Włodzimierz FEHLER
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

DOI 10.14746/ps.2015.1.6

INFORMACYJNY WYMIAR ZAGROŻEŃ DLA BEZPIECZEŃSTWA WSPÓŁCZESNEJ POLSKI

Punktem wyjścia do podjęcia próby naszkicowania panoramy najistotniejszych zagrożeń w sferze bezpieczeństwa informacyjnego współczesnej Polski powinno być przede wszystkim określenie sposobu rozumienia tego czym jest bezpieczeństwo informacyjne oraz zagrożenie bezpieczeństwa informacyjnego. Analizując działania podejmowane przez różnorodne podmioty w celu uzyskiwania i utrzymywania pożądanych stanów bezpieczeństwa, można dostrzec dwie podstawowe strategie. Jedna, oparta o negatywne rozumienie bezpieczeństwa koncentruje się na przedsięwzięciach ukierunkowanych na maksymalizację poziomu skutecznej ochrony przed zidentyfikowanymi zagrożeniami, druga, oparta na pozytywnym pojmowaniu bezpieczeństwa skupia się na korzystnym dla zainteresowanego podmiotu (bądź podmiotów) kształtowaniu otoczenia, aby w ten sposób oddalać i minimalizować możliwości powstawania i materializowania się zagrożeń. Obydwa podejścia chociaż przy różnych założeniach pokazują iż zagrożenie jest kategorią o kluczowym znaczeniu dla bezpieczeństwa. Jest to jeden z tych czynników sprawczych, który w różnych konfiguracjach oddziałuje na bezpieczeństwo w taki sposób, że zmuszeni jesteśmy je postrzegać nie jako kategorię statyczną, ale jako zmienny w czasie proces. W powyższym kontekście podejmowanie wysiłków zmierzających do określania istoty pojęcia „bezpieczeństwo informacyjne" oraz „zagrożenie informacyjne" jawi się jako zadanie ważne tak dla rozwijania teorii bezpieczeństwa, jak i wypełniania postulatu użyteczności dociekań naukowych.

W przypadku bezpieczeństwa informacyjnego i związanych z nim zagrożeń mamy spore zamieszanie. Jego istotę ukazują funkcjonujące w literaturze przedmiotu definicje bezpieczeństwa informacyjnego koncentrujące się wokół kwestii ochrony informacji niejawnych czy też bezpieczeństwa systemów teleinformatycznych. Przykładowo Piotr Potejko uważa, że: „bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, przez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem" (Potejko, 2009: 194). Istnienie takiego podejścia potwierdza Krzysztof Liedl pisząc: „Bezpieczeństwo informacyjne bardzo często rozumiane jest przez praktyków jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania" (Liedl, 2008: 19). Nieco szersze w stosunku do tych stanowisk ujęcie proponuje Leszek F. Korzeniowski według którego „przez bezpieczeństwo informacyjne podmiotu (człowieka lub organizacji), należy rozumieć możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą" (Korzeniowski,

2012: 147). Spoglądając na powyższe przykłady należy uznać, iż nie jest to poprawny, odpowiadający współczesnej roli informacji opis istoty bezpieczeństwa informacyjnego. W adekwatnym ujęciu bezpieczeństwo informacyjne należy widzieć jako „stan w którym zapewniona jest swoboda dostępu i przepływu informacji połączona z racjonalnym i prawnym wyodrębnieniem takich ich kategorii, które podlegają ochronie ze względu na bezpieczeństwo podmiotów których dotyczą" (Fehler, 2012: 13–14). Jeżeli chodzi o rangę i znaczenie zagrożeń informacyjnych to określa ją to, iż żyjemy w epoce globalnego społeczeństwa informacyjnego, w którym informacja obok kapitału i pracy decyduje o zasobności, wysokim standardzie życia oraz perspektywach rozwoju państw, społeczeństw i jednostek. Zważywszy na to, że zagrożenia informacyjne mogą powstawać na gruncie różnie skonfigurowanych sytuacji, w których występuje: brak informacji, ograniczenie dostępu do informacji, nadmiar informacji, informacja zmanipulowana, informacja sfałszowana, informacja nieczytelna, informacja pozyskana nielegalnie, informacja zdezaktualizowana itp. można przyjąć, że zagrożenie informacyjne to „sytuacja w której mamy do czynienia z uświadomionymi lub nie, ograniczeniami lub nadużyciami w zakresie zgodnego z prawem dostępu oraz swobodnego posługiwania się aktualną, rzetelną integralną i właściwie ochranianą pod kątem poufności informacją" (ibidem: 27).

Jeżeli chodzi o kategorie zagrożeń związanych z istnieniem społeczeństwa informacyjnego, w ramach którego współcześnie funkcjonujemy, to istnieje wiele ich klasyfikacji. Mieczysław Lubański, opierając się na ustaleniach badaczy amerykańskich i brytyjskich, wskazuje w tej materii na:

– nierówności związane z tworzeniem dwubiegunowego społeczeństwa składającego się z osób posiadających dostęp do nowych technologii i tych, którzy takiego dostępu nie mają;
– zagrożenia dla prywatności;
– występowanie różnych form nadużyć informacyjnych;
– dezintegrujący wpływ na małe społeczności;
– zwiększone możliwości zagrożeń dla bezpieczeństwa informacyjnego różnych podmiotów;
– prymat stosowanych technologii przekazu nad jego treścią;
– umacnianie dominacji kultury masowej;
– umacnianie homogenizacji;
– odchodzenie od wartości związanych ze służbą publiczną i odpowiedzialnością społeczną (Lubański, 2004: 36).

Z kolei Piotr Sienkiewicz, sporządzając wykaz szans i zagrożeń dla demokracji w społeczeństwie informacyjnym, wymienia: *infoterroryzm*, kulturę masową, *e-dżihad*, zwiększone możliwości indoktrynacji, nadmiar informacji, niedobór wiedzy, pokusę autorytaryzmu oraz *syndrom orwellowski* (Sienkiewicz, 2011: 216). Patrząc na zagrożenia bezpieczeństwa informacyjnego z perspektywy gospodarczej i społecznej, można wskazać na:

– zwiększoną podatność zwirtualizowanych rynków finansowych na wstrząsy wynikające z dogodnych warunków do działania kapitału spekulacyjnego;
– zagrożenie bezrobociem związane z rozwojem automatyzacji i robotyzacji redukującej znaczenie siły roboczej;

– nadmierne rozszerzanie władzy i zasięgu wielkich korporacji;
– utrwalenie istniejących nierówności gospodarczych wynikające z dysproporcji w zakresie dostępu do informacji;
– depersonalizację więzi międzyludzkich, związaną z rozszerzaniem się komunikowania przy pomocy środków technicznych (zanik postaw altruistycznych, instrumentalizacja kontaktów interpersonalnych);
– indywidualizację życia społecznego;
– dekulturację wynikającą z tego, iż społeczeństwo informacyjne jako twór globalny staje się coraz bardziej wspólnotą ziemian, zatracając tożsamości narodowe i kulturowe;
– elitaryzm mediów wynikający z wzrastającego stopnia złożoności ich obsługi;
– rozwój różnorodnych form przestępczości informacyjnej;
– ograniczenia w sferze ochrony prywatności (Fehler, 2003: 33–34).

W aktualnych uwarunkowaniach funkcjonowania państwa polskiego, dostrzegając obecność tak realną jak i potencjalną większości wskazanych powyżej zagrożeń za najważniejsze uznać należy:
– ograniczanie dostępu do informacji związane z nadmierną uznaniowością i restrykcyjnością systemu ochrony tajemnic, słabościami systemu udostępniania informacji publicznych, wykluczeniem cyfrowym, hermetyzacją specjalistycznej terminologii (np. medycznej, prawniczej, ekonomicznej);
– naruszanie wolności informacyjnej związane z rozwojem różnych form inwigilacji;
– niedoskonałości systemu ochrony danych osobowych;
– zapóźnienia w wprowadzaniu e-administracji;
– przestępczość w sferze informacyjnej.

Istotnym źródłem zagrożeń w zakresie dostępu do informacji publicznej w Polsce jest kwestia ochrony prawnie określonych tajemnic. W obecnej legislacyjnej rzeczywistości istnieje ich ponad pięćdziesiąt rodzajów. Można zatem powiedzieć, iż stworzono gąszcz tajemnic, których ustanowienie i ochrona w założeniu ma stanowić element bezpieczeństwa w wymiarze państwowym, instytucjonalnym i indywidualnym. Taki stan rzeczy w wielu przypadkach powoduje jednak skutki odwrotne do zamierzonych. Z jednej bowiem strony, informacje, które stanowią tajemnice nieustannie „wyciekają", często stając się nie tylko sensacyjnym materiałem medialnych doniesień, ale także impulsem do politycznych przetasowań tak w kręgach rządowych, jak i gospodarczych. Z drugiej zaś strony, przy pomocy systemu ochrony informacji niejawnych, ogranicza się lub uniemożliwia obywatelom sięganie po informacje, które powinny być dla nich dostępne. Można zatem powiedzieć, iż system ochrony informacji niejawnych z założenia mający stanowić element bezpieczeństwa informacyjnego w wielu przypadkach jest jedną z barier blokujących społeczeństwu dostęp do należnych mu informacji. Niektóre jego rozwiązania są zresztą zgodne z partykularnymi oczekiwaniami urzędów, instytucji i indywidualnych dysponentów informacji bez uwzględnienia istoty wolności informacyjnej i rzeczywistego interesu społecznego. Niewiele zmieniła w tej materii nowa *Ustawa o ochronie informacji niejawnych*, w mnogości jej przepisów nadal łatwo się pogubić, a obywatele domagający się prawa do informacji często natrafiają na mur nie do przebicia. Wprawdzie decyzje o utajnieniu informacji można zgodnie z przepi-

sami nowej ustawy zaskarżyć, ale skargi badają *Agencja Bezpieczeństwa Wewnętrznego* i *Służba Kontrwywiadu Wojskowego* – twórcy i strażnicy systemu (Pytlakowski, 2011). Można w tym miejscu zauważyć, iż jest to m.in. konsekwencja dość powszechnego rozumienia istoty bezpieczeństwa informacyjnego w bardzo zawężony sposób (przede wszystkim jako ochrony informacji).

Jeżeli chodzi o systemowe rozwiązania w zakresie dostępu do informacji publicznej to ich powstanie wiąże się z realizacją jednego z podstawowych praw człowieka i obywatela, jakim jest prawo do poszukiwania, domagania się, otrzymywania i rozpowszechniania informacji (Górzyńska, 2006: 13). Istotą dostępu do informacji publicznej jest traktowanie jawności jako zasady, a tajemnicy jako wyjątku. Nieskrępowany dostęp do informacji tworzy warunki do porozumienia i uczestnictwa obywateli w życiu publicznym, wzmacnia ich pozycję wobec państwa, sprzyja transparentności w różnych sferach życia publicznego, blokuje powstawanie i sprzyja ujawnianiu zjawisk patologicznych np. korupcji czy niegospodarności. Jak zauważa Grzegorz Rydlewski: „kwestia powszechnego dostępu do zasobów informacji będących w posiadaniu podmiotów publicznych, w tym szczególnie podmiotów administracji publicznej, to zagadnienie nie tylko ważne w kontekście praw obywateli oraz podmiotów społecznych i gospodarczych, ale problem niezwykle skomplikowany […]. W obszarze tego zagadnienia dochodzi niejednokrotnie do konieczności rozstrzygania konfliktów wartości i krzyżowania się dyspozycji zawartych w różnych normach prawa" (Rydlewski, Szustakiewicz, Golat, 2012: 9–10). Sytuację komplikuje np. występowanie podwójnej właściwości sądowej (sądy powszechne i sądy administracyjne) w sprawach decyzji administracyjnych odmawiających udostępnienia informacji na wniosek podmiotu zainteresowanego. Kolejne problemy generuje fakt współistnienia przepisów dotyczących: prawa do informacji, ochrony danych osobowych oraz ochrony informacji niejawnych i tajemnic zawodowych. Ten gąszcz przepisów powoduje różnorodność interpretacyjną i zakłóca praktyczne realizowanie prawa do informacji publicznej. Symptomatyczne jest w tym kontekście uchwalenie nowelizacji *Ustawy o dostępie do informacji publicznej* dokonanej w 2011 r. Zgodnie z jej treścią podmioty wykonujące zadania publiczne mogły nie udzielać informacji, które osłabiłyby zdolność negocjacyjną *Skarbu Państwa* w procesie gospodarowania mieniem albo przy zawieraniu umów międzynarodowych czy w pertraktacjach unijnych. Kolejne ograniczenie dotyczyło informacji, które utrudniałyby ochronę interesów majątkowych państwa w postępowaniu przed sądem czy trybunałem. Jak zauważył w dyskusji przed uchwaleniem poprawki Artur Bodnar z *Helsińskiej Fundacji Praw Człowieka*: „projekt ustawy jest skandaliczny, słabo przygotowany i niezgodny z konstytucją" (Wybranowski, Wikariak, 2012). Również inne organizacje pozarządowe (m.in. *Fundacja Batorego*, *Stowarzyszenie Gazet Lokalnych*) wskazywały na to, iż okoliczności umożliwiające odmowę dostępu do informacji publicznej zostały ujęte zbyt szeroko i nie dość precyzyjnie. W związku z tym wystąpiły do Prezydenta RP z apelem o niepodpisywanie ustawy lub o jej skierowanie do *Trybunału Konstytucyjnego*. Prezydent Bronisław Komorowski postanowił jednak ustawę podpisać, a jednocześnie wystąpił z wnioskiem do *Trybunału Konstytucyjnego* o zbadanie jej zgodności z *Konstytucją RP*, ale tylko w zakresie poprawności procesu legislacyjnego. 18 kwietnia 2012 r. *Trybunał Konstytucyjny* orzekł, iż tryb ustawodawczy, w jakim przyjęto nowe-

lizację ustawy, nie odpowiadał konstytucyjnym rygorom procesu legislacyjnego. Wraz z wyrokiem TK nowelizacja utraciła moc[1].

W powyższym kontekście należy wspomnieć także o próbach rozwiązań pozytywnych. Do takich należała nowelizacja z 16 września 2011 r. (weszła w życie w grudniu 2011 r.). W jej ramach ustanowiono piąty (obok ogłaszania w Biuletynie Informacji Publicznej, dostępu na wniosek i w drodze wyłożenia lub wywieszenia w miejscach ogólnie dostępnych oraz wstępu na posiedzenia kolegialnych organów władzy pochodzących z powszechnych wyborów) tryb udostępniania informacji publicznej – *Centralne Repozytorium Informacji Publicznej* – CRIP. Repozytorium zostało wprowadzone jako narzędzie ułatwiające dostęp, przeszukiwanie oraz ponowne wykorzystywanie informacji publicznej. W związku z koniecznością doprecyzowania zasad działania CRIP 8 listopada 2013 r. Sejm uchwalił kolejną nowelizację (weszła w życie 10 marca 2014 r.), w ramach której oprócz usprawnienia prowadzenia (CRIP) przewidziano utworzenie *Scentralizowanego Systemu Dostępu do Informacji Publicznej* – SSDIP.

Rekapitulując, powyższy fragment rozważań można powiedzieć, iż prawo dostępu do informacji publicznej jest – mimo prób jego usprawnienia – w znacznym stopniu blokowane licznymi rozwiązaniami pozwalającymi urzędnikom odmawiać lub przewlekać w czasie udzielanie informacji. Postulowane zmiany, które mają zmniejszyć ograniczenia to m.in. sprecyzowanie definicji informacji publicznej, powołanie organu odpowiedzialnego za ten obszar, minimalizacja ograniczeń i wyjątków w dostępie. Z tym ostatnim wiąże się zreformowanie i kompleksowe ujęcie systemu tajemnic i innych form reglamentacji w dostępie do informacji publicznej (Sibiga, 2012).

Jeżeli chodzi o wykluczenie cyfrowe – czyli „rozróżnienie pomiędzy osobami które korzystają z komputerów i Internetu a tymi, którzy odcięci są od wielu informacji z powodu braku dostępu lub nie korzystania z tych technologii" (Krejtz, Nowak, 2009: 7) – to pogłębioną analizę tak społecznych, jak i technologicznych aspektów korzystania z Internetu w Polsce zawiera „Diagnoza Społeczna" (Batorski, 2013: 357–380). W pierwszej połowie 2013 r. komputery posiadało 70% gospodarstw domowych, a dostęp do Internetu 66,9%. Warto jednak wskazać, że chociaż Internet w Polsce nie jest już dobrem rzadkim, to jest on najwolniejszy w całej Unii Europejskiej[2]. W badaniach przeprowadzonych na potrzeby „Diagnozy Społecznej 2013" uchwycono charakterys-

---

[1] TK nie oceniał treści kwestionowanego przepisu, gdyż związany był zakresem wyznaczonym przez wniosek Prezydenta. Zbadał wyłącznie konstytucyjność trybu przyjęcia nowelizacji. Prezydent RP Bronisław Komorowski wnioskował o zbadanie konstytucyjności nowelizacji ustawy o dostępie do informacji publicznej, podjętej ze względu na potrzebę implementacji *Dyrektywy 2003/98/WE w sprawie ponownego wykorzystania informacji sektora publicznego Parlamentu Europejskiego i Rady* z 17 listopada 2003 r.

[2] Taki wniosek wynika z raportu firmy *Cisco*, która trzeci rok z rzędu zleciła badanie Internetu. Realizowały je uniwersytety w Oksfordzie oraz Oviedo, a sprawdzono w nim jakość łączy (przede wszystkim szybkość pobierania i wysyłania danych) w 72 państwach. Polska zajęła dość dobrą, 30 pozycję wspólnie ze Słowacją. Jednak przed nami są wszystkie pozostałe państwa UE, w tym Rumunia i Bułgaria. Zbliżone wyniki można znaleźć w serwisie *Netindex.com* korzystającym – podobnie jak w badaniu *Cisco* – z serwisu *Speedtest.net*. W tym zestawieniu Polska – ze średnią szybkością 8,08 Mb/s – jest przed Hiszpanią (7,81 Mb/s), ale również za Bułgarią, Rumunią, Niemcami i Francją. Liderem obu zestawień jest Korea Południowa (34,08 Mb/s).

tyczny trend – przyrost ilości osób, które mają komputer z dostępem do sieci w domu, ale z niego nie korzystają. W 2009 r. było to 13%, dorosłych Polaków w 2011 r. – 14%, a w 2013 – 15%. Są to przede wszystkim osoby starsze, słabiej wykształcone, emeryci i renciści, mieszkańcy małych miast i wsi. Niekorzystanie z komputerów i Internetu, jak wynika z badań, wiąże się z brakiem motywacji i umiejętności korzystania z dostępu do sieci oraz z brakiem wiedzy, do czego mógłby się przydać Internet. Nie mają znaczenia bariery finansowe, istotne dla ok. 9% gospodarstw, ani brak technicznych możliwości posiadania Internetu w miejscu zamieszkania, deklarowany przez ledwie 1% badanych. Znaczenie ma wiek – 48% internautów to osoby w wieku 16–34 lata. W tej grupie nie korzysta z sieci 7,5% osób. Natomiast osoby w wieku 45 lat i więcej stanowią 30% użytkowników i aż 84% niekorzystających. Najmniej użytkowników jest wśród emerytów i rencistów. Podział cyfrowy wiąże się także z wielkością miejscowości zamieszkania. Dostęp do komputera i sieci posiada prawie 78% gospodarstw domowych w miastach, a tylko 61% na wsi. Zakres korzystania z Internetu jest też zróżnicowany regionalnie. Odsetek gospodarstw podłączonych do sieci w województwach wschodnich jest niższy niż w innych częściach państwa. Najmniej dostępna jest sieć w województwach świętokrzyskim, lubelskim i warmińsko-mazurskim. Przodują w tym rankingu województwa: pomorskie, wielkopolskie, małopolskie i mazowieckie. Jeżeli chodzi o umiejętności i sposoby korzystania z komputerów i Internetu to są one niskie. Zdecydowanie najwięcej użytkowników posiada kompetencje związane z podstawowymi formami korzystania z komputerów i Internetu. Według danych z „Diagnozy Społecznej 2013" 55% użytkowników posługuje się pocztą elektroniczną. Proste umiejętności obsługi edytora tekstu (kopiowanie, wklejanie tekstu) posiada ok 60%, korzystanie z arkusza kalkulacyjnego deklaruje 35%, a przygotować elektroniczną prezentację potrafi zaledwie 23%. Polacy nie dbają też o bezpieczeństwo w sieci. Jak pokazały wyniki badania przeprowadzonego w 27 państwach europejskich w 2012 r. przez Microsoft ponad połowa (56%) całości respondentów i aż 79% ankietowanych z Polski nie posiadała wiedzy na temat zapobiegania kradzieży tożsamości, zaś 84% polskich internautów (przy wyniku dla całego badania na poziomie 73%) nic nie wiedziało o najnowszych działaniach służących ochronie reputacji internetowej. Aż 66% z ankietowanych w Polsce w ogóle nie poszerzało swej wiedzy na temat ochrony reputacji w Internecie oraz zapobiegania kradzieży tożsamości. Wskaźnik dla pozostałych państw był znacznie mniejszy i wynosił 39% (Polak, 2012). Taki negatywny stan rzeczy potwierdza badanie *Eurobarometru* przeprowadzone w 2013 r. dotyczące m.in. działań chroniących przed zagrożeniami w Internecie. Wynika z niego, iż zaledwie 22% polskich użytkowników zainstalowało oprogramowanie antywirusowe (w UE 46%), 20% deklarowało, że nie otwiera e-maili od nieznanych nadawców (w UE – 40%), 19% ostrożnie udostępnia swoje dane osobowe na stronach internetowych (w UE – 34%), 21% korzysta tylko ze znanych i zaufanych stron www (w UE – 32%), 9% zmieniało ustawienia bezpieczeństwa w przeglądarce internetowej lub kontach portali społecznościowych (w UE–16%) (*Badania*, 2013).

Generalnie zagrożone wykluczeniem są przede wszystkim osoby starsze i słabiej wykształcone. Dotyczy to też osób o niższych dochodach i mieszkających w mniejszych miejscowościach. Problem cyfrowego wykluczenia nie ogranicza się wyłącznie do podziału na tych, którzy posiadają dostęp do nowoczesnych środków komunikacji

i na tych, którzy go nie mają. Dotyczy także samego korzystania i poziomu jego wszechstronności, które prowadzi do społecznego i ekonomicznego wykluczenia. Fakt korzystania bądź nie z nowoczesnych technologii informacyjnych w tym Internetu wciąż silnie różnicuje polskie społeczeństwo. Konsekwencją tego podziału może być postępujące rozwarstwienie społeczeństwa i pogłębianie skali społecznego wykluczenia. Niestety jak zauważa Dominik Batorski większość działań podejmowanych w Polsce na rzecz upowszechnienia Internetu i przeciwdziałania wykluczeniu cyfrowemu w zbyt dużym stopniu koncentruje się na kwestiach infrastrukturalnych. Widoczna jest dostrzegana także w poprzednich latach nieskuteczność działań administracji państwowej i samorządowej. Mimo znacznej ilości środków finansowych przeznaczonych w ramach programów operacyjnych na przeciwdziałanie wykluczeniu cyfrowemu, a także na budowę sieci szerokopasmowych, skala tego wykluczenia nie ulega zmniejszeniu (Batorski, 2011: 327).

Hermetyzm językowy to kwestia rzadko podejmowana w kontekście zagrożeń informacyjnych. Jest jednak faktem, iż lawinowy rozwój wiedzy spowodował hermetyzację języków specjalistycznych w wielu dziedzinach i praktyczną niedostępność aparatu pojęciowego dla osób z innych kręgów zawodowych. Szczególnie groźne jest to w obszarach związanych z codzienną egzystencją i zaspokajaniem potrzeb życiowych, w ramach których wchodzimy w dobrowolne i wymuszone interakcje z takimi specjalistycznymi dziedzinami jak m.in.: prawo, medycyna, finanse, administracja. Ograniczone kompetencje zwykłych obywateli i hermetyzacja języka w dziedzinach newralgicznych dla ich egzystencji, to zjawiska, które mogą prowadzić nie tylko do indywidualnych strat materialnych i psychicznych, lecz także do skutków niekorzystnych z punktu widzenia jakości demokracji i zaufania obywateli do państwa (Szczepankowska, 2012).

W przypadku inwigilacji mimo pozytywnych konotacji łacińskiego źródłosłowia (*invigilo*, *inwigilare* – czuwać nad czymś, nad kimś) jest to termin współcześnie kojarzony w sposób zdecydowanie pejoratywny z działaniem państw autorytarnych i totalitarnych, które w swej praktyce ustrojowej szeroko i w zasadzie bez ograniczeń stosują zarówno jawne, jak i tajne systemy nadzoru, śledzenia i obserwowania społeczeństwa. W ujęciu słownikowym inwigilacja jest określana jako „tajny nadzór nad kimś, dyskretna, systematyczna obserwacja kogoś przez organa policyjne albo przez detektywów prywatnych" (Kopaliński, 2000: 236), „tajny nadzór nad kimś, systematyczna obserwacja kogoś, śledzenie" (Dubisz, 2003: 1239). W ujęciu kryminalistycznym inwigilację definiuje się jako „systematyczne śledzenie działalności określonych osób wchodzących w sferę zainteresowania policji, m.in. w przeszłości karanych oraz osób, które podejrzewa się o dokonywanie przestępstw" (Czeczot, Tomaszewski, 1996: 70). W tym sensie jest to działalność legalna i konieczna. W państwie demokratycznym inwigilacja jest dopuszczana na postawie przepisów ustaw, w sytuacjach związanych z zapewnieniem przestrzegania przepisów prawa i zwalczania zagrożeń dla bezpieczeństwa. Jednak należy pamiętać, iż jest to działalność, która powinna podlegać ścisłej reglamentacji i kontroli tak, aby nie naruszała konstytucyjnego prawa społeczeństwa do prywatności. W szczególności zaś korzystanie z uprawnień do różnych form inwigilacji przez państwowe służby odpowiedzialne za bezpieczeństwo wymaga odpowiedniego wyważenia stopnia zaspokojenia potrzeb związanych z:

– skuteczną ochroną przed realnymi i potencjalnymi zagrożeniami dla bezpieczeństwa;
– efektywnym działaniem służb policyjnych i specjalnych;
– zapewnieniem praworządności działań organów państwa;
– zagwarantowaniem ochrony prywatności, wolności wypowiedzi i danych osobowych (Adamski, 2012: 16).

W początkach drugiej dekady XXI w. Polska w wielu aspektach przekroczyła lub jest bliska przekroczenia granicy pomiędzy niezbędnym dla bezpieczeństwa zakresem nadzoru a zachowaniem gwarancji w zakresie prawa do prywatności. Obecnie (2015 r.) uprawnionych do inwigilowania jest aż dziewięć służb. Katalog przestępstw, przy których można stosować inwigilację liczy około 200 pozycji ukrytych w przepisach karnych różnych ustaw. Należy dodać, iż spis czynów, w związku z którymi można stosować różne formy inwigilacji, może być poszerzany za pomocą umów i porozumień międzynarodowych. Nie muszą być one ratyfikowane przez parlament. Ponieważ Polska zawiera umowy nie tylko z państwami demokratycznymi, istnieje możliwość uzupełnienia tego katalogu np. o czyny, ścigane na Białorusi czy w ChRL. Jak zauważają Małgorzata Szumańska i Dorota Głowacka – autorki raportu o sytuacji w zakresie ochrony prywatności w Polsce – „Publiczne i prywatne bazy danych, kamery na ulicach, skanery na lotniskach, karty dostępu w biurach, nagrywane rozmowy, 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" (Szumańska, Głowacka, 2011: 5). Problem pogłębia fakt, iż trudno dostrzec pogłębione zainteresowanie tym zjawiskiem w ujęciu procesualnym. Na ogół pojawiają się informacje o pojedynczych nadużyciach. Można mówić zatem także o deficycie wiedzy w zakresie konsekwencji związanych z rozwojem społeczeństwa nadzorowanego. Celnie ujęła to Irena Lipowicz, *Rzecznik Praw Obywatelskich* stwierdzając: „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" (Siedlecka, 2010).

Sfery szczególnie dotknięte i zagrożone różnymi inwigilacyjnymi formami gromadzenia informacji to systemy telekomunikacyjne oraz intensywnie nasycana monitoringiem wizyjnym przestrzeń publiczna. Zbieranie i retencja[3] danych telekomunikacyjnych obywateli jest możliwe m.in. w przypadku: nielegalnego wyrębu lub przywłaszczenia drewna wartości powyżej 76 zł, nieudzielenia dziennikarzowi informacji przez kierownika jednostki organizacyjnej; wykroczeń skarbowych (np. nieprowadzenia księgi przychodów i rozchodów), podejrzenia pomówienia, znieważenia czy naruszenia nietykalności cielesnej. Najpopularniejszym środkiem inwigilacji telekomunikacyjnej jest kontrola połączeń tzw. bilingowanie. Daje ono m.in. możliwość gromadzenia informacji dotyczących tego gdzie przebywała oraz z kim, kiedy i gdzie spotykała się

[3] Obowiązkowe gromadzenie tzw. danych transmisyjnych, czyli informacji o szczegółach wszystkich rodzajów połączeń telekomunikacyjnych w celach związanych z bezpieczeństwem państwa.

osoba poddana bilingowi. W dodatku bilingowanie można stosować w ramach działań kontrolnych, planistycznych bądź analitycznych, czyli w praktyce także, wówczas gdy nie doszło do przestępstwa. Nie ma też wymogu, by osoba, której dane telekomunikacyjne są sprawdzane, była o cokolwiek podejrzana. Wystarczy, że kontaktuje się z osobą podejrzaną lub „analizowaną", albo np. że bierze udział w przetargu ogłaszanym przez podmiot z udziałem skarbu państwa (Siedlecka, 2012). Ten środek inwigilacji można stosować bez jakiejkolwiek kontroli. W efekcie Polska stała się liderem Unii Europejskiej w sięganiu po dane telekomunikacyjne. Istota zagrożeń związanych z analizowanym problemem w syntetycznym ujęciu sprowadza się do:

– istnienia możliwości wkraczania w sferę osobistych wolności z błahych powodów i bez dostatecznych uzasadnień;
– podważenia zasady domniemania niewinności i umieszczenia szerokich (praktycznie nieograniczonych) rzesz obywateli na liście podejrzanych;
– pozyskiwania danych telekomunikacyjnych przez służby bez żadnej zewnętrznej kontroli;
– nierespektowania tajemnic zawodowych (adwokackiej, radcy prawnego, dziennikarskiej i innych), których zniesienie możliwe jest tylko w określonych przypadkach;
– nieinformowania osób, których dane były przedmiotem zainteresowania;
– możliwości przechowywania zgromadzonych danych także w sytuacji kiedy okazują się one zbędne do celów prowadzonych dochodzeń i sprawdzeń.

Istotnym elementem wpływającym na obraz skali i zakresu inwigilacji jest także stosowanie podsłuchu operacyjnego. Co pewien czas odżywa publiczna dyskusja o podsłuchach, które dziś może stosować dziewięć służb. Mogą to robić tylko w celu wykrycia wymienionych w odpowiednich ustawach ściśle określonych groźnych przestępstw oraz gdy inne środki zawiodą. Długi czas tajne były nawet bardzo ogólne statystyki tych działań. Dopiero 21 czerwca 2011 r. Prokurator generalny Andrzej Seremet przesłał odpowiednią informację marszałkom obu izb parlamentu. Było to wykonaniem nowelizacji *Ustawy o prokuraturze*, która wprowadziła zasadę, że prokurator generalny ma przedstawiać Sejmowi i Senatowi coroczną, jawną informację o liczbie wniosków i przypadków zastosowania technik operacyjnych oraz o efektach sądowego i prokuratorskiego nadzoru nad tymi czynnościami.

Ze sprawozdania wynikało, że w 2010 r. wszystkie uprawnione podmioty skierowały wnioski o zarządzenie kontroli i utrwalanie rozmów lub wnioski o zarządzenie kontroli operacyjnej łącznie wobec 6723 osób. Wobec 6453 osób sąd zarządził kontrolę i utrwalanie rozmów lub kontrolę operacyjną. Odmówił tego wobec 52 osób. Wobec 218 osób zgody nie wyraził prokurator (*Sześć tysięcy*, 2011). W roku 2011 liczba wniosków o wskazywane wyżej formy kontroli wyniosła 5188 zarządzono ją wobec 4863 osób. Sąd oddalił wnioski wobec 39 osób a prokuratura wobec 286. Był to spadek o ok. 25% w stosunku do roku 2010. Była to głównie zasługa *Policji* (3979 wniosków). O ile pozostałe służby uprawnione do stosowania kontroli operacyjnej nieznacznie zmniejszyły swoje zapotrzebowanie (884 wnioski), o tyle *Policja* mocno je zredukowała. Zmniejszenie aktywności *Policji* mogło wynikać z nowelizacji ustawy *Kodeks postępowania karnego* oraz *Ustawy o Policji* z 11 czerwca 2011 r. Ta ostatnia zmiana nałożyła na wnioskującego obowiązek przedstawienia materiałów, uzasadniających

potrzebę zastosowania środków kontroli operacyjnej[4]. O ponad połowę wzrósł też w roku 2011 procent wniosków odrzuconych na etapie weryfikacji prokuratorskiej oraz sędziowskiej. W roku 2010 odrzucono tylko 4% wniosków, podczas gdy w roku 2011 odrzuconych zostało ponad 6% wniosków (*Pełny zapis*, 2013:3–4). W 2012 r. uprawnione służby wnioskowały o zarządzenia kontroli i utrwalania rozmów lub stosowania kontroli operacyjnej wobec 4206 osób. Było to o 982 osób mniej niż w 2011 r., kiedy wnioskami objęto 5188 osób i o 2517 mniej niż w 2010 r., kiedy dotyczyło to 6723 osób. Sądy zarządziły kontrolę wobec 3956 osób oraz odmówiły jej zarządzenia wobec 25 osób. Uprawnieni prokuratorzy nie wyrazili zgody na wnioski wobec 225 osób (*Trochę mniej podsłuchów*, 2013). W 2013 r. policja i inne służby wnioskowały o zarządzenia kontroli i utrwalania rozmów lub stosowania kontroli operacyjnej wobec 4509 osób. Sąd wyraził zgodę w 4278 przypadkach, a odmówił w 16. Na poziomie prokuratorskim nie było zgody na wnioski wobec 215 osób (*W 2013 policja*, 2014). W 2014 r. liczba wniosków do sądów o zarządzenia kontroli i utrwalania rozmów lub stosowania kontroli operacyjnej wzrosła. Służby skierowały do sądów 5 tys. 435 wniosków o zgodę na tego typu czynności, czyli o 926 więcej niż w 2013 r. Sądy zgodę wydały w przypadku 5221 osób (o 943 więcej niż w 2013 r.) i odmówiły zgody wobec 12 osób, (w 2013 wobec 16 osób). Z kolei prokurator generalny i prokuratorzy okręgowi nie wyrazili w 2014 r. zgody na kontrolę w przypadku 202 osób (*Więcej podsłuchów*, 2015). Widać zatem iż po przejściowym spadku związanym z wzmocnieniem kontroli procesu zatwierdzania wniosków o kontrolę w 2011 r. następuje wzrost wniosków służb o stosowanie tego typu kontroli.

Dodać w tym miejscu należy, że trzykrotnie (dwukrotnie w 2011 r. i raz w 2012 r.) billingowanie i inne przepisy o czynnościach operacyjnych zaskarżyła do Trybunału Konstytucyjnego *Rzecznik Praw Obywatelskich* Irena Lipowicz, a *Prokurator generalny* Andrzej Seremet w 2012 r. wniósł trzy skargi na nieproporcjonalnie rozdęty katalog przestępstw uprawniających do czynności operacyjnych i na „billingowanie". W Trybunale Konstytucyjnym znalazło się więc w 2012 r. w sumie siedem skarg na inwigilację. Prezes Trybunału Konstytucyjnego Andrzej Rzepliński zdecydował o połączeniu w jedną wszystkich tych spraw. Ponieważ nigdy jeszcze TK nie wypowiadał się jednocześnie w kwestii uprawnień wszystkich służb w dziedzinie inwigilacji liczono, iż może ustanowić standard, którego musiał będzie trzymać się ustawodawca. 30 lipca 2014 r. po dwóch latach od wniesienia ostatniej skargi Trybunał obradujący w pełnym składzie wydał wyrok, w którym stwierdził m.in.: że brak niezależnej kontroli pobierania billingów przez służby, brak zasad niszczenia podsłuchów osób zaufania publicznego oraz niektóre podstawy prawne kontroli operacyjnej są niekonstytucyjne. W sentencji wyroku TK wskazał m.in., na ryzyko nadużyć i niedostateczne gwarancje proceduralne wynikające z braku niezależnej kontroli zewnętrznej pobierania przez uprawnione służby danych telekomunikacyjnych obywateli (billingi, informacje o miejscach logowania się telefonów itp.). W odniesieniu do kontroli operacyjnej za niezgodne z konstytucją

[4] Prokuratorska oraz sądowa ocena tych materiałów może prowadzić do odrzucenia wniosku (np. z powodu niewykazania wyczerpania innych możliwości dowodowych lub niewykazania, że osoba, której dotyczy wniosek, popełniła lub zamierza popełnić jedno z przestępstw, w przypadku których podsłuch jest dozwolony).

uznano przepisy ustaw w zakresie, w którym nie przewidują gwarancji niezwłocznego i protokolarnego zniszczenia materiałów, co do których nie uchylono tajemnicy – zwłaszcza podsłuchów wobec adwokatów, dziennikarzy lub innych zawodów zaufania publicznego, zobowiązanych do zachowania tajemnicy zawodowej. W przepisach dotyczących ABW za niekonstytucyjny uznano brak wskazania zakresu niejawnych działań Agencji w ramach wykrywania i ścigania „innych przestępstw godzących w bezpieczeństwo państwa". Niezgodne z ustawą zasadniczą przepisy mają stracić moc obowiązującą po 18 miesiącach. W reakcji na wyrok TK premier Ewa Kopacz zapowiedziała, że prace nad zmianami ustaw dotyczących służb specjalnych będą prowadzone w Sejmie. Za pośrednictwem *Centrum Informacyjnego Rządu* premier poinformowała też, że powstanie projekt określający zasady kontroli operacyjnej prowadzonej przez służby specjalne. Projekt nowelizacji dotyczący billingów i podsłuchów oraz stosowania innych metod kontroli operacyjnej przez służby ma opracować zespół powołany przy *Kolegium ds. służb specjalnych* przez premier E. Kopacz na wniosek nadzorującego służby szefa kancelarii premiera Jacka Cichockiego (TK, 2014). Jak zauważyła Barbara Grabowska z *Helsińskiej Fundacji Praw Człowieka* wyrok TK jest wyważony i wielowątkowy. Trybunał wskazał wprawdzie jako wymóg konstytucyjny obowiązek stworzenia zasad kontroli nad pozyskiwaniem przez służby danych telekomunikacyjnych. Nie określił jednak czy powinien robić to sąd, *Generalny Inspektor Ochrony Danych Osobowych*, czy inny specjalnie utworzony organ. TK nie wskazał też czy ma to być kontrola poprzedzająca, czy następcza. Kwestie uregulowania tych problemów znalazły się zatem w gestii ustawodawcy, który tym samym stanął przed dużym wyzwaniem merytorycznym i czasowym związanym z koniecznością dokonania zmian w ciągu 18 miesięcy (Grabowska, 2014).

Ważnym składnikiem inwigilacji jest także niekontrolowany rozwój różnych form monitoringu wizyjnego. Monitorowane są ulice, placówki handlowe, obiekty sportowe, banki, biurowce, szkoły i przedszkola. Kamery nadzorują też osiedla, urzędy, drogi, stacje benzynowe, parkingi, hotele, szpitale, zakłady pracy, place zabaw. Można powiedzieć, że lista miejsc bez monitoringu systematycznie się zmniejsza. Głównym zagrożeniem jest to, że monitoringu nie reguluje prawo. Wyjątkiem są opisane w ustawach uprawnienia straży miejskiej i Policji oraz przepisy dotyczące bezpieczeństwa imprez masowych i kasyn. Dochodzi więc do sytuacji, w której monitoring narusza prywatność, ale nie wiadomo, kto, gdzie i w jakim celu monitoruje. Nie wiadomo też jakie prawa przysługują w konkretnych sytuacjach. Nie do końca wiadomo też kto oprócz sądów i prokuratury może dysponować materiałem z monitoringu. Istotny problem stanowią coraz szersze możliwości dodatkowej automatycznej analizy danych z monitoringu. W fazie badań naukowych, ale też pierwszych zastosowań praktycznych, są programy komputerowe, które interpretują obraz z kamer i łączą go z innymi danymi w bazie. Może to być na przykład system, wykrywający obce osoby na terenie instytucji albo osoby z policyjnych rejestrów na ulicy. Duże wątpliwości budzi dość często podnoszony argument, iż monitoring zdecydowanie poprawia stan bezpieczeństwa publicznego (Szumańska, Głowacka, 2011: 17). W polskim przypadku jedyne naukowe badanie, jakie przeprowadził Paweł Waszkiewicz nie potwierdziło związku funkcjonowania monitoringu z po-

prawą bezpieczeństwa[5]. Można zatem zgodnie z aktualnym stanem wiedzy naukowej stwierdzić, że nie ma dowodów na to, że monitoring w przestrzeni publicznej rzeczywiście się sprawdza[6]. Na skalę zagrożeń związanych z żywiołowym rozwojem monitoringu zwrócił uwagę w piśmie skierowanym 24 sierpnia 2011 r. do Ministra Spraw Wewnętrznych i Administracji *Generalny Inspektor Ochrony Danych Osobowych* stwierdzając, że monitoring stosowany jako środek wspomagający utrzymanie bezpieczeństwa i porządku, budzi coraz więcej kontrowersji powstających 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**.** Jednocześnie *Generalny Inspektor* sformułował wymagania w zakresie monitoringu mające zapewnić właściwe standardy ochrony prywatności. W ramach tych rekomendacji *Generalny Inspektor* wskazał, że prawo dotyczące monitoringu powinno określić:

– miejsca i okoliczności w jakich stosowanie monitoringu jest dopuszczalne;
– miejsca w których co do zasady monitoringu nie można stosować;
– sposoby oznaczania obszarów i obiektów objętych monitoringiem;
– prawa i obowiązki podmiotu prowadzącego monitoring;
– prawa osób objętych monitoringiem;
– zasady dotyczące wykorzystywania danych zebranych w procesie monitoringu;
– organy kontrolne i wydające zezwolenia na prowadzenie monitoringu;
– odpowiedzialność karną za łamanie prawa dotyczącego monitoringu (*Wymagania*, 2011: 9–11).

Jeżeli chodzi o zagrożenia związane ze sferą ochrony danych osobowych, to należy podkreślić iż Konstytucja RP na mocy artykułów 47 i 51 chroni prywatność i autonomię informacyjną jednostki. Ponieważ nowe technologie powodują, iż informacje na temat życia obywateli można coraz sprawniej gromadzić, wymieniać, kojarzyć na niespotykaną dotychczas skalę, obecne polskie przepisy dotyczące ochrony danych osobowych należy uznać za nieprzystające do współczesnych wymogów. Aktów prawnych, które o tym decydują, jest kilkaset. Według *Generalnego Inspektora* brak jest pełnej wiedzy o tym, ile publicznych baz danych funkcjonuje w Polsce. Nawet dane o liczbie rejestrów publicznych są rozbieżne w poszczególnych opracowaniach. Na pewno jest ich w Polsce kilkaset rodzajów i wciąż pojawiają się nowe np. w oświacie, ochronie zdrowia[7], księgach wieczystych czy ewidencji działalności gospodarczej. Nie do końca

---

[5] Paweł Waszkiewicz z Uniwersytetu Warszawskiego badał w 2009 r. w Warszawie skrzyżowanie ulic Żelaznej i Chłodnej, nad którym umieszczono kamerę. Obszarem kontrolnym było skrzyżowanie ulic Siennej i Miedzianej, gdzie nie zainstalowano żadnego urządzenia. Drugie porównanie dotyczyło skrzyżowania ulic Anielewicza i Smoczej oraz Nowolipki i Smoczej (obszar kontrolny). Spadek liczby przestępstw nastąpił i na obszarze z kamerą, i bez niej.

[6] W brytyjskich badaniach, które zrealizowali David Farrington i Brandon Welsch (Home Office Research Study, 2002 r.) nie uchwycono zasadniczego wpływu monitoringu wizyjnego na poziom przestępczości. Istotny spadek przestępstw odnotowano jedynie na parkingach. Natomiast na innych obszarach takich jak centra miast, bloki komunalne i transport publiczny takiego związku nie wykazano. Wedle brytyjskiej policji odsetek niewykrytych sprawców przestępstw jest taki sam w Greenwich (747 kamery), jak w Chelsea (100 kamer).

[7] W 2011 roku prezydent RP podpisał dwie ustawy przyzwalające na budowę megabaz danych – o *Systemie Informacji Medycznej* (SIM) i o *Systemie Informacji Oświatowej* (SIO). Pierwszy obej-

wiadomo, kto decyduje o przyznaniu do nich dostępu. Jednocześnie *Generalny Inspektor* nie wie, jaki jest rzeczywisty zakres dostępu do tej informacji i jak jest ona wykorzystywana. Zasadne jest zatem pytanie o to, kto i w jakim zakresie ma dostęp do danych obywateli, a przede wszystkim, kto dopuszcza konkretnego urzędnika do każdego z tych zasobów. Na domiar złego uprawnienia do dostępu do danych w rejestrach publicznych „rozdaje się" bez głębszego zastanowienia. Ważną kwestią jest też bezpieczeństwo danych w rejestrach publicznych. Chodzi zarówno o zabezpieczenie przed dostępem nieuprawnionym, jak i zbyt szerokim dostępem podmiotów uprawnionych. Nagminną praktyką jest, iż podmioty publiczne uzyskują dostęp do danych, których nie potrzebują, po czym takie informacje kopiują i przetwarzają. Należy zwrócić uwagę, że obecne przepisy powstały zanim w powszechnym użyciu znalazł się nowoczesny internet. *Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych* pochodzi z 1981 r., *dyrektywa UE w sprawie. ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* z 1995 r., *Ustawa o ochronie danych osobowych* z 1997 r. w dużej mierze oparta została o dyrektywę UE. Zamiast podsumowania tego fragmentu można zacytować słowa Davida Lyona: „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. […] było wiele okazji, żeby się o tym przekonać" (Leszczyński, 2011).

Przechodząc do kwestii zagrożeń informacyjnych związanych z sferą e-administracji trzeba rozpocząć od tego, że zgodnie z syntetycznym ujęciem e-administracja czy *e-goverment* to proces wykorzystania technologii informatycznych do poprawienia jakości i sprawności zarządzenia sprawami państwowymi, świadczenie usług administracyjnych, zwiększenie zaangażowania obywateli. Na całym świecie przekonano się, że dzięki elektronicznej administracji petenci oszczędzają czas i nerwy. Mniej jest też okazji do korupcji (Poznański, 2011). Elektroniczna administracja to nie tylko wygoda dla obywateli. To także ułatwienie dla władz rządowych i samorządowych ponieważ zintegrowane systemy przepływu dokumentów pozwalają zmniejszyć koszty funkcjonowania urzędów i oszczędzać pieniądze podatników. W obecnych polskich realiach załatwienie sprawy przez Internet w dużej części polskich urzędów wciąż jest fikcją. Chociaż są one dobrze zinformatyzowane, nie przekłada się to na ułatwienie życia przeciętnemu obywatelowi. Nadal trudno mówić o załatwianiu spraw urzędowych bez ruszania się z domu. Zwykle kończy się na możliwości znalezienia informacji w Inter-

---

mie w zasadzie wszystkich, a drugi ok. 20 proc. obywateli. Od początku ich budowa budziła sprzeciw, zwłaszcza SIO. Organizacje zajmujące się ochroną konstytucyjnych praw i wolności uznały, że system ten zagraża prawu do prywatności. Nowy SIO ma zastąpić stary, wprowadzony w 2005 roku, Gromadził on jedynie zestawienia zbiorcze uczniów, opisanych według płci, wieku czy typu szkoły. W nowym systemie gromadzone będą informacje o konkretnych uczniach, identyfikowanych przez numer PESEL. Dane będą zbierane przez cały okres edukacji, od przedszkola po egzamin na studia. Minister edukacji będzie miał zatem dostęp do pełnych „profili edukacyjnych" ok. 6 mln przedszkolaków i uczniów, w tym i do danych wrażliwych – o ich dysfunkcjach i korzystaniu z pomocy psychologicznej. W nowym SIO będą też dane o 600 tys. pracowników oświaty.

necie i ewentualnie pobraniu odpowiedniego formularza. Resztę trzeba załatwić tradycyjnie. Symbolem porażki unowocześnienia urzędów jest to, że w niektórych z nich przez Internet można zarezerwować miejsce w kolejce do tradycyjnego okienka. Nie sprawdza się także system elektroniczna *Platforma Usług Administracji Publicznej* (ePUAP), czyli system elektronicznych skrzynek podawczych, na które można wysyłać wnioski, skargi czy pytania. Chociaż ma je ok. 90% urzędów, obywatele wciąż rzadko z nich korzystają (Rochowicz, Szymańska, Baranowska, Stróżyk, 2012). Niemal dziewięć na dziesięć urzędów, choć ma system do elektronicznego zarządzania dokumentacją, i tak drukuje wszystkie dokumenty i formularze (Czubkowska, Żółciak, 2012). Obecnie głównym źródłem zagrożeń jest brak koncepcji informatyzacji. Chaotyczne działania i brak współpracy, spowodowały błędy w decyzjach i obniżyły jakość rezultatów prowadzonych przedsięwzięć. Administracja publiczna realizuje dziś kilkaset projektów informatycznych. Część z tych projektów obarczona jest systemowymi wadami, których istota sprowadza się do (*Państwo 2,0*, 2012):

– braku kompleksowego i perspektywicznego podejścia oraz koordynacji przy przygotowywaniu i wdrażaniu projektów;
– braku kompleksowej wizji, potrzeb użytkowników;
– błędnego oparcia projektów o perspektywę techniczno-sprzętową;
– realizacji części projektów „od końca" bez logicznej sekwencyjności;
– skupiania się w ocenach projektów na rozliczeniach formalnych, a nie na realnych korzyściach dla obywateli;
– rozwijania przez różne instytucje równoległych systemów bez uwzględnienia ich kompatybilności i wzajemnej komunikacji;
– przyjmowania rozwiązań niedostosowywanych do realnych i zmieniających się w czasie potrzeb użytkowników;
– braku analiz kosztów utrzymania projektów, sieci oraz systemów po ich wdrożeniu[8];
– niewystarczającej współpracy z interesariuszami;
– nieuwzględniania w harmonogramach oraz budżetach fazy testowania.

Trzeba też pamiętać, iż część decyzji finansowych w latach 2007–2010 nie była tak przejrzysta, jak być powinna. Procesy te objęte zostały śledztwem CBA oraz prokuratury. W konsekwencji, wiosną 2012 r. Komisja Europejska zamroziła wypłatę 3,7 mld zł na tworzenie polskiej *e-administracji* (Poznański, 2012). Po powołaniu nowego resortu administracji i cyfryzacji jego ówczesny szef Michał Boni na uporządkowanie e-administracji przewidział dwa lata. Najszybciej rozpoczęto korekty systemu ePUAP. Nie wprowadzono jednak zaplanowanych na 2015 rok dowodów elektronicznych, z której to opcji zrezygnowano w 2014 r. Warto też zauważyć, iż ramach porządkowania spraw *e-administracji* 8 stycznia 2014 r. Rada Ministrów przyjęła *Program Zintegrowanej Informatyzacji Państwa*, w ramach którego próbuje się uporządkować wcześniejsze zaniedbania.

---

[8] Środki finansowe na utrzymanie systemu wspierającego ogólnopolski numer alarmowy „112" były zagwarantowane w ramach jednego z projektów do końca marca 2012 r. Ani w studium wykonalności, ani w samym wniosku projektowym nie zajęto się kwestią utrzymania sieci po zakończeniu projektu.

Jeżeli chodzi o ostatni analizowany nurt zagrożeń, czyli przestępczość przeciwko informacji to jest to kategoria zdefiniowana głównie w przepisach rozdziału XXXIII Kodeksu karnego (*Ustawa*, 1997), w którym zawarto artykuły opisujące następujące rodzaje przestępstw: ujawnienie lub wykorzystywanie tajemnicy państwowej, ujawnienie lub wykorzystywanie informacji pozyskanych w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, ujawnienie tajemnicy służbowej przez funkcjonariusza publicznego, bezprawne uzyskiwanie informacji stanowiących cudzą tajemnicę, bezprawne posługiwanie się urządzeniami ograniczającymi swobodę wymiany informacji, ujawnienie bezprawnie uzyskanych informacji innym osobom, utrudnianie lub udaremnianie zapoznania się przez osobę uprawnioną z istotnymi informacjami, sabotaż komputerowy. Wskazać należy także na rozdział XVII k.k. – *Przestępstwa przeciwko Rzeczypospolitej Polskiej*. W rozdziale tym uregulowano m.in. kwestie związane ze szpiegostwem. Szpiegostwo w tym ujęciu jest działaniem przestępczym na szkodę państwa polegającym na gromadzeniu, przechowywaniu i przekazywaniu informacji obcemu wywiadowi. Jedną z jego form jest szpiegostwo komputerowe polegające na zdobywaniu danych zawartych na komputerowych nośnikach informacji. Inna grupa przestępstw związanych z informacją to przestępstwa przeciwko wiarygodności dokumentów (rozdział XXXIV k.k.) popełniane przez ich fałszowanie w różnej formie zarówno w całości, jak i w częściach. Należy pamiętać także, iż w rozdziale XXXV k.k. obejmującym przestępstwa przeciwko mieniu do grupy czynów zabronionych, zaliczono: kradzież programu komputerowego, kradzież karty bankomatowej, oszustwo telekomunikacyjne, oszustwo komputerowe, paserstwo programu komputerowego. Na koniec trzeba wymienić niektóre przestępstwa przeciwko bezpieczeństwu powszechnemu opisane w rozdziale XX k.k. przewidującym odpowiedzialność karną za sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach m.in. przez: wprowadzenie zakłóceń, uniemożliwiających lub w inny sposób wpływających na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych. Do tego należy dodać przepisy karne ustawy o ochronie danych osobowych (art. 49–54). Częściowy obraz skali przestępczości informacyjnej zarysowują dostępne statystyki policyjne ujęte w tabeli 1. W okresie 2005–2014 widać wyraźnie, iż najwięcej czynów przestępczych popełniano w zakresie: podrabiania dokumentów, posługiwania się dokumentem innej osoby, naruszania tajemnicy korespondencji, utrudniania lub udaremniania korzystania z informacji. Warto zauważyć natomiast stosunkowo znikomą ilość przestępstw przeciwko tajemnicy państwowej oraz przestępstw w zakresie danych informatycznych. W odniesieniu do powyższego obrazu należy jednak uwzględnić tzw. ciemną liczbę przestępstw niewykrytych. Trudno oszacować jej wielkość ale biorąc po uwagę stosunkowo niską świadomość społeczną w zakresie ochrony przestrzeni informacyjnej oraz możliwości tkwiące we współczesnych technologiach na pewno jest ona znaczna.

Podsumowując, można powiedzieć, iż współczesny wymiar zagrożeń dla bezpieczeństwa informacyjnego Polski wiąże się przede wszystkim z wielowątkowo rozumianymi kwestiami dostępu do informacji. Składają się nań rozliczne bariery prawne, techniczne i świadomościowe. Wyraźnie zaznacza się także niebezpieczny trend do rozwijania różnorodnych form nadzoru informacyjnego godzących w wolność informacyjną i prawo do prywatności.

Tabela 1

Przestępczość informacyjna w latach 2005–2014

Rodzaj przestępstwa	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Ujawnienie tajemnicy państwowej	6	9	14	12	16	16	14	12	5	2
Ujawnienie tajemnicy służbowej i zawodowej	131	159	133	121	155	162	131	159	148	127
Naruszenie tajemnicy korespondencji	430	538	616	694	982	1194	1583	1657	2203	2868
Niszczenie danych informatycznych	2	3	6	6	6	7	3	9	14	10
Udaremnianie lub utrudnianie korzystania z informacji	152	201	244	366	555	690	885	796	765	743
Sabotaż komputerowy	1	19	11	13	34	22	38	35	37	27
Wytwarzanie programu komputerowego do popełnienia przestępstwa	6	9	4	12	23	35	38	21	42	47
Podrabianie dokumentów	19 937	19 217	18 319	17 340	17 804	16 427	15 888	17 148	17 579	16 652
Posługiwanie się dokumentem innej osoby	30 777	27 610	22 698	20 717	18 854	16 155	13 423	12 078	12 415	14 280

Źródło: Opracowanie własne na podstawie http://statystyka.policja.pl/portal/st/1117/ (20.04.2015).

Bibliografia

Adamski D. (2012), *Zasady wykorzystywania przez służby specjalne danych telekomunikacyjnych w aspekcie obowiązującego stanu prawnego*, http://wolnyinternet.panoptykon.org/story/materia-y-z-konferencjidostęp (10.08.2012).

Badania: 70 proc Polaków uważa, że wzrosło zagrożenie w sieci (2013), http://naukawpolsce.pap.pl/aktualnosci/news,398137,badania-70-proc-polakow-uwaza-ze-wzroslo-zagrozenie-w-sieci.html (20.04.2015).

Batorski D. (2011), *Korzystanie z technologii informacyjno-komunikacyjnych*, w: *Diagnoza społeczna 2011. Warunki i jakość życia Polaków*, (red.) J. Czapiński, T. Panek, Warszawa.

Batorski D. (2013), *Polacy wobec technologii cyfrowych-uwarunkowania dostępności i sposobów korzystania*, w: *Diagnoza społeczna 2013. Warunki i jakość życia Polaków*, (red.) J. Czapiński, T. Panek, Warszawa.

Czeczot Z., Tomaszewski T. (1996), *Kryminalistyka ogólna*, Toruń.

Czubkowska S., Żółciak T. (2012), *Trudna informatyzacja samorządów*, „Dziennik Gazeta Prawna", 25.07.2012.

Fehler W. (2012), *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne*, Warszawa.

Fehler W. (2003), *Społeczeństwo informacyjne jako składnik procesu globalizacji*, w: *Problemy polityki bezpieczeństwa wobec procesów globalizacji*, (red.) J. Świniarski, J. Tymanowski, Toruń.

Grabowska: wyrok TK ws. zasad inwigilacji – wyzwaniem dla ustawodawcy (2014), http://wyborcza.pl/1,91446,16402998,Grabowska__wyrok_TK_ws__zasad_inwigilacji___wyzwaniem.html#ixzz3XsCDfWCh6 (18.04.2015).

Górzyńska T. (2006), *Geneza i rozwój prawa do informacji*, w: *Prawo informacji. Prawo do informacji*, (red.) W. Góralczyk jun., Warszawa.

Kopaliński W. (2000), *Słownik wyrazów obcych i zwrotów obcojęzycznych z suplementem*, Warszawa.

Korzeniowski L. F. (2012), *Podstawy nauk o bezpieczeństwie*, Warszawa.

Krejtz K., Nowak A. (2009), *Znaczenie internetu dla funkcjonowania jednostki w społeczeństwie informacyjnym*, w: *Diagnoza internetu 2009*, (red.) K. Krejtz, Warszawa.

Leszczyński A. (2011), *Statystycznie podobny do Breivika*, rozmowa z prof. Davidem Lyonem, „Gazeta Wyborcza", 1.08.2011.

Liedl K. (2008), *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń.

Lubański M. (2004), *Społeczeństwo informacyjne a cywilizacja informatyczna*, w: *Dylematy cywilizacji informatycznej*, (red.) A. Szewczyk, Warszawa.

Państwo 2,0 nowy start dla e-admnistracji (2012), http://mac.gov.pl/dzialania/raport-panstwo-2-0--nowy-start-dla-e-administracji/ (26.08.2012).

Polak w Internecie: mniej świadomy zagrożeń od przeciętnego Europejczyka (2012), Wyniki badania Microsoft na temat światowego bezpieczeństwa w sieci, http://tech.wp.pl/kat,1009785,title,Polak-w-Internecie-mniej-swiadomy-zagrozen-od-przecietnego-Europejczyka,wid,14242896,wiadomosc.html?ticaid=1f010 (23.08.2012).

Potejko P. (2009), *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, (red.) K. A. Wojtaszczyk, A. Materska-Sosnowska, Warszawa.

Poznański P. (2011), *Po co nam elektroniczne urzędy?*, „Gazeta Wyborcza" Dodatek Teleinformatyka, 19.05.2011.

Poznański P. (2012), *Cyfrowa klapa polskich urzędów. Bruksela wstrzymała nam 3,7 mld zł*, „Gazeta Wyborcza", 24.04.2012.

Pytlakowski P. (2010), *Gęba na kłódkę*, „Polityka", 6.11.2010.

Pełny zapis przebiegu posiedzenia Komisji Spraw Wewnętrznych (nr 106) Komisji Sprawiedliwości i Praw Człowieka (nr 127) Komisji do Spraw Służb Specjalnych (nr 71) 12 wrzesień 2013 (2013), http://orka.sejm.gov.pl/zapisy7.nsf/0/DA9262FD2F485D74C1257BF0002DC2E3/%24File/0234907.pdf (20.04.2015).

Rochowicz P., Szymańska B., Baranowska K., Stróżyk J. (2012), *Co hamuje rozwój e-państwa*, „Rzeczpospolita", 26.04.2012.

Rydlewski G., Szustakiewicz P., Golat K. (2012), *Udzielanie informacji przez administrację publiczną (teoria i praktyka)*, Warszawa.

Sibiga G., (2012), *Niezbędna reforma prawa do informacji*, „Rzeczpospolita", 14.05.2012.

Siedlecka E. (2010), *Rezygnacja z prywatności na rzecz bezpieczeństwa poszła za daleko*, Rozmowa z Ireną Lipowicz Rzecznikiem Praw Obywatelskich, „Gazeta Wyborcza", 15.10.2010.

Siedlecka E. (2012), *Sąd nad wszechobecną inwigilacją*, „Gazeta Wyborcza", 10.07.2012.

Siedlecka E. (2012), *Pozorne cywilizowanie bilingowania*, „Gazeta Wyborcza", 30.05.2012.

Sienkiewicz P. (2011), *Zagrożenia dla demokracji w społeczeństwie informacyjnym*, w: *Transformacje demokracji*, (red.) L. W. Zacher, Warszawa.

Szczepankowska I. (2012), *Polszczyzna w komunikacji prawno-sądowej dawnej Rzeczypospolitej*, http://www.rjp.pan.pl/index.php (10.08.2012).

Sześć tysięcy podsłuchów w jeden rok (2011), http://prawo.rp.pl/artykul/683476.html (18.04.2015).

Szumańska M., Głowacka D. (2011), *Nadzór 2011. Próba podsumowania*, http://panoptykon.org/ (10.08.2012).

TK opublikował uzasadnienie wyroku ws. zasad inwigilacji (2014), http://prawo.rp.pl/artykul/1146889.html (20.04.2015).

Trochę mniej podsłuchów w ubiegłym roku (2013), http://www.lex.pl/czytaj/-/artykul/troche-mniej-podsluchow-w-ubieglym-roku (19.04.2015).

Ustawa kodeks karny (1997), Dz. U., Nr 88, poz. 553 z późn. zm.

W 2013 roku policja i inne służby chciały podsłuchu 4509 osób (2014), http://www.tvn24.pl/wiadomosci-z-kraju,3/w-2013-roku-policja-i-inne-sluzby-chcialy-podsluchu-4509-osob,414768.html (18.04.2015).

Więcej podsłuchów i sprawdzania bilingów w 2014 roku (2015), http://www.lex.pl/czytaj/-/artykul/wiecej-podsluchow-i-sprawdzania-bilingow-w-2014-roku (20.04.2015).

Wybranowski W., Wikariak S. (2012), *Ograniczenie dostępu do informacji publicznej*, http://www.rp.pl/artykul/718542.html?print=tak&p=0 (15.08.2012).

Wymagania w zakresie monitoringu (2012), dokument opracowany przez Generalnego Inspektora Danych Osobowych i przesłany Ministrowi Spraw Wewnętrznych i Administracji 24.08.2011, http://www.giodo.gov.pl/1520106/id_art/4278/j/pl/ (18.08.2012).

STRESZCZENIE

Artykuł stanowi próbę naszkicowania panoramy najistotniejszych zagrożeń w sferze bezpieczeństwa informacyjnego współczesnej Polski. Punktem wyjściowym prowadzonych rozważań jest krytyczna analiza dotychczas stosowanych ujęć terminów „bezpieczeństwo informacyjne" i „zagrożenie informacyjne". W dalszej części po ukazaniu głównych zagrożeń charakterystycznych dla globalnego społeczeństwa informacyjnego autor wskazuje listę zasadniczych zagrożeń informacyjnych dla bezpieczeństwa współczesnej Polski, zaliczając do nich: ograniczanie dostępu do informacji związane z: nadmierną uznaniowością i restrykcyjnością systemu ochrony tajemnic, słabość systemu udostępniania informacji publicznych, wykluczenie cyfrowe, hermetyzację specjalistycznej terminologii, naruszanie wolności informacyjnej związane z rozwojem różnych form inwigilacji, niedoskonałości systemu ochrony danych osobowych, zapóźnienia w wprowadzaniu e-administracji, przestępczość w sferze informacyjnej. Posługując się tak wyspecyfikowanym katalogiem zagrożeń autor dokonuje ich szczegółowej egzegezy, ukazując zarówno skalę, jak i realne oraz potencjalne ich konsekwencje. W konkluzji rodzi to wniosek, iż współczesny wymiar zagrożeń dla bezpieczeństwa informacyjnego Polski wiąże się przede wszystkim z wielowątkowo traktowanymi kwestiami dostępu do informacji.

THE INFORMATION DIMENSION OF THREATS TO THE SECURITY OF POLAND

ABSTRACT

The article attempts to depict the most important spectrum of the threats to the Poland's information security. The initial point that is being considered refers to the critical analysis of terms applied to information security and information threats. In further part of the article the author after broad presentation of threats characteristic of globalization indicates the list of the fundamental information threats to security of today's Poland including limitation of access to information which depends on excessive free choice decision, restrictive practices of classified information protection system, weakness of make information available to the public, digital ex-

clusion, impenetrability of special expert's terminology, infringement of rights to information by various forms of surveillance, imperfection of personal data protection system, delay of implementation of e administration, breaking law and crime in information domain. Specifying the catalogue of threats the author provides critical analysis in details and depicts the range of real and potential threats and their consequences. In his concluding remarks claims that contemporary dimension of threats to Poland's security is connected first of all with various issues related with access to information.