Nadzór
2 0 1 1

Próba podsumowania

Małgorzata Szumańska
Dorota Głowacka

PANOPTYKON
FUNDACJA

Spis treści

Wprowadzenie

1 2 3 4 5 6 7

Społeczeństwo nadzorowane już funkcjonuje. We wszystkich bogatych państwach świata życie codzienne jest pełne przypadków nadzoru, nie tylko od rana do wieczora, lecz przez całą dobę i 7 dni w tygodniu. Niektóre z tych przypadków zakłócają ustalony porządek dnia, jak kiedy dostajemy mandat za przejechanie na czerwonym świetle, chociaż jedynym świadkiem jest kamera. Jednak większość z nich stanowi obecnie element składowy naszej codzienności, którego nawet nie zauważamy.

Raport o społeczeństwie nadzorowanym, David Murakami Wood (red.), Surveillance Studies Network, 2006 r.

Publiczne i prywatne bazy danych, kamery na ulicach, skanery na lotnikach, karty dostępu w biurze, nagrywane rozmowy, ochrona, biometria, czipy, geolokalizacja, cyfrowe ślady. Niemal każda nasza aktywność jest rejestrowana, a nasze życie coraz ściślej monitorowane. Choć nie wszyscy zdajemy sobie z tego sprawę, żyjemy w społeczeństwie nadzorowanym. Społeczeństwo nadzorowane jest faktem.

Co to dla nas oznacza? Z jednej strony, nadzór daje nam wygodę korzystania z usług dopasowanych do naszego profilu oraz poczucie, że żyjemy w świecie, który można kontrolować; z drugiej – skrywa swoje mroczne oblicze: nadużycia, naruszenia praw człowieka. Dzisiejsze techniki nadzoru są wyzwaniem dla wolności, jaką znamy, i stawiają nas przed pytaniem o jej sens i znaczenie we współczesnym świecie.

Nadzór i inwigilacja kojarzy nam się nieodzownie z Wielkim Bratem – państwem. I słusznie, bo współczesne państwa chcą jak najlepiej zarządzać swoimi obywatelami i jak najściślej kontrolować przybyszów z zewnątrz. Jednak wielkich braci jest znacznie więcej. Dzisiejszy nadzór to nie tylko państwo, ale również organizacje ponadnarodowe, a także prywatne firmy, którym kontrola klientów i pracowników pozwala generować większe zyski.

Współczesnego nadzoru najczęściej nie odbieramy jako czegoś uciążliwego, większość z nas na co dzień nawet go nie zauważa. Powoli, metodą małych kroków, jesteśmy oswajani z kolejnymi sposobami na kontrolowanie naszego życia. Uważamy je za coś naturalnego i neutralnego, za pewną cywilizacyjną konieczność, przed którą nie ma ucieczki.

Dzisiejszy nadzór wykracza poza stosowanie nowych technologii, jednak ściśle się z nimi wiąże. Nie chodzi tylko o możliwości obliczeniowe najnowszych komputerów czy parametry techniczne kamer monitoringu, ale również o to, że nasza komunikacja z innymi, zdobywanie wiedzy, uczestnictwo w kulturze i społeczeństwie odbywa się w coraz większym stopniu za pośrednictwem nowych technologii. Są one źródłem szans, jednak stwarzają również nowe możliwości sprawowania nadzoru nad społeczeństwem. W cyfrowym środowisku pozostawiamy po sobie trwałe ślady, które

mogą stać się narzędziem cyfrowego nadzoru.

Z rozwojem nowych technologii wielu z nas łączy duże nadzieje. W wielu przypadkach jest to uzasadnione, jednak często naiwnie sądzimy, że technologia może stanowić proste panaceum na złożone społeczne problemy. Dotyczy to szczególnie decydentów politycznych, którzy szukają łatwych i spektakularnych rozwiązań, nie zastanawiając się nad społecznymi kosztami ich wdrożenia. Doskonałym przykładem są pomysły na walkę z przestępczością za pomocą np. monitoringu wizyjnego czy blokowania stron internetowych.

Największym sprzymierzeńcem nadzoru jest strach. Od zawsze uważany był za skuteczne narzędzie polityczne, jednak jego znaczenie wzrosło po tragicznych zamachach terrorystycznych z początku naszego wieku. W wielu krajach posłużyły one za pretekst do wprowadzenia daleko posuniętych ograniczeń praw i wolności. Żyjemy w świecie, w którym panuje obsesja zagrożenia, w którym każdy jest potencjalnym podejrzanym. Wierzymy, że trzeba kontrolować wszystkich, że zbieranie jak największej liczby informacji pozwoli nam zapanować nad zagrożeniem – przewidzieć, co się wydarzy, kto i kiedy zaatakuje. Jednak stopień skomplikowania rzeczywistości, w jakiej funkcjonujemy, często wymyka się nawet najbardziej zaawansowanym algorytmom.

Jak nadzór wpływa na nas? Przede wszystkim

> **Na razie odnoszę wrażenie, że jest społeczna aprobata dla używania rozmaitych środków technicznych dla poprawy bezpieczeństwa, kosztem prywatności. Ja jednak uważam, że rezygnacja z prywatności na rzecz bezpieczeństwa poszła za daleko.**
>
> **Irena Lipowicz w wywiadzie *Lipowicz: Rezygnacja z prywatności na rzecz bezpieczeństwa poszła za daleko*, „Gazeta Wyborcza", 15 października 2010 r.**

sprzyja podejrzliwości. Jego obecność jest sygnałem, że innym nie do końca można ufać. Tymczasem relacje społeczne opierają się na zaufaniu, a jego podkopywanie może być szczególnie niebezpieczne w takim kraju jak Polska, gdzie od lat narzekamy na jego deficyt.

Konsekwencją rozwoju społeczeństwa nadzorowanego jest ograniczenie prywatności jednostek, ich autonomii informacyjnej i tajemnicy korespondencji. Ale to nie wszystko. Nadzór może również wiązać się z ograniczeniami wolności słowa czy prawa do informacji, a przez to prowadzić do pogłębiania się przepaści informacyjnej: państwo i korporacje wiedzą o nas coraz więcej, my o nich – coraz mniej.

We współczesny nadzór wpisane jest również zagrożenie dyskryminacją i wykluczeniem. Jego podstawą jest zbieranie informacji o ludziach i dzielenie ich na kategorie, które są następnie podstawą zróżnicowanego traktowania. Niejednokrotnie jesteśmy przedmiotem profilowania w trakcie robienia zakupów czy przeglądania stron internetowych. Ale konsekwencje działania takich mechanizmów mogą być dużo poważniejsze. Ludzie, którzy z jakiegoś powodu zostali zakwalifikowani do grupy ryzyka (np. ze względu na pochodzenie etniczne czy religię), stają się ofiarami wykluczenia i dyskryminacji.

Nadzór ma zazwyczaj służyć naszemu bezpieczeństwu, zwiększeniu efektywności działania (np. państwa lub firmy) czy oszczędnościom finansowym. Jednak przeciwstawianie tak formułowanych, pragmatycznych celów szeroko pojętej wolności czy prywatności jest niebezpiecznym uproszczeniem. Alternatywa „albo wolność, albo bezpieczeństwo" jest z gruntu fałszywa. Nierzadko zwiększenie nadzoru rzeczywiście służy bezpieczeństwu publicznemu, ale równie często argument „dla naszego bezpieczeństwa" stanowi jedynie zasłonę dymną, która skrywa zupełnie inne cele: polityczne bądź finansowe. W niektórych przypadkach duże zaufanie do technologii nadzoru może też prowadzić do odwrócenia uwagi od alternatywnych, skuteczniejszych metod zapewniania bezpieczeństwa.

Debatując na temat współczesnego nadzoru, często jesteśmy konfrontowani z przeświadczeniem, że cały problem sprowadza się do ochrony naszej własnej prywatności; że wystarczy kontrolowanie tego, co publikujemy w Internecie, oraz jakie informacje udostępniamy firmom polującym na nasze dane, aby ten problem rozwiązać. Oczywiście świadomość tego, gdzie kryją się zagrożenia, i wiedza, jak ich unikać, są niezwykle ważne. Jednak sami możemy się ochronić tylko w ograniczonym zakresie. Przepaść między potencjałem informacyjnym państwa i technologicznym zapleczem wielkich korporacji a tym, jaki poziom świadomości i pole manewru ma pojedynczy człowiek, jest przytłaczająca. Dlatego tak duże znaczenie ma zapewnienie maksymalnej transparentności działania instytucji nadzorujących, monitorowanie ich praktyk i rozliczanie z nadużyć.

W SIECI DANYCH

Współczesny nadzór realizuje się przede wszystkim poprzez zbieranie i integrowanie informacji o poszczególnych jednostkach. W krajach zachodnich problem tworzenia i wykorzystywania zbiorów danych stał się przedmiotem zainteresowania prawników i ustawodawców w latach 70. Miało to związek z postępem technologicznym, jaki dokonał się w drugiej połowie XX w. Rozmaite rejestry funkcjonowały wprawdzie już dużo wcześniej, jednak konieczność manualnego przetwarzania zawartych w nich danych stanowiła naturalne ograniczenie możliwości ich wykorzystania. Refleksja nad zagrożeniami związanymi z automatyzacją i komputeryzacją tych procesów doprowadziła do zauważania potrzeby ochrony danych osobowych.

Polska Konstytucja stoi na straży nie tylko prawa do prywatności (art. 47), ale również wywodzonego z niego prawa do autonomii informacyjnej jednostki, czyli prawa do ochrony swoich danych osobowych (art. 51). Na poziomie europejskim wartości te chronić ma przede wszystkim Dyrektywa o ochronie danych (95/46/WE) oraz Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Wdrożeniem unijnej dyrektywy jest polska ustawa o ochronie danych osobowych.

Coraz częściej mówi się o tym, że obowiązujące regulacje nie przystają do naszej cyfrowej rzeczywistości. Upowszechnienie się Internetu stwarza nowe wyzwania na ochrony prawa do prywatności. Informacje dotyczące naszego życia są coraz powszechniej dostępne, a technologia pozwala nie tylko na coraz sprawniejsze ich gromadzenie, ale również na ich wymianę, koncentrację i kojarzenie na niespotykaną do tej pory skalę.

W odpowiedzi na te wyzwania Komisja Europejska zainicjowała w listopadzie 2010 r. proces reformy prywatności, wydając komunikat *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, który zawierał ogólną koncepcję nowelizacji dyrektywy o ochronie danych osobowych oraz główne obszary, jakie powinny zostać uwzględnione przy opracowywaniu nowych przepisów. Celem reformy jest dostosowanie obecnych regulacji do nowych wyzwań dla ochrony prywatności związanych z rozwojem nowoczesnych technologii.

Niezależnie od oczekiwania na zreformowanie prawa Unii Europejskiej w Polsce również rozpoczęto prace nad przygotowaniem nowej ustawy o ochronie danych osobowych. Elementem tego procesu są tematyczne konferencje, które mają służyć wypracowaniu postulatów reform, a następnie zainicjować zmiany legislacyjne w prawie krajowym. Proces polski ma uprzedzać i uzupełniać proces unijny.

Art. 47 Konstytucji
Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Art. 51 Konstytucji
1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

W krajach zachodnich problemy związane z rozwojem społeczeństwa nadzorowanego zostały już dostrzeżone, są przedmiotem badań i analiz (*surveillance studies*) oraz obywatelskiego monitoringu. W Polce wciąż brakuje systematycznego zainteresowania tematem, a nawet języka do opisu nowych zjawisk. Debata publiczna dopiero się rodzi. Media coraz częściej informują o przypadkach nadużyć, jednak nie są w stanie pokazać ich w kontekście szerszych procesów. Skutkiem braku wiedzy i świadomości problemu w społeczeństwie jest deficyt demokratycznej kontroli nad praktykami nadzoru.

Fundacja Panoptykon powstała po to, by diagnozować wyzwania i zagrożenia związane z rozwojem społeczeństwa nadzorowanego, by inicjować i animować społeczną kontrolę nadzorujących i praktyk nadzoru. Punktem odniesienia dla naszej oceny obserwowanych działań są podstawowe prawa i wolności. Zależy nam na tym, by takie cele, jak zapewnianie bezpieczeństwa publicznego czy usprawnienia w zarządzaniu, były realizowane z poszanowaniem prywatności, wolności słowa i prawa do informacji oraz nie prowadziły do wykluczenia ani dyskryminacji jakichkolwiek jednostek czy grup społecznych.

Jesteśmy przekonani, że szczególne znaczenie ma w tym kontekście kształt stanowionego i obowiązującego prawa. Z jednej strony, drogą zmian prawa wprowadza się nowe formy nadzoru państwa nad obywatelami. Z drugiej jednak – prawo może służyć obronie obywateli zarówno przed działaniami państwa, jak i podmiotów prywatnych, może stanowić również narzędzie kontroli ich działań. Nie rozwiąże ono każdego problemu i nie ochroni przed wszystkimi zagrożeniami, ale jego rola jest mimo wszystko nie do przecenienia.

Świadomość znaczenia prawa dla funkcjonowania społeczeństwa nadzorowanego skłoniła nas do realizacji rocznego projektu (październik 2010 r. – październik 2011 r.), którego celem jest monitoring kluczowych zmian prawa oraz wydarzeń politycznych, które przekładają się na realia funkcjonowania współczesnego nadzoru w Polsce. W ramach projektu wyróżniliśmy kilka kluczowych tematów: monitoring wizyjny, nadzór w sferze telekomunikacji i uprawnienia służb oraz integracja publicznych baz danych – na których koncentrowaliśmy naszą uwagę i działania.

Z pewnością nie udało nam się namierzyć i skomentować wszystkich istotnych zmian prawa i znaczących wydarzeń, jednak projekt ten pokazał nam, jak wiele dzieje się na styku prawa i nadzoru, oraz utwierdził nas w przekonaniu, że zmiany w tym obszarze trzeba systematycznie monitorować. Lista projektów legislacyjnych, które przywoływaliśmy na naszej stronie internetowej, liczy kilkadziesiąt pozycji. Wokół tych z nich, które uznaliśmy za najważniejsze, staraliśmy się ogniskować dalsze działania, m.in. współpracę z mediami oraz oficjalne interwencje.

Raport stanowi podsumowanie tego rocznego projektu. Nie zawiera jednak przeglądu wszystkich tematów, którymi zajmowaliśmy się w jego ramach. Skupiamy się w nim przede wszystkim na tych z nich, które – w naszej ocenie – najlepiej ukazują napięcia i wyzwania związane ze współczesnym nadzorem. Staramy się wskazać kluczowe problemy i zagrożenia oraz zarysować najważniejsze wchodzące w grę wartości. Natomiast w końcowej tabeli prezentujemy rozszerzoną listę najważniejszych problemów, którymi zajmowaliśmy się w ramach projektu, oraz związanych z nimi aktów prawnych.

> **To nieprawda, że stoimy przed wyborem: albo prywatność, albo bezpieczeństwo. Po pierwsze, podstawowe ludzkie prawa, takie jak prawo do prywatności, są ważne i powinny być przestrzegane niezależnie od okoliczności. Po drugie, nie ma też żadnych dowodów na to, że większy nadzór nad prywatnym życiem ludzi naprawdę zwiększa możliwości łapania terrorystów. Przez blisko dziesięć lat, które upłynęły od zamachów na World Trade Center, było wiele okazji, żeby się o tym przekonać.**
>
> David Lyon w wywiadzie *Statystycznie podobny do Breivika*, „Gazeta Wyborcza", 1 sierpnia 2011 r.

Monitoring wizyjny

1 2 3 4 5 6 7

Obywatele nie mogą mieć pewności, że monitoring wykorzystywany jest w sposób celowy i adekwatny, nie wiedzą zazwyczaj, w jaki sposób przetwarzane są dane pozyskiwane za jego pomocą (jak są zabezpieczone, jak długo przechowywane, kto ma do nich dostęp, do jakich celów mogą być wykorzystane), zazwyczaj nie są nawet informowani o tym, że znajdują się w przestrzeni, która podlega monitoringowi.

Fragment stanowiska Fundacji Panoptykon w konsultacjach *Całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej*, 15 stycznia 2011 r.

Dynamiczny rozwój monitoringu wizyjnego budzi spory niepokój. Z jednej strony, chodzi o jego wątpliwą skuteczność w zapewnianiu bezpieczeństwa, z drugiej – o do tej pory niezbadane skutki społeczne i brak debaty publicznej na ten temat. W Polsce bardzo potrzebne jest wprowadzenie regulacji prawnej, która ucywilizuje funkcjonowanie monitoringu oraz zapewni szerszy dostęp do informacji na temat praw i obowiązków z nim związanych.

Kamery monitoringu stają się naturalnym elementem naszego otoczenia – uważne oko może je wypatrzeć właściwie na każdym kroku: na osiedlach, ulicach i placach, w sklepach, restauracjach, centrach handlowych, budynkach użyteczności publicznej, biurach, bankach, hotelach, kantorach, na stacjach benzynowych, lotniskach, w środkach komunikacji publicznej, szpitalach, żłobkach, przedszkolach i szkołach.

Z monitoringu korzystają instytucje publiczne w celu wykonywania swoich zadań związanych z utrzymaniem porządku i bezpieczeństwa, ale także np. ochrony mienia czy kontroli pracowników. Oprócz tego kamery wykorzystywane są przez podmioty prywatne i w tym przypadku wachlarz zastosowań jest jeszcze szerszy: od ochrony przed kradzieżami po śledzenie zachowań klientów.

Choć monitoring upowszechnia się na całym świecie, stosunek do niego jest różny w poszczególnych krajach. „Ojczyzną CCTV" jest Wielka Brytania, jest ona również krajem, w którym nasycenie kamerami w stosunku do liczby mieszkańców jest prawdopodobnie najwyższe na świecie. W wielu europejskich państwach monitoring nie jest jednak tak rozpowszechniony, a jego wykorzystanie, np. w przestrzeni publicznej, budzi znacznie większe kontrowersje. Polsce wciąż daleko do „standardów" brytyjskich, jednak i u nas kamery wykorzystywane do nadzoru cieszą się coraz większą popularnością.

Systemy kamer wykorzystywanych do monitorowania zdarzeń i zachowań ludzi nazywa się w rozmaithy sposób: monitoring wizyjny, kamery przemysłowe, wideonadzór czy nadzór wideo, a także CCTV (skrót od angielskiego *closed circuit television*).

Monitoring jest najbardziej rozpowszechniony w dużych miastach, ale również mniejsze miejscowości starają się dotrzymać im kroku. Kamery na ulicach traktowane są jako wyraz nowoczesności i dbałości o bezpieczeństwo, dlatego władze miast chwalą się zakupem kolejnych urządzeń i z dumą umieszczają na rogatkach hasło „miasto monitorowane"; nawet jeśli miejski monitoring obejmuje raptem kilka kamer.

Europejczycy o monitoringu

Badanie zrealizowane kilka lat temu w pięciu europejskich stolicach pokazały, że największym poparciem monitoring wizyjny cieszy się w Londynie (ponad 94%), a najmniejszym w Berlinie (56%) (Leon Hempel, Eric Töpfer, *Urbaneye: CCTV in Europe. Final Report*, 2004 r.).

W polskich badaniach za zwiększeniem liczby kamer w przestrzeni publicznej opowiedziało się ponad 61% ankietowanych. Zdaniem prawie 15% należy dążyć do utrzymania bądź ograniczenia ich liczby (N=1003) (wyniki badań zrealizowanych w latach 2010-2011 przez Julię Skórzyńską-Ślusarek, Fundację Panoptykon i Fundację Projekt: Polska, we współpracy z Millward Brown SMG/KRC; raport w przygotowaniu).

Rzeczywista skala wykorzystania monitoringu w Polsce jest zagadką, nikt bowiem nie prowadził odpowiednich badań ani statystyk. Wiadomo jednak, że palmę pierwszeństwa, jeśli chodzi o nasycenie kamerami, dzierży stolica. Z budżetu Warszawy na 2011 r. wynika, że w ramach miejskiego systemu monitoringu działa 407 kamer. To zestawienie nie uwzględnia jednak wszystkich kamer instalowanych przez instytucje publiczne, których – jak się szacuje – może być nawet kilka razy więcej. Aby jednak wyobrazić sobie skalę wykorzystania monitoringu w stolicy, trzeba w tych rachunkach uwzględnić liczbę prawdopodobnie tysięcy kamer montowanych przez podmioty prywatne.

Do dynamicznego rozwoju monitoringu wizyjnego w Polsce nie przystaje poziom obowiązujących regulacji prawnych, które mają charakter bardzo fragmentaryczny. Uregulowane są – i to zazwyczaj na dużym poziomie ogólności – jedynie niektóre przypadki wykorzystania tego narzędzia. Ustawa o bezpieczeństwie imprez masowych określa, jakie warunki powinien spełniać monitoring np. na stadionach; ustawy o Policji oraz o strażach gminnych określają uprawnienia tych służb. Oprócz tego obowiązuje kilka aktów regulujących wykorzystanie monitoringu w ściśle określonych warunkach, jednak większość przypadków jego wykorzystania – szczególnie przez podmioty prywatne – zupełnie wymyka się regulacjom prawnym.

W celi, na stadionie, w kasynie

W ciągu ostatnich 12 miesięcy zmieniano bądź wprowadzano co najmniej kilka aktów prawnych regulujących funkcjonowanie monitoringu. Wszystkie zmiany odnosiły się jednak do bardzo konkretnych i specyficznych jego zastosowań.

Przyjęte zmiany dotyczyły:

1) zasad instalacji kamer w celach osadzonych uznanych za „szczególnie narażonych";
2) zasad wykorzystywania monitoringu w placówkach dla nieletnich;
3) wykorzystywania kamer w szpitalach psychiatrycznych;
4) wymogów dla monitoringu wykorzystywanego w trakcie imprez masowych;
5) wprowadzenia monitoringu wizyjnego m.in. w pomieszczeniach przeznaczonych dla osób zatrzymanych, policyjnych izbach dziecka, pokojach przejściowych;
6) monitoringu w kasynach.

Nad przygotowaniem projektu aktu prawnego regulującego w sposób kompleksowy warunki korzystania z monitoringu od dłuższego już czasu ma pracować Ministerstwo Spraw Wewnętrznych i Administracji. Konkretnych efektów jednak na razie nie widać. Na problemy wynikające z takiego stanu rzeczy uwagę zwracali uwagę kilkakrotnie m.in. Rzecznik Praw Obywatelskich i Generalny Inspektor Ochrony Danych Osobowych. Do ostatniego wystąpienia GIODO w tej sprawie do MSWiA dołączono Wymagania w zakresie regulacji monitoringu, w których wskazano najważniejsze wymogi, jakie powinna spełniać projektowana ustawa oraz główne kierunki, w których powinna zmierzać.

Poszczególne kraje bardzo różnią się od siebie w zakresie prawnego uregulowania działania monitoringu wizyjnego. Niektóre ściśle określają ramy prawne dla prywatnych systemów monitoringu, w innych prawne ograniczenia obejmują jedynie

> **Monitoring wizyjny i audiowizualny stosowany jako środek wspomagający utrzymanie bezpieczeństwa i porządku w miejscach zarówno otwartych, jak i zamkniętych publicznie, budzi coraz więcej kontrowersji. Powstają one nie tylko na gruncie wątpliwości co do samego faktu jego stosowania, ale coraz większych dysproporcji między celem, któremu ma służyć, i ograniczeniem prawa do prywatności, jakie wprowadza jego stosowanie. Należy zwrócić uwagę również, że dysproporcje te narastają wraz ze stosowaniem coraz to nowszych rozwiązań technologicznych.**

Fragment wystąpienia GIODO do MSWiA sygnalizującego potrzebę przyjęcia kompleksowej regulacji działania monitoringu wizyjnego, 24 sierpnia 2011 r.

funkcjonowanie tych publicznych. Tylko nieliczne państwa (np. Belgia, Dania, Francja, Hiszpania) zdecydowały się na kompleksowe uregulowanie działania monitoringu w odrębnym akcie prawnym. Częstszym przypadkiem jest rozproszenie przepisów w różnych dokumentach. Najczęściej podstawowymi aktami, które znajdują zastosowanie w takim przypadku, są ustawy dotyczące ochrony danych osobowych.

W CZYM PROBLEM?

1 Ponieważ brakuje w Polsce aktu, który w sposób kompleksowy regulowałby działanie monitoringu wizyjnego, brakuje również jasnych reguł jego wykorzystywania. Chociaż wszystkich obowiązują ogólne zasady ochrony prywatności i dóbr osobistych innych osób, brak szczegółowych uregulowań w tej sferze sprawia, że z monitoringu korzysta, kto chce i jak chce.

Nie mamy – jako osoby nadzorowane – właściwie żadnej kontroli nad tym, gdzie są instalowane kamery i jaką przestrzeń obejmują swym zasięgiem, w jakim celu są wykorzystywane, gdzie i jak długo przechowywane są nagrania, kto nimi administruje oraz kto i na jakich zasadach może mieć do nich dostęp.

2 Monitoring wizyjny przedstawiany jest jako narzędzie nowoczesne i bardzo skuteczne, jeśli chodzi o realizację głównego celu, jakim jest poprawa bezpieczeństwa. Tymczasem wyniki badań realizowanych w krajach zachodnich każą zachować daleko idący sceptycyzm. Badania te albo nie przynoszą jednoznacznych wyników, albo prowadzą do wniosku, że obecność kamer w nie wpływa na poziom przestępczości.

W Polsce praktycznie nie bada się ani wpływu monitoringu wizyjnego na życie społeczne, ani jego

Skuteczność monitoringu wizyjnego w walce z przestępczością nie budzi żadnych wątpliwości. Według danych z Komendy Stołecznej Policji, w miejscach objętych monitoringiem, po zainstalowaniu kamer przestępczość spadła o 50-60%.

Informacja umieszczona na stronie Zakładu Obsługi Systemu Monitoringu w Warszawie.

skuteczności w zakresie zwiększania bezpieczeństwa. Do wyjątków należy badanie Pawła Waszkiewicza z Uniwersytetu Warszawskiego zrealizowane na warszawskiej Woli. Podobnie jak w badaniach zachodnich nie udało się wykazać wpływu kamer na bezpieczeństwo. Okazało się, że przestępczość spadła zarówno na obszarach objętych monitoringiem, jak i – i to większym stopniu – na obszarach bez kamer. Wyniki te sugerują, że kluczowy wpływ na poziom bezpieczeństwa mają zupełnie inne czynniki.

Wyniki badań

W ramach szeroko zakrojonych badań porównawczych realizowanych przez Davida Farringtona i Brandona Welscha nie udało się wykazać zasadniczego wpływu monitoringu wizyjnego na poziom przestępczości. Jego statystycznie istotny spadek badacze odnotowali jedynie na parkingach samochodowych, podczas gdy na innych badanych obszarach, obejmujących centra miast, bloki komunalne i transport publiczny, nie udało im się wykazać takiego związku (Brandon C. Welsh, David P. Farrington, *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research Study 252, 2002 r.).

Wdrażanie rozwiązań mogących naruszać prawa obywatelskie i związanych z poważnymi kosztami dla budżetu publicznego (…) powinno być poprzedzone i oparte na rzetelnych badaniach. Podawanie „danych" o spadku liczby przestępstw nawet o 90% budzi niedowierzanie każdej osoby zajmującej się zjawiskiem przestępczości. Koszt badań czterech obszarów na warszawskiej Woli zamknął się w kwocie mniejszej niż utrzymanie jednej kamery przez pięć miesięcy.

Paweł Waszkiewicz, *Wielki Brat. Rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne*, Warszawa 2011, s. 203.

3 W Polsce bardzo brakuje poważnej debaty publicznej dotyczącej kierunków rozwoju monitoringu wizyjnego, brakuje dyskusji nad zaletami i wadami tego narzędzia. Koresponduje to z brakiem wiedzy społeczeństwa na temat funkcjonowania monitoringu. Większość z nas nie ma możliwości przekonania się, jak działa on w praktyce, dlatego też większość wyobrażeń na jego temat czerpiemy z mediów. Te jednak są często zupełnie bezkrytyczne wobec tego narzędzia i rzadko mogą być źródłem rzetelnej wiedzy. Oczywiście, pojawiają się w nich również informacje o nadużyciach związanych z monitoringiem, ale są to raczej wyjątki, w dodatku ukazane najczęściej w charakterze bulwersujących ciekawostek, a nie jako przejaw szerszego problemu, z którym powinniśmy się zmierzyć.

Media same bardzo chętnie korzystają z nagrań z monitoringu, ponieważ stanowi to bardzo łatwy sposób uatrakcyjnienia przekazu. Duży wpływ na kształtowanie się wyobrażeń o działaniu monito-

Nie ma „cudownych środków" walki z przestępczością. Na tle innych metod prewencji kryminalnej systemy CCTV wypadają przeciętnie, tzn. ich skuteczność opiera się na wierze, że właściwie działają. Liczba ok. 10 tysięcy interwencji rocznie podejmowanych przez policję i straż miejską na podstawie informacji pochodzących od operatorów warszawskiego systemu CCTV przestaje robić tak duże wrażenie, jeżeli uwzględnić, że pochodzą od 200 operatorów. Oznacza to dostrzeżenie mniej niż jednego wykroczenia lub przestępstwa przez 40 godzin pracy.

Paweł Waszkiewicz, *Wielki Brat Rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne*, Warszawa 2011, s. 204.

ringu mają z pewnością różnego rodzaju programy kryminalne (wykorzystujące prawdziwe nagrania bądź przedstawiające fikcyjne historie), które przekonują o niezwykłej przydatności i skuteczności tego narzędzia. Rzadziej natomiast można w nich zobaczyć prozę życia: tysiące zarejestrowanych danych, których nie ma kto analizować, setki nagrań, które nie umożliwiają identyfikacji, dziesiątki pomyłek.

4 Zakup pojedynczej kamery niższej jakości nie stanowi dużego wydatku. Jeśli jednak przemnożymy jej cenę przez liczbę wykorzystywanych kamer, dodamy do tego koszt innego niezbędnego sprzętu oraz koszty związane z obsługą i eksploatacją monitoringu, okaże się, że wydajemy na niego ogromne pieniądze. Ile dokładnie? Niestety, nie wiadomo. Pewne jest tylko to, że koszty te ponosimy my wszyscy. I to nie tylko płacąc podatki, są one ukryte również w cenach towarów i usług.

W przypadku kamer montowanych za pieniądze publiczne szczególne znaczenie ma transparentność ponoszonych wydatków. Niestety, pozostawia ona obecnie sporo do życzenia, zwłaszcza w kontekście ryzyk generowanych na styku polityki i biznesu. Sektorowi bezpieczeństwa zależy przede wszystkim na generowaniu popytu na kamery i inne tego typu produkty, decydentom – na zdobyciu punktów u swoich wyborców. W związku z tym brakuje momentu weryfikacji, czy pieniądze są wydawane rzeczywiście sensownie i zgodnie ze społecznym interesem.

Ile kosztuje monitoring?

Roczne utrzymanie jednej kamery w Warszawie kosztuje ponad 34 tys. zł. Na rozbudowę monitoringu w 2011 r. przewidziano 2,5 mln zł, na jego modernizację – 450 tys. zł, a na utrzymanie Zakładu Obsługi Systemu Monitoringu – prawie 13,9 mln zł. To jednak tylko część kosztów utrzymania publicznych kamer w stolicy, które rozproszone są w różnych miejscach Budżetu Miasta Stołecznego Warszawy na 2011 rok.

GIODO O MONITORINGU

Zgodnie z rekomendacjami GIODO sformułowanymi w *Wymaganiach w zakresie regulacji monitoringu* **prawo powinno określić:**

1) warunki i okoliczności, w jakich monitoring może być wykorzystywany;
2) miejsca, w których monitoring co do zasady nie może być stosowany;
3) wymogi techniczne i organizacyjne, jakie musi spełniać każdy, kto chce korzystać z tego narzędzia;
4) sposób oznaczenia przestrzeni objętej monitoringiem;
5) organy odpowiedzialne za kontrolę legalności monitoringu oraz wydawanie zezwoleń na jego zastosowanie;
6) prawa i obowiązki podmiotu prowadzącego monitoring;
7) prawa osób nim objętych;
8) zasady dotyczące przechowywania i wykorzystywania zebranych danych.

Przede wszystkim należy poinformować osoby, które mogą znaleźć się w zasięgu monitoringu, że jest on stosowany, jaki jest jego cel i kto nim zarządza. Każdy, kto zamierza z tego narzędzia korzystać, powinien wykazać zasadność jego stosowania, w tym proporcjonalność do celu, jakiemu ma służyć. Wprowadzenie monitoringu powinna poprzedzać analiza, czy można zastosować inne, mniej ingerujące w prywatność, środki.

Należy wskazać te przypadki i okoliczności, które powinny stanowić bezwzględne granice dla stosowania monitoringu. Obszary objęte szczególną ochroną prywatności – takie jak biura, stołówki, kafejki, bary, poczekalnie, toalety, prysznice i szatnie – nie powinny być monitorowane. W przypadku, gdy ktoś zamierza objąć monitoringiem tego typu miejsca, powinien wcześniej przeprowadzić ocenę jego wpływu na ochronę danych i prywatności oraz zgłosić projekt wprowadzenia takiego systemu do kontroli.

Ze względu na swój inwazyjny charakter nagrywanie dźwięku nie powinno być co do zasady dozwolone, a wykorzystywanie „inteligentnych narzędzi monitoringu" powinno być dopuszczalne jedynie po przeprowadzeniu oceny wpływu ich zastosowania na ochronę prywatności oraz po przeprowadzeniu kontroli wstępnej.

Dla każdego systemu monitoringu powinien być określony okres przechowywania danych, po którym muszą być one usuwane. GIODO rekomenduje okres nie dłuższy niż 7 do 30 dni.

Wartości do zważenia

BEZPIECZEŃSTWO

Monitoring wizyjny jest wielofunkcyjną technologią, którą wykorzystuje się w różnych celach. Jednak przede wszystkim ma on służyć zapewnianiu bezpieczeństwa. Z pewnością w niektórych sytuacjach kamery mogą sprzyjać realizacji tego celu. Są przydatne np. w takich miejscach, jak banki. Jednak badania wskazują, że stosowanie monitoringu na masową skalę mija się z celem. Czasem – wtedy, kiedy spychają na dalszy plan bardziej skuteczne metody albo zniechęcają ludzi do reagowania w przypadku niebezpiecznych sytuacji – kamery mogą wręcz obniżać poziom naszego bezpieczeństwa,

FINANSE PUBLICZNE

Instalacja, obsługa i utrzymanie kamer niosą za sobą realne koszty dla finansów publicznych. To rodzi pytania o zasadność oraz transparentność ponoszonych wydatków.

PRYWATNOŚĆ

Masowe wykorzystanie kamer monitoringu prowadzi do naruszeń prawa do prywatności. Problemem są zarówno możliwe wycieki czy nadużycia, jak i wkraczanie tego narzędzia nadzoru w kolejne sfery naszego życia. Ograniczenia prywatności są oczywiście w demokratycznym społeczeństwie możliwe, można mieć jednak poważne wątpliwości, czy w tym przypadku oficjalnie deklarowane cele są rzeczywiście realizowane.

SWOBODA DZIAŁALNOŚCI GOSPODARCZEJ

Jest ona wartością chronioną na poziomie Konstytucji. Przedsiębiorcy wykorzystują kamery do różnych celów, służą one zarówno ochronie mienia, jak i zarządzaniu. Niekiedy bywają przydatne, ale jednocześnie stwarzają liczne zagrożenia dla prywatności, co stawia pod znakiem zapytania celowość i proporcjonalność ich wykorzystywania na masową skalę.

JAKIE TO RODZI ZAGROŻENIA?

1 Coraz większe rozpowszechnienie kamer monitoringu może prowadzić do naruszeń prywatności. Podglądactwo i różnego rodzaju nadużycia są niemal wpisane w sposób działania tego narzędzia. Zdarza się, że kamery montowane są w miejscach intymnych, takich jak toalety czy przebieralnie, czasem nawet bez naszej wiedzy.

Polacy o monitoringu

Ze zdaniem: „Myślę, że jedną z zalet zastosowania monitoringu jest to, że nie trzeba się samemu o pewne rzeczy martwić. Jeżeli np. widzę, że ma miejsce jakaś kradzież albo bójka, to wiem, że nie muszę interweniować, bo ludzie, którzy dyżurują przy kamerach, się tym zajmą" zgodziło się prawie 44% ankietowanych. Przeciwne stanowisko reprezentowało niecałe 34% osób (N=1003) (wyniki badań zrealizowanych w latach 2010-2011 przez Julię Skórzyńską-Ślusarek, Fundację Panoptykon i Fundację Projekt: Polska, we współpracy z Millward Brown SMG/KRC; raport w przygotowaniu).

Zdarza się również, że nagrania są przekazywane mediom albo wyciekają do Internetu.

Konkretne przypadki nadużyć, często bardzo medialne, nie wyczerpują jednak problemu. Naruszenie prywatności może stanowić już sama obecność kamer w przestrzeni publicznej. Szczególnie, jeśli przybiera ona taki rozmiar, że poruszając się po mieście, musimy liczyć się z zarejestrowaniem prawie każdego kroku przez kamery. Niedługo wolni od ich spojrzenia będziemy jedynie we własnym domu, oczywiście pod warunkiem, że żadna z nich nie zajrzy wścibsko do naszego okna. A takie przypadki nie są niczym wyjątkowym.

2 Montaż i korzystanie z monitoringu są niezwykle proste, co z pewnością wpływa na jego popularność. Wykorzystanie tego narzędzia na szeroką skalę może jednak prowadzić do odwrócenia uwagi od innych, często dużo skuteczniejszych rozwiązań. Warto pamiętać również o tym, że przeznaczenie środków na monitoring oznacza zazwyczaj ograniczenie wydatków na inne cele. Skutki takiej polityki mogą być zupełnie odwrotne do zamierzonych. Dobrze ilustruje to przypadek brytyjski, gdzie w związku ze wzrostem finansowania monitoringu ograniczono wydatki na inne formy prewencji kryminalnej. Obecnie ta polityka spotyka się z coraz większą krytyką.

3 Dynamiczny rozwój monitoringu stawia nas przed pytaniami o jego dalekosiężne społeczne skutki. Do ciekawych wniosków

prowadzą badania współrealizowane przez Fundację Panoptykon. Okazuje się, że popularność monitoringu wiąże się z przekonaniem, że dzięki niemu jesteśmy zwolnieni z odpowiedzialności za to, co dzieje się wokół. Może to potwierdzać tezę, że obecność kamer prowadzi do rozproszenia czy przeniesienia odpowiedzialności, czego skutkiem może być spadek poziomu bezpieczeństwa. Innym potencjalnym zagrożeniem, które należy brać pod uwagę, jest obniżenie poziomu wzajemnego zaufania. Kamery stanowią bowiem sygnał, że wokół czai się zagrożenie, a innym nie można już ufać.

Nie jest jeszcze zbadany wpływ ciągłej obecności kamer na rozwój i postawy życiowe dzieci i młodzieży. Wychowywanie się z poczuciem ciągłej zewnętrznej kontroli może prowadzić do utrwalenia mechanizmów ulegania za cenę niższego poziomu internalizacji pożądanych społecznie wartości i osłabienia wewnętrznych mechanizmów kontroli. Niestety, w Polsce masowo instaluje się kamery w szkołach, a nawet przedszkolach i żłobkach, bez refleksji i badania ewentualnych skutków ubocznych.

ETPCz o kamerach

Kwestię stosowania monitoringu wizyjnego kilkakrotnie badał Europejski Trybunał Praw Człowieka. Jednym z kluczowych orzeczeń ETPCz wyznaczającym standardy w tym zakresie jest wyrok w sprawie Peck przeciwko Zjednoczonemu Królestwu (28 stycznia 2003 r., skarga nr 44647/98). Sprawa dotyczyła zarejestrowania przez kamery monitoringu próby samobójczej jednego z mieszkańców. Fragmenty nagrania przedostały się do brytyjskich mediów, a Peck – mimo prób zamazania wizerunku – został przez wiele osób rozpoznany. Ponieważ w chwili, gdy znajdował się w zasięgu kamer, nie brał udziału w żadnym publicznym wydarzeniu, a nagrania z jego udziałem zostały udostępnione przez służby policyjne środkom masowego przekazu, Trybunał orzekł naruszenie art. 8 Europejskiej Konwencji Praw Człowieka, czyli prawa do prywatności. Istotą naruszenia była nie tyle sama obecność telewizji przemysłowej w miejscu publicznym, ile niewłaściwy sposób przechowywania i zabezpieczenia nagrań.

UCZEŃ W OKU KAMERY

Jednym z pomysłów Ministerstwa Edukacji Narodowej na poprawę bezpieczeństwa i dyscypliny w szkołach było upowszechnienie monitoringu wizyjnego. W związku z tym w 2007 r. uruchomiono specjalny program *Monitoring wizyjny w szkołach i placówkach*, którego podstawą było rozporządzenie wydane przez Radę Ministrów 6 września 2007 r. W ramach programu szkoły mogły ubiegać się o dofinansowanie montażu kamer na terenie szkoły i wokół niej.

Decyzji o finansowaniu szkolnych kamer z budżetu państwa nie poparto żadnymi twardymi danymi. Jak czytamy w programie: „Monitoring wizyjny staje się standardowym wyposażeniem instytucji, obiektów i miejsc, w których stale lub czasowo przebywa znaczna liczba osób. Szkoły i placówki oświatowe nie powinny odbiegać od współczesnych standardów, szczególnie w sferze zapewnienia uczniom i wychowankom bezpiecznych warunków nauki, wychowania i opieki".

Program wywołał kontrowersje, przede wszystkim dlatego, że w rozporządzeniu przewidziano dofinansowanie nie tylko kamer, ale również sprzętu rejestrującego dźwięk. Po protestach m.in. ze strony RPO i GIODO w 2008 r. zlikwidowano taką możliwość.

To jednak nie rozwiązało wszystkich problemów. Nie określono bowiem zasad funkcjonowania szkolnego monitoringu, nie wiadomo więc na przykład, gdzie i w jaki sposób mają być instalowane kamery, kto może mieć dostęp do nagrań, jak długo mogą być one przechowywane (w rozporządzeniu przewidziano jedynie minimalny okres przechowywania – 30 dni).

RPO w swoim wystąpieniu z 15 lutego 2010 r. zwrócił również uwagę, że brakuje podstawy ustawowej dla montowania kamer w szkołach, podczas gdy organy władzy publicznej powinny działać tylko na podstawie i w granicach prawa, a ograniczenia praw i wolności (w tym przypadku prawa do prywatności) powinno mieć podstawę ustawową.

W związku z tą krytyką w sprawozdaniu z realizacji programu zawarto rekomendację dotyczącą podjęcia działań zmierzających do nowelizacji ustawy o systemie oświaty, tak by zapewnić podstawę prawną dla działania monitoringu w szkołach. Treść sprawozdania została jednak zmieniona w trakcie uzgodnień międzyresortowych i ostateczna wersja przyjęta przez Radę Ministrów nie zawiera tego postulatu.

Na realizację programu wydano łącznie prawie 109 mln zł, w tym prawie 77 mln z budżetu państwa. Czy dzięki temu w szkołach jest bezpieczniej? MEN przekonuje, że tak, i powołuje się na opinie dyrektorów szkół. Niestety, prawdziwej ewaluacji działania programu nie przeprowadzono. Nie badano ani jego rzeczywistego wpływu na bezpieczeństwo, ani na inne aspekty funkcjonowania szkoły.

Stwarzanie bezpiecznych warunków nauki nie sprowadza się wyłącznie do ochrony dziecka przed fizyczną bądź psychiczną przemocą ze strony innych uczniów. Budowanie poczucia bezpieczeństwa to także, a może przede wszystkim, stwarzanie warunków do swobodnego i nieskrępowanego rozwoju młodych ludzi w atmosferze wzajemnego zaufania oraz poszanowania przyrodzonej i niezbywalnej godności człowieka. (...) Trudno jest mówić o budowaniu poczucia bezpieczeństwa wśród dzieci uczących się w szkole bądź placówce oświatowej, w której każdy krok jest śledzony przez oko kamery, a uczeń może być nagrywany nawet w sytuacjach najbardziej intymnych.

Fragment wystąpienia RPO do MEN w sprawie braku dostatecznego umocowania ustawowego dla instalowania w szkole kamer monitoringu wizyjnego, 15 lutego 2010 r.

Ważny problem na marginesie… Obrazy miast w Internecie

W ostatnich miesiącach w mediach szczególnie intensywnie dyskutowano wprowadzenie do Polski usługi Google Street View. Zapewnia ona możliwość obejrzenia panoramicznych zdjęć z poziomu ulicy i pozwala użytkownikom na wyświetlanie wybranych części miasta. Zdjęcia wykonują specjalne kamery znajdujące się dachach samochodów Google, które pojawiły się w niektórych polskich miastach. GSV wzbudziło wiele kontrowersji w innych państwach europejskich, w których usługa ta była dostępna wcześniej. I nie chodziło tylko o zdjęcia twarzy czy prywatnych posesji. Okazało się, że Google poza fotografowaniem krajobrazu przechwytywał informacje z niezabezpieczonych sieci Wi-Fi.

W 2009 r. w Japonii grupa prawników oraz profesorów prawa konstytucyjnego zainicjowała kampanię przeciwko „widokowi z ulicy", dowodząc łamania przezeń „podstawowych praw człowieka". Usługa spotkała się też z krytyką we Francji, Niemczech, Grecji, Wielkiej Brytanii i Czechach. Ostatnio Google przegrał także proces w Szwajcarii. Sąd, rozpoznając powództwo szwajcarskiego organu ds. ochrony danych osobowych, nakazał firmie ręczne zamazywanie twarzy osób i samochodowych tablic rejestracyjnych widocznych na zdjęciach szwajcarskiego Street View, uznając system automatycznego zamazywania newralgicznych obszarów za niewystarczający.

Wątpliwości związane z funkcjonowaniem GSV zgłaszał także polski GIODO. Zanim GSV wkroczyło do Polski, firma musiała zadeklarować m.in., że nie będzie pobierać danych z sieci Wi-Fi, wykonywać zdjęć powyżej określonej wysokości, nie będzie także przechowywać obrazów źródłowych z Polski (bez zamazanych twarzy) oraz z wyprzedzeniem poda, kiedy i gdzie będą wykonywane zdjęcia.
Na podobnej zasadzie jak GSV działa kilka innych serwisów (np. Norc.pl). Wkroczyły one do Polski wcześniej, bez specjalnego medialnego rozgłosu.

Retencja i dostęp służb do danych telekomunikacyjnych

1 2 3 4 5 6 7

Nie ma dowodu na to, że retencja danych telekomunikacyjnych prowadzi do lepszej ochrony przed przestępczością. Z drugiej strony, obserwujemy, że generuje ona koszty na poziomie milionów euro, naraża na ryzyko prywatność niewinnych ludzi, narusza tajemnicę korespondencji w komunikacji elektronicznej oraz otwiera drogę do masowego zbierania informacji o całej populacji.

Fragment listu ponad stu organizacji z 23 krajów europejskich – w tym Fundacji Panoptykon – do komisarzy europejskich: Cecilii Malmström, Viviane Reding i Neelie Kroes, 22 czerwca 2010 r.

Kluczowy problem związany z retencją danych telekomunikacyjnych tkwi w mechanizmie gromadzenia danych o wszystkich obywatelach, na wszelki wypadek, zgodnie z zasadą, że każdy jest „potencjalnie podejrzany". Takie podejście trudno uznać za uzasadnione w demokratycznym państwie. Wyzwaniem związanym z retencją, ale od niej niezależnym, jest ustalenie rygorystycznych zasad dostępu do przechowywanych przez operatorów danych telekomunikacyjnych, który powinien być możliwy tylko w ściśle określonych przypadkach i pod kontrolą niezależnych organów.

Retencja danych telekomunikacyjnych to obowiązkowe gromadzenie tzw. danych transmisyjnych, czyli informacji o szczegółach wszystkich rodzajów połączeń telekomunikacyjnych w celach związanych z bezpieczeństwem publicznym. Część tego typu informacji jest przechowywana przez operatorów telekomunikacyjnych przez pewien czas z związku z prowadzoną przez nich działalnością. W przypadku obowiązkowej retencji dane o wszystkich połączeniach są przechowywane po to, by w razie potrzeby mogły po nie sięgnąć uprawnione służby i organy.

Operatorzy sieci i dostawcy publicznie dostępnych usług telekomunikacyjnych mają obowiązek przechowywać wszystkie informacje niezbędne do ustalenia, kto, kiedy, gdzie, z kim i w jaki sposób połączył się lub próbował połączyć. W przypadku sieci telefonicznych są to takie dane, jak numer telefonu, czas połączenia czy stacja przekaźnikowa,

w zasięgu której znajdowały się telefony wykonującego i odbierającego połączenie. W przypadku Internetu jest to kilkadziesiąt różnych cyfrowych śladów, które pozostawiają po sobie jego użytkownicy. Tego typu informacje o każdym z nas są gromadzone rutynowo „na wszelki wypadek", w oderwaniu o konkretnych spraw czy podejrzeń.

Obowiązek zatrzymywania danych na temat wszystkich połączeń telekomunikacyjnych przez

Europejskie sądy o retencji

W kilku europejskich krajach sądy konstytucyjne miały okazję zabrać głos w sprawie retencji danych telekomunikacyjnych. Przepisy wprowadzające dyrektywę zostały uchylone w Bułgarii (która ponownie implementowała dyrektywę do swojego porządku prawnego), Rumunii, Niemczech i Czechach. Najdalej idący był wyrok rumuński, w którym sąd wypowiedział się kategorycznie przeciwko zasadzie prewencyjnego gromadzenia danych o obywatelach. Uznał, że retencja godzi w domniemanie niewinności oraz stoi w sprzeczności z prawem do prywatności i wolności wypowiedzi.

okres od pół roku do dwóch lat nałożyła na państwa członkowskie Unii Europejskiej Dyrektywa o retencji danych (2006/24/WE). Poszczególne kraje bardzo różnie wdrożyły dyrektywę, jedne zapewniły służbom łatwy i szeroki dostęp do danych, inne zdecydowały się ograniczyć możliwość korzystania z nich do wybranej liczby przestępstw i wprowadzić kontrolę sądu. Co ciekawe, raport Komisji z ewaluacji wdrożenia dyrektywy pokazał, że żadne państwo członkowskie nie wdrożyło jej zgodnie z założeniami. Niektóre kraje (Szwecja, Austria) w ogóle nie implementowały dyrektywy, natomiast w kilku akty wdrażające zostały uznane za niekonstytucyjne.

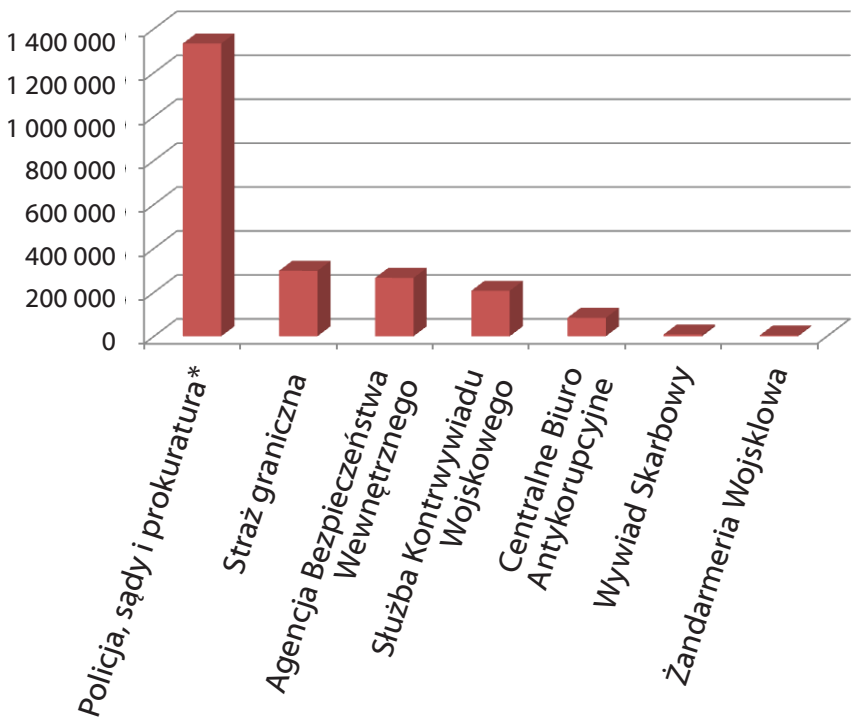
Retencja w wersji zaproponowanej przez dyrektywę pomyślana była jako środek nadzwyczajny, wykorzystywany w przypadku najgroźniejszych przestępstw. Polski ustawodawca wdrożył ją w sposób sprzeczny z tą ideą. Rozwiązania wprowadzone nowelizacją Prawa telekomunikacyjnego z 24 kwietnia 2009 r. przewidują możliwość pobierania danych retencyjnych w celu wykrywania wszystkich przestępstw, a także w ogólnie pojętych celach prewencyjnych.

Prawo telekomunikacyjne nakłada na operatorów obowiązek zatrzymywania danych dotyczących połączeń telefonicznych i ruchu w sieci przez 24 miesiące, czyli maksymalny okres przewidziany przez dyrektywę. Dostęp do tych danych mają sądy, prokuratura oraz siedem służb. Ich pobieranie odbywa się za pośrednictwem operatora na

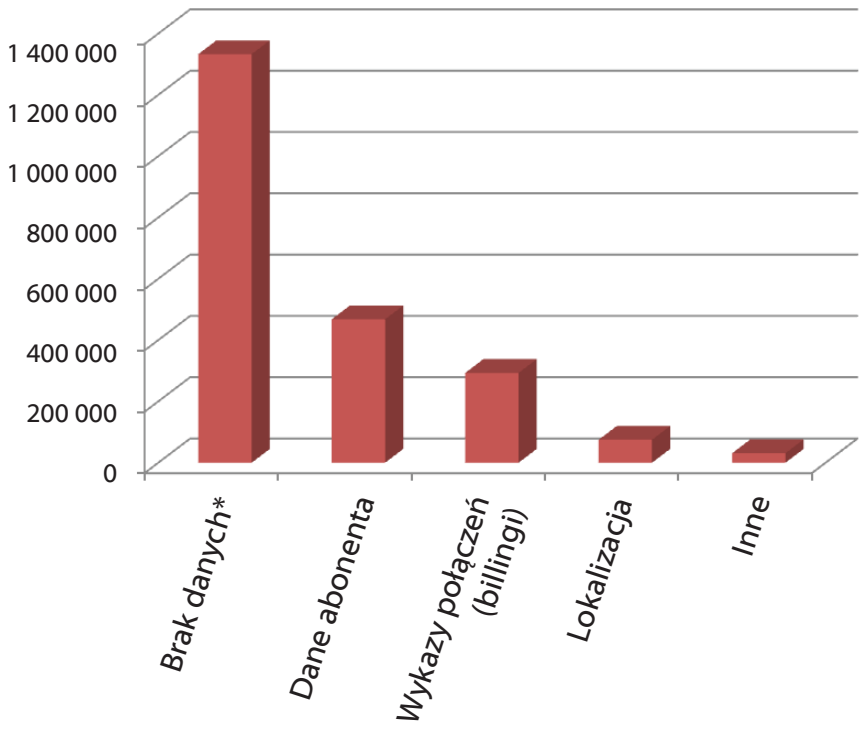
podstawie wniosku upoważnionego funkcjonariusza bądź bezpośrednio za pomocą elektronicznego interfejsu. Wszystkie uprawnione służby mogą korzystać z danych telekomunikacyjnych bez kontroli sądu czy prokuratora. Nie zapewniono również żadnej innej realnej metody weryfikacji tego, czy przyznane służbom uprawnienia nie są nadużywane.

Z danych udostępnionych przez Urząd Komunikacji Elektronicznej wynika, że w 2009 r. służby, policja i sądy sięgały po dane telekomunikacyjne ponad milion razy, a w 2010 r. (kiedy weszła w życie wspomniana nowelizacja prawa telekomunikacyjnego) – prawie milion czterysta tysięcy. „Śledztwo" przeprowadzone przez Sekretarza Kolegium ds. Służb Specjalnych Jacka Cichockiego pokazało, że bardzo trudno ustalić, co kryje się za tymi statystykami. Sądy, prokuratura i policja, które łącznie – jak można oszacować – generują ponad połowę zapytań, odpowiedziały, że nie prowadzą statystyk związanych z pobieraniem danych. W tym przypadku nie wiemy więc nawet, o jaki rodzaj zapytań chodziło (dane abonenta, wykazy połączeń czy lokalizację telefonu). Ilustrują to wykresy opracowane na podstawie danych zebranych i udostępnionych przez Jacka Cichockiego.

Pobieranie danych telekomunikacyjnych
(w okresie od 1 stycznia 2009 r. do 31 października 2010 r.)



Rodzaje pobieranych danych telekomunikacyjnych
(w okresie od 1 stycznia 2009 r. do 31 października 2010 r.)



*Dane szacunkowe

Taka sytuacja spotkała się z krytyką wielu podmiotów, nie tylko organizacji społecznych, ale również Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych czy Naczelnej Rady Adwokackiej. Do Trybunału Konstytucyjnego trafiły dwa wnioski o stwierdzenie niezgodności z Konstytucją przepisów dotyczących retencji danych. Krytyka zaowocowała przygotowaniem przez stronę rządową specjalnego raportu, w którym zawarto propozycje zmian prawa. Kierunki proponowanych zmian są jak najbardziej słuszne, trudno jednak uznać je za wystarczające.

Milion billingów

W Polsce szersza dyskusja na temat retencji danych telekomunikacyjnych została w dużej mierze sprowokowana przez artykuł Ewy Siedleckiej *Milion billingów* („Gazeta Wyborcza", 9 listopada 2010 r.). Największe wrażenie robiła informacja – uzyskana przez Fundację Panoptykon w drodze dostępu do informacji publicznej od Urzędu Komunikacji Elektronicznej – że w Polsce w 2009 r. ponad milion razy pobierano dane dotyczące połączeń telekomunikacyjnych. Premier Donald Tusk powołał specjalny zespół pod kierownictwem Sekretarza Kolegium ds. Służb Specjalnych Jacka Cichockiego, który miał wyjaśnić, co dokładnie kryje się za tymi statystykami.

W CZYM PROBLEM?

1 Czy obowiązkowa retencja danych wszystkich obywateli jest akceptowalnym narzędziem walki z przestępczością w demokratycznym państwie? Jest to kluczowe pytanie, na które w polskiej debacie publicznej brakuje miejsca. Można mieć zatem wątpliwości zarówno co do skuteczności, jak i niezbędności tego narzędzia. Pewne jest natomiast to, że rutynowe zatrzymywanie informacji o wszystkich połączeniach generuje wiele ryzyk z punktu widzenia ochrony podstawowych praw i wolności. Przede wszystkim stawia pod znakiem zapytania zasadę domniemania niewinności, a nas wszystkich – w roli podejrzanych.

2 Obowiązujące prawo przewiduje bardzo szeroki i łatwy dostęp do danych podlegających retencji. Informacje dotyczące połączeń wykorzystywane są w sprawach cywilnych (np. rozwodowych), w ramach postępowań dotyczących nawet najdrobniejszych przestępstw, w ogólnie pojętych celach prewencyjnych. W tej sytuacji wkroczenie w sferę naszych osobistych wolności może mieć miejsce w sprawach błahych i bez dostatecznego uzasadnienia.

Retencja danych w Trybunale Konstytucyjnym

Zdaniem RPO – Ireny Lipowicz – obowiązujące przepisy dotyczące retencji danych telekomunikacyjnych są niezgodne z Konstytucją oraz europejską Konwencją o ochronie praw człowieka i podstawowych wolności. W sposób niedopuszczalny ingerują one w tajemnicę komunikowania się, która obejmuje nie tylko samą treść przekazu, ale również takie elementy, jak: dane dotyczące użytkowników, dane lokalizacyjne czy informacje o próbach uzyskania połączeń.

17 stycznia RPO zwróciła się do premiera Donalda Tuska o zajęcie stanowiska oraz podjęcie odpowiednich działań w tej sprawie, a 1 sierpnia skierowała do TK wniosek o stwierdzenie niezgodności z Konstytucją przepisów dotyczących retencji danych.

W swoim piśmie kwestionuje ona bardzo luźne zasady udostępniania danych podlegających retencji. RPO zwraca uwagę, że:

1) przepisy nie określają sprecyzowanego celu gromadzenia danych;
2) brakuje wskazania kategorii osób, w stosunku do których niezbędne jest respektowanie ich tajemnicy zawodowej;
3) warunkiem uzyskania dostępu do danych nie jest wyczerpanie innych, mniej ingerujących w sferę praw lub wolności, możliwości pozyskania niezbędnych informacji;
4) brakuje jakiejkolwiek zewnętrznej formy kontroli;
5) część danych nie podlega zniszczeniu nawet wtedy, gdy okazały się nieprzydatne.

W krytyce obowiązujących przepisów jeszcze dalej idzie wniosek z 28 stycznia 2011 r. skierowany do TK przez grupę posłów SLD (sygnatura K 2/11). Wnioskodawcy podważają samą ideę retencji:

1) obowiązek zatrzymywania danych telekomunikacyjnych ma charakter powszechny i dotyczy praktycznie każdego użycia telefonu, faksu, e-maila, telefonii internetowej;
2) możliwości pozyskiwania danych nie są ograniczone do przypadków wykrywania i ścigania poważnych przestępstw, a przez to stoją w sprzeczności z dyrektywą retencyjną;
3) brakuje kontroli wewnętrznej i zewnętrznej nad korzystaniem z danych.

SŁUŻBY POZA KONTROLĄ GIODO

Organem, który odpowiada w Polsce za ochronę danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych. Jednak jego uprawnienia w stosunku do służb są bardzo ograniczone. Informacje niejawne oraz uzyskane w wyniku czynności operacyjno-rozpoznawczych nie podlegają obowiązkowi rejestracji. W przypadku przetwarzania tego typu danych przez CBA, ABW, Agencję Wywiadu i Służbę Kontrwywiadu Wojskowego GIODO nie ma możliwości kontrolowania, czy są one przetwarzane zgodnie z prawem, wydawania decyzji nakazujących usunięcie uchybień, zabezpieczenie bądź usunięcie danych ani rozpatrywania skarg obywateli na niezgodne z prawem przechowywanie ich danych.

Zapewnienie efektywnej kontroli nad przetwarzaniem informacji o obywatelach przez służby stanowi duże wyzwanie organizacyjne i pociąga za sobą wydatki. Jednak utrzymanie obecnego stanu rzeczy może sprzyjać nadużyciom. Dlatego od dłuższego czasu podkreśla się potrzebę rozszerzenia uprawnień GIODO albo poddanie działań służb kontroli innego zewnętrznego organu.

3 Co więcej, pozyskiwanie danych telekomunikacyjnych nie podlega żadnej zewnętrznej formie kontroli. W przypadku służb sięganie po te dane nie wymaga zgody sądu ani prokuratora. Prawo nie przewiduje również żadnych innych form weryfikacji tego, jak uprawnione podmioty korzystają ze swoich uprawnień.

4 Spod obowiązującej regulacji nie są wyłączone osoby, w stosunku do których niezbędne jest respektowanie tajemnicy zawodowej: lekarskiej, adwokackiej, radcy prawnego, notarialnej lub dziennikarskiej, których zniesienie jest możliwe tylko w ściśle określonych przypadkach.

5 Część danych gromadzonych przez służby nie podlega zniszczeniu nawet wtedy, gdy okażą się one zbędne. W przypadku niektórych służb brakuje obowiązku usuwania tego typu danych, mimo że z Konstytucji (art. 51 ust. 2) wynika, iż władze publiczne nie powinny gromadzić innych danych niż niezbędne w demokratycznym państwie prawnym.

6 Osoby, których dane były pobierane przez służby, nie są o tym fakcie informowane, więc nie mają żadnej wiedzy ani wpływu na to, co dzieje się z informacjami na ich temat.

Napięcie między wolnością a bezpieczeństwem jest jednym z głównych wyzwań współczesnego państwa, a rozwiązanie tego problemu jest zawsze trudne. Obowiązujący stan prawny w kwestii pozyskiwania informacji przez państwo nie pozwala na właściwe wyważenie tych dwóch godnych konstytucyjnej ochrony dóbr. Dotyczy to w szczególności informacji objętych tajemnicą komunikowania się. Jest to obszar szczególnie wrażliwy, związany ze sferą naszej wolności, a więc jego prawidłowa regulacja ma fundamentalne znaczenie.

Irena Lipowicz, *Między wolnością a bezpieczeństwem*, „Rzeczpospolita", 15 marca 2011 r.

7 Nakłada się na to problem ogólnego braku transparentności działań służb w tym zakresie i nieinformowanie społeczeństwa o sposobie korzystania z przysługujących im uprawnień.

8 Koszty związane z retencją przerzucone są na operatorów telekomunikacyjnych (w niektórych państwach europejskich koszty te ponoszą bądź partycypują w nich instytucje publiczne korzystające z danych retencyjnych). Taka sytuacja nie tylko w sposób nieuzasadniony obciąża przedsiębiorców i wpływa na wysokość naszych rachunków, ale także sprzyja brakowi dyscypliny po stronie służb i może wpływać na pobieranie zbyt dużej liczby danych.

Wartości do zważenia

BEZPIECZEŃSTWO

Można mieć wątpliwości, czy obowiązkowe zatrzymywanie danych telekomunikacyjnych wpływa na poprawę bezpieczeństwa i stanowi warunek skutecznej walki z przestępczością. Z pewnością ułatwia ono działanie służbom, ale to nie jest wystarczający argument przemawiający za ograniczeniem praw wszystkich obywateli. Porównanie sytuacji w państwach korzystających i niekorzystających z retencji nie prowadzi do wniosku, że narzędzie to usprawniło europejską walkę z terroryzmem czy poważną przestępczością.

Najpoważniejsze przestępstwa można ścigać za pomocą innych metod. Często tradycyjne metody śledcze okazują się w takich przypadkach bardziej skuteczne, ponieważ doświadczeni przestępcy zdają sobie sprawę z ryzyk związanych z korzystaniem z nowych technologii i starają się je neutralizować.

PRYWATNOŚĆ I TAJEMNICA KORESPONDENCJI

Rutynowe zbieranie informacji o wszystkich obywatelach trudno uzasadnić na gruncie obowiązującego porządku konstytucyjnego. Ograniczenia prawa do prywatności (art. 47), ochrony danych osobowych (art. 51) i tajemnicy komunikowania się (art. 49) są wprawdzie dopuszczalne na gruncie art. 31 Konstytucji, ale w tym przypadku jest ono nieproporcjonalne do celu i trudno uznać je za konieczne w demokratycznym państwie.

SWOBODA DZIAŁALNOŚCI GOSPODARCZEJ

Wątpliwości budzi przerzucenie na przedsiębiorców kosztów zatrzymywania i udostępniania danych zbędnych z punktu widzenia świadczenia usług.

Co proponuje strona rządowa?

Raport przygotowany pod kierownictwem Sekretarza Kolegium ds. Służb Specjalnych zawiera propozycje kierunków zmian obowiązującego prawa, mające na celu zapewnienie większej kontroli nad działaniami służb:

1) skrócenie okresu zatrzymywania danych do roku;
2) ograniczenie możliwości korzystania z danych retencyjnych do ścigania przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata, oraz przestępstw popełnianych za pomocą środków komunikacji elektronicznej (np. tzw. przestępstw komputerowych); umożliwienie sądom sięgania po te dane wyjątkowo w przypadku innych przestępstw; zapewnienie dostępu do danych służbom specjalnym działającym w celu zapewnienia bezpieczeństwa państwa;
3) wprowadzenie we wszystkich uprawnionych organach instytucji wewnętrznego (powołanego przez kierownika organu, ale z gwarancjami nieusuwalności) pełnomocnika ds. ochrony danych telekomunikacyjnych, który miałby kontrolować praktyki postępowania z danymi i przygotowywać sprawozdania zawierające statystyki;
4) wprowadzenie obowiązku informowania prokuratora o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez służby;
5) wprowadzenie bezwzględnego obowiązku niszczenia niepotrzebnych danych;
6) wprowadzenie obowiązku prowadzenia statystyk dotyczących korzystania z danych telekomunikacyjnych i podawania ich do publicznej wiadomości;
7) powołanie niezależnego organu, złożonego z członków wybieranych przez Sejm, kontrolującego pracę operacyjną służb specjalnych, do którego obowiązków należałoby m.in. prowadzenie kontroli w służbach, rozpatrywanie skarg obywateli na ich działanie oraz przygotowywanie jawnych i niejawnych sprawozdań ze swoich działań.

JAKIE TO RODZI ZAGROŻENIA?

1 Obowiązek gromadzenia wielu bardzo szczegółowych danych dotyczących połączeń wykonywanych przez wszystkich członków społeczeństwa stwarza bardzo duże zagrożenie dla prywatności. Dane telekomunikacyjne pozwalają na stworzenie szczegółowego obrazu życia prywatnego danej osoby – swoistego „cyfrowego profilu", zbudowanego z informacji na temat sieci społecznych kontaktów, mapy przemieszczania się i nawyków. Takie dane umożliwiają nie tylko patrzenie wstecz, ale również na profilowanie i przewidywanie naszych zachowań w przyszłości. Dlatego dane telekomunikacyjne powinny być chronione na wielu poziomach: możliwość dostępu do nich po stronie organów władzy publicznej powinna być ograniczona do szczególnie uzasadnionych przypadków. Konieczna jest również kontrola nad tym, w jaki sposób te dane są przetwarzane przez operatorów. Czy są wykorzystywane zgodnie z przeznaczeniem? Czy są usuwane, kiedy okażą się zbędne? Czy są odpowiednio zabezpieczone przez możliwością wycieków?

2 Automatyczne procesy profilowania stwarzają ryzyko błędów, które mogą mieć daleko idące konsekwencje dla sytuacji jednostki.

3 Obecne ukształtowanie przepisów, dające wielu podmiotom szeroki i niekontrolowany dostęp do danych telekomunikacyjnych,

stwarza bardzo duże ryzyko nadużyć. Możliwe jest sięganie do tych danych telekomunikacyjnych na masową wręcz skalę, często w sprawach błahych lub kiedy nie ma to żadnego prawnego uzasadnienia (np. w prywatnych sprawach funkcjonariuszy).

4 W przypadku zawodów zaufania publicznego (dziennikarzy, lekarzy, prawników) retencja stwarza dodatkowe ryzyko w postaci podważenia zasady poufności, zagrożenia dla tajemnicy zawodowej czy ochrony źródeł informacji dziennikarskich. Jest to problem, na który bardzo trudno znaleźć remedium.

Dziennikarze pod lupą

Ważnym impulsem dla rozpoczęcia w Polsce szerszej debaty publicznej na temat retencji danych telekomunikacyjnych była głośna w październiku 2010 r. sprawa „inwigilacji" dziesięciu dziennikarzy największych polskich mediów, których billingi i dane lokalizacyjne w latach 2005–2007 były swobodnie pobierane przez służby.

Według informacji Obserwatorium Wolności Mediów Helsińskiej Fundacji Praw Człowieka nie był to odosobniony przypadek pobierania danych telekomunikacyjnych dziennikarzy przez organy ścigania i inne służby. Do HFPC zgłasza się z tym problemem coraz więcej dziennikarzy. Taka praktyka jest sprzeczna ze standardami Europejskiego Trybunału Praw Człowieka, który wielokrotnie wskazywał, że ujawnianie źródeł informacji dziennikarskiej narusza art. 10 Europejskiej Konwencji Praw Człowieka, tj. prawo do wolności słowa.

Część dziennikarzy podjęła próbę wyjaśnienia sprawy i wyciągnięcia konsekwencji wobec osób odpowiedzialnych za pobieranie danych telekomunikacyjnych. Dotychczas jednak polskie sądy nie dopatrzyły się w żadnej z tych spraw przekroczenia uprawnień funkcjonariuszy.

Sprawa „inwigilacji" dziennikarzy odbiła się szerokim echem także poza granicami Polski. Pobieranie dziennikarskich billingów „wytknęła" nam m.in. Privacy International w raporcie rocznym *Prawo do prywatności w Europie a prawa człowieka 2010*. W ogólnym podsumowaniu Polska zajęła 21 pozycję, osiągając wynik poniżej średniej Unii Europejskiej. Według raportu PI wyższymi standardami ochrony prywatności mogą pochwalić się m.in. Słowenia, Rumunia, Słowacja czy Węgry.

HISTORIA ŻYCIA W TELEFONIE

Na intrygujący pomysł wywołania debaty publicznej na temat retencji danych telekomunikacyjnych wpadł Malte Spitz – niemiecki polityk Partii Zielonych. Po batalii w sądzie udało mu się uzyskać nakaz udostępnienia przez operatora telekomunikacyjnego wszystkich danych związanych z używaniem jego prywatnego telefonu komórkowego.

Okazało się, że polityk otrzymał w sumie od firmy telekomunikacyjnej 35 831 informacji zgromadzonych w ciągu poprzedzających 6 miesięcy (tak długo należało w Niemczech przechowywać dane telekomunikacyjne, zanim przepisy dotyczące retencji zostały uchylone przez sąd konstytucyjny; w Polsce okres ten jest cztery razy dłuższy). Obok historii połączeń czy wykazu wiadomości tekstowych znalazły się tam również dane geolokalizacyjne.

Informatycy jednej z niemieckich gazet powiązali otrzymane informacje i stworzyli interaktywną mapę, dzięki której przez pół roku możemy ze szczegółami śledzić życie polityka. Przesuwając myszką po osi czasu, można łatwo sprawdzić, kiedy i gdzie Spitz przebywał, kiedy pracował, kiedy odpoczywał, jak często rozmawiał przez telefon oraz wysyłał SMS-y, kiedy korzystał z Internetu. Dodatkowo dane telekomunikacyjne zestawiono z informacjami publicznie dostępnymi na blogu i Twitterze polityka. Jeśli zatem napisał on w portalu społecznościowym, że określonego dnia zjadł kolację w dobrej restauracji, posługując się interaktywną mapą, jesteśmy w stanie w prosty sposób namierzyć, gdzie dokładnie mieścił się ten lokal.

Eksperyment wywołał w niemieckich mediach burzę wokół możliwości inwigilacji obywateli za pomocą technologii, którą każdy z nas nosi w kieszeni. Sam Spitz natomiast naraził się na falę krytyki zwolenników Zielonych. Z zestawienia ujawnionych informacji wynikało bowiem, że zbyt często lata samolotami, podczas gdy bardziej przyjazne środowisku byłyby podróże pociągiem...

Czy istnieje alternatywa dla retencji danych?

Operatorzy przechowują przez pewien czas część danych telekomunikacyjnych na potrzeby świadczenia usług i prowadzenia rozliczeń. Dzieje się to bez względu na obowiązki wynikające z Prawa telekomunikacyjnego. Gdyby nie było w polskim prawie obowiązku retencji, dane te należałoby kasować, jak tylko staną się zbędne z punktu widzenia świadczenia usług przez operatorów. Wszystkie te informacje mogą być wykorzystane do ścigania przestępstw w ramach instytucji tzw. zamrażania danych, która jest stosowana w niektórych krajach europejskich i możliwa na gruncie polskiego prawa (art. 218a Kodeksu postępowania karnego).

Na wniosek uprawnionej służby w związku z konkretnym toczącym się postępowaniem wskazane dane są zatrzymywane przez operatora telekomunikacyjnego. Zamrożenie dokonywane jest natychmiastowo, co skutecznie zapobiega utracie cennych informacji. Aby jednak uzyskać dostęp do zamrożonych danych, potrzebna jest zgoda sądu. Taka forma zabezpieczenia informacji przewidziana jest w Konwencji Rady Europy o cyberprzestępczości. Stosowanie takiego rozwiązania zamiast powszechnej retencji danych znaczenie zwiększyłoby poziom ochrony praw i wolności, bez dużego uszczerbku dla sprawności działania organów ścigania.

Bez względu na to, czy retencja zostanie utrzymana, czy zastąpiona innym mechanizmem, kluczowe znaczenie ma ustalenie jasnych zasad dostępu do jakichkolwiek danych telekomunikacyjnych (nie tylko tych ewentualnie podlegających obowiązkowi retencji) oraz wprowadzenie efektywnej kontroli nad tym, jak uprawnione organy korzystają z tych uprawnień. Oto najważniejsze postulaty:

1) zaostrzenie ogólnych zasad dostępu do danych telekomunikacyjnych, przede wszystkim poprzez stworzenie zamkniętego katalogu przestępstw i innych spraw (np. zaginięcia), które upoważniają do sięgania do danych telekomunikacyjnych oraz weryfikację katalogu uprawnionych do tego organów;
2) stworzenie skutecznych mechanizmów nadzoru nad służbami, przede wszystkim poprzez wprowadzenie wymogu uzyskiwania zgody sądu bądź prokuratora (zgoda następcza w nagłych przypadkach) na dostęp do różnego rodzaju danych telekomunikacyjnych; zapewnienie zewnętrznej kontroli (np. GIODO) nad przetwarzaniem danych przez organy uprawnione do korzystania z danych retencyjnych oraz wypracowanie efektywnych mechanizmów wewnętrznej kontroli nad przetwarzaniem danych telekomunikacyjnych w policji i innych służbach; wprowadzenie mechanizmów zewnętrznej kontroli praktyk przechowywania danych przez operatorów telekomunikacyjnych;
3) wprowadzenie sprawnych mechanizmów niszczenie niepotrzebnych danych; wprowadzenie obowiązku informowania obywatela po zakończeniu postępowania o pobieraniu jego danych, stworzenie możliwości wnoszenia skarg do niezależnego organu;
4) zobowiązanie organów upoważnionych do dostępu do danych telekomunikacyjnych do prowadzenia szczegółowych statystyk dotyczących korzystania przez nie z tych danych.

Rekomendacje Fundacji Panoptykon dotyczące zmian prawa w zakresie retencji i dostępu do danych telekomunikacyjnych są szczegółowo omówione w raporcie *Internet a prawa podstawowe. Ekspresowy przegląd problemów regulacyjnych*.

Ważny problem na marginesie…
Technologie w rękach służb

Ustawa o Policji stanowi, że kontrola operacyjna może polegać m.in. na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie. Analogiczne bardzo szerokie i nieprecyzyjne sformułowane uprawnienia zostały zawarte również w ustawach: o Straży Granicznej, o Żandarmerii Wojskowej i wojskowych organach porządkowych, o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, o Centralnym Biurze Antykorupcyjnym, o Służbie Wywiadu Wojskowego oraz Służbie Kontrwywiadu Wojskowego, o kontroli skarbowej.

W tej sytuacji nie jest jasne, jakich konkretnie środków mogą używać służby przy prowadzeniu kontroli operacyjnej ani jakie konkretnie informacje mogą być w dany sposób pozyskiwane. Służby nie powinny mieć możliwości dowolnego korzystania ze wszelkich dostępnych w danym momencie środków, ponieważ może to prowadzić do nadużyć. Takie ukształtowanie uprawnień służb jest nie do pogodzenia ze standardami konstytucyjnymi.

Do Trybunału Konstytucyjnego trafiły wnioski o stwierdzenie niezgodności wskazanych przepisów z Konstytucją: 28 stycznia 2011 r. wystąpiła z nim grupa posłów SLD (sygnatura K 2/11), a 29 czerwca 2011 r. – RPO (sygnatura K 23/11).

"Agencja Bezpieczeństwa Wewnętrznego w zakresie swojej właściwości jest uprawniona do stosowania wszelkich środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów. Niewątpliwie uzyskiwanie i utrwalanie przez Agencję Bezpieczeństwa Wewnętrznego danych o miejscach przebywania osób podejrzanych, ich samochodów i innych pojazdów, którymi się poruszają, stanowi realizację jej ustawowego uprawnienia i pozostaje w zakresie właściwości Agencji Bezpieczeństwa Wewnętrznego (…) odpowiedź na pytanie wnioskodawcy zawiera się i wynika wprost z treści przywołanego przepisu ustaw".

Fragment odpowiedzi ABW na sformułowane przez HFPC we wniosku o udostępnienie informacji publicznej z 13 grudnia 2010 r. pytanie o to, czy w ramach środków technicznych wykorzystywanych przy wykonywaniu kontroli operacyjnej ABW stosuje system nawigacji satelitarnej GPS w celu uzyskania i utrwalania danych o miejscach przebywania osób, 19 stycznia 2011 r.

Wymiana informacji między organami ścigania

1 2 3 4 5 6 7

W pełni rozumiemy zarówno konieczność implementacji regulacji prawa Unii Europejskiej do polskiego porządku prawnego, jak i uzasadnioną potrzebę usprawnienia współpracy międzynarodowej w zakresie zwalczania przestępczości. Pragniemy jednak zwrócić uwagę, że cele te nie mogą być realizowane kosztem podstawowych praw obywateli.

Fragment listu Fundacji Panoptykon do MSWiA w sprawie ustawy o wymianie informacji między organami ścigania państw UE, 4 marca 2011 r.

Międzynarodowa wymiana informacji jest niezbędna, aby w sposób skuteczny ścigać sprawców niektórych poważnych przestępstw. Trzeba sobie jednak zdawać sprawę z ryzyk związanych z przekazywaniem informacji do innych krajów. Umożliwienie wymiany na szeroką skalę i bez kontroli najpewniej nie przełoży się na skuteczność działania służb, może natomiast stanowić poważne zagrożenie dla podstawowych praw i wolności.

Ustawa o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (uchwalona 16 września 2011 r.) zakłada stworzenie systemu informatycznego, który umożliwi łatwe i szybkie przekazywanie danych między policją, niektórymi innymi służbami (m.in. Centralnym Biurem Antykorupcyjnym, Agencją Bezpieczeństwa Wewnętrznego, Służbą Celną, Żandarmerią Wojskową), organami podatkowymi i organami kontroli skarbowej różnych państw członkowskich. Służby będą zobowiązane wzajemnie udostępniać sobie informacje gromadzone według przysługujących im kompetencji w prawie krajowym, nie tylko w celu wykrywania i ścigania sprawców przestępstw, ale również – ogólnie pojętego zapobiegania przestępczości.

Nowa ustawa pozwoli polskiej policji na obszarze całej UE i innych państw strefy Schengen sprawdzić materiały zebrane w toku prowadzenia kontroli operacyjnej wobec osoby podejrzanej, porównywać odciski linii papilarnych lub kod DNA z danymi zgromadzonymi w zagranicznych bazach. Znacznie łatwiej będzie uzyskać informację o majątku skazanego w Polsce cudzoziemca, co ma usprawnić proces odzyskiwania mienia pochodzącego z przestępstwa, które znajduje się za granicą. W zamian polskie służby będą miały obowiązek

udzielić tych samych informacji na żądanie organów ścigania innych państw UE.

System wymiany informacji w danym państwie koordynować będzie tzw. punkt kontaktowy, do którego będą wpływały wnioski o udostępnienie danych od organów innych państw. W Polsce zostanie on utworzony w ramach Komendy Głównej Policji. Komórka ta otrzyma bezpośredni dostęp *on-line* do wszystkich ważniejszych centralnych baz danych, takich jak: PESEL, Krajowy Rejestr Karny, Centralna Ewidencja Pojazdów i Kierowców, ogólnokrajowa ewidencja wydanych i unieważnionych dowodów osobistych i inne. W zakresie wykrywania korzyści pochodzących z przestępstwa zadania punktu kontaktowego będzie pełnić krajowe biuro ds. odzyskiwania mienia.

Obowiązek uchwalenia ustawy wynika z przepisów UE, przede wszystkim z dwóch decyzji ramowych: nr 960 oraz nr 977. Celem pierwszej decyzji jest harmonizacja i uproszczenie przepisów dotyczących wymiany informacji między organami ścigania UE, a drugiej – wprowadzenie wspólnych zasad ochrony danych osobowych, które będą podlegać takiej wymianie. Szacuje się, że realizacja projektu będzie kosztować ok. 28 mln zł.

Dodatkowe uprawnienia przy okazji

Największe kontrowersje wokół projektu ustawy wzbudziły propozycje wprowadzenia „przy okazji" istotnych zmian w kilku obowiązujących już aktach prawnych, m.in. w ustawie o Policji. W pierwotnej wersji projekt ustawy znacząco poszerzał uprawnienia służb w zakresie dostępu do informacji o naszym majątku. Zaproponowane przez MSWiA rozwiązania przewidywały możliwość dość swobodnego (poza kontrolą sądową) sięgania do niektórych danych objętych tajemnicą bankową, ubezpieczeniową czy skarbową. Przepisy te miały ułatwiać organom ścigania namierzanie mienia pochodzącego z przestępstwa. Gdy projekt był już w Sejmie, przez media przetoczyła się fala krytyki proponowanych rozwiązań. Ostatecznie dodatkowe ułatwienia policji i innych służb w pozyskiwaniu danych finansowych zostały usunięte z projektu ustawy na etapie prac sejmowych.

> **Rząd, pod przykrywką dostosowania polskiego prawa do kilku decyzji Rady Europejskiej w trybie ekstraszybkim, na ostatnich posiedzeniach Sejmu przepycha przepisy, które w mocno kontrowersyjny sposób poszerzają uprawnienia policji i służb specjalnych.**
>
> **Ewa Siedlecka, *Zmylić przeciwnika*, „Gazeta Wyborcza", 25 sierpnia 2011 r.**

KRYTYKA GIODO

Gdy projekt ustawy został po raz pierwszy opublikowany przez MSWiA pod koniec 2010 r., spotkał się z ostrą krytyką GIODO. Jednym z głównych zarzutów był niejasny stosunek proponowanych regulacji do ustawy o ochronie danych osobowych.

Ustawy tej nie stosuje się tylko wówczas, gdy inne ustawy szczególne przewidują dalej idącą ochronę. Tymczasem ustawa o wymianie informacji miała być traktowana jako lex specialis w stosunku do ustawy o ochronie danych osobowych, choć proponowane przepisy zapewniały ochronę prywatności na znacznie niższym poziomie.

Pierwotny projekt ustawy pomijał także kwestię kontroli organu zewnętrznego nad przekazywaniem danych osobowych polskich obywateli za granicę, mimo że kompetencje „krajowego organu nadzoru" w tym zakresie zostały przewidziane w jednej z implementowanych decyzji ramowych.

Zastrzeżenia GIODO wobec pierwotnej wersji projektu były tak poważne, że zdecydował się on zanegować projekt w całości.

Na skutek uwag GIODO w dalszych pracach nad projektem ustawy uwzględniono środki wzmacniające ochronę danych osobowych, uzależniając możliwość przekazania jakichkolwiek informacji za granicę od spełnienia wymogów ustawy o ochronie danych osobowych i poszanowania praw człowieka. Na etapie prac sejmowych dodano także przepis o kontrolnych uprawnieniach GIODO. Nadal jednak wiele rozwiązań budzi spore wątpliwości.

W CZYM PROBLEM?

1 Zastrzeżenia budzą warunki wymiany danych między służbami, które mają obowiązek przekazywać je nie tylko na wniosek, ale także z urzędu, „jeżeli istnieje uzasadnione podejrzenie, że informacje te przyczynią się do wykrycia i zatrzymania sprawców przestępstw lub zapobieżenia przestępstwu na terytorium UE". Przepis ten jest bardzo nieprecyzyjny, co stoi w sprzeczności z obowiązującymi w prawie krajowym ograniczeniami w przekazywaniu danych o własnych obywatelach za granicę oraz kluczową zasadą ochrony danych osobowych – zasadą adekwatności.

2 Ustawa nie zakłada obowiązku szczegółowego uzasadnienia potrzeby sięgania po dane przez organy ścigania innego kraju, a jedynie możliwość poproszenia przez kraj zobowiązany do ich transferu o dodatkowe informacje na temat sprawy, której dotyczą, oraz sposobu ich wykorzystania. Uznaniu państwa przekazującego pozostawiono też to, czy zażąda ono usunięcia, anonimizacji lub zablokowania otrzymanych danych po ich wykorzystaniu. Zabrakło rozwiązań, które po stronie organów korzystających z danych wymuszałoby odpowiedni poziom samokontroli oraz weryfikację sposobu ich wykorzystania, przechowywania i zabezpieczenia.

3 Obowiązek transferu danych może dotyczyć podejrzenia popełnienia jakiegokolwiek przestępstwa. Co prawda państwo może odmówić ich przekazania, jeśli żądanie związane jest z popełnieniem czynu zabronionego zagrożonego w Polsce karą do roku pozbawienia wolności lub łagodniejszą, ale w praktyce oznacza to, że tak inwazyjny środek może być stosowany także w przypadku najlżejszych występków. Co więcej, wymiana danych jest możliwa również w celach prewencyjnych. Można wprawdzie odmówić ich przekazania, jeśli byłoby to niewspółmierne do celu, w jakim wystąpiono z wnioskiem, jednak biorąc pod uwagę wspomniany brak obowiązku przekazywania szczegółowych informacji dotyczących wykorzystania danych, takie zabezpieczenie może mieć iluzoryczny charakter.

4 Pojawiają się wątpliwości, czy ustawa w sposób właściwy wdraża prawo unijne. Z jednej strony, decyzja ramowa dotyczy przekazywania danych w ramach współpracy organów policyjnych i sądowych państw UE, tymczasem polski ustawodawca ogranicza krąg podmiotów objętych regulacją do organów ścigania, z wyłączeniem sądów. Z drugiej strony, projekt umożliwia przekazywanie danych przykładowo także do Interpolu (Międzynarodowej Organizacji Policji Kryminalnych), który nie jest organem ścigania żadnego z państw członkowskich, a także do państw niebędących członkami UE. Identyczne zasady mogą więc znaleźć zastosowanie w przypadku przekazywania danych polskich obywateli państwom UE, które są zobligowane normami prawa europejskiego do przyjęcia i przestrzegania regulacji dotyczących ochrony danych osobowych, oraz państwom trzecim, które nie są w bezpośredni sposób związane tymi przepisami.

5 Wiele zastrzeżeń budzi sposób pracy nad ustawą. Ministerstwo Spraw Wewnętrznych i Administracji właściwie nie przewidziało konsultacji społecznych projektu umożliwiającego przecież bardzo głęboką ingerencję w prawa obywateli. Projekt został przesłany do zaopiniowania trzem podmiotom. Do zgłoszenia uwag nie zaproszono nie tylko organizacji społecznych, ale również np. Generalnego Inspektora Ochrony Danych Osobowych, który ostatecznie zaangażował się w prace nad projektem z własnej inicjatywy.

Kalendarium prac nad ustawą

2010 r.

- **22 listopada – MSWiA publikuje projekt ustawy**

2011 r.

- **1 sierpnia – projekt wpływa do Sejmu**
- **5 sierpnia – zostaje skierowany do I czytania**
- **18 sierpnia – I czytanie: projekt zostaje skierowany do Komisji Administracji i Spraw Wewnętrznych**
- **29 sierpnia – sprawozdanie Komisji**
- **30 sierpnia – II czytanie**
- **31 sierpnia – III czytanie: głosowanie – 268 głosów za, 138 głosów przeciw, 1 głos wstrzymujący się**
- **5 września – ustawa zostaje przekazana do Senatu**
- **13 września – głosowanie: wprowadzono 2 poprawki**
- **16 września – głosowanie w Sejmie: przyjęto poprawki**

Stan na 7 października 2011 r.

Na kolejnych etapach procedury było jeszcze mniej czasu na konsultacje, analizy czy opinie. Kiedy projekt wpłynął do Sejmu, prace nad nim nabrały prawdziwie zawrotnego tempa. Okres od przekazania projektu do Sejmu do czasu głosowania w Senacie trwał niewiele ponad miesiąc! Dla porównania, średni czas procedowania nad projektami ustaw w Sejmie w ramach upływającej właśnie kadencji Parlamentu wynosił 144 dni (od wpłynięcia projektu ustawy do Sejmu do momentu przekazania jej do Senatu); przy czym statystyka ta obejmuje również ustawy przyjmowane w trybie pilnym, w tym 18 aktów uchwalonych w czasie krótszym niż tydzień (dane udostępnione przez Sejmometr.pl). Dopiero burza medialna wywołana m in. publikacjami „Gazety Wyborczej" sprawiła, że prace nad projektem na chwilę wstrzymano. Nie znaleziono już jednak czasu na dyskusję, więc „dla świętego spokoju" wykreślono najbardziej kontrowersyjne przepisy i projekt ustawy szybko trafił do Senatu.

JAKIE TO RODZI ZAGROŻENIA?

1 Brakuje gwarancji, że działający wewnątrz struktur policji punkt kontaktowy będzie w stanie weryfikować zapytania otrzymywane od zagranicznych służb; w praktyce może je po prostu automatycznie realizować. Istnieje więc ryzyko, że organy ścigania będą zbyt swobodnie

> **Zapytaliśmy pilotującego projekt wiceministra spraw wewnętrznych Adama Rapackiego, czy uważa, że to w porządku, aby tak znaczące poszerzenie uprawnień policji i służb przemycać w Sejmie w ekstraszybkim trybie, bez uczciwej debaty? – To może rzeczywiście nieszczęśliwie wyszło. Jeśli projekt będzie budził duże kontrowersje, to jesteśmy skłonni zrezygnować z uprawnień, które nie są konieczne do wykonania unijnych decyzji, i powrócić do tego w przyszłym parlamencie – zadeklarował.**
>
> **Ewa Siedlecka, *MSWiA chce łatwiejszych podsłuchów i kontroli majątku bez zgody sądu*, „Gazeta Wyborcza", 25 sierpnia 2011.**

Wartości do zważenia

PRYWATNOŚĆ

Ustawa wzbudza szereg wątpliwości związanych z przestrzeganiem standardów ochrony prywatności. Przekazywanie danych osobowych do państw trzecich wiąże się z dużym zagrożeniem z punktu widzenia poszanowania praw i wolności jednostek. Dlatego proces ten jest zgodnie z ustawą o ochronie danych osobowych obwarowany szczególnymi gwarancjami. Co do zasady nie można przekazywać danych tam, gdzie standard ich ochrony jest niższy niż na terytorium Polski. Ustawa o wymianie informacji dopuszcza natomiast dość swobodne przekazywanie zagranicznym służbom szerokiego katalogu danych o polskich obywatelach, przy zachowaniu niewielkich środków bezpieczeństwa. Zapewnienia MSWiA o adekwatności pozyskiwanych danych i surowej odpowiedzialności karnej za niezgodne z prawem ich przetwarzanie – przy braku efektywnych mechanizmów kontrolnych – nie brzmią przekonująco.

BEZPIECZEŃSTWO

Ustawa ma przede wszystkim „usprawnić i przyśpieszyć wymianę informacji między organami ścigania państw członkowskich UE w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania przestępczości i jej zwalczania". Ma służyć również wykrywaniu i identyfikacji korzyści pochodzących z przestępstwa. Cele te jednak można realizować, bez większego uszczerbku dla skuteczności działania, przy zapewnieniu zdecydowanie wyższego poziomu kontroli procesu przekazywania danych oraz gwarancji przestrzegania podstawowych praw i wolności. Mimo wprowadzonych w trakcie prac nad ustawą zmian przyjęte rozwiązania są bardzo daleko idące i budzą wątpliwości pod kątem adekwatności i proporcjonalności.

wymieniać się danymi obywateli, nie ograniczając się do niezbędnych przypadków.

2 Istnieje możliwość, że nasze dane zostaną przekazane do miejsc, w których nie zostaną zabezpieczone w odpowiedni sposób oraz będą wykorzystywane niezgodnie z przeznaczeniem. Polskie instytucje nie będą miały odpowiednich narzędzi, by efektywnie kontrolować sposób wykorzystywania danych przekazanych za granicę.

Hak na opozycjonistę

O tym, jakie niebezpieczeństwa może rodzić automatyczne przekazywania danych przez organy ścigania za granicę, mogliśmy się przekonać na przykładzie sprawy udostępnienia przez polską prokuraturę na prośbę Białorusi danych dotyczących kont bankowych białoruskiego działacza Centrum Praw Człowieka „Viasna" Alesia Bielackiego.

Na rachunkach aktywisty zgromadzone były środki przeznaczone na działalność wspierającą prawa człowieka na Białorusi. 4 sierpnia 2011 r. Bielacki został zatrzymany przez białoruskie władze. Działaczowi zarzucono zatajenie dochodów przechowywanych w zagranicznych bankach (m.in. w Polsce, na Litwie). Zdaniem przedstawicieli organizacji pozarządowych do jego aresztowania przyczyniły się informacje bezrefleksyjnie ujawnione Białorusi przez polskie władze.

Ważny problem na marginesie… Pasażerowie pod szczególnym nadzorem

Dane pasażerów lotniczych PNR (*Passenger Name Record*) są to przechowywane przez przewoźników informacje, które wprowadza każdy z nas, rezerwując bilet lotniczy. Najczęściej zawierają imię i nazwisko, datę urodzenia, adres, telefon, e-mail pasażera, trasę podróży, formę płatności za bilet, numer karty kredytowej. Linie lotnicze gromadzą dane PNR na swój własny użytek od lat. Dziś jednak dane te znajdują nowe zastosowanie.

Coraz więcej państw uważa PNR za narzędzie przydatne do walki z międzynarodową przestępczością (przede wszystkim terroryzmem) i nakazuje przewoźnikom udostępnianie ich również organom ścigania. Wszystko dlatego, że z rejestrów PNR można wiele dowiedzieć się o podróżnym, np. o jego stanie zdrowia (gdy prosi o wózek inwalidzki) czy o przekonaniach religijnych (gdy zamawia koszerny posiłek). Posługując się natomiast odpowiednim oprogramowaniem, w kilka sekund można ustalić rutynę podróżowania poszczególnych osób, a nawet powiązania zachodzące pomiędzy konkretnymi osobami (jeśli np. kupują bilet razem, posługują się tym samym numerem karty kredytowej lub telefonu, często latają w to samo miejsce).

Pierwszym krajem, który zaczął korzystać z danych PNR, były Stany Zjednoczone po 11 września 2001 r. W 2004 r. UE podpisała z USA pierwszą umowę, obligującą europejskie linie lotnicze do przekazywania informacji o pasażerach amerykańskiemu Departamentowi Spraw Wewnętrznych. Umowa ta wzbudza szereg wątpliwości, głównie dlatego, że USA powszechnie uznaje się za kraj, w którym standardy

przetwarzania danych osobowych nie odpowiadają gwarancjom obowiązującym w regulacjach europejskich. W dodatku obywatele obcych państw nie są objęci ochroną przewidzianą w amerykańskiej ustawie o prywatności z 1974 r. Zgodnie z dyrektywą o ochronie danych osobowych UE nie powinna przekazywać danych swoich obywateli do państw trzecich o niższym poziomie bezpieczeństwa danych.

Dlatego też obecnie negocjowana jest nowa umowa z USA (a w przyszłości także z innymi krajami), która ma podnieść standardy ochrony prywatności Europejczyków. W dodatku w samej UE trwają też prace nad dyrektywą wprowadzającą europejski rejestr PNR, który umożliwi swobodną wymianę informacji między przewoźnikami a organami ścigania z różnych państw członkowskich.

Pomysł przekazywania danych przez linie lotnicze budzi jednak wiele kontrowersji. Krytycy wskazują, że brakuje obiektywnego dowodu (np. stosownych statystyk) potwierdzającego tezę, iż dane PNR są cenne w zwalczaniu terroryzmu i poważnej międzynarodowej przestępczości. Brakuje kluczowych mechanizmów kontrolnych i gwarancji zapobiegających dalszemu wykorzystywaniu danych w kraju, do którego zostaną przekazane. W kontekście wykorzystywania danych PNR dla celów egzekwowania prawa wątpliwości budzi także wiarygodność gromadzonych informacji, które nie są w żaden sposób weryfikowane przez linie lotnicze. Najbardziej jednak niepokoi pomysł automatycznego profilowania każdego z nas pod kątem oceny ryzyka wystąpienia zagrożenia terrorystycznego.

Podejrzani wegetarianie

Wielka Brytania jest na razie jedynym krajem, w którym wdrożono system przekazywania danych o pasażerach w ramach UE. Przy okazji ujawniono, że brytyjska policja miała w 2009 r. swobodny dostęp do PNR prawie 49 tys. pasażerów. Jak donoszą brytyjskie media, w efekcie „przeskanowania" takiej liczby podróżnych opracowano 14 tys. raportów na temat potencjalnie podejrzanych osób. Pasażerów, którzy – według brytyjskich organów ścigania – mogą stanowić w przyszłości zagrożenie dla bezpieczeństwa państwa, oznaczano czerwonymi flagami.

Aby „zasłużyć" na flagę, wystarczyło zamówić wegetariański posiłek na pokładzie, poprosić o miejsce nad skrzydłem, kupić bilet w jedną stronę czy zamówić rezerwację *last minute*. Naturalnie, podejrzani byli także pasażerowie lecący na Bliski Wschód, do Pakistanu, Afganistanu czy Iraku. Policyjna akcja doprowadziła do aresztowania 2 tys. osób, głównie piłkarskich chuliganów i drobnych przestępców. Udało się zatrzymać także kilka osób poszukiwanych za poważne przestępstwa (morderstwa, gwałty). Nie namierzono jednak żadnego terrorysty.

System informacji medycznej

1 2 3 4 5 6 7

Zachowanie w tajemnicy danych o stanie zdrowia pacjentów jest ważną zasadą, którą akcentuje również Europejski Trybunał Praw Człowieka w Strasburgu, nie tylko ze względu na szacunek dla prywatności pacjenta, ale także zaufanie do lekarzy i służby zdrowia. Trybunał wskazuje, że na państwie ciążą daleko idące „pozytywne obowiązki" w sferze danych objętych tajemnicą lekarską, przede wszystkim w postaci stworzenia odpowiedniego prawa krajowego, zawierającego rozwiązania pozwalające zapobiegać ujawnianiu danych o stanie zdrowia poszczególnych osób.

Fragment listu Fundacji Panoptykon do Prezydenta Bronisława Komorowskiego w sprawie ustawy o systemie informacji w ochronie zdrowia, 9 maja 2011 r.

Wszystkim nam zależy na dobrze działającej i przyjaznej służbie zdrowia. Jednak aby osiągnąć ten cel, nie możemy dbać tylko o łatwy przepływ informacji, ale również o zabezpieczenie prywatności oraz innych praw pacjentów, zaangażowanie zainteresowanych podmiotów w proces wypracowywania propozycji zmian oraz zapewnienie odpowiedniej transparentności przy ich wprowadzaniu w życie.

Ustawa z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, przewidująca stworzenie nowego, zintegrowanego systemu informatycznego, stanowi jeden z kluczowych elementów pakietu, który ma uzdrowić polską służbę zdrowia. W mediach ten element reformy jest zazwyczaj przedstawiany jako mało kontrowersyjny. Tymczasem duża część zaproponowanych rozwiązań może budzić poważne wątpliwości.

W tworzonym systemie znajdą się przede wszystkim dane pacjentów, ale też personelu medycznego, począwszy od pielęgniarek i lekarzy, na administracji szpitali skończywszy. Jednym z podstawowych efektów reformy ma być upowszechnienie prowadzenia dokumentacji medycznej w formie elektronicznej i uruchomienie specjalnej platformy internetowej ułatwiającej korzystanie z usług. Taka wizja informatyzacji służby zdrowia najczęściej pojawia się w mediach, choć w rzeczywistości jej konsekwencje będą dla pacjentów dużo dalej idące.

W systemie przetwarzane będą informacje o osobach korzystających ze świadczeń, m.in. imię, nazwisko, płeć, obywatelstwo, data urodzenia, numer PESEL, numer dokumentu tożsamości, adres, stan cywilny, wykształcenie, informacje o przysługującym ubezpieczeniu i innych uprawnieniach, stopniu niepełnosprawności, a także – i przede wszystkim – tzw. jednostkowe dane medyczne, czyli informacje

o naszych chorobach, zażywanych lekach, wizytach u lekarzy i udzielanych świadczeniach. Znajdą się w nim wszelkie możliwe informacje, które pojawiają się w którymkolwiek z systemów ochrony zdrowia.

Podstawowym założeniem reformy jest integracja tych wszystkich informacji. Chodzi o to, by dane gromadzone dotychczas na użytek konkretnych jednostek służby zdrowia mogły zostać ze sobą powiązane i udostępnione w ramach projektowanego systemu. Co to oznacza? Niestety, ustawa nie daje jednoznacznej odpowiedzi na to pytanie. Ministerstwo Zdrowia podkreśla jednak, że dane medyczne nie będą przechowywane w jednej centralnej bazie danych, ale zawsze w miejscu udzielenia świadczenia.

System ma mieć powszechny charakter – obejmie on nas wszystkich i w żaden sposób nie będzie się można z niego „wypisać". System ma być powiązany z bazą PESEL: nie będzie można korzystać ze świadczeń medycznych „poza systemem". Można będzie natomiast odmówić przetwarzania swoich danych w tzw. rejestrach dziedzinowych, gromadzących m.in. informacje na temat rozmaitych schorzeń.

System będzie miał bardzo złożony charakter. W jego skład wejdzie szereg powiązanych ze sobą baz danych Systemu Informacji Medycznej (który będzie zbierał informacje o wszystkich udzielanych i planowanych świadczeniach) oraz licznych rejestrów (zawierających np. informacje o usługach NFZ, dawcach krwi, chorobach zakaźnych, nowotworach). Jednak precyzyjny kształt systemu nie jest znany. Uchwalana ustawa zakłada bowiem, że do systemu mogą być dołączane nowe rejestry, które będzie mógł tworzyć minister zdrowia. Co może się w nich znaleźć? Ta kwestia pozostaje cały czas otwarta.

Nie jest to jedyne ważne zagadnienie, które nie zostało wyjaśnione na poziomie ustawowym. W ustawie brakuje precyzyjnego określenia kręgu podmiotów, które będą miały dostęp do danych medycznych, oraz podstaw prawnych i zasad, na jakich ma się to odbywać. Nie wiadomo również, w jaki sposób i w jakim zakresie dane objęte systemem będą przetwarzane. Ustawa przewiduje gromadzenie ich w trzech modułach: podstawowym, statystyczno-rozliczeniowym i zleceń. Jednak opis modułów i ich funkcjonalność – a co za tym idzie: podstawowe zasady postępowania z informacjami w nich zawartymi – zostaną uregulowane dopiero w rozporządzeniach.

Wszystko wskazuje na to, że w modelu statystyczno-rozliczeniowym będą przetwarzane informacje dotyczące poszczególnych pacjentów, choć – jak podkreślał w jednym ze swoich pism Generalny Inspektor Ochrony Danych Osobowych – cele statystyczne nie uzasadniają takiego rozwiązania. Ministerstwo Zdrowia odpowiedziało, że wyraz „statystyczny" został użyty w znaczeniu „semantycznym" (!) i „zasady postępowania z informacjami zostaną uregulowane w aktach wykonawczych do projektu ustawy".

Wartości do zważenia

ZDROWIE

Celem wprowadzenia zintegrowanego systemu informacji medycznej jest poprawa funkcjonowania opieki zdrowotnej w Polsce i optymalizacja polityki państwa w tym obszarze. Jeśli stworzony system będzie sprawnie działał, korzystanie z opieki zdrowotnej może być łatwiejsze i wygodniejsze dla pacjentów.

Nie oznacza to jednak, że wprowadzone zmiany bezpośrednio przełożą się na standard leczenia. Obecnie – nie tylko w służbie zdrowia – największym wyzwaniem jest nie tyle dostęp do informacji, co ich selekcja oraz odpowiednie wykorzystanie. Bez odpowiedniego przygotowania lekarzy i systemu pod tym kątem cała reforma może nie przynieść zadowalającego efektu.

„Pytanie, która informacja jest istotna i przydatna, jak jej użyć w konkretnym przypadku – oto wyzwania, przed którymi staje lekarz, który ma – jak obliczono w Europie – średnio 12 minut na pacjenta".

Marek Balicki (Anna Mazgal, *Pacjent obnażony*, 2 sierpnia 2011 r., krytykapolityczna.pl).

PRYWATNOŚĆ

Dane medyczne mają wyjątkowy charakter: należą do grupy tzw. danych wrażliwych, które są szczególnie chronione na gruncie polskiego prawa, a także prawa Unii Europejskiej. Dodatkowo dane medyczne chroni tajemnica lekarska, a także zasady etyki zawodowej lekarzy.

Niewłaściwe przetwarzanie informacji tego typu stwarza szczególne ryzyko dla praw podstawowych, może prowadzić do dyskryminacji (np. stosunkach pracy) i nieodwracalnych szkód. W dodatku dane te mają wymierną wartość rynkową (np. dla firm ubezpieczeniowych), co sprawia, że sektor medyczny jest szczególnie narażony na wycieki i różnego rodzaju nadużycia.

W Polsce już obecnie mamy duży problem z zachowaniem poufności danych medycznych. Przypadki różnego rodzaju nadużyć są niemal codziennym elementem funkcjonowania służby zdrowia. Integracja danych – zwłaszcza dokonana bez dbałości o odpowiedni sposób zabezpieczeń – może wydatnie zwiększyć to ryzyko.

W krajach, w których systemy informacji medycznej zaczęły funkcjonować kilka lat temu, bardzo duża grupa zgłoszeń związanych z naruszeniem standardów ochrony danych osobowych dotyczy służby zdrowia. Raport brytyjskiego Komisarza ds. Informacji (odpowiednika polskiego GIODO) wskazuje, że w Wielkiej Brytanii odsetek ten wynosi ok. 30%.

wanych konstytucyjnie praw i wolności, np. prawa do prywatności.

Ministerstwo Zdrowia szacuje, że roczny poziom oszczędności wynikających z wdrożenia systemu może sięgnąć nawet 5% wydatków. Czas pokaże, czy te założenia uda się zrealizować. Na razie trzeba ponieść wydatki związane z wdrożeniem systemu.

Zgodnie z uzasadnieniem do projektu ustawy koszt uruchomienia dwóch elektronicznych platform służących do wymiany danych w ramach systemu szacuje się na prawie 770 mln zł, a koszt ich rocznej eksploatacji – na ponad 80 mln zł.

FINANSE PUBLICZNE

Jednym z podstawowych celów projektu jest optymalizacja nakładów i szczelne gospodarowanie środkami publicznymi. To bardzo ważny cel, choć trzeba pamiętać, że zgodnie z polską Konstytucją (art. 31) dbałość o finanse publiczne ani efektywność zarządzania nie może samoistnie uzasadniać ograniczenia gwaranto-

W CZYM PROBLEM?

1 Ustawa, która ma stanowić ramy dla tworzonego systemu, jest niezwykle lakoniczna i ogólnikowa, co kontrastuje z wagą i poziomem skomplikowania całego przedsięwzięcia. Uzasadnienie projektu jest napisane hermetycznym językiem i nie odnosi się do kluczowych problemów. Nie wiadomo, jak naprawdę system będzie działał. Sam proces jego tworzenia również trudno uznać za transparentny. Nie przesądza to o końcowym fiasku przedsięwzięcia, ale sprawia, że najważniejsze decyzje są podejmowane poza kontrolą demokratyczną.

2 Ustawa ta nie stwarza wystarczających gwarancji dla ochrony prywatności pacjentów. Nie określa w sposób precyzyjny zasad przetwarzania danych o pacjentach w systemie ani tego, kto i na jakiej podstawie będzie miał do nich dostęp. W wielu kluczowych miejscach odsyła do rozporządzeń, co stoi w sprzeczności z zasadą, że dane osobowe nie mogą być przetwarzane bez podstawy ustawowej (art. 51 ust. 1 Konstytucji). Stawia to pod znakiem zapytania konstytucyjność przyjętych rozwiązań.

3 W ramach prac nad ustawą nie przedstawiono żadnych analiz wpływu proponowanych regulacji na prawa pacjentów, co w przypadku tworzenia systemu generującego tak wiele ryzyk i operującego na bardzo wrażliwych danych wydaje się niezbędne. Można mieć w związku z tym wątpliwości, czy zakres informacji, jakie mają być gromadzone w systemie, jest niezbędny i adekwatny do realizowanego celu oraz czy poziom planowanych zabezpieczeń jest odpowiedni do zagrożeń. Nie przeanalizowano również alternatywnych rozwiązań, które mogłyby realizować zbliżone cele, stwarzając jednocześnie lepsze gwarancje ochrony praw pacjentów.

4 Tworzenie i wdrażanie systemu ma się odbywać na poziomie centralnym, pod kierownictwem Ministerstwa Zdrowia. Nie ma zatem mowy o stopniowym integrowaniu części w większą całość. Jest to rozwiązanie bardziej ryzykowne, ponieważ wymaga większych przygotowań, a każde niepowodzenie rodzi więcej komplikacji niż w przypadku systemu budowanego oddolnie, w sposób rozproszony.

Dwie ścieżki informatyzacji

We Francji i Danii wybrano odmienne sposoby tworzenia systemów informacji medycznej. W Danii z sukcesem budowano go „z dołu do góry": najpierw – w oparciu o oczekiwania zaangażowanych podmiotów – tworzono pojedyncze systemy w mniejszej skali, a po przetestowaniu standaryzowano je na poziomie krajowym. Ten przypadek kontrastuje z sytuacją we Francji, gdzie wybrano podejście centralistyczne. System nie zyskał zaufania użytkowników, a jego wdrażanie skończyło się porażką (Wiktor Górecki, *Przestroga znad Sekwany*, „Menedżer Zdrowia" 7/2009 i *Primum participare*, „Menedżer Zdrowia" 5/2010).

5 W tworzenie ustawy i samego systemu nie zaangażowano w dostatecznym zakresie społeczeństwa obywatelskiego i podmiotów, które będą miały wpływ na jego funkcjonowanie. Na zgłaszanie uwag w konsultacjach społecznych przewidziano tydzień, co w przypadku tak ważnego i skomplikowanego projektu świadczy o zupełnym lekceważeniu głosu zainteresowanych podmiotów.

6 Tworzeniu systemu i związanych z nim przepisów nie towarzyszy właściwie żadna debata publiczna, a co za tym idzie – pacjenci nie tylko nie mają wpływu na to, w jakim systemie będą się leczyć, ale nie mają nawet wiedzy na temat wprowadzanych zmian. Poważna dyskusja nie pojawiła się ani w mediach, ani w parlamencie w trakcie prac nad ustawą. Tymczasem w wielu krajach systemy informacji w ochronie zdrowia napotkały na ostry opór społeczny, często także ze strony środowiska lekarskiego.

A może osobiste USB dla każdego pacjenta?

W Niemczech w 2008 r. przeciw wprowadzeniu odpowiednika polskiego systemu informacji medycznej ostro zaprotestowało jedno ze stowarzyszeń lekarskich (NAV Virchow Bund). Niemieccy lekarze wezwali rząd do zaprzestania prac nad publicznym rejestrem zdrowia, wskazując na zagrożenia dla poufności danych. Jako alternatywę dla scentralizowanego systemu stowarzyszenie zaproponowało wprowadzenie specjalnych dysków przenośnych USB z zakodowanymi danymi medycznymi, które każdy pacjent nosiłby przy sobie.

JAKIE TO RODZI ZAGROŻENIA?

1 Integracja danych medycznych wymaga dużego zaufania do państwa. Możliwość poznania za pomocą „jednego kliknięcia" całej historii korzystania ze służby zdrowia, a zatem informacji niekiedy bardzo wrażliwych, daje instytucjom publicznym niezwykłe narzędzie władzy nad obywatelem. Bez odpowiednich zabezpieczeń ochrony danych oraz gwarancji transparentności istnieje zagrożenie, że władza ta będzie nadużywana.

2 Dane medyczne są niezwykle cenne dla wielu podmiotów (np. pracodawców, firm ubezpieczeniowych), dlatego są szczególnie wrażliwe na różnego rodzaju nadużycia. Trzeba zdawać sobie sprawę z tego, że nie ma niezawodnych zabezpieczeń, jednak bez prawa, które w sposób jasny ustala standardy technologiczne i zasady dostępu do danych, ryzyko wszelkiego rodzaju wycieków wyraźnie wzrasta.

3 Pośpiech, brak refleksji nad alternatywnymi rozwiązaniami i konsekwencjami wdrożenia systemu w obecnym kształcie oraz lekceważenie głosów krytyki może prowadzić do sytuacji, w której system nie tylko nie będzie spełniał standardów bezpieczeństwa, ale będzie również niefunkcjonalny i nieprzejrzysty. To może skutkować brakiem zaufania i akceptacji użytkowników systemu i w efekcie doprowadzić do fiaska całego projektu.

Pod lupą ABW

Zgodnie z art. 9 ustawy o systemie informacji w ochronie zdrowia funkcjonalności elektronicznych platform umożliwiających wymianę danych w ramach systemu określić ma w drodze rozporządzenia minister zdrowia po zasięgnięciu opinii szefów Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu.

Mają one bowiem spełniać wymogi umożliwiające realizację ustawowch zadań tych służb. Analogiczne przepisy wprowadzane są również w innych tworzonych bądź nowelizowanych ustawach, które dotyczą różnych publicznych baz danych (np. w nowelizacji ustawy o dowodach osobistych z 9 czerwca 2011 r.).

System informacji oświatowej

1 2 3 4 5 6 7

Katalog danych, które mają być przetwarzane i przez wiele lat przechowywane w systemie, jest bardzo szeroki. Co więcej, obejmuje on swym zakresem również dane wrażliwe (dotyczące np. niepełnosprawności czy korzystania z pomocy psychologicznej). Integracja na poziomie centralnym tak szerokiego zakresu danych jednostkowych będzie stanowić daleko idącą ingerencję w konstytucyjnie chronione prawa i wolności. Dlatego powinna ona zostać poddana wnikliwej ocenie pod katem spełniania wymogów przewidzianych w art. 31 ust. 3 Konstytucji, przede wszystkim wymogu konieczności w demokratycznym państwie. W naszej opinii przyjęte rozwiązania trudno uznać za niezbędne, realizacja celów ustawy jest bowiem możliwa przy zastosowaniu środków mniej ingerujących w prawa i wolności jednostek.

Fragment apelu Fundacji Panoptykon, Fundacji Rodzice Szkole, Stowarzyszenia Projekt: Polska, Społecznego Monitora Edukacji oraz Stowarzyszenia Rzecznik Praw Rodziców skierowanego do Prezydenta Bronisława Komorowskiego w sprawie ustawy o systemie informacji oświatowej, 17 maja 2011 r.

Przykład SIO pokazuje, jak przekonanie o przydatności zbierania danych jednostkowych w każdym możliwym przypadku zamyka oczy zarówno na ryzyka, jak i alternatywne rozwiązania. Niestety, zagrożenia związane z funkcjonowaniem nowego systemu mogą przeważyć na ewentualnymi korzyściami.

Nowy System Informacji Oświatowej zastąpić ma dotychczasowy system funkcjonujący od 1 stycznia 2005 r. Konieczność reformy wynika z zastrzeżeń wobec działania starego SIO. Obecnie wszystkie szkoły i inne placówki przygotowują zestawienia zbiorcze dotyczące uczniów, które nie zawierają danych osobowych, a jedynie informacje, ilu z nich charakteryzuje się daną cechą, np. ile dziewczynek i ilu chłopców uczęszcza do danej szkoły, ile osób wybrało dany profil kształcenia i ile uzyskało na egzaminie daną ocenę. Wszystkie te informacje trafiają następnie do SIO, dzięki czemu można stworzyć odpowiednie statystyki dla całego kraju.

Dane te stanowią podstawę dla prowadzenia polityki oświatowej państwa, w tym wydatkowania środków finansowych. Problem polega na tym, że zebrane dane nie zawsze są kompletne i rzetelne. Skomplikowany sposób ich agregacji, który polega na ich wielostopniowym scalaniu przez instytucje różnego szczebla, generuje wiele błędów. Co więcej, brakuje mechanizmów weryfikacji, czy wszystkie szkoły w sposób właściwy skompletowały wymagane dane oraz czy dostarczyły do SIO zestawienia zbiorcze.

Nowa ustawa o systemie informacji oświatowej (uchwalona 15 kwietnia 2011 r.) ma być odpowiedzią na te problemy. Najważniejsza zmiana polega na tym, że zamiast danych zbiorczych mają być zbierane tzw. dane jednostkowe, dotyczące poszczególnych przedszkolaków i uczniów. System ma również umożliwiać ich weryfikację z zewnętrznymi bazami danych (np. PESEL), przez co ma zapobiegać pomyłkom i oszustwom.

Katalog danych gromadzonych w systemie ma być bardzo szeroki. Poza imieniem, nazwiskiem i numerem PESEL, czyli danymi służącymi identyfikacji, do SIO trafi długa lista informacji związanych – czasem dość luźno – z korzystaniem z systemu oświaty: od miejsca zamieszkania przez dane o uczestnictwie w zajęciach dodatkowych, wynikach egzaminów, korzystaniu z pomocy materialnej po informacje o wypadkach na terenie szkoły czy uzyskaniu karty rowerowej. Wśród informacji zbieranych w SIO znajdą się również dane wrażliwe, dotyczące np. rodzaju niepełnosprawności, korzystania z poradni psychologiczno-pedagogicznej i rodzaju wystawionej diagnozy, korzystania z zajęć socjoterapii, psychoterapii czy terapii dla zagrożonych uzależnieniem.

Wszystkie te dane trafią do centralnej bazy prowadzonej przez Ministerstwo Edukacji Narodowej. Będą one zbierane przez całą ścieżkę edukacyjną: od przedszkola aż do przyjęcia na studia. W praktyce oznacza to, że każda osoba korzystająca z systemu oświaty będzie miała w SIO swój szczegółowy profil, w którym przez kilkanaście lat będą zbierane setki rozmaitych związanych z nią informacji.

Już obecnym systemie gromadzone są dane jednostkowe nauczycieli, jednak w nowym SIO ich zakres zostanie poszerzony. Nauczyciele mają być identyfikowani za pomocą imienia, nazwiska i numeru PESEL, a nie – jak dotychczas – jedynie numeru PESEL. Nowy SIO obejmie 5 milionów uczniów, około 900 tysięcy przedszkolaków, a także 600 tysięcy słuchaczy i ponad 600 tysięcy nauczycieli. Poza danymi o uczniach i nauczycie-

> **Wprowadzenie do bazy informacji oświatowych danych tak wrażliwych o dziecku jak: rodzaj niepełnosprawności, zagrożenie niedostosowaniem społecznym czy objęcie pomocą psychologiczno-pedagogiczną (...) spowoduje naznaczenie dziecka określoną etykietą wartościującą, która w konsekwencji zdeterminuje sposób traktowania go na dalszych szczeblach edukacji.**
>
> **Fragment pisma Polskiego Towarzystwa Psychologicznego do przewodniczącego sejmowej Komisji Edukacji, Nauki i Młodzieży, 3 marca 2011 r.**

lach system będzie zbierał również informacje o szkołach i innych placówkach oświatowych. Będzie on obejmował centralną bazę danych SIO (na poziomie MEN) oraz lokalne bazy danych SIO (na poziomie poszczególnych placówek).

Większość danych ucznia zgromadzonych w centralnej bazie SIO ma być anonimizowana po upływie 5 lat od dnia wprowadzenia do tego zbioru ostatniej informacji, czyli 5 lat po ukończeniu ostatniej szkoły bądź rozpoczęciu studiów. Natomiast dane nauczycieli mają być anonimizowane po 10 latach od wprowadzenia do systemu ostatniej informacji. Oznacza to, że dane raz umieszczone w bazie prowadzonej przez MEN nigdy z niej nie znikną, tylko po pewnym czasie zostaną oderwane od imion, nazwisk i numerów PESEL. Dane gromadzone w lokalnych bazach danych SIO mają być po upływie 5-letniego okresu usuwane, chyba że na dalsze ich przechowywanie zgodę na piśmie wyrazi pełnoletni uczeń (wcześniej jego rodzice) albo nauczyciel.

W CZYM PROBLEM?

1 Integrowanie szerokiego katalogu informacji o uczniach i nauczycielach, w tym danych wrażliwych, oznacza daleko idącą ingerencję w prywatność jednostek. Proponowane rozwiązanie powinno zatem przejść test konieczności i proporcjonalności w demokratycznym państwie. Jego potencjalna przydatność czy wygoda dla władzy nie może być wystarczającym usprawiedliwieniem. Niestety, w uzasadnieniu ustawy oraz w wypowiedziach przedstawicieli MEN brakuje argumentów, które uzasadniałyby taką ingerencję.

Sprawne zarządzanie oświatą nie wymaga integrowania na poziomie centralnym tak szerokiego zakresu danych poszczególnych uczniów i nauczycieli. Do realizacji tego celu wystarczające są dane zbiorcze, ewentualnie wykorzystanie danych jednostkowych w bardzo podstawowym zakresie. Zamiast uciekać się do zbierania szerokiego katalogu danych indywidualnych, można uszczelnić system za pomocą metod prostszych, a jednocześnie skuteczniejszych, poprzez np. rezygnację z wielostopniowego systemu integracji danych, zapewnienie systemu kontroli wprowadzania danych do systemu oraz szkoleń dla pracowników.

Art. 31 Konstytucji

1. Wolność człowieka podlega ochronie prawnej.
2. Każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje.
3. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Wartości do zważenia

PRAWO DO NAUKI

Polska Konstytucja gwarantuje prawo do nauki (art. 70 ust. 1). Dążenie do jego realizacji może w określonych sytuacjach usprawiedliwiać ograniczenia innych praw przysługujących jednostkom, co znajduje wyraz chociażby w obowiązku szkolnym.

Realizacja prawa do nauki nie jest bezpośrednim celem ustawy o systemie informacji oświatowej, jednak niektóre z zaproponowanych rozwiązań mogą wpływać na realizację tego prawa pośrednio.

PRYWATNOŚĆ

Integracja szerokiego zakresu danych o uczniach i nauczycielach nieuchronnie prowadzić będzie do ograniczania ich prawa do prywatności i autonomii informacyjnej. Kluczowe pytanie dotyczy tego, na ile ta ingerencja jest uzasadniona, a na ile zamierzone cele można uzyskać za pomocą mniej ingerujących w prywatność metod.

W dyskusji na temat SIO pojawia się argument, że skoro pewne informacje są już teraz zbierane przez szkoły, przekazanie ich ministerstwu nie wpłynie na poziom ochrony prywatności. Nic bardziej mylnego. Sytuacja jednostki wygląda zupełnie inaczej, gdy informacje o niej są rozproszone, tak że w posiadaniu poszczególnych podmiotów znajduje się ich wąski zakres, a inaczej – gdy zostają zgromadzone w jednym miejscu i stają się dostępne za pomocą „jednego kliknięcia".

Co więcej, adekwatność proponowanych rozwiązań należy oceniać zawsze z punktu widzenia celu, który ma zostać osiągnięty. Cały szereg informacji o uczniu jest niezbędny kadrze pedagogicznej po to, by otoczyć go właściwą opieką, a zupełnie niepotrzebny ministerstwu.

FINANSE PUBLICZNE

Dyscyplina finansowa i sprawne zarządzanie sektorem oświaty są podstawowymi celami, które przyświecają ustawie o systemie informacji oświatowej. Cel finansowy nie może być jednak samoistnym usprawiedliwieniem dla wprowadzania ograniczeń gwarantowanych konstytucyjnie praw i wolności.

Kluczowe pytanie sprowadza się do tego, na ile ewentualne usprawnienia w zarządzaniu oświatą przełożą się na realizację celów usprawiedliwiających takie ograniczenia (np. prawa do nauki) i czy ich osiągnięcie nie jest możliwe za pomocą środków mniej ingerujących w podstawowe prawa i wolności.

2 Analiza zaproponowanych rozwiązań prowadzi do wniosku, że skalę integrowanych danych (w tym gromadzenie danych wrażliwych) i czas ich przechowywania trudno uznać za adekwatne w stosunku do celów regulacji. Szczególne wątpliwości budzi idea zachowywania w centralnej bazie danych wszystkich wprowadzonych informacji. Ich charakter oraz szeroki zakres umożliwi tworzenie bardzo charakterystycznych profili jednostkowych, których anonimizacja może okazać się nieskuteczna. Wszystko to budzi wątpliwości co do konstytucyjności wdrażanych rozwiązań, przede wszystkim jeśli chodzi o poszanowanie prywatności (art. 47) oraz autonomii informacyjnej jednostki (art. 51).

3 W trakcie prac nad ustawą zabrakło realnej i poważnej dyskusji na temat zasadności proponowanych rozwiązań oraz możliwości wprowadzenia rozwiązań alternatywnych. Zlecone w trakcie prac analizy Biura Analiz Sejmowych albo nie odnosiły się do istoty problemu, albo ich sens został wypaczony w trakcie parlamentarnej dyskusji.

JAKIE TO RODZI ZAGROŻENIA?

1 Wdrożenie nowego SIO znacząco zmieni pozycję jednostki wobec państwa. W jednym miejscu zostanie zgromadzony gigantyczny zestaw informacji (również tych wrażliwych) na temat milionów Polaków. Nie znaczy to oczywiście, że dane te muszą zostać użyte niezgodnie z przeznaczeniem, ale zagrożenie nadużyciami władzy ze strony państwa wobec swoich obywateli będzie realne.

2 Zebranie tak szerokiego zakresu danych w jednym miejscu stwarza wysokie ryzyko wycieków. Bezpieczeństwo danych zależy oczywiście od przyjętych gwarancji prawnych i rozwiązań technologicznych, jednak – jak pokazuje doświadczenie – za licznymi nadużyciami stoją użytkownicy systemu. Biorąc pod uwagę skalę integrowanych danych oraz fakt, że dostęp do systemu będzie bardzo szeroki, trudno wykluczyć potencjalne nadużycia, zwłaszcza że dane te będą miały bardzo wymierną wartość dla wielu podmiotów.

3 Integrowanie wrażliwych informacji dotyczących niepełnosprawności czy objęcia pomocą psychologiczno-pedagogiczną niezwykle głęboko ingeruje w prywatność, a jednocześnie stwarza zagrożenie dyskryminacją. Zwiększa bowiem ryzyko stygmatyzacji uczniów z problemami, może również prowadzić do sytuacji, w której rodzice w obawie przed negatywnymi konsekwencjami dla swoich dzieci będą unikać szukania dla nich pomocy psychologicznej.

4 Istnieje ryzyko, że raz stworzony system będzie podlegać przeobrażeniom. W przyszłości może się pojawić pokusa, by zbierać

więcej informacji, na szerszą skalę łączyć je ze sobą czy wykorzystać zebrane dane do nowych, nieplanowanych pierwotnie celów. Może się okazać, że za kilka lat w SIO będzie gromadzony jeszcze szerszy zakres danych niż obecnie (np. e-dzienniki), że do dostępu do nich zostanie upoważniony szerszy krąg osób (np. podmioty komercyjne) albo że z SIO zostaną zintegrowane kolejne bazy danych (np. uniwersyteckie).

SIO w Trybunale Konstytucyjnym

14 lipca 2011 r. grupa posłów Prawa i Sprawiedliwości złożyła do Trybunału Konstytucyjnego wniosek o stwierdzenie niezgodności z Konstytucją art. 14 i 18 ustawy o systemie informacji oświatowej (sygnatura K 26/11), zgodnie z którymi informacja o objęciu ucznia pomocą psychologiczno-pedagogiczną organizowaną przez szkołę oraz formy tej pomocy należą do tzw. danych dziedzinowych, które mają być gromadzone w systemie. Wnioskodawcy podkreślają, że tego typu dane są informacjami ściśle prywatnymi o wyjątkowym stopniu wrażliwości, które znajdują się pod szczególną ochroną konstytucyjną prawa do prywatności i związanego z nim prawa do autonomii informacyjnej jednostki.

Aneks

1 2 3 4 5 6 7

Temat	Akty prawne	Etap legislacyjny	Najważniejsze założenia	Głos Fundacji Panoptykon
Reforma ochrony prywatności	▪ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych	4 listopada 2010 r. Komisja Europejska ogłosiła komunikat *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej* zapowiadający nowelizację dotychczasowej dyrektywy. Zakończyła się faza konsultacji komunikatu. Na początku 2012 r. Komisja ma przedstawić projekt nowych regulacji.	Nowelizacja dyrektywy ma na celu harmonizację standardów bezpieczeństwa danych osobowych we wszystkich państwach UE, a także dostosowanie zasad ochrony prywatności do nowych zjawisk i wyzwań, związanych przede wszystkim z rozwojem nowoczesnych technologii (Internet, przetwarzanie danych genetycznych). Rewizja dyrektywy ma dotyczyć również przepisów w obszarze współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych (kontrola nad środkami inwigilacji obywateli przez organy ścigania i służby specjalne).	▪ Oficjalne wystąpienia, m.in. stanowisko w konsultacjach *Całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej*; uwagi Fundacji Panoptykon i Helsińskiej Fundacji Praw Człowieka do stanowiska polskiego Rządu wobec komunikatu Komisji; ▪ udział w konferencjach i dyskusjach, m.in. konferencji „Reforma ochrony prywatności" i kolejnych konferencjach tematycznych: „Ochrona danych osobowych w prawie pracy i w prawie ubezpieczeń społecznych – stan obecny i perspektywy zmian", „Bezpieczeństwo w Internecie"; ▪ teksty publikowane na stronie internetowej (np. *Co się zmieni w ustawie o ochronie danych osobowych*) i wypowiedzi dla mediów.
	▪ Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r. Nr 133 poz. 883) ➔ **Ustawa z 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych** (Dz.U. z 2010 r. Nr 229 poz. 1497)	Nowelizacja ustawy weszła w życie 7 marca 2011 r.	Ustawa o ochronie danych osobowych wdrożyła postanowienia dyrektywy do polskiego porządku prawnego. Zmiany wprowadzone nowelizacją z 2010 r. nie są przełomowe, odnoszą się głównie do uprawnień Generalnego Inspektora Ochrony Danych Osobowych. Nowelizacja upoważnia go do: 1) stosowania tzw. grzywny w celu przymuszenia; 2) kierowania „wystąpień" do administratorów danych, u których kontrola ujawniła nieprawidłowości; 3) występowania z wnioskami o podjęcie inicjatywy legislacyjnej do właściwych organów; 4) tworzenia biur zamiejscowych. Nowelizacja wprowadza ponadto nowy rodzaj przestępstwa – udaremnianie lub utrudnianie prowadzonej kontroli GIODO. Wprowadzone zmiany nie odpowiadają na największe obecnie wyzwania w zakresie ochrony danych osobowych. GIODO zapowiedział rozpoczęcie prac nad głębszą reformą prawa ochrony danych osobowych w Polsce.	
Retencja danych telekomunikacyjnych	▪ Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE	Trwa proces rewizji i przygotowania nowych rozwiązań prawnych.	Dyrektywa wprowadza obowiązek przechowywania przez operatorów we wszystkich krajach UE informacji o połączeniach telekomunikacyjnych przez okres od pół roku do dwóch lat i udostępniania ich instytucjom publicznym w celu ścigania najpoważniejszych przestępstw, przede wszystkim terroryzmu. Komisja Europejska przedstawiła krytyczny raport dotyczący wdrożenia dyrektywy w państwach członkowskich.	▪ Oficjalne wystąpienia, m.in. stanowisko Fundacji Panoptykon i Helsińskiej Fundacji Praw Człowieka dotyczące ewaluacji dyrektywy przekazane posłom Parlamentu Europejskiego; ▪ badanie skali korzystania z retencji przez poszczególne służby za pomocą wniosków o dostęp do informacji publicznej; uzyskanie od UKE danych statystycznych dotyczących retencji, które stały się podstawą dla publikacji artykułu Ewy Siedleckiej *Milion billingów* („Gazeta Wyborcza", 9 listopada 2010 r.). ▪ udział w licznych konferencjach i dyskusjach, m.in. debacie „Bilingi, inwigilacja, interes publiczny" zorganizowanej przez RPO, dyskusji panelowej „Retencja danych w demokratycznym państwie prawnym" zorganizowanej przez GIODO w ramach polskich obchodów Dnia Ochrony Danych Osobowych, konferencji „Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli?" zorganizowanej przez Naczelną Radę Adwokacką; ▪ liczne teksty, opracowania, komentarze i raporty publikowane na stronie internetowej; ▪ artykuły prasowe (np. Katarzyna Szymielewicz, *Gorący spór o prywatność danych*, „Rzeczpospolita", 22 kwietnia 2011 r.), wywiady (np. *Kto ograniczy zaglądanie w billingi?*, „Gazeta Wyborcza", 19 kwietnia 2011 r.) i wypowiedzi dla mediów.
	▪ Ustawa z 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz.U. z 2009 r. Nr 85 poz. 716) ➔ **Projekt ustawy o zmianie ustawy – Prawo telekomunikacyjne niektórych innych ustaw**	Ministerstwo Infrastruktury zakończyło konsultacje projektu nowelizacji ustawy.	Nowelizacja Prawa telekomunikacyjnego wdrażająca do polskiego porządku prawnego postanowienia dyrektywy wykroczyła poza jej założenia, dając wielu organom bardzo szeroki i niekontrolowany dostęp do danych retencyjnych. W Polsce czas obowiązkowej retencji wynosi dwa lata. Dane mogą być wykorzystywane w sprawach cywilnych, do ścigania wszystkich rodzajów przestępstw i w szeroko pojętych celach prewencyjnych. Są one udostępniane służbom bez kontroli sądowej. Projekt nowelizacji ustawy zakłada ograniczenie możliwości korzystania z danych retencyjnych przez sądy cywilne. Nad przygotowaniem dalej idących zmian pracuje zespół pod kierownictwem Sekretarza Kolegium ds. Służb Specjalnych. Grupa posłów i – niezależnie – Rzecznik Praw Obywatelskich zgłosili do Trybunału Konstytucyjnego wnioski o stwierdzenie niezgodności przepisów dotyczących retencji danych z Konstytucją (więcej na ten temat w części: *Retencja i dostęp służb do danych telekomunikacyjnych*).	

Temat	Akty prawne	Etap legislacyjny	Najważniejsze założenia	Głos Fundacji Panoptykon
System informacji oświatowej	➔ **Ustawa z 15 kwietnia 2011 r. o systemie informacji oświatowej** (Dz.U. z 2011 r. Nr 139 poz. 814)	Ustawa wchodzi w życie 30 kwietnia 2012 r.	W Systemie Informacji Oświatowej od przedszkola aż do przyjęcia na studia będą gromadzone dane dotyczące każdego z polskich uczniów. Katalog gromadzonych danych ma być bardzo szeroki i obejmować także dane wrażliwe dotyczące np. korzystania z pomocy psychologiczno-pedagogicznej. System ma ułatwić bardziej efektywne zarządzanie oświatą. Grupa posłów zgłosiła do TK wniosek o stwierdzenie niezgodności części przepisów ustawy z Konstytucją (więcej na ten temat w części: *System informacji oświatowej*).	▪ Oficjalne wystąpienia, m.in. stanowisko skierowane do posłów komisji sejmowych; apel Fundacji Panoptykon i Stowarzyszenia Projekt: Polska do senatorów o odrzucenia ustawy; apel Fundacji Panoptykon, Fundacji Rodzice Szkole, Stowarzyszenia Projekt: Polska, Społecznego Monitora Edukacji oraz Stowarzyszenia Rzecznik Praw Rodziców do Prezydenta o skierowanie ustawy do TK; ▪ teksty i analizy publikowane na stronie internetowej; ▪ artykuły prasowe (np. Małgorzata Szumańska, *System inwigilacji oświatowej?*, „Rzeczpospolita", 13 maja 2011 r.) i wypowiedzi dla mediów.
System informacji medycznej	➔ **Ustawa z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia** (Dz.U. z 2011 r. Nr 113 poz. 657)	Ustawa wchodzi w życie 1 stycznia 2012 r. Niektóre z kluczowych przepisów, warunkujące pełną funkcjonalność systemu, zaczną obowiązywać 1 sierpnia 2014 r.	Ustawa przewiduje wprowadzenie jednego z największych systemów publicznych baz danych w Polsce. Będzie on zawierał dane medyczne, które są danymi wrażliwymi, podlegającymi szczególnej ochronie. Przyjęta ustawa jest bardzo lakoniczna i nie określa w sposób precyzyjny zasad postępowania z danymi przetwarzanymi w systemie. Wiele kluczowych kwestii rozstrzygnie się dopiero na poziomie rozporządzeń (więcej na ten temat w części: *System informacji medycznej*).	▪ Oficjalne wystąpienia, m.in. apel do prezydenta o skierowanie ustawy do TK; ▪ teksty publikowane na stronie internetowej; ▪ artykuły publicystyczne (np. Anna Mazgal, *Pacjent obnażony*, 2 sierpnia 2011 r., krytykapolityczna.pl) i wypowiedzi dla mediów.
Monitoring wizyjny w zakładach karnych i aresztach śledczych	➔ **Ustawa z 5 stycznia 2011 r. o zmianie ustawy – Kodeks karny wykonawczy** (Dz.U. z 2011 r. Nr 39 poz. 201)	Nowelizacja ustawy weszła w życie 25 marca 2011 r.	Nowelizacja rozszerza zasady stosowania monitoringu wizyjnego w zakładach karnych na nową kategorię osadzonych – zagrożonych ze względu na ważną rolę, jaką mogą odegrać w procesie sądowym.	▪ Teksty publikowane na stronie internetowej (np. *Jeszcze więcej kamer w celach? Analiza nowelizacji k.k.w.*).
Blokowanie stron internetowych	➔ **Projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, uchylającej decyzję ramową 2004/68/WSiSW**	Projekt dyrektywy został przygotowany. Trwają ostatnie uzgodnienia dotyczące jego treści.	UE pracuje nad dyrektywą mającą służyć lepszej ochronie dzieci, przede wszystkim walce z tzw. pornografią dziecięcą. Duże wątpliwości wzbudzają jednak rozwiązania, które przewidują blokowanie stron internetowych zawierających tego typu treści. Obowiązkowe stosowanie tego narzędzia przez państwa członkowskie nie pomoże uporać się z zabronionymi treściami w sieci, a wymaga stworzenia infrastruktury monitorującej ruch w Internecie, która wywrze duży wpływ nie tylko na jego funkcjonowanie, ale również respektowanie prawa do prywatności użytkowników.	▪ Oficjalne wystąpienia, m.in. apel do premiera wzywający do odrzucenia przez Polskę propozycji blokowania stron internetowych; ▪ organizacja debaty „Blokowanie stron internetowych – rok po: początek cenzury czy odpowiedź na realne zagrożenia?" pod patronatem RPO; ▪ teksty, opracowania, komentarze publikowane na stronie internetowej; ▪ artykuły prasowe (np. Katarzyna Szymielewicz, Józef Halberszstadt, Jakub Śpiewak, *Blokowaniew internecie – to nie działa!*, „Gazeta Wyborcza", 25 lipca 2011 r.) i wypowiedzi dla mediów.
Odpowiedzialność pośredników za treści w Internecie	▪ Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) ▪ Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. Nr 144 poz. 1204 z późn. zm.) ➔ **Projekt ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną**	Planowana jest rewizja dyrektywy. Zakończyły się konsultacje służące wypracowaniu jej założeń. Planowana jest nowelizacja ustawy. Założenia nowelizacji zostały przyjęte przez Radę Ministrów. Projekt ustawy nie trafił jednak do Sejmu.	Dyrektywa oraz implementująca ją ustawa zawierają reguły odpowiedzialności tzw. pośredników za treści umieszczane przez użytkowników w Internecie. Polskie przepisy z jednej strony nie zapewniają realizacji praw osób, których prawa zostały naruszone w sieci, a z drugiej – stawiają pośredników roli „prywatnych cenzorów", stwarzając w ten sposób zagrożenie dla wolności słowa (niebezpieczeństwo automatycznego blokowania wszystkich kontrowersyjnych treści). Projekt nowelizacji ustawy służyć ma doprecyzowaniu procedury usuwania treści i zmniejszeniu niepewności prawnej z tym związanej.	▪ Oficjalne wystąpienia, m.in. uwagi w ramach konsultacji społecznych do projektu założeń nowelizacji ustawy o świadczeniu usług drogą elektroniczną; uwagi w procesie konsultacji społecznych na temat przyszłości handlu elektronicznego w ramach wspólnego rynku oraz implementacji dyrektywy o handlu elektronicznym; ▪ teksty publikowane na stronie internetowej i wypowiedzi dla mediów.

Temat	Akty prawne	Etap legislacyjny	Najważniejsze założenia	Głos Fundacji Panoptykon
Kontrola nad działaniami operacyjnymi służb	➔ **Ustawa z 4 lutego 2011 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw** (Dz.U. z 2011 r. Nr 53 poz. 273)	Nowelizacja ustawy weszła w życie 11 czerwca 2011 r.	Nowelizacja wprowadza większą kontrolę nad czynnościami operacyjnymi. Jej główne założenia to: 1) jawność statystyk dotyczących stosowania kontroli operacyjnej; 2) dopuszczalność prowadzenia kontroli operacyjnej tylko w postępowaniu karnym i tylko w sprawie o przestępstwa (także skarbowe) wymienione w zawartym w ustawie katalogu; 3) obowiązek uzasadniania wniosku o stosowanie kontroli przez policję; 4) uregulowanie instytucji zgody następczej sądu na zastosowanie kontroli operacyjnej; 5) obowiązek zniszczenia materiałów pochodzących z kontroli po jej zakończeniu.	▪ Teksty publikowane na stronie internetowej (np. *Większa kontrola nad czynnościami operacyjnymi – wchodzi w życie nowela k.p.k.*)
Przekazywanie informacji między służbami różnych państw	➔ **Ustawa z 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej**	Ustawa czeka na podpis prezydenta.	Ustawa umożliwia przekazywanie danych polskich obywateli za granicę bez względu na rodzaj przestępstwa, z którym ma to związek, oraz bez obowiązku weryfikacji sposobu wykorzystania przekazanych danych. Nie ogranicza także kręgu podmiotów, które mogą żądać przekazania informacji do organów ścigania innych państw UE, ale włącza w jego zakres także np. Interpol (więcej na ten temat w części: *Wymiana informacji między organami ścigania*).	▪ Oficjalne wystąpienia, m.in. opinia skierowana do MSWiA; ▪ teksty publikowane na stronie internetowej (np. *Przekazywanie danych organom ścigania innych państw UE. Jakie zagrożenia niesie ze sobą nowy projekt MSWiA?*) i wypowiedzi dla mediów.
Bezpieczeństwo w trakcie EURO 2012	➔ **Ustawa z 31 sierpnia 2011 r. o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw**	Ustawa podpisana przez prezydenta 20 września 2011 r. Większość przepisów wchodzi w życie po upływie 30 dni od dnia ogłoszenia.	Ustawa przewiduje wprowadzenie szeregu środków mających poprawić bezpieczeństwo w czasie trwania turnieju finałowego EURO 2012 (choć niektóre z uchwalonych rozwiązań będę obowiązywały także po jego zakończeniu). Z punktu widzenia ochrony prywatności największe wątpliwości budzi wprowadzenie procedury tzw. *police screening*, przewidującej nowe uprawnienia policji do sprawdzania obywateli polskich ubiegających się o akredytację na EURO 2012 i sporządzania opinii na ich temat (bez uzasadnienia czy możliwości ich zaskarżenia) oraz przekazywania tych opinii na żądanie UEFA. Inne kontrowersyjne rozwiązania dotyczą m.in. wprowadzenia monitoringu wizyjnego w pomieszczeniach przeznaczonych dla osób zatrzymanych oraz stworzenia bazy danych kibiców.	▪ Oficjalne wystąpienia, m.in. stanowisko wobec projektu ustawy przekazane Marszałkowi Sejmu; ▪ teksty publikowane na stronie internetowej i wypowiedzi dla mediów.
Nowe dowody osobiste	▪ Ustawa z 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. z 2010 r. Nr 167 poz. 1131) ➔ **Ustawa z 9 czerwca 2011 r. o zmianie ustawy o dowodach osobistych i ustawy o ewidencji ludności** (Dz.U. z 2011 r. Nr 133 poz. 768)	Nowelizacja ustawy weszła w życie 30 czerwca 2011 r.	Nowe dowody mają być wyposażone w bezstykowy interfejs, co nie zostało przekonująco uzasadnione, a może stwarzać potencjalne zagrożenie dla bezpieczeństwa danych. Co więcej, przyjęto rozwiązania, zgodnie z którymi Ministerstwo Spraw Wewnętrznych i Administracji będzie miało możliwość gromadzenia danych o lokalizacji obywateli posługujących się dowodem osobistym do składania podpisu elektronicznego. Nowe dowody miały zostać wprowadzone 1 lipca 2011 r., ale ostatnia nowelizacja ustawy przesunęła ten termin na 1 stycznia 2013 r.	▪ Teksty na stronie internetowej (np. *Co warto wiedzieć o nowych dowodach osobistych?*) i wypowiedzi dla mediów.
Retencja danych pasażerów linii lotniczych	▪ Globalne podejście UE w sprawie przekazywania danych pasażerów lotniczych (PNR) państwom trzecim – komunikat Komisji z **21 września 2010 r.** ➔ **Projekt dyrektywy w sprawie retencji danych pasażerów lotniczych (PNR)**	Projekt dyrektywy został przedstawiony przez KE w lutym 2011 r.	Komunikat zawiera podstawowe zasady i minimalne wymogi przekazywania danych PNR. Jest dokumentem wyjściowym dla stworzenia dyrektywy dotyczącej PNR oraz dla negocjowania umów przekazywania danych zawieranych z państwami trzecimi. Dyrektywa ma wprowadzić europejski rejestr PNR umożliwiający swobodną wymianę tych danych między liniami lotniczymi a organami ścigania państw członkowskich. Ma ona służyć zapobieganiu i wykrywaniu terroryzmu oraz innych poważnych przestępstw (więcej na ten temat w tabeli: *Na marginesie… Pasażerowie pod specjalnym nadzorem*).	▪ Teksty na stronie internetowej (np. *Jest projekt dyrektywy w sprawie retencji danych pasażerów lotniczych (PNR)*); ▪ artykuły prasowe (np. Dorota Głowacka, *Kto się boi pasażerów linii lotniczych?*, „Rzeczpospolita", 9 marca 2011 r.).

Temat	Akty prawne	Etap legislacyjny	Najważniejsze założenia	Głos Fundacji Panoptykon
Pliki *cookies*	▪ Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z 25 listopada 2009 r. zmieniająca Dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów ➔ **Projekt ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw**	Ministerstwo Infrastruktury zakończyło konsultacje projektu nowelizacji ustawy wdrażającego postanowienia dyrektywy.	Dyrektywa służyć ma m.in. wzmocnieniu ochrony prywatności użytkowników Internetu. Część z proponowanych zmian Prawa telekomunikacyjnego wiąże się z koniecznością wdrożenia dyrektywy. Dotyczą one m.in. obowiązków informacyjnych związanych z wykorzystywaniem plików *cookies*, które umożliwiają profilowanie internautów i rejestrowanie ich codziennej działalności w sieci. Ustawodawca pozostał przy tzw. modelu *opt-out*, który zakłada, że użytkownik Internetu do momentu zgłoszenia wyraźnego sprzeciwu wyraża domyślną zgodę na przechowywanie i uzyskiwanie dostępu do plików *cookies*. Badania pokazują jednak, że niewiele osób korzystających z sieci, poświęca czas na modyfikowanie domyślnych ustawień prywatności i odpowiednią konfigurację przeglądarek internetowych.	▪ Oficjalne wystąpienia, m.in. uwagi do projektu nowelizacji ustawy w ramach konsultacji społecznych; ▪ teksty publikowane na stronie internetowej (np. *Debata w Ministerstwie Infrastruktury: twarde ciastko do zgryzienia…*) i wypowiedzi dla mediów.

Stan na 7 października 2011 r.

Autorki
Małgorzata Szumańska
Dorota Głowacka

Korekta
Urszula Dobrzańska

Wydawca
Fundacja Panoptykon / www.panoptykon.org

Projekt graficzny, skład i łamanie
CityLab / www.citylab.pl

Raport powstał dzięki wsparciu Fundacji im. Stefana Batorego.

FUNDACJA IM. STEFANA BATOREGO

Warszawa, październik 2011 r.

Warszawa
2011

PANOPTYKON
FUNDACJA