekonomista. Od czasu studiów związany ze środowiskiem nacjonalistyczno-islamistycznym. Od 1983 r. robił karierę w szeregach Partii Dobrobytu (Refah Partisi). W latach 1994–1998 był burmistrzem Stambułu. W 1998 r. został zdjęty ze stanowiska i skazany na 10 miesięcy więzienia za podżeganie do nienawiści religijnej (odsiedział 4 miesiące), co jego zwolennicy traktowali jako akt męczeństwa za wiarę. W 2001 r. założył Partię Sprawiedliwości i Rozwoju (Adalet ve Kalkınma Partisi) i został jej przewodniczącym. W latach 2003–2014 sprawował urząd premiera Turcji, a od 2014 r. jest prezydentem kraju. Od objęcia urzędu prezydenta przez Erdoğan w Turcji wszczęto ok. dwóch tysięcy spraw karnych przeciwko osobom oskarżonym o obrażę głowy państwa. Obrazą prezydenta jest w Turcji przestępstwem, za które grozi kara do czterech lat więzienia. Jeszcze jako burmistrz Stambułu Erdoğan wypowiedział słynną formułę: „Meczezy to nasze koszary, kopuły to nasze hełmy, minarety to nasze bagnety, a wierni to nasi żołnierze”. Więcej na temat prezydenta Turcji zob. O. Burçak Belli i in., *Boss znad Bosforu*, „Forum” 2016, nr 8, s. 38–41; M. Kokot, *Turcja na drodze do sułtanatu*, „Gazeta Wyborcza” z 20 maja 2016 r.

³Dżihadym zdefiniować można jako ponadnarodowy ruch wojskowy w świecie muzułmańskim. Jego

uczestnicy (dżihadysty) chcą stworzyć świat, w którym wszystkie granice dzielące ummę (społeczność muzułmańską) na różne państwa i narody zostaną trwale usunięte. Islam głoszony przez dżihadystów to ultra-konserwatywna, wojownicza odmiana salafizmu (idei powrotu do „czystego islamu” i ścisłego przestrzegania jego doktryny z okresu pierwszych muzułmanów) i wahhabickiego purytanizmu (ideologii, na której opiera się system religijny i społeczno-polityczny Arabii Saudyjskiej). Islam wyznawany przez dżihadystów opiera się na radykalnej reinterpretacji klasycznej koncepcji dżihadu jako broni ofensywnej, która ma mu zapewnić hegemonię nad światem. Dżihadysty dzielą wszystkich muzułmanów na „ludzi raju” (samiych siebie) i „ludzi piekła” (wszystkich pozostałych). Każdego wiernego, jeśli jego interpretacja Koranu i szariatu nie odpowiada modelowi dżihadystów, uznają za członka tej drugiej grupy – apostatę i bezbożnika, którego trzeba usunąć ze świętej społeczności Allaha.

⁴W rzeczywistości przecież jest odwrotnie: zachodni przywódcy jak ognia unikają używania przymiotnika „muzułmański” obok rzeczownika „terroryzm” lub „terrorysta”, a gdy na przykład jakiś dziennikarz w Wielkiej Brytanii użyje niefortunnie tego określenia, ścigany jest z urzędu przez wymiar sprawiedliwości, jego redakcja zaś płaci wielotysięczną karę.

⁵Ciekawe uzasadnienie społecznego wykluczenia, skoro to przecież islam oraz wiele religijnych autorytetów i przywódców zabrania muzułmanom integrować się z chrześcijanami.

⁶[PAP], *Policja zdobyła poufne dokumenty dot. niemieckich dżihadystów z IS*, <http://wiadomosci.wp.pl/kat,1356,title,Policja-zdobyła-poufne-dokumenty-dot-niemieckich-dzihadystow-z-IS,wid,18201138,wiadomosc.html>; [PAP], *Brytyjska telewizja informuje, że jest w posiadaniu danych ok. 22 tys. dżihadystów z tzw. Państwa Islamskiego*, <http://wiadomosci.wp.pl/kat,1356,title,Brytyjska-telewizja-informuje-ze-jest-w-posiadaniu-danych-ok-22-tys-dzihadystow-z-tzw-Panstwa-Islamskiego,wid,18206487,wiadomosc.html>.

⁷[IAR], *Zamknięcie granic nie pomogło. Wystarczy 10 tys. euro*, http://wiadomosci.wp.pl/kat,1356,-title,Zamkniecie-granic-nie-pomoglo-Wystarczy-10-tys-euro,wid,18283394,wiadomosc.html?tid=1170f7&_tictsn=5.

⁸M. Parfieniuk, *Tak Afgańczycy próbują dostać się na Zachód. Stare szlaki są dla nich zamknięte, dla*

tego wybierają Moskwę, Indie, a nawet Kubę, http://wiadomosci.wp.pl/kat,1356,title,Tak-Afganczycy-probuja-dostac-sie-na-Zachod-Stare-szlaki-sadla-nich-zamkniete-dlatego-wybijaja-Moskwe-Indie-a-nawet-Kube,wid,18280878,wiadomosc.html?tid=117714&_tictsn=5.

⁹P. Jendroszyk, *W Niemczech znikają imigranci. To mogą być terroryści*, http://wiadomosci.wp.pl/kat,1041267,title,W-Niemczech-znikaja-imigranci-To-moga-byc-terrorysci,wid,18230115,wiadomosc.html?tid=1170f8&_tictsn=5.

¹⁰Recep Tayyip Erdoğan, wypowiadając się na zakończenie majowego szczytu humanitarnego w Stambule, oznajmił, że turecki parlament zablokuje proces legislacyjny, jeśli Ankara nie uzyska zniesienia wiz do końca czerwca. Podkreślił, iż w razie braku decyzji UE żadna ustawa w ramach wdrażania porozumienia o readmisji nie wyjdzie z parlamentu Republiki Turcji. Erdoğan oświadczył również, że dotychczas nie wpłynęły żadne pieniądze z obiecanych Turcji przez UE 6 mld euro w ramach porozumienia migracyjnego, zgodnie z którym od początku kwietnia 2016 r. uchodźcy, którzy wjechali nielegalnie do Grecji, mają być przetransportowani z tego kraju do Turcji. Za każdego Syryjczyka wydalanego z UE ma przybywać legalnie do UE inny Syryjczyk. W zamian Bruksela zobowiązała się do finansowego wsparcia Ankary kwotą 6 mld euro, z czego 3 mld euro do 2018 roku, oraz do zniesienia od lipca unijnych wiz dla obywateli tureckich. Jednak to liberalizacja wizowa jest kluczowym elementem porozumienia z Turcją. Prezydent Turcji postawił Unii ultimatum: albo UE zniesie wizy do końca czerwca 2016 r., jak przewidywał termin wprowadzenie przepisów, albo Turcja nie zgodzi się na główny punkt porozumienia, czyli umowę dotyczącą odsyłania nielegalnych imigrantów do Turcji w zamian za przyjęcie przez UE uchodźców z tureckich obozów. Choć Komisja Europejska zgodziła się na liberalizację, nawet bez spełnienia wszystkich kryteriów, Angela Merkel deklarowała, że nie pozwoli na uchylanie się Turcji od swoich zobowiązań. Do 15 lipca 2016 r. szczególnie mocne było jej stanowisko w kwestii kontrowersyjnego prawa antyterrorystycznego w Turcji; [PAP], *Prezydent Turcji: nie otrzymaliśmy pieniędzy w ramach umowy z UE*, <http://wiadomosci.wp.pl/kat,1356,title,Prezydent-Turcji-nie-otrzymalismy-pieniedzy-w-ramach-umowy-z-UE,wid,18348409,wiadomosc.html>.

¹¹[PAP], *„Bild”: Liberalizacja systemu wizowego dla Turcji dopiero w 2017 r.*, <http://wiadomosci.dziennik.pl/swiat/artykuly/521463,bild-liberalizacja-systemu-wizowego-ue-dla-turcji-dopiero-w-2017-r.html>.

¹²J. Matusiak, *Imigranci. Kto chce, może zniknąć*, <http://matusiakj.blogspot.com/2016/03/imigranci-kto-chce-moze-zniknac.html>.

¹³W Turcji wpływy Hizmetu sięgały do niedawna najwyższych szczebli władzy państwowej. Jego zwolennikami są policjanci, wojskowi, prokuratorzy,

sędziowie i dziennikarze... w sumie miliony ludzi. 75-letni dziś Gülen, mieszkający od 1999 r. w Saylorsburgu w Pensylwanii (USA), był mentorem, a potem sojusznikiem Recepty Tayyipa Erdoğan, kiedy ten zakładał na początku XXI wieku Partię Sprawiedliwości i Rozwoju, i piastował urząd premiera. Od grudnia 2013 r., kiedy wybuchł skandal korupcyjny, który dotknął Erdoğan, jego otoczenie i rodzinę, uważany jest za wroga prezydenta Turcji. Gülena oskarżono zaocznie o stworzenie „równoległego państwa”, wprowadzanie swoich zwolenników na kluczowe stanowiska w instytucjach państwa, w tym w policji i sądownictwie oraz próbę obalenia Erdoğan. Zatrzymano ok. 1,8 tys. osób podejrzanych o przynależność do „siatki” powiązanej z Gülenem, w tym wysokich funkcjonariuszy policji, wielu dziennikarzy i przedstawicieli wymiaru sprawiedliwości. Zamknięto również redakcje gazet związane z Hizmetem. Zatrzymane osoby przedstawia się jako spiskowców ściganych na podstawie przepisów antyterrorystycznych. Podejrzewa się, że ogromne fundusze międzynarodowego ruchu Gülena pochodzą z dochodów tureckich grup przestępczych, w tym z przemytu afgańskiej heroiny. Po nieudanym puczu wojskowym z 15 lipca 2016 r. prezydent Erdoğan oskarżył Gülena o jego zorganizowanie i zażądał od USA ekstradycji do Turcji przywódcy Hizmetu. W więzieniach osadzono lub zwolniono z pracy tysiące osób posądzanych o sympatie z Gülenem; [PAP], *Media w USA ostro o przejęciu „Zaman”: „Zamach Erdoğan na prasę”*, <http://wiadomosci.wp.pl/kat,1356,title,-Media-w-USA-ostro-o-przejeciu-Zaman-Zamach-Erdogana-na-prase,wid,18201638,wiadomosc.html>.

¹⁴Podczas rozmowy dziennikarz francuskiej gazety „La Croix” zadał papieżowi pytanie, czy według niego obawa przed przyjmowaniem imigrantów jest uzasadniona. Ojciec Święty odpowiedział: „Nie sądzę, aby istniała obawa wobec islamu jako takiego, ale wobec ISIS i jego chęci podboju, która częściowo jest zaczerpnięta z islamu. Prawdą jest, że idea podboju tkwi w duszy islamu. Jednakże w ten sam sposób można interpretować cel Ewangelii św. Mateusza, gdzie Jezus wysłał swoich uczniów do wszystkich narodów, jeśli mówimy o samej idei podboju. W obliczu islamskiego terroryzmu lepiej byłoby zadać sobie pytanie o sposób, w jaki zachodni model demokracji był eksportowany do krajów takich jak Irak, gdzie już wcześniej był silny rząd, albo Libii, gdzie istnieje struktura plemienna. Nie możemy się rozwijać, nie biorąc tych kultur pod uwagę. Jak powiedział niedawno pewien Libijczyk – Kiedyś mieliśmy jednego Kaddafiego, teraz mamy pięćdziesięciu”; [La Croix], *Papież przyrównał Państwo Islamskie do Jezusa i jego uczniów*, <http://wiadomosci.wp.pl/kat,1329,title,Papiez-przyrownal-Panstwo-Islamskie-do-Jezusa-i-jego-uczniow,wid,18342151,wiadomosc.html>.

Tadeusz Tomaszewski

JESZCZE O TYM, CZY WARTO BADAĆ KOPIE I INNE WTÓRNE ODWZOROWANIA PISMA RĘCZNEGO

Każdy przypadek zlecenia badań rękopisów niewystępujących w formie pierwowpisów wymaga indywidualnego podejścia i oceny materiału badawczego w kontekście okoliczności sprawy.



TADEUSZ TOMASZEWSKI – prof. dr hab., prorektor ds. zasobów ludzkich i kształcenia ustawicznego, kierownik Katedry Kryminalistyki WPiA Uniwersytetu Warszawskiego.

W praktyce opiniodawczej, a nawet także w fachowej literaturze kryminalistycznej, występują zróżnicowane poglądy co do możliwości poddawania badaniom identyfikacyjnym zapisów wykonanych pismem ręcznym, a w szczególności podpisów, w sytuacji niedysponowania ich pierwowpisami¹. Rozbieżności w tym względzie dotyczą zarówno zakresu możliwych do przeprowadzenia badań kopii rękopisów lub innej formy ich odwzorowania, jak i interpretacji wyników uzyskiwanych w takich badaniach. Z pewnym uproszczeniem można stwierdzić, że zarysowują się w tym względzie dwa skrajne stanowiska: w świetle pierwszego kopie rękopisów lub występujące w innej postaci obrazy rękopisów co do zasady poddają się badaniom pismoznawczym i mogą stanowić wystarczający materiał, na którym buduje się od strony dowodowej ustalenia faktyczne w sprawie, natomiast drugie stanowisko wyklucza jakiegokolwiek badania takiego materiału, gdyż mogą one prowadzić do bezzasadnego przypisania danej osobie wykonania kwestionowanego podpisu bądź zapisu ręcznego, a nawet być źródłem błędnego rozstrzygnięcia sprawy. Oba te stanowiska w takiej postaci można uznać za niewłaściwe, a w każdym razie za zbyt uproszczone, gdyż każdy przypadek zlecenia badań rękopisów niewystę-

pujących w formie pierwowpisów wymaga indywidualnego podejścia i oceny materiału badawczego w kontekście okoliczności sprawy.

Podejście aprobowane szeroką dopuszczalność badań kopii lub wtórnych odwzorowań rękopisów jest niebezpieczne o tyle, że jakość materiału badawczego obiektywnie uniemożliwia badanie niektórych przynajmniej właściwości pisma ręcznego, nie mówią już o tym, że wszelkie dywagacje na temat autentyczności poddawanych analizie podpisów pozbawione są podstaw. Przejawem błędów, które mogą być następstwem takiego podejścia, są na przykład nagminne w polskiej praktyce sądowej przypadki formułowania przez biegłych badających kopie podpisów wniosków w kategoriach prawdopodobieństwa („podpis prawdopodobnie został nakreślony przez X”), podczas gdy taki wniosek w świetle wiedzy o współczesnych technicznych możliwościach fałszowania sygnatur jest co najmniej nieuzasadniony; co więcej – może prowadzić do błędnych ustaleń stanu faktycznego przez organ procesowy, który nie rozumie niuansów ekspertyzy pismoznawczej. Z kolei całkowite negowanie możliwości badania kopii (bądź innych obrazów pierwotnych rękopisów) jest rozumowaniem szkodliwym dla praktyki opiniodawczej,

zwłaszcza jeśli weźmie się pod uwagę, iż nie zawsze oryginał spornego dokumentu zawierający pierwopis podpisu jest osiągalny, zaś kopia dokumentu jest jedynym dostępnym odwzorowaniem kwestionowanego rękopisu. Rezygnacja z jego badań, w takim zakresie, w jakim pozwalają na to metodologiczne zasady ekspertyzy dokumentów, oznaczałaby zatem utratę informacji, która wzbogaciłaby wiedzę organu procesowego.

Problem możliwości badania kopii a nie pierwopisu rękopisu dowodowego był już przedmiotem szerszych rozważań zamieszczonych na łamach niniejszego czasopisma w rubryce *Z PRAKTYKI EKSPERTA DOKUMENTÓW*². Można więc odwołać się do prezentowanych tam poglądów i argumentów. Sprowadzają się one do opisanego dylematu, czy biegły, któremu zlecono przeprowadzenie ekspertyzy pismoznawczej na podstawie kopii powinien odmówić wykonania badań, czy też – choćby w ograniczonym zakresie – je prowadzić. Brak oryginalnego dokumentu nie tylko bowiem uniemożliwia przeprowadzenie analizy technicznej środka kryjącego, jakim wykonano oryginalne zapisy lub podpisy, bądź podłoża (papieru), na którym występują rękopisy, ale przede wszystkim uniemożliwia wypowiedzenie się co do ewentualnego podrobienia danego dokumentu i zawartych w nim elementów graficznych, w tym podpisów. Ponadto brak pierwopisu zapisów rękopiśmiennych ogranicza zakres możliwych do przeprowadzenia badań, bowiem ich kopia lub inna forma wtórnego odwzorowania nie oddaje pełnego obrazu pisma ręcznego, włącznie z takim jego cechami jak naciskowość i cieniowanie pisma, wiązanie znaków, ich budowa czy modelunek. Tego rodzaju właściwości mają zaś znaczenie dla oceny spontaniczności i swobody nakreślenia rękopisu bądź podpisu i pośrednio dla wnioskowania o ich autentyczności.

Biegły powołany do wydania opinii ma obowiązek przygotowania sobie właściwego pola ekspertyzy³, co w tym przypadku oznacza jego powinność poszukiwania pierwopisu kwestionowanego rękopisu poprzez zwrócenie się do organu zarządzającego ekspertyzę o dostarczenie oryginału dokumentu dowodowego. Jeśli jednak z powodów obiektywnych takiego dokumentu nie otrzyma, a względu metodyki badań temu się nie sprzeciwiają, nie powinien rezygnować z ustaleń opartych na kopii, chociaż musi mieć świadomość wynikających z tego powodu ograniczeń badawczych i wyraźnie poinformować o nich organ procesowy. Muszą oczywiście wystąpić zarazem przesłanki do prowadzenia takich zawężonych badań, w tym odpowiednia jakość kopii lub innego wtórnego odwzorowania rękopisu, która pozwoli na analizę właściwości graficznych pisma ręcznego. Należy przy tym pamiętać, że w przypadku ustalenia zgodności takich właściwości w materiale dowodowym i porównawczym nie daje to jeszcze podstaw do wniosku (nawet wyrażonego w skali prawdopodobieństwa) o wykonaniu rękopisu dowodowego przez osobę, od której pochodzą wzory porównawcze, chociaż samo stwierdzenie zgodności cech pisma dowodowego i porównawczego może być wartościową informacją dla organu procesowego, kierującą dalsze postępowanie. Natomiast stwierdzenie braku zgodności takich cech może pozwolić na kateryczne wykluczenie podejrzanego o sporządzenie kwestionowanego rękopisu, zatem w takiej sytuacji walor dowodowy opinii z tego punktu widzenia jest jeszcze większy.

Jak podkreślono, każdy przypadek takich badań wymaga indywidualnego podejścia i ostrożności w opiniowaniu, zwłaszcza że nośnik służący do utrwale-
nia obrazu pisma ma znaczenie dla zakresu możliwych do przeprowadzenia badań

i formułowanych na ich podstawie wniosków. Może się na przykład okazać, iż inne będą możliwości wnioskowania w sytuacji dysponowania przez biegłego kopią kserograficzną, a inne – kopią kalkową. W tym kontekście warto podkreślić, że postęp techniczny nie tylko wpływa na zwiększenie liczby kopii dokumentów funkcjonujących w obrocie prawnym, ale współcześnie daje także szerokie możliwości wytwarzania innych niż typowe kopie odwzorowań pisma ręcznego. Przykładem może być fotograficzne utrwalenie obrazu pisma ręcznego, co wobec ogromnej popularności telefonów komórkowych, które pełnią zarazem funkcję aparatu fotograficznego, powoduje, że również taka forma wtórnego odwzorowania spornego rękopisu pojawia się jako potencjalny przedmiot badań eksperta pisma.

W praktyce eksperckiej Katedry Kryminalistyki Uniwersytetu Warszawskiego zdarzył się przypadek badań zapisów tekstowych i podpisu tworzących kwestionowany testament, uwidocznionych na zdjęciu wykonanym telefonem komórkowym. Zlecająca ekspertyzę pozaprocesową córka domniemanego spadkodawcy wyjaśniła, iż znalazła oryginał testamentu, który na wszelki wypadek sfotografowała telefonem komórkowym, jednak później dokument ten zaginął, wskutek czego nie było możliwe dostarczenie do badań oryginału dokumentu dowodowego ani nawet jego dobrej jakości kopii kserograficznej. Na dowód pochodzenia zdjęcia przedstawiła opinię wydaną przez firmę specjalizującą się w badaniu cyfrowych nośników pamięci. Nietypowa forma materiału badawczego pozwoliła w tym przypadku na wykazanie wybranych zgodnych właściwości graficznych i cech grafizmu zawartych w piśmie dowodowym i porównawczym, chociaż – co oczywiste – brak dostępu do oryginału dokumentu dowodowego uniemożliwił wypowiedzenie się wprost co do sporządzenia kwestiono-

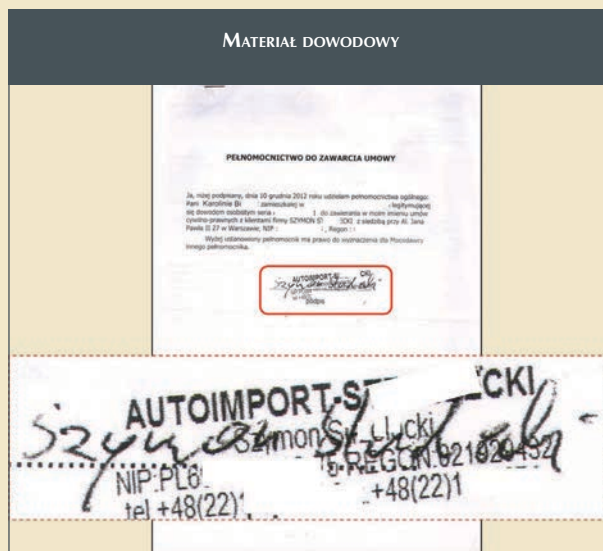
wanego testamentu przez spadkodawcę, a tym bardziej co do autentyczności samego testamentu.

Jeszcze większe możliwości utrwalania obrazu dokumentów zawierających pismo ręczne daje technika komputerowa. Dowodzi tego opisany dalej przypadek, przy czym jest on o tyle interesujący, że połączył dwie formy wtórnego odwzorowania kwestionowanych podpisów – za pomocą skanogramu, który został zmultiplikowany dzięki wydrukowi komputerowym dokumentów zawierających sporne sygnatury i kopiom kserograficznym takich wydruków.

Sprawa, której dotyczyła wspomniana ekspertyza była związana z podejrzeniem popełnienia oszustwa na szkodę co najmniej kilkudziesięciu osób usiłujących kupić samochody, które na ich zamówienie miały zostać sprowadzone przez prywatną firmę⁴. Siedzibę firmy stanowił mały lokal wynajęty w jednym z prestiżowych biurowców w Warszawie, co miało podnieść zaufanie klientów. Zwabieni obiecującymi reklamami w Internecie mieli oni kontakt jedynie z sekretarką firmy, która sama została wynajęta drogą mailową, gdyż pocztą elektroniczną przesłano jej skan umowy o pracę. Sekretarka Karolina B., późniejsza oskarżona, pobierała wysokie zaliczki od klientów, wydając im w zamian kopie umów zlecenia o sprowadzenie pojazdu mechanicznego oraz kopie wystawionych na nią pełnomocnictw do zawarcia takich umów. Na wszystkich tych dokumentach widniał podpis o brzmieniu *Szymon S...cki*, występujący w obrębie odбитki pieczętki firmowej zawierającej nazwisko właściciela (takie samo jak brzmienie podpisu) i dane firmy. Ponieważ obiecane samochody nie zostały sprowadzone, oszukani klienci zawiadomili organy ścigania, które usiłowały ustalić sprawców całego procederu. W szczególności chodziło o sprawdzenie, czy Karolina B. jedynie wykonywała w do-

brej wierze polecenia nieznane-
go jej osobiście pracodawcy oraz
czy Szymon S., którego nazwisko
widniało w dokumentach dowo-
dowych był faktycznym właścicie-
lem firmy i czy to on podpisywał
dokumenty firmowe. Sam Szy-
mon S. okazał się młodym, słabo
wykształconym człowiekiem
nadużywającym alkoholu i nar-
kotyków, który mieszkał w małym
miasteczku kilkaset kilometrów
od Warszawy. Z jego wyjaśnień
wynikało, że nie wiedział o dzia-
łalności firmy zarejestrowanej
na jego nazwisko, chociaż po-
twierdził, że jego koledzy mieli go
prosić o podpisanie jakiegoś do-
kumentu, o którym nic więcej nie
potrafił powiedzieć.

Zgodnie z postanowieniem o dopusz-
czeniu dowodu z opinii biegłego, przed-
miotem badań były 44 dokumenty za-
tytułowane PEŁNOMOCNICTWO DO ZAWARCIA
UMOWY, stanowiące wydruki komputerowe
zawierające wskazane podpisy Szymon S...
cki, umieszczone w obrębie odbitki pie-
czętarki o treści: AUTOIMPORT S...CKI. Podpisy
te, w świetle postanowienia sądu, trakto-
wane były jako zasadniczy materiał do-
wodowy. Ponadto jednak w przekazanych
aktach ujawniono 40 innych dokumentów
(w tym 38 umów o sprowadzenie samo-
chodu), w których występowały podpisy
analogiczne w formie graficznej i brzmie-
niu, które również włączono do materiału
badawczego. Dokładna analiza cech gra-
fizmu oraz właściwości topograficznych
i mierzalnych zawartych we wszystkich
tych podpisach, jak również zastosowanie
metody superprojekcji (nałożenia na sie-
bie) wykazały, że wszystkie takie sygna-
tury odwzorowywały ten sam podpis. Tak
więc przedmiotem badań był w istocie je-
den podpis wzorcowy powielony w 88 ko-
piach. Należy przy tym podkreślić, że tego



Ryc. 1. Sposób wykonania kwestionowanych podpisów

rodzaju powielenie dotyczyło zarówno
samych podpisów, jak też odbitek pie-
czętarki firmowej zawierającej m.in. nazwę
firmy i nazwisko jej właściciela. Wszystkie
omawiane podpisy były bowiem tak samo
sytuowane w stosunku do odbitki pieczę-
tarki i jej detali graficznych, co dowodziło,
że ich pierwowzorem był w całości podpis
wraz z odbitką pieczętarki. Przy czym w do-
kumentach dowodowych PEŁNOMOCNICTWO
DO ZAWARCIA UMOWY oba te elementy – pod-
pis i odbitka pieczętarki – położone były
w tym samym miejscu na podłożu. Spo-
sób nakreślenia podpisów dowodowych
i umiejscowienia ich w dokumencie PEŁNO-
MOCNICTWO DO ZAWARCIA UMOWY w stosunku
do odbitki pieczętarki przedstawiony został
w powiększeniu na ryc. 1.

Dokonane wstępne ustalenia zdawały
się zatem potwierdzać informacje uzyska-
ne w toku postępowania przygotowaw-
czego od późniejszej oskarżonej Karoliny
B., zgodnie z którymi drogą elektroniczną
otrzymała ona pełnomocnictwo do działa-
nia w imieniu właściciela firmy i wzór umo-
wy. Jak podała oskarżona, otrzymała ona

umowę o pracę i pełnomocnictwo do zawierania umów w imieniu Szymona S.: *Na umowie tej była pieczęć firmy z jego podpisem; umowa nie była ani skanem, ani kserokopią, była stworzona na komputerze. Pieczęć z podpisem można było kopiować, jak mi była kiedyś potrzebna, to ją skopiowałam do innego dokumentu. Ja wydrukowałam tę umowę i pełnomocnictwo* (cytat z protokołu przesłuchania). Można więc było założyć, że wzorcowy podpis znajdował się w jednym z dokumentów, który został przesłany pocztą elektroniczną, a następnie dokument ten wydrukowano i wielokrotnie kopiowano, względnie podpis ten wraz z odbitką pieczęci metodą „kopiuj-wklej” przenoszono do innych dokumentów, które również drukowano i kopiowano.

Fakt, że podpisy dowodowe występowały jako odwzorowania podpisu wytworzonego w opisany sposób, a więc że nie dysponowano pierwopisami kwestionowanych podpisów (w tym podpisu stanowiącego wzorzec dla podpisów dowodowych), wpływał w istotny sposób na zakres badań oraz formułowane na ich podstawie wnioski. Po pierwsze, w takiej sytuacji nieuprawnione było bezpośrednie wypowiedzianie się o ewentualnym nakreśleniu kwestionowanych podpisów przez osoby, od których pochodził materiał porównawczy, w szczególności nie można było stwierdzić, czy podpisy na spornych dokumentach były sygnaturami autentycznymi, nakreślonymi przez Szymona S. Znane są bowiem metody fałszowania dokumentów poprzez „przeniesienie” do nich właściwych podpisów i wydrukowanie dokumentów zawierających takie podpisy. Zresztą w świetle wyjaśnień oskarżonej tak właśnie wytworzono podpisy występujące w udzielonych jej pełnomocnictwach. Można było jedynie dążyć do stwierdzenia zgodności lub wykazania różnic w cechach grafizmu (w tym w za-

kresie budowy i modelunku liter oraz ich detali graficznych, a także właściwości pomiarowych i topograficznych) zawartych w badanych podpisach dowodowych i porównawczych. Zgodnie z wcześniejszymi uwagami, w omawianym przypadku wynik badań w zależności od stwierdzenia w porównywanych podpisach cech zgodnych bądź różniących warunkował zakres możliwych do podjęcia wniosków identyfikacyjnych. Po drugie, brak pierwopisów powodował ograniczenia w zakresie możliwości badania wszystkich cech, jakie zwykle uwzględnia się w pismoznawczej analizie identyfikacyjnej, już choćby z tego powodu, że dowodowe kopie (wydruki) ze względu na jakość odwzorowania linii graficznej tworzącej podpisy utrudniały analizę szczegółów budowy znaków literowych, sposobu ich wiązania oraz tzw. cieniowania pisma związanego z naciskiem środka pisarskiego na podłoże. Trudności te spotęgowane były jeszcze przez sposób wytworzenia dokumentów zawierających podpisy, który osłabiał widoczność lub możliwości badań niektórych ich cech. Podpisy dowodowe umożliwiały wprawdzie analizę sposobu ich nakreślenia oraz badanie zawartych w nich cech grafizmu, jednak słabe odwzorowanie niektórych detali i cech szczegółowych (np. związanych z rozkładem nacisku środka pisarskiego na podłoże) utrudniał pełną analizę pismoznawczą. Dla zminimalizowania trudności w analizie cech szczegółowych wykorzystano laboratoryjną aparaturę badawczą pozwalającą na wzmocnienie obrazu analizowanych podpisów i redukcję szumów tła.

Podpisy dowodowe, a właściwie – jak wyżej wskazano – jeden podpis powielony w wielu kopiach, były sygnaturami czytelnymi, złożonymi z członu imienia i nazwiska, zawierającymi łącznie 12 znaków, przy czym dwa z nich były powtórzone. Dzięki temu dla przeprowadzenia zleco-

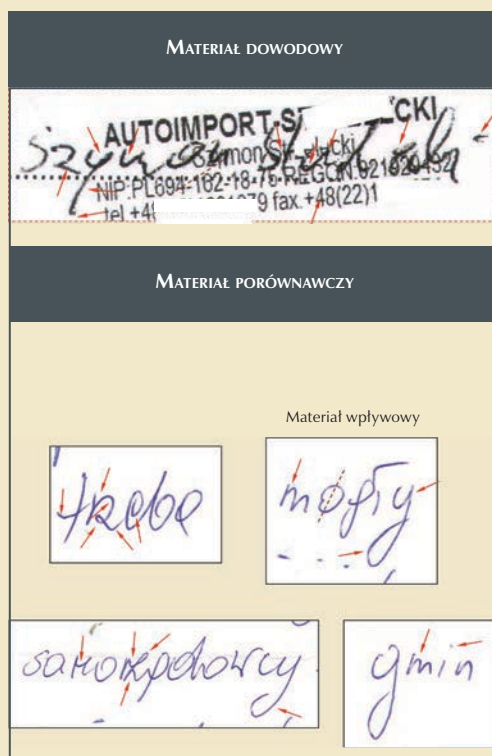
nych badań możliwa była do wykorzystania metoda graficzno-porównawcza według metodyki stosowanej do badania zapisów tekstowych, obejmująca dodatkowo analizę cech geometryczno-strukturalnych związaną z badaniem położenia podpisów (podpisu) oraz poszczególnych ich elementów na podłożu.

Z okoliczności sprawy, jak również z pytań zawartych w postanowieniu o powołaniu biegłego wynikało, że głównym zadaniem ekspertyzy była pomoc w określeniu stanu faktycznego sprawy, polegająca na potwierdzeniu lub sfalsyfikowaniu wyjaśnień oskarżonej Karoliny B. oraz Szymona S., któremu także postawiono zarzuty. W związku z tym podstawowym zadaniem ekspertyzy wskazanym w postanowieniu miało być ustalenie, kto nakreślił sporne podpisy – Karolina B. czy Szymon S. Niestety, same pytania zostały tak sformułowane [*czy podpisy (kopie podpisów) (...) o treści Szymon S...cki (...) pochodzą od oskarżonego Szymona S.; czy podpis złożony na pełnomocnictwie naniesiony na pieczęci AUTOIMPORT S...CKI został sporządzony przez oskarżoną Karolinę B.*], iż wynikało z nich, że organ procesowy oczekiwał wskazania bezpośredniego wykonawcy podpisów, pomimo ograniczeń wynikających z materiału badawczego. Gwoli ścisłości warto jednak dodać, że sąd zmodyfikował treść swojego postanowienia, gdyż w drugim postanowieniu mówił już o jednym podpisie, który był wzorcem dla pozostałych kopii.

Dlatego przekazany do badań materiał porównawczy obejmował oboje oskarżonych. W przypadku wzorów porównawczych Karoliny B. był to materiał dostatecznie reprezentatywny, aby mógł stanowić podstawę badań identyfikacyjnych, gdyż zawierał zarówno próbki bezwzględne (tj. występujące w dokumentach niezwiązanych z daną sprawą), jak i pobrane na polecenie (względne), cho-

ciaż mankamentem tego drugiego był brak próbek oddających brzmienie kwestionowanej sygnatury. Nie stanowiło to jednak zasadniczej przeszkody w wykorzystaniu tego materiału, bowiem, jak się okazało, decydujące znacznie miała tutaj klasa pisma i nawyki pisarskie zawarte w materiale porównawczym tej osoby i materiale dowodowym, zaś cały materiał porównawczy był jednorodny graficznie. Natomiast konieczne okazało się uzupełnienie materiału porównawczego pochodzącego od oskarżonego Szymona S., gdyż materiał pierwotnie dostarczony był zróżnicowany graficznie, zawierający na jednym biegunie podpisy i zapisy tekstowe wykonane starannie i w wolnym tempie, na drugim zaś nakreślone w niestarannej formie, z wysoką dynamiką i zanikiem czytelności części znaków. Na wniosek biegłego materiał ten poszerzono o wzory wpływowe, które okazały się wartościowe diagnostycznie, gdyż zawierały powtarzalne cechy grafizmu i topograficzno-pomiarowe związane m.in. z konstrukcją i modelunkiem, jak również sposobem wiązania znaków tworzących podpisy własne oskarżonego, które mogły stanowić odpowiednią podstawę dla ustaleń o zgodności bądź niezgodności cech stwierdzonych w materiale dowodowym. W badaniach porównawczych wykorzystano pomocniczo także inne niekwestionowane zapisy tekstowe Szymona S., które umożliwiły głębsze zorientowanie się w możliwościach graficznych tej osoby znajdujących odbicie w obrazie jej pisma ręcznego i manierze jego kreślenia (pismo niestaranne, z zanikiem czytelności liter, o nieregularnej linii).

W głównej fazie badań identyfikacyjnych analizie komparatystycznej poddano podpisy dowodowe (w zasadzie jeden z wielu analogicznych podpisów powielonych z tego samego wzorca), zestawiając je kolejno z materiałem porównawczym pochodzącym od obojga oskarżonych.

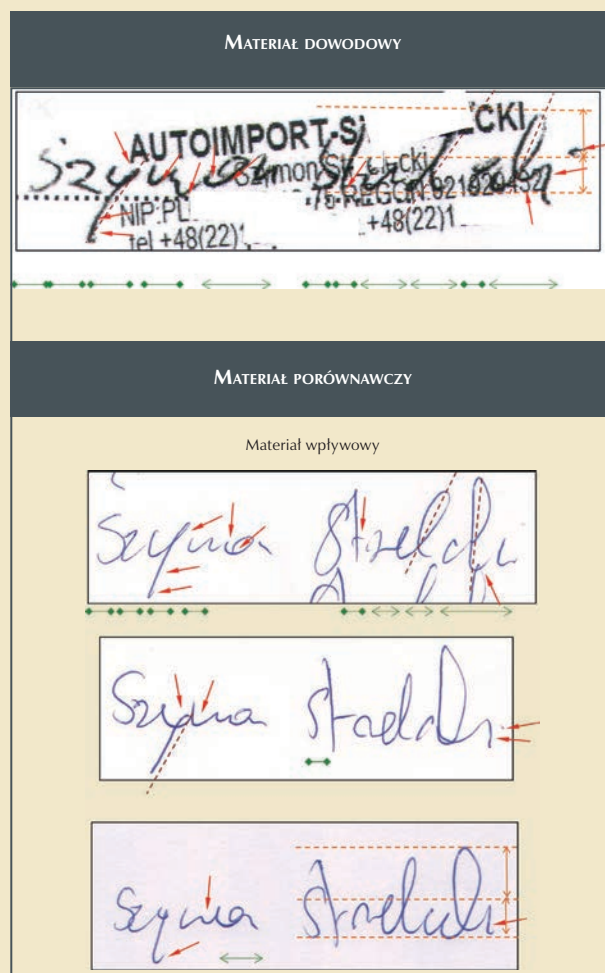


Ryc. 3. Cechy różniące w materiale dowodowym i materiale porównawczym Karoliny B.

pisma), pomimo jedynie waloru grupowego w badaniach identyfikacyjnych pisma ręcznego, znacząco różnicowała podpisy dowodowe i badany materiał porównawczy, prowadząc do wniosku o charakterze eliminacyjnym. Przykłady cech różniących w materiale dowodowym i porównawczym Karoliny B. pokazano na ryc. 2 i 3. Zatem nawet taki niepełnowartościowy od strony podpisów dowodowych materiał rękopiśmienny pozwalał na dokonanie ustaleń kluczowych dla rozstrzygnięcia winy oskarżonej.

Z drugiej strony analiza komparatystyczna wykorzystująca materiał porównawczy oskarżonego Szymona S. wykazała liczne zgodności lub choćby zbieżności graficzne w stosunku do podpisów dowodowych (ich wzorca). Wśród takich zgodności lub zbieżności należy w szczególności wymienić:

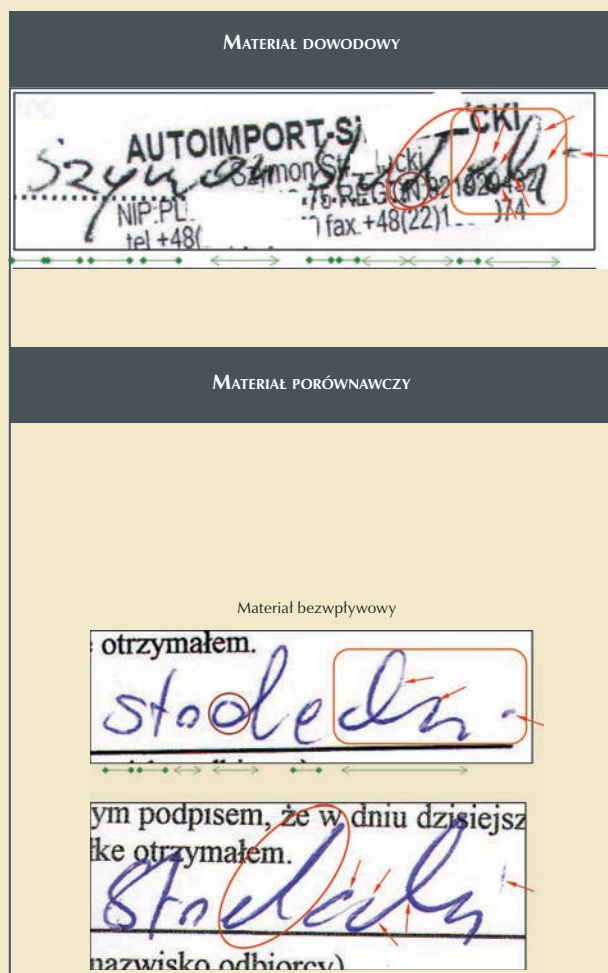
- manierę kreślenia podpisów dowodowych (podpisu wzorcowego) i własnych podpisów oskarżonego, mającą wpływ na zewnętrzny obraz graficzny badanych sygnatur (niestandardne kreślenie, zmiana wielkości liter, sytuowanie ich na różnych wysokościach);
- dynamikę oraz stopień spontaniczności kreślenia podpisów, które wykonane zostały w szybkim tempie, przy czym jest prawdopodobne, że czynnik ten miał wpływ na wspomnianą wyżej formę graficzną badanych sygnatur; wcześniej stwierdzono, że podpisy porównawcze Szymona S. prezentowały duże zróżnicowanie w zakresie dynamiki i staranności kreślenia, jednak spora ich część (w tym zarówno wzory bezwplywowe, jak i pobrane) była wykonana w taki sposób, że dawała zbieżny do podpisu dowodowego obraz graficzny;
- właściwości topograficzno-geometryczne oraz stosunki wielkościowe analizowanych podpisów, takie jak kąt nachylenia pisma (w tym niejednokrotne nachylenie grammatycznych liter), zmienna wysokość i szerokość liter, powiększanie lub zmniejszanie tych samych znaków w sygnaturze dowodowej i podpisach porównawczych, analogiczne powiększanie odległości międzyznakowych, bieg linii pisma i linii nakrywowej, sposób sytuowania względem siebie poszczególnych liter i ich elementów graficznych;
- rozkład impulsu pisma związany z bezpośrednim łączeniem liter, przy czym wprowadzie podpisy porównawcze za-



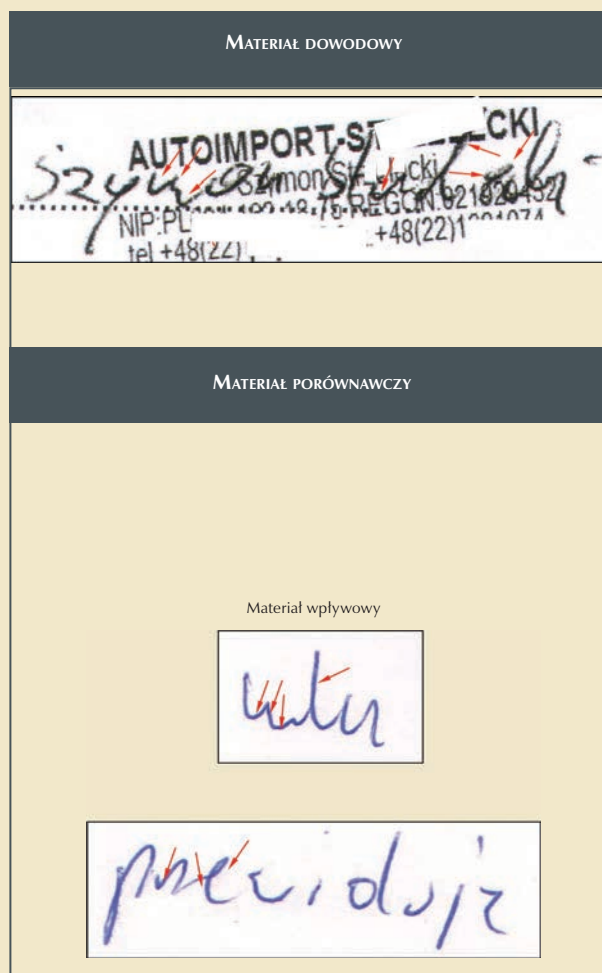
Ryc. 4. Cechy zgodne w materiale dowodowym i materiale porównawczym Szymona S.

wierały zróżnicowane warianty rozkładu impulsu pisma (można przyjąć, że było to związane z niską klasą pisma ich wykonawcy), jednak niektóre z nich w pełni powtarzały rozkład impulsu pisma stwierdzony w podpisach dowodowych. Jednocześnie na podkreślenie zasługuje zbieżny sposób wykonania wiązań międzyznakowych, związany z konstrukcją łączonych ze sobą liter;

- budowę i sposób kreślenia odpowiadających sobie w badanych podpisach liter i nieczytelnych znaków oraz sposób wykonania



Ryc. 5. Cechy zgodne w materiale dowodowym i materiale porównawczym Szymona S.



Ryc. 6. Cechy zgodne w materiale dowodowym i materiale porównawczym Szymona S.

ich licznych detali graficznych (np. budowa gramu w literach *m*, pętlicowe łączenie elementu śródlinijnego z trzonem podlinijnym w literach *y* i prawostronne zaginanie zakończenia trzonu w takich literach, sposób wykonania owalu w literach *o*, inicjowanie minuskuły *n* od poziomej adiustacji początkowej, przesuwanie znaku diakrytycznego w literze *i* w prawą stronę).

Przykłady cech zgodnych w materiale dowodowym i porównawczym Szymona S. pokazano na ryc. 4–6.

Uzyskane rezultaty badań komparatystycznych opartych na materiale porównawczym Szymona S. wskazywały na możliwość sporządzenia przez niego podpisu stanowiącego wzorec dla wszystkich podpisów dowodowych. Na taki wniosek miało wpływ stwierdzenie w porównywanym materiale rękopiśmiennym zgodnych i wartościowych diagnostycznie cech związanych z budową liter, w tym o nietypowym modelunku bądź konstrukcji. Uznano zatem, że ich wystąpienie w materiale dowodowym i porównaw-

czym nie jest przypadkowe. Nie było jednak możliwe sformułowanie bezpośredniego wniosku identyfikującego Szymona S. jako wykonawcę dowodowej sygnatury wzorcowej z podanych wcześniej powodów: braku pierwowpisu tej sygnatury oraz niemożliwości uwzględnienia w badaniach powielonych podpisów dowodowych wszystkich cech branych zwykle pod uwagę w analizie pismoznawczej. W opinii zawarto zarazem stwierdzenie, że gdyby dostarczono do badań pierwowpis podpisu stanowiącego wzorec dla podpisów dowodowych, końcowy wniosek opinii mógłby zostać zweryfikowany, włącznie z kategorięcznym jego sformułowaniem o narysowaniu sygnatury stanowiącej wzorec dla podpisów dowodowych przez oskarżonego.

Prezentowany kazus stanowi potwierdzenie tezy, iż celowe jest poddawanie badaniom nawet kopii rękopisów dowodowych bądź też utrwalonego w inny sposób ich obrazu graficznego. W tym przypadku badania takie pomogły sądowi rozpatrującemu sprawę w określeniu działań składających się na prowadzenie przestępnego procederu oszustwa i modus operandi sprawców, jak również ustaleniu roli, jaką odegrali w tym procederze poszczególni oskarżeni. Zawsze jednak należy pamiętać o ograniczeniach metodologicznych, jakie towarzyszą badaniom takiego materiału oraz o zakresie możliwych do wyciągnięcia w takim przypadku wniosków identyfikacyjnych.

¹Por. np. E. Buduj, *Problemy badania dokumentów nie będących oryginałami. Możliwości i granice kryminalistycznego wnioskowania*, [w:] *Problematyka dowodu z ekspertyzy dokumentów*, t. II, red. Z. Kegel, Wrocław 2002, s. 875–878; M. Goc, *Współczesny model ekspertyzy pismoznawczej. Wykorzystanie nowych metod i technik badawczych*, Warszawa–Szczecin 2015, s. 222–229; J. Grzegory, *Możliwości opiniowania o autentyczności podpisu na podstawie kopii*, [w:] *Aktualne tendencje w badaniach dokumentów*, red. Z. Kegel, Wrocław 2010, s. 219–234; M. Owoc, *Zakres badań pismoznawczych na kserokopiach*, [w:] *Problematyka dowodu z ekspertyzy dokumentów*, dz. cyt., s. 886–890; E.A. Slyter, *Forensic Signature Examination*, Charles C. Thomas Publ. 1995, s. 64–68. Jednocześnie jest interesujące, że w literaturze zagranicznej problem ten nie stanowi zasadniczego tematu rozważań, natomiast

w większym zakresie akcentuje się niebezpieczeństwo polegające na łatwości, z jaką „produkuje” się dokumenty przy użyciu kopiarek i techniki komputerowej oraz trudności w ich kryminalistycznym badaniu. Por. W.J. Flynn, *The Examination of Computer-Generated Documents*, [w:] *Scientific Examination of Questioned Documents*, red. J.S. Kelly, B.S. Lindblom, CRC Press 2006, s. 193–196; K.M. Koppenhaver, *Forensic Document Examination. Principles and Practice*, Humana Press 2007, s. 58–59

²P. Girdwoyń, T. Tomaszewski, *Możliwości opiniowania na podstawie kopii w kryminalistycznych badaniach dokumentów*, „Człowiek i Dokumenty” 2009, nr 12, s. 39 i n.

³Por. T. Tomaszewski, *Dowód z opinii biegłego w procesie karnym*, Kraków 2000, s. 54.

⁴Sprawa o sygn. akt XII K 138/13 prowadzona przez Sąd Okręgowy w Warszawie.

Monika Krucińska

IRAN – Z LECHISTANU DO PERSJI

To naprawdę zaskakujące, jak wiele informacji o historii, tradycjach, kulturze i geografii poszczególnych krajów zawierają książeczki paszportowe przez nie wydane. Wystarczy umieć dostrzec i odczytać zapisy, symbole i obrazki w nich zawarte.



Dzisiaj przed nami „podróż” po paszporcie kraju oddalonego od Polski o tysiące kilometrów. Kraju o odmiennej religii, kulturze, odwiedzanego raczej przez zatwardziałych podróżników niż przeciętnych globtroterów. Iran – znany dawniej jako potężna Persja – to państwo przeważnie kojarzące się z tajemniczością, a czasem, jak każde nieznanne, odbierane jako wrogie i niebezpieczne. Kraj turystycznie nieodkryty, a posiadający wiele wspaniałych zabytków. Starożytne miasta, niektóre nadal rozwijające się, inne porzucone już przed wiekami, świadczą o roli, jaką kraj ten odgrywał w kontaktach między Wschodem a Zachodem. Od stuleci cały świat zna takie nazwy jak Persepolis czy Isfahan.

Lechistan¹, czyli Polskę w języku perskim, i Persję – kraje tak odległe pod każdym względem – łączy emocjonalna więź zapoczątkowana w ciężkich czasach II wojny światowej, kiedy Irańczycy gościli na swojej ziemi 120 tysięcy polskich uchodźców ewakuowanych z ZSRR. Dodatkowo, jak podkreślają przedstawiciele dyplomatyczni, w odległej historii, kiedy nazwa „Polska” została wymazana z mapy Europy, Iran jako jeden z dwóch krajów na świecie nie uznał faktu utracenia przez nasze państwo niepodległości. Podobno na dworze irańskim zawsze stało pu-

ste krzesło oczekujące na przedstawiciela Rzeczypospolitej Polskiej.

Biometryczny, czterdziestostronicowy paszport Islamskiej Republiki Iranu wydawany od 20 lutego 2011 roku ma obwolutę koloru bordo o fakturze skóry groszkowej (fot. 1). Na froncie okładki możemy dostrzec symbol państwa oraz treści dotyczące rodzaju dokumentu, a także oznaczenie umieszczenia w nim danych biometrycznych. Tradycyjnie elementy te wykonano techniką foliodruku w kolorze złotym.

W użyciu są także nowsze dokumenty ze zmodyfikowaną formą elementów zabezpieczeń. Wydawane od 2014 roku dokumenty liczące 32 strony mają zmienioną formę nadruków, zabezpieczeń holograficznych i postać znaku wodnego (fot. 2).

Na froncie okładki informacje podane są w językach perskim i angielskim. Językiem urzędowym obowiązującym w Iranie jest farszi, czyli perski. Posiada on pewne naleciałości i sporo zapożyczeń z arabskiego, jednakże w rzeczywistości jest zupełnie inny. W różnych częściach kraju występuje wiele dialektów i akcentów, przez co dany wyraz używany w jednym miejscu może być zupełnie niezrozumiały dla mieszkańców innych rejonów. Fonetycznie irański perski ma sześć samogłosek i dwadzieścia trzy spółgłoski. Językiem angielskim komunikatywnie władą niewielki

MONIKA KRUCIŃSKA – wykładowca w Centralnym Ośrodku Szkolenia Straży Granicznej w Koszalinie.



Fot. 1. Obwoluta biometrycznego paszportu Iranu



Fot. 2. Obwoluta nowszego wzoru paszportu Iranu³

odsetek Irańczyków. Jest to spowodowane w dużej mierze antyamerykańską polityką obowiązującego od czasów rewolucji reżimu. Z tego też względu przedstawiciele starszego pokolenia (które odebrało edukację jeszcze za czasów szacha Rezy Pahlawiego) znają ten język lepiej niż młodzież. Poziom angielskiego przeciętnego Irańczyka opiera się na znajomości kilku fraz². Ciekawostką może być informacja o kolejności zapisu cyfr w liczbie – od lewej do prawej, czyli identycznie jak u nas, w przeciwieństwie do alfabetu, który zapisuje się od prawej do lewej.

Oprócz nadruków językowych na okładce umieszczony jest naro-

dowy symbol w postaci godła (fot. 3). Jego motyw powtarza się na wybranych stronach dokumentu, między innymi na wyklejkach czy też jako element transparentnej folii kinograficznej.

Godło wprowadzone po rewolucji islamskiej i obaleniu szacha Mohammada Rezy Pahlawiego zastąpiło symbol obowiązujący w okresie monarchii. Ma ono postać stylizowanego napisu: الله (czyt. Allah), tj. Bóg w języku perskim. Godło to podkreśla pozycję, jaką w Islamskiej Republice Iranu zajmuje religia muzułmańska. Graficznie składa się z czterech półksiężyców oraz umieszczonego pośrodku miecza. Pięć części godła sym-



Fot. 3. Znak godła państwowego umieszczony na okładce paszportu zwykłego Iranu



Fot. 4. Pierwsza wyklejka starszego wzoru paszportu zwykłego Iranu



Fot. 5. Symbol godła naniesiony farbą zmienną optycznie

bolizuje pięć filarów islamu: wyznanie wiary, modlitwę, jałmużnę, post i pielgrzymkę do Mekki. Nad mieczem umieszczona jest shadda – znak diakrytyczny w języku perskim używany do zaakcentowania. Kształt godła przypomina tulipan, co ma nawiązywać do starożytnego przekonania, że jeśli młody żołnierz umrze w walce za ojczyznę, na jego grobie będą rosły czerwone tulipany. W ostatnich latach emblemat ten został uznany za symbol męczeństwa. Znak godła został zaprojektowany przez Hamida Nadimiego a oficjalnie zatwierdzony 9 maja 1980 roku przez ajatollaha Ruhollaha Chomeiniego⁴.

Na pierwszej wyklejce starszego wzoru paszportu symbol godła umieszczony jest przy górnej krawędzi strony (fot. 4). Naniesiony farbą zmienną optycznie, techniką sitodruku, tworzy ciekawe efekty wizualne (fot. 5).

Na elementy tła składają się linie offsetowe wykazujące cechy druku irysowego

i reliefowego w kolorystyce żółto-beżowo-brązowej. W centralnej części widoczne są dwunastoramienne rozety wzajemnie wypełniające się, każda innym wzorem.

Wokół rozety poprowadzona jest ramka wykonana drukiem wklęsłym, w którym



Fot. 6. Efekt kątowy na pierwszej wyklejce paszportu



Fot. 7. Strona tytułowa paszportu zwykłego Iranu

to motywie widoczny jest także efekt irysowy. Obok ramki biegnie linia mikrodruku w języku perskim. Z kolei w dolnej części strony zlokalizowany jest efekt kątowy przedstawiający napis IRAN (fot. 6).



Fot. 8. Pierwsza wyklejka oraz strona tytułowa nowszego wzoru paszportu Iranu⁵

Wyklejki udekorowane wzorami niemającymi początku ani końca, o charakterystycznej regularności, a także strona tytułowa (fot. 7) przywodzą na myśl przepiękne mozaiki i witraże, którymi zdobione są irańskie meczety. Dla nas – ludzi żyjących w XXI wieku i zakorzenionych w chrześcijańskiej kulturze europejskiej – nie mają one prawdopodobnie głębszego znaczenia poza dostarczaniem wrażeń estetycznych wynikających z urody form geometrycznych. Budzą tęsknotę za harmonią i spokojem, skłaniają do rozmyślań nad pięknem, nieskończonością i ludzką perfekcją. Jednak dla wyznawców islamu niosą one o wiele więcej treści i znaczeń. To szczególny sposób wyrażenia podziwu dla bożej doskonałości. Symbolizujący nieskończoną naturę Boga – człowiek w swoim życiu może najwyżej nieudolnie kopiować jego dzieła, ale nie są mu dostępne początek ani koniec wszystkiego. Zapełnianie dużych powierzchni powtarzającymi się wzorami oddaje też efekt wszechobecności Boga i zachęca do kontemplacji⁶.

Dla porównania chciałabym przedstawić obecne komponenty paszportu wydawanego od 2014 roku. Na fot. 8 prezentuję pierwszą wyklejkę oraz stronę tytułową. Elementy tła giloszowego mają dobrze widoczne cechy druku irysowego i reliefowego o wyraźnie zmodyfikowanych – w porównaniu ze starszą wersją dokumentu – kolorach i wzorach. Na pierwszej wyklejce paszportu na uwagę zasługują detale wykonane techniką druku wklęsłego. Są to rozeta umieszczona w centralnej części i położony poniżej stylizowany kwiat tulipana wykonany farbą zmienną optycznie.



Fot. 9. Strona personalizacyjna⁷



Fot. 10. Strona personalizacyjna paszportu zwykłego wydawanego od 2014 roku⁸

Na rewersie strony tytułowej znajduje się strona z danymi personalizacyjnymi, które, podobnie jak wizerunek posiadacza, a także powtórzony wizerunek, zostały naniesione za pomocą drukarki atramentowej. Całość zabezpieczono następnie transparentną folią kinograficzną (fot. 9).

W nowszym wzorze dokumentu nie występuje powtórzony wizerunek posiadacza (fot. 10).

Zarówno w jednym, jak i w drugim przypadku elementem chroniącym dane właściciela jest folia transparentna o unikalnym wzorze, gdzie na pierwszy plan wysuwają się emblematy narodowe (fot. 11), ale również, co jest szczególnie zauważalne w nowszym wzorze dokumentu, standardowe międzynarodowe symbole, takie jak róża wiatrów czy kula ziemiska (fot. 12).

Jest to z pewnością interesujące i z innego punktu widzenia atrakcyjne rozwiązanie jeśli chodzi o ochronę danych właściciela.

Przyjrzyjmy się teraz stronom wizowym dokumentu (fot. 13). Jak już wspomniałam, starszy wzór dokumentu posiadał 40 stron, natomiast w nowym jest ich 32. Informacja o liczbie stron zawarta jest na pierwszej wyklejce paszportu. Główną stroną w starszym wzorze powtarza się na każdej stronie, jest jednolity. Posiada cechy druku irysowego i jest z całą pewnością antykseryczny, reliefowy.

W świetle przechodzącym możemy zaobserwować przede wszystkim wielotonowy, umiejscowiony znak wodny umieszczony w specjalnie przygotowanym na to miejscu i nie zabezpieczającą z mikrodrukiem oraz flagą narodową (fot. 14). Ponadto przy dolnej krawędzi stron widoczny jest stylizowany ornament z efektem recto-verso.

Wzór flagi narodowej Iranu (fot. 15) został ustanowiony 29 lipca 1980 roku i jest od-



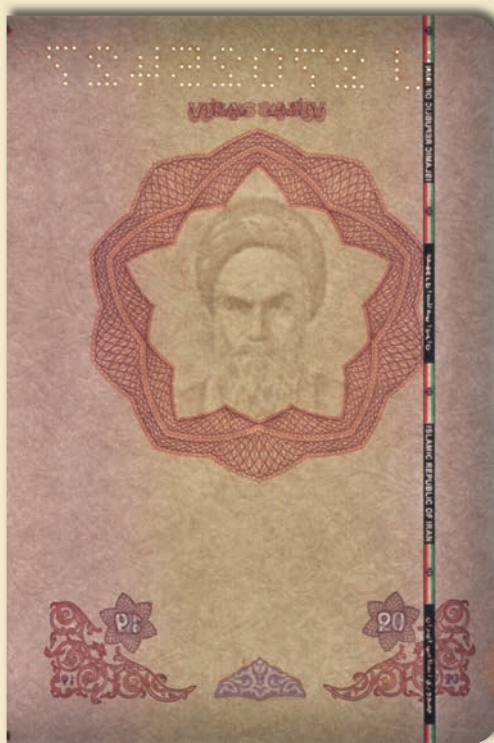
Fot. 11. Transparentna folia holograficzna zabezpieczająca dane właściciela w starszym wzorze paszportu⁹



Fot. 12. Transparentna folia holograficzna zabezpieczająca dane właściciela zamieszczona w nowszym dokumencie¹⁰



Fot. 13. Strona wizowa paszportu starszego wzoru



Fot. 14. Strona dokumentu w świetle przechodzącym



Fot. 15. Flaga Iranu¹¹



Fot. 16. Gilosz stron wizowych dokumentu nowego wzoru¹²



Fot. 17. Mauzoleum Omara Khayyama w Niszapur¹³

zwierciedleniem zmian, jakie zaszły w kraju po rewolucji islamskiej. Na fladze w postaci horyzontalnych pasów występują od góry do dołu trzy kolory: zielony – symbolizujący religię islamską, biały – pokój i czerwony – męstwo.

Białe wzory na zielonym i czerwonym kolorze to słowa *Allahu Akbar* (Bóg jest wielki) powtórzone 22 razy (dwa rzędy po 11 wyrażień) dla upamiętnienia daty zwycięstwa rewolucji – 22 Bahman 1357 kalendarza irańskiego, tj. 11 lutego 1979 roku.

Na białym pasie dodatkowo umieszczone jest godło Iranu w kolorze czerwonym – stylizowany napis *Allah*¹⁴.

Gilosz stron dokumentu nowego wzoru posiada cechy zdecydowanie bardziej futurystyczne, czego przykładem może być chociażby zróżnicowany motyw tła, atrakcyjniejsze wzory i kolory (fot. 16).

Dla uatrakcyjnienia go użyto motywów kultury i sztuki irańskiej, czego przykładem



Fot. 18. Strona paszportu nowszego wzoru w świetle przechodzącym¹⁵



Fot. 19. Strona wizowa paszportu starszego wzoru w świetle ultrafioletowym

może być widoczne na stronie 17 Mauzoleum Omara Khayyama (fot. 17), perskiego matematyka, astronoma, filozofa i poety, który jest powszechnie uważany za jednego z najbardziej wpływowych średnio-wiecznych naukowców.

W nowszym paszporcie zrezygnowano z nitki zabezpieczającej. Występują za to znaki wodne wielotonowy i jednotonowy – oba umiejscowione (fot. 18). Ponadto w świetle przechodzącym widoczny jest element recto-verso umieszczony przy krawędziach zewnętrznych.

Myszę, że nikt z nas nie ma większego problemu z rozpoznaniem wizerunku postaci wykorzystanego jako znak wodny. Jest to oczywiście szyicki przywódca duchowny i polityczny Iranu – ajatollah Ruhollah Musawi Chomeini (ur. 24 września 1902 r. w Chomejn, zm. 3 czerwca 1989 r.

w Teheranie). W latach 1979–1989 pełnił funkcję Najwyższego Przywódcy. Do dzisiaj w Iranie spotkać można miejsca pamięci, murale poświęcone duchownemu, na przemian i w parze z wizerunkiem obecnego przywódcy Iranu.

W świetle ultrafioletowym zarówno na stronach wizowych (fot. 19), jak i na stronie z danymi widoczne są odcinki nici zabezpieczającej, a także licznie występujące różnokolorowe włókna zabezpieczające.

Przeglądając dokument Iranu, na drugiej wyklejce możemy spotkać się z interesującą adnotacją odnoszącą się do pewnych relacji politycznych Iranu. Chodzi tu o stosunki z państwem Izrael. Wzajemna wrogość Izraela i Iranu przekłada się głównie na spory terytorialne i nie ma związku z samą religią czy kulturą. Iran oficjalnie nie uznaje

żydowskiego kraju, określając go mianem „okupowanej Palestyny” i zakazując swoim obywatelom podróży doń, co znalazło wyraz w paszporcie w postaci nadruku: *Po posiadacz tego paszportu nie jest uprawniony do podróżowania do okupowanej Palestyny.*

W dokumencie natkniemy się również na dodatkowe karty, z których jedna strona zawiera uzupełniające adnotacje urzędowe, a strony kolejne przeznaczone są na wpisanie dzieci i zamieszczenie ich wizerunków.

Paszport irański starszego wzoru, chociaż zawierający dane biometryczne, posiada podstawowy system zabezpieczeń zamieszczony na wszystkich jego poziomach. Wydaje się, że na specjalną uwagę zasługuje jedynie transparentna folia holograficzna dająca dość ciekawe wrażenia

wizualne. Całościowo dokument wydaje się mało efektowny, chociaż oczywiście nie jest to jego kluczowa rola. Natomiast nowszy wzór dokumentu zbliżony jest do europejskich standardów, występują w nim zarówno nowocześniejsze zabezpieczenia w papierze, jak i techniki drukarskie czy kompozycje tła stawiające na różnorodność, skomplikowane i antykseryczne wzory. Nowszy wzór dokumentu jest ciekawy artystycznie, posiada nietuzinkową kompozycję tła i sprawnie wykorzystuje poszczególne obszary zabezpieczeń. Poprzez takie rozwiązania oferuje dodatkową wartość – poznawczą, dającą możliwość wszechstronnej interpretacji dokumentu jako wizytówki przedstawiającej kraj.

¹Państwo Lecha pojawia się w Biblii już w czasach Abrahama, a w kronikach perskich w 6 w. p.n.e. i do dzisiaj Persowie oraz Turcy nazywają nasz kraj Lechistanem.

²<http://www.naszaslodkabezdomnosc.pl/2014/11/03/iran-jezyki-i-porozumiewanie-sie/#>.

³https://upload.wikimedia.org/wikipedia/commons/f4/Iranian_Biometric_Passport_Cover.jpg.

⁴Na podst.: https://en.wikipedia.org/wiki/Emblem_of_Iran.

⁵<http://edisonetd.net/>.

⁶<http://www.matematyka.wroc.pl/doniesienia/tajemnice-islamskich-ornamentow>.

⁷<http://edisonetd.net/>.

⁸Tamże.

⁹Tamże.

¹⁰Tamże.

¹¹<http://flagpedia.net/data/flags/ultra/ir.png>.

¹²<http://edisonetd.net/>.

¹³[https://upload.wikimedia.org/wikipedia/commons/b/be/Omar_Khayyam's_Tomb_\(Neyshabur\)_001.jpg](https://upload.wikimedia.org/wikipedia/commons/b/be/Omar_Khayyam's_Tomb_(Neyshabur)_001.jpg).

¹⁴https://pl.wikipedia.org/wiki/Flaga_Iranu.

¹⁵<http://edisonetd.net/>.

Monika Olbryś-Zegarowska, Tomasz Turek

WALKA O WOLNOŚĆ I HONOR... WALKA O OJCZYZNĘ

Dramatyczne boje powstania warszawskiego w sierpniu 1944 roku, między innymi o redutę PWPW, przyniosły ogromne straty w ludziach i zniszczenia budynków. Jednak powstańcy udowodnili, że za ideał wolności warto poświęcić życie.



Przez pięć lat okupacji niemieckiej Polacy byli prześladowani i masowo mordowani przez Niemców. Dlatego, mimo przeważającej siły militarnej wroga, zdecydowali się na walkę o wolność. Przypomnijmy fakty: powstanie warszawskie było zbrojnym wystąpieniem Polaków przeciwko okupantowi niemieckiemu podczas II wojny światowej. Trwało od 1 sierpnia do 3 października 1944 roku. Powstanie, które w założeniu miało objąć ziemię całej Polski, udało się w zasadzie przeprowadzić wyłącznie w stolicy. Heroiczne walki z wrogiem mającym przewagę w uzbrojeniu, a później także liczebną, trwały 63 dni.

Pierwszego sierpnia, gdy wybiła godzina 17.00, przeciwko żołnierzom niemieckim stacjonującym w Warszawie w liczbie około 16 tys. stanęło około 50 tys. żołnierzy z Armii Krajowej i innych ugrupowań niepodległościowych. Niestety, zaledwie 5 tys. z nich było dobrze uzbrojonych. Natomiast armia niemiecka dysponowała bronią pancerną, artylerią i lotnictwem.

Jednym z ważnych punktów wojskowego oporu powstańców był kompleks maszynowych gmachów Polskiej Wytwórni Papierów Wartościowych. Odbity przez Polaków z rąk niemieckich 2 sierpnia, przez 27 dni stanowił redutę powstańczą broniącą wojskom niemieckim dostęp do Starówki.

Dziś PWPW ma główną siedzibę w tych samych murach, w których rozegrały się tra-

giczne wojenne wydarzenia. Patrzymy więc na naszą spółkę nie tylko jako na producenta banknotów, dokumentów zabezpieczonych i kart plastikowych, lecz również z perspektywy historycznej: jako na strażnika pamięci walk o niepodległość Polski w 1944 roku.

Historia odbicia PWPW z rąk niemieckich i obrony jej gmachów przed próbami odzyskania ich przez okupanta, a później ich utraty, jest jedną z wielu tragicznych historii związanych z walkami w Warszawie podczas powstania. Została wielokrotnie i szczegółowo opisana, głównie przez jednego z uczestników tamtych wydarzeń, Juliusza Kuleszę, który do swych prac zebrał liczne relacje walczących w tym miejscu żołnierzy.

Nie sposób opisać w krótkim artykule szeregu skomplikowanych zależności i decyzji związanych z działaniami bojowymi w PWPW. Czytelnikowi musi więc wystarczyć jedynie skrót opracowany na podstawie książki Juliusza Kuleszy.

Jak wspomniano, Wytwórnia oraz budynek mieszkalny jej pracowników, znajdujące się w czasie okupacji w rękach niemieckich, zostały zdobyte przez powstańców w drugim dniu powstania – 2 sierpnia 1944 r. Atak na PWPW przeprowadzono trzema grupami uderzeniowymi: 1. z boku PWPW, 2. na tyły PWPW, 3. od środka – metodą „konja trojańskiego”: siłami grupy PWB/17/S pod dowództwem por. „Białego” (Czesława Lecha)¹.

MONIKA OLBRYŚ-ZEGAROWSKA – absolwentka Wydziału Prawa Uniwersytetu w Białymstoku, kierownik wydziału obsługi kancelaryjno-archiwalnej w PWPW S.A.

Po kilku godzinach walk drużyny powstańcze, w tym wytwórniana grupa PWB/17/S obsadziły strategiczne stanowiska w gmachach produkcyjnych firmy i w budynku mieszkalnym.

Ze specyficznym zabarwieniem wspomina te wydarzenia jeden z powstańców z PWB, Stefan Gąsania: *I tak o godz. 12 drugiego sierpnia zaczęło się polowanie na Niemców po korytarzach Wytwórni. Przez kilka minut byliśmy prawie bez broni i amunicji. Wydostaliśmy się z kolegą z korytarza na podwórze, stąd zza bel ze ścinkami ostrzelaliśmy okno portierni, w które uprzednio rzuciłem granaty (...). Ja zostałem bez broni, kolega miał jeszcze kilka naboju w automacie (...). Nagle widzimy, jak oknem w piwnicy wydostaje się nasz żołnierz, powstaniec z taśmami amunicji na piersiach, autematem i granatami, a za nim inni. Tak przyszła pomoc powstańców Starówki dla Wytwórni. I teraz zaczęła się prawdziwa zabawa, a o godz. 13 Wytwórnia została całkowicie opanowana².*

Grupa Romana Marchla (pseud. „Rom”) obsadziła budynek mieszkalny pracowników PWPW, mieszczący się obok kompleksu fabrycznego przy ulicy Rybaki 35. W tym czasie w podziemiach gmachu powstał także punkt sanitarny kierowany przez doktor Hannę Petrynowską (pseud. „Rana”). Działał tu również centralny magazyn żywności dla Armii Krajowej.

Siły powstańcze w Warszawie nie były na tyle liczne i dobrze uzbrojone, by opanować całe miasto. Dlatego już od pierwszych dni Niemcy organizowali kontrataki – w tym próby odzyskania gmachu PWPW m.in. za pomocą czołgów Panther i piechoty. Kompleks fabryczny znalazł się też pod stałym, silnym ostrzałem artyleryjskim. Specyfika walk w mieście powodowała konieczność wznoszenia barykad w poprzek ulic, w celu uniemożliwienia wjazdu w nie czołgom niemieckim. Takie barykady powstały też w okolicy Wytwórni. Mimo tego ostrzał i bombardowa-



Fot. 1. Już na początku powstania warszawskiego Niemcy próbowali odbić gmach PWPW z rąk Polaków poprzez m. in.: ataki bombowe, ostrzał z pociągu pancernego, użycie dział szturmowych, moździerzy oraz miotaczy min i płomieni. Na zdjęciu bombardowany gmach PWPW

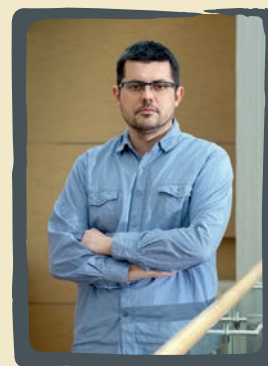
nia powodowały duże straty i wywoływały pożary okolicznych zabudowań. Gmach Wytwórni, który powstał w latach 1926–1929, był nowoczesną i solidną konstrukcją z betonu i stali. Jednak wokół znajdowało się wiele kamienic oraz zabudowań drewnianych, które łatwo ulegały pożarom, stanowiąc zagrożenie dla ludzi. Po 10 sierpnia ostrzał PWPW zaczął wspomagać niemiecki ciężki uzbrojony kuter rzeczny.

W pierwszych dniach powstańcy broniący kompleksu Wytwórni dawali sobie znakomicie radę, jednak z czasem, wobec zintensyfikowanych ataków wroga, ich sytuacja stawała się coraz trudniejsza. Dlatego stałą załogę PWPW wzmacniały jednostki Armii Krajowej walczące wcześniej w innych punktach miasta. Nasilały się bombardowania z powietrza, przybywało coraz więcej rannych. *Za stół operacyjny dla leżących rannych służyła leżanka lekarska, a dla ciężkich przypadków (np. dla amputacji) – podłoga, którą zaścielało się prześcieradłem i praca szła*

w pozycji kłęzącej (...). Szczęściem dla nas było, gdy ranny okazał się mniej odporny przy zabiegu i po prostu zemdlął, gorzej bywało z tzw. twardzielami, którzy z bólu wykrzykiwali co im ślina na język przyniosła – wspominała jedna z sanitariuszek¹.

19 sierpnia nastąpił pierwszy dzień niemieckiego walnego szturmu na Stare Miasto z udziałem lotnictwa bombowego, pociągu pancernego, dział szturmowych, goliatów, moździerzy, miotaczy min i płomieni. 24 sierpnia na kompleks PWPW i jej budynek mieszkalny uderzyła seria ataków niemieckiego lotnictwa, artylerii i piechoty. Bomby rozbiły i zapaliły zbiorniki łatwo palnego płynu używanego w poligrafii. Płyn ten, płonąc, lał się przez wielkie dziury w stropach do kondygnacji podziemnych, gdzie kwatrowali polscy żołnierze.

25 sierpnia budynek mieszkalny pracowników PWPW został utracony przez Polaków po użyciu przez Niemców gazów bojowych.



TOMASZ TUREK – absolwent Wydziału Polonistyki Uniwersytetu Warszawskiego. Redaktor ŻYCIA WYTWÓRNI, we-wnętrznego tygodnika PWPW S.A.



Fot. 2. Niemieckie działo szturmowe Ferdinand przed budynkiem mieszkalnym przy ul. Rybaki, w pobliżu gmachów PWPW
Źródło: CAW, nr A14781.

26 sierpnia transporter ładunków wybuchowych rozerwał ogrodzenie PWPW, co umożliwiło Niemcom dostanie się do budynku i opanowanie jego górnych pięter. Rozpoczęły się zaciekle walki wewnątrz. Zła pozycja powstańców powodowała, że byli oni stopniowo spychani coraz niżej, tracili wielu żołnierzy – zabitych i rannych. Zmęczenie, brak snu i bardzo wysoka temperatura spowodowana pożarem górnych kondygnacji gmachu osłabiła możliwości utrzymania Wytwórni w polskich rękach.

28 sierpnia załamał się opór powstańców – resztki oddziałów walczących w kompleksie PWPW wycofały się na Stareńkę. Ludność cywilna i ranni z lazaretu, schronieni na terenie Wytwórni, dostali się w ręce Niemców. Ci spośród nich, którzy

brali udział w obronie, zostali rozstrzelani. Podczas zajmowania ostatniego schronu w PWPW okupanci zabili bezbronną doktor Hannę Petrynowską „Ranę”, która zażywała szpitalem.

W ciągu 27 dni walk o PWPW zginęło tu od 80 do 100 żołnierzy, gmach został zniszczony w 60 proc., a maszyny i urządzenia w 80 proc.

Po wojnie kompleks gmachów PWPW został odbudowany, a Wytwórnia podjęła ponownie produkcję w latach 50. XX wieku.

Firma kultywuje tradycję powstańczą poprzez coroczne uroczystości przy tablicy upamiętniającej walki na jej terenie. Natomiast w tym roku, 27 sierpnia zorganizowana została rekonstrukcja walk powstańczych o Redutę PWPW.



Fot. 3. Gmach Wytwórni w roku 1945. Zdjęcie z archiwum PWPW

¹J. Kulesza, *W murach PWPW*, Warszawa 2003, s. 85.

²Tamże, s. 89.

³Relacja Haliny Czech-Wisłockiej, Archiwum środowiska byłych żołnierzy zgrupowania AK „Róg”.

Nowe 50 franków

Prawie 20 lat po wprowadzeniu ósmej serii franków szwajcarskich Narodowy Bank Szwajcarii podjął decyzję o wydaniu serii 9, która zawiera zaawansowany zestaw zabezpieczeń wkomponowany w imponujący projekt graficzny.

Tematem przewodnim banknotu pięćdziesięciofrankowego jest wiatr. Pozostałe banknoty w serii przedstawiają kolejno: czas (10 fr.), światło (20 fr.), wodę (100 fr.), materię (200 fr.) i język (1000 fr.).

Jak przedstawić wiatr? Manuela Pfrunder, projektantka serii, zdecydowała się na zaprezentowanie na przedniej stronie banknotu wizerunku dłoni trzymającej dmuchawiec z nasionami porośniętymi przez wiatr. Na stronie odwrotnej widnieje paralotnia lecąca między szczytami szwajcarskich gór. Na froncie banknotu możemy również zobaczyć glob z zaznaczonymi kierunkami wiatrów. Motyw strzałek meteorologicznych wykorzystany jest także w tle giloszowym.

Szwajcarski Bank Narodowy wskazuje na 15 różnych elementów zabezpieczających, w które wyposażony jest banknot 50 franków. Niektóre zabezpieczenia znane są z poprzednich serii.

W prześwicie możemy obserwować dwa różne znaki wodne oraz element wykonany techniką mikroperforacji. Jednym z najbardziej rzucających się w oczy elementów jest OVMI Spark® w postaci wizerunku globu. Element zmienia kolor od złotego do zielonego. W dolnej części umieszczone są dwukolorowe strzałki przedstawiające kierunki wiatru, wydrukowane techniką stalorytniczą. Nadruk ten częściowo znajduje się na pasku holograficznym.

Elementem powtarzającym się na banknocie jest szwajcarski krzyż widoczny jako okienko, mikroperforacja i efekt kątowy.

Banknot wydrukowano na podłożu Durasafe produkcji firmy Lanquart. Jest to polimer pokryty z obu stron warstwą papieru o gramaturze 35 g/m².

„Infosecura” 2016, nr 68, s. 6–8.

Zarządzanie kryzysem humanitarnym

Uchodźcy z Syrii, Iraku, Libii i innych krajów Afryki i Azji bardzo często dokonują pierwszej rejestracji w Niemczech, pomimo że do Europy trafiają przez Grecję lub Włochy.

Niemieckie władze zwykle mają problem z ustaleniem wiarygodnej tożsamości napływającej ludności, ponieważ uchodźcy najczęściej nie dysponują żadnym dokumentem.

Ministerstwo Spraw Wewnętrznych Niemiec zdecydowało o wydawaniu dokumentu będącego dowodem dokonanej rejestracji bez konieczności ustalenia wiarygodnej tożsamości. Od stycznia 2016 r. takim dokumentem jest Ankunftsachweis, czyli dokument przybycia lub certyfikat osoby starającej się o azyl. Nie jest

to dokument tożsamości ani gwarancja udzielenia ochrony. Służy jedynie celom rejestracyjnym i umożliwia uzyskanie pomocy humanitarnej.

Dokument jest elementem bezbłędnie zorganizowanego systemu administracyjnego. W punkcie rejestracyjnym uchodźcy podają swoje dane. Każdej osobie wykonuje się fotografię i pobiera odciski wszystkich palców. W celu uniknięcia wielokrotnej rejestracji zebrane dane sprawdzane są w centralnej bazie danych Fast ID.

Sam dokument Ankunftsachweis jest wykonany na podłożu papierowym według minimalnych wymagań ICAO i Unii Europejskiej. Podłoże zabezpieczono za pomocą znaku wodnego i włókien zabezpieczających. Druk zawiera gilosze z mikrotekstami, nadruki widoczne w świetle UV i numerację typograficzną. Personalizacja zabezpieczona jest za pomocą folii z Kinegramem®. Nowy element zabezpieczający to czytany maszynowo kod 2D, którego weryfikacja jest możliwa za pomocą smartfonu.

„Infosecura” 2016, nr 68, s. 13.

Brak chipa – brak ochrony?

Nowoczesne elektroniczne paszporty i dokumenty tożsamości są trudne do podrobienia. Dlatego przestępcy szukają możliwości uzyskania autentycznych dokumentów na podstawie fałszywych dokumentów podstawowych.

Dokumenty takie jak akt urodzenia wydawane są na czas nieokreślony, natomiast poziom ich zabezpieczenia w niektórych krajach jest bardzo niski. Centralne rejestry ludności związane z dokumentami podstawowymi są najczęściej niedostępne dla podmiotów zagranicznych. Ponadto w każdym kraju certyfikaty urodzenia wyglądają inaczej i brak jest informacji na temat wzorów tych dokumentów wydawanych na świecie.

Niemiecka firma Veridos podjęła próbę podniesienia bezpieczeństwa dokumentów podstawowych, wprowadzając do niemieckich aktów urodzenia czytany maszynowo kod 2D zawierający dane personalne naniesione na dokumencie. Kod jest powiązany z systemem Veridos IMAGO, który w razie potrzeby wydania dokumentu podróży czyta kod 2D i transferuje dane bezpośrednio do formularza aplikacyjnego, eliminując w ten sposób możliwość pomyłki. Dane są jednocześnie weryfikowane przez system walidacji dokumentów.

„Infosecura” 2016, nr 68, s. 14.

Połączenie API i OpSec

API Holographics ogłosił rozpoczęcie rozmów na temat sprzedaży holograficznej części firmy (pierwotnie ulokowanej w Salford, UK) grupie OpSec Security. Jest to zgodne z polityką firmy, której głównym celem jest dostarczanie rozwiązań holograficznych typu brand protection i materiałów dekoracyjnych dla przemysłu opakowaniowego.

Dział holograficzny API przejęty przez OpSec rozszerzy możliwości tej firmy pod kątem produkcji folii i laminatów dedykowanych do dokumentów zabezpieczonych.

„Tax Stamp News” 2016, vol. 8, nr 3.

Rosja rozszerza system track & trace

Od stycznia 2016 roku wszyscy hurtownicy i detaliści z branży sprzedaży alkoholu w Rosji rozpoczęli wprowadzanie krajowego elektronicznego systemu monitoringu produktów (EGAIS). System ten został również rozszerzony na produkty browarnicze, co oznacza, że muszą do niego dołączyć także producenci piwa.

Rosyjskie banderole akcyzowe są nośnikami dla danych EGAIS – zawierają kod alfanumeryczny i kod 2D. Detaliści zostaną wyposażeni w specjalne oprogramowanie, które będzie zainstalowane we wszystkich punktach sprzedaży, w celu rejestracji każdego produktu uzyskanego od wytwórców, dystrybutorów i importerów. Zarejestrowane dane będą później porównywane z danymi uzyskanymi od dystrybutorów.

System obliży również sprzedawcę do zeskanowania kodu EGAIS przy sprzedaży każdego produktu alkoholowego konsumentowi (w wyniku skanowania kodu kreskowego produkt jest rozpoznawany jako wyrób alkoholowy i system nie zezwoli na wydrukowanie rachunku, dopóki nie zostanie zweryfikowany kod EGAIS). Jeśli kod nie zostanie potwierdzony lub system znajdzie jakieś niezgodności, sprzedaż danego produktu nie będzie mogła dojść do skutku.

Rosyjskie banderole akcyzowe zawierają liczne elementy zabezpieczające, takie jak:

- włókna zabezpieczające typu Zona, wyglądające jak sznur żółtych koralików świecących w świetle UV na zielono, nawleczonych na czerwony, nieaktywny w UV sznurek,
- termochromowy papier, na którym pod wpływem wyższej temperatury pojawiają się niebieskie kropki,
- pasek holograficzny z demetalizowanymi elementami ornamentowymi,
- optycznie zmienny element Flash,
- element OVI zmieniający kolor od magenty do zielonego,
- nitka zabezpieczająca (element rzadko stosowany w banderolach akcyzowych),
- mikroteksty,
- nacięcia.

„Tax Stamp News” 2016, vol. 8, nr 3, s. 3 i 8.

oprac: Joanna Gurtowska

ŚWIATOWE ŻYCIE EKSPERTÓW – KONFERENCJE, TARGI I WYSTAWY

2016

WRZESIEŃ

26–28 WORLD E-ID AND CYBERSECURITY,
Marseille, France
www.worlde-idandcybersecurity.com

26–29 ACAMS 15TH ANNUAL AML AND FINANCIAL CRIME CONFERENCE,
Las Vegas, USA
www.acams.org

PAŹDZIERNIK

5–8 INTERGRAF 2015
Seville, Spain
www.securityprinters.org

18–20 BIOMETRICS 2016
London, UK
www.biometricsandidentity.com

LISTOPAD

9–11 4TH BORDER MANAGEMENT CONFERENCE,
Bangkok, Thailand
www.apsca.org

13–15 ABA/ABA MONEY LAUNDERING ENFORCEMENT CONFERENCE,
Washington DC, USA
www.aba.com

14–16 11TH SECURITY DOCUMENT SUMMIT,
Beijing, China
www.sds-china.com.cn

29.11–1.12 TRUSTECH INCORPORATING CARTES,
Cannes, France
www.trustech-event.com

GRUDZIEŃ

5–7 HIGH SECURITY PRINTING ASIA
Singapore
www.hsp-asia.com

opracowanie: Jerzy Banaś

Redakcja zastrzega sobie prawo do zmiany tytułów, skracania i adiustacji tekstów. Wydawca nie ponosi odpowiedzialności za fakty i poglądy zawarte w artykułach oraz za treść ogłoszeń i reklam. Materiałów niezaakceptowanych nie publikujemy, nie wynagradzamy i nie odsyłamy.