Z Kroniki prac nad retencją danych: przełom 2005 i 2006 roku.

Piotr Waglowski[1]

Prace nad „retencją danych" zarówno w Unii Europejskiej jak i w Polsce trwały od dłuższego czasu. W niniejszym opracowaniu koncentruje się jednak na kluczowym momencie procesu stanowienia prawa, tj. na okresie bezpośrednio poprzedzającym przyjęcie stosownych regulacji zarówno w polskiej ustawie Prawo telekomunikacyjne, jak również na szczeblu unijnym – w formie stosownej dyrektywy.

Opracowanie, które w tej chwili Szanowny Czytelnik ma w ręku stanowi jedynie swoistą kronikę wydarzeń przełomu lat 2005/2006. Nie stanowi ono jednak opracowania naukowego, chyba, że ktoś uzna je za przyczynek do badań nad historią doktryn politycznych i prawnych rodzącego się właśnie „społeczeństwa informacyjnego".

LIBE

W pierwszej części niniejszego opracowania warto chwilę poświęcić informacji o wydarzeniach nieco wcześniejszych, a mianowicie o tym, że Komisja Wolności Obywatelskich LIBE[2], która zajmowała się projektem dyrektywy dotyczącej zatrzymywania sygnałów telekomunikacyjnych (retencją danych), przyjęła 24 listopada 2005 roku raport Alexandra Nuno Alvaro. Raport został przyjęty stosunkiem głosów 33 (za) do 8 (przeciw) z pięcioma głosami wstrzymującymi się.

Parlamentarzyści zgodzili się, że istnieje konieczność zbierania danych telekomunikacyjnych przez odpowiednie służby, jednak tylko w przypadku pewnych sytuacji. Taka procedura wina być ograniczona do szczególnych form popełnienia poważnych przestępstw. Chodzi o to, by podsłuchu komunikacji elektronicznej nie można było zlecić w przypadku drobnych spraw, a jedynie w przypadku, gdy podejrzewa się kogoś o działania terrorystyczne lub udział w zorganizowanej grupie przestępczej. Członkowie komisji uznali, że zbyt szeroka możliwość stosowania podsłuchu będzie wykorzystywana przez władze krajów członkowskich w sposób niezgodny z pierwotnym przeznaczeniem projektowanej właśnie regulacji.

Komisja LIBE usunęła również kontrowersyjny zapis projektu dyrektywy, na mocy którego kraje członkowskie mogłyby wykorzystywać przejęte dane (podsłuchane) "w innych celach[3]". To kolejny punkt zapalny. Zapis ten zaproponowała Komisja... LIBE skróciła czas, w jakim dane mogłyby być przechowywane (już po ich "ujęciu"). Jej zdaniem ten okres to nie mniej niż sześć miesięcy, jednak nie więcej niż dwanaście miesięcy. Komisja w swojej propozycji chciała, by te okresy wynosiły odpowiednio dwanaście i 24 miesiące.

A co jeśli jakaś firma nie będzie chciała przejmować dla państwa sygnałów obywateli (albo wykorzysta te informacje w niecnych celach)? LIBE dodała pewne ograniczenie do sankcji przewidzianej przez Komisje dla takich podmiotów: sankcja taka ma być "efektywna, proporcjonalne i możliwa do cofnięcia[4]".

Wreszcie - LIBE uznała, że w projektowanej dyrektywie winien się znaleźć zapis, zgodnie z którym jedynie specjalne organy państwowe, te mianowicie, które zajmują się wymiarem sprawiedliwości[5] winny mieć dostęp do przejętych danych. A jeśli jakieś kraje trzecie chciałyby mieć do nich dostęp, to może się to odbyć jedynie na podstawie umowy międzynarodowej.

---

[1] Piotr Waglowski, prawnik, autor serwisu VaGla.pl Prawo i Internet, słuchacz studiów doktoranckich prowadzonych w Instytucie Nauk Prawnych Polskiej Akademii Nauk, w omawianych dniach członek zarządu stowarzyszenia Internet Society Poland. Niniejsze opracowanie powstało w oparciu o materiały zgromadzone w ramach serwisu VaGla.pl Prawo i Internet z przeznaczeniem do publikacji w materiałach konferencyjnych konferencji „Future of Internet Security. Bezpieczeństwo i retencja danych", mającej odbyć się w Krakowie w dniu 2 marca 2006 roku. Materiały poświęcone „retencji danych telekomunikacyjnych" zgromadzone są pod adresem: http://prawo.vagla.pl/retencja_danych.

[2] the Civil Liberties, Justice and Home Affairs

[3] ang. „other related purposes"

[4] ang „effective, proportionate and dissuasive"

[5] ang. „judicial authorities"

Z tym się wiąże inna sprawa: jeśli organy ścigania[6] w kraju członkowskim będą chciały mieć dostęp do zebranych danych, to mogą go uzyskać jedynie za zgodą wymiaru sprawiedliwości. Komisja i Rada chciały, by ten dostęp do gromadzonych danych miały dowolne władze - w zależności od regulacji danego kraju członkowskiego. Na podstawie propozycji LIBE określone władze nie miałyby dostępu do całości zgromadzonych przekazów, a jedynie do danych związanych z konkretną sprawą. Znów pojawił się potencjalny konflikt: Komisja chciała, by służby miały dowolny dostęp do całej bazy przekazów zbieranych przez przedsiębiorców telekomunikacyjnych, możne by rzec: in genere.

Co mają zbierać te firmy telekomunikacyjne? Komisja LIBE uznała, że nie koniecznie winny to być informacje o nieskutecznych połączeniach. U podstawy takiej decyzji leżało to, że dziś firmy telekomunikacyjne zbierają informacje o udanych połączeniach ze względu na bilingi, ale raczej nie przechowują danych o połączeniach nieudanych (takich, które nie zakończyły się nawiązaniem połączenia, innymi słowy - o próbach nawiązania połączenia). LIBE widziała tu możliwość pozostawienia kwestii zbierania informacji o połączeniach nieudanych państwom członkowskim.

Ale jedną z ciekawszych kwestii jest stanowisko LIBE, zgodnie z którym państwa członkowskie winny w pełni pokrywać koszty retencji danych. Dotyczy to wszystkich kosztów (zarówno tych związanych z inwestycjami w infrastrukturę konieczną do stworzenia warunków do gromadzenia danych, jak i te, związane z eksploatacją systemu).

Już w momencie przyjęcia przez LIBE swojego stanowiska wiadomym było, że jeśli przed końcem roku nie dojdzie do uzyskania kompromisu pomiędzy Parlamentem Europejskim i Radą, wówczas Rada przeforsuje własne rozwiązania. Prezydencji Brytyjskiej niezwykle zależało na przyjęciu dyrektywy, a to również ze względów politycznych. Niedawne ataki w londyńskim metrze, oraz udział Wielkiej Brytanii w wielkiej koalicji antyterrorystyczna u boku USA. Przyjęcie dyrektywy miało być głównym sukcesem Wielkiej Brytanii - czasowego przywódcy Unii Europejskiej.

Przy okazji batalii związanej z "retencją danych" po raz kolejny okazało się, że Parlament Europejski (składający się z polityków wybieranych wszak w wyborach bezpośrednich, a więc zależnych od swoich wyborców) ma inne zdanie w kluczowych kwestiach niż przedstawiciele rządów.

Polska debata na forum Komisji do Spraw Unii Europejskiej

Polska brała również udział w pracach Unijnej Rady. Warto w tym miejscu odnotować wypowiedź Podsekretarza stanu w Ministerstwie Sprawiedliwości Andrzeja Grzelaka, na forum sejmowej Komisji do Spraw Unii Europejskiej[7]: "Z uwagi na ostatnie ataki terrorystyczne w Europie prezydencja brytyjska uznała przyjęcie aktu prawnego w sprawie retencji danych telekomunikacyjnych za swój priorytet. Będzie dążyła do zakończenia prac nad dokumentem do końca tego roku". Minister Grzelak zrelacjonował posłom historię prac nad regulacją unijną: "Dotychczasowe prace w zakresie przetrzymywania danych toczą się od 28 kwietnia 2004 r. Przedłożony wówczas projekt decyzji ramowej miał odmienną podstawę prawną i w efekcie poszerzony zakres przedmiotowy w stosunku do prezentowanego projektu dyrektywy. Sejm miał już okazję zapoznać się z podstawowymi kwestiami wyznaczającymi zakres obowiązku przetrzymywania danych, takimi jak katalog danych, okresy przetrzymywania i koszty związane z tym obowiązkiem dzięki przedstawionej i pozytywnie zaopiniowanej przez Komisję do Spraw Unii Europejskiej w dniu 1 grudnia 2004 r. informacji rządu w sprawie decyzji ramowej o przetrzymywaniu danych".

Poseł Tadeusz Iwiński (SLD) miał wątpliwości, które wyartykułował na forum wspomnianej komisji słowami[8]: "Chciałbym prosić pana ministra o dokładniejsze przedstawienie projektów regulacji, dlatego że to, co pan minister powiedział, jest szalenie mgliste, a poza tym rzecz dotyczy ogromnie delikatnej materii. Wspomnę tylko o dwóch sprawach. Rok temu, gdy Polska nie miała jeszcze swoich eurodeputowanych, ci z nas, ja również się znalazłem w tym gronie 54, którzy przez prawie 3 miesiące mieli prawo, jako byli obserwatorzy uczestnictwa w debatach Parlamentu Europejskiego i byli świadkami, a niektórzy z nas brali w tym udział, ogromnie burzliwej debaty właśnie na ten temat.

[6] ang. „enforcement authorities"
[7] Na podstawie stenogramu Komisji do Spraw Unii Europejskiej /nr 3/ z dnia 16 listopada 2005, dostępnego na stronach Sejmu w formie Biuletynu (http://orka.sejm.gov.pl/Biuletyn.nsf/0/03055CCD1E1A2B30C12570C900373825?OpenDocument)
[8] Ibidem.

Sprawa była kwestionowana przez wielu eurodeputowanych do PE i nie tylko. Po drugie, mówię to jako wiceprzewodniczący Zgromadzenia Parlamentarnego Rady Europy, czyli organizacji, która dba szczególnie o prawa człowieka i demokrację – w tej sprawie stanowisko niektórych rządów i wielu parlamentów jest bardzo powściągliwe. Oczywiście, trzeba walczyć z terroryzmem, i to jest poza dyskusją. Ale jeżeli słyszę od pana ministra opinię, że będą przechowywane nie treści e-maili czy treści sms-ów, a tylko informacje o połączeniach, to po pierwsze, nie mam specjalnego zaufania, że tak będzie, po drugie, jaki będzie system kontroli i po trzecie, jak to się będzie odbywało? Sprawa dotyczy wyjątkowo delikatnej tematyki przestrzegania praw człowieka i praw jednostki i nie można wobec niej przechodzić w sposób oczywisty. Chcę przypomnieć, że w ubiegłym tygodniu w parlamencie brytyjskim odrzucono zdecydowaną większością głosów, i to również członków Labour Party, projekt rządu, który zaostrzał regulacje w mniej więcej tej samej sprawie, ponieważ uznano, że to idzie za daleko i narusza prawa człowieka".

Kolejne wątpliwości zgłosił [9] Poseł Andrzej Gałażewski (PO): „Jest pewna niespójność między stanowiskiem rządu a tym projektem dyrektywy. My, jako Komisja, de facto oceniamy projekt aktu prawnego, czyli projekt dyrektywy. Osobiście uważam, że jest on tak sformułowany, że można go poprzeć. Rząd też popiera ten projekt dyrektywy, a jednocześnie w stanowisku rządu są pewne uwagi, które odbiegają od projektu dyrektywy. Chciałbym powiedzieć o dwóch sprawach. Pierwsza: w stanowisku rządu jest akceptacja dla rozszerzania czasu przechowywania danych z 12 czy 6 miesięcy, w zależności od typu danych, do 24 miesięcy. Nie znalazłem takiej alternatywy w projekcie dyrektywy. Tam jest po prostu powiedziane, że okres przechowywania jest 12 miesięcy i 6 miesięcy dla danych z komunikacji internetowej. Nie ma mowy o możliwości rozszerzenia na 24 miesiące. Druga sprawa dotyczy rekompensaty za dodatkowe czynności ponoszone przez operatorów związane z przechowywaniem danych. Wydaje mi się, że projekt dyrektywy nakłada na państwo obowiązek pokrywania tych kosztów. Natomiast tutaj jest, i pan minister to potwierdził, mówiąc, że nasze prawo telekomunikacyjne każe ponosić te koszty bez zwrotu operatorowi. Oczywiście w projekcie dyrektywy jest mowa o dodatkowych kosztach, jakie ona niesie, ale ze stanowiska rządu wynika, że rząd nie ma zamiaru pokrywać tych dodatkowych kosztów i raczej by widział to w formie pokrywania przez operatorów. Oczywiście nie zostanie podniesiona stawka za korzystanie z internetu i de facto to użytkownicy internetu i telekomunikacji będą ponosili koszty prewencji przestępczości. Jest to niefortunne, ponieważ państwo powinno ponosić te koszty. I dyrektywa zmusza do tego rządy. Dyrektywa wiąże obie strony, nie tylko rząd, i każe dostosowywać nasze prawo narodowe do jej ram, ale mogą się również na nią powoływać operatorzy, którzy też czytają akty prawne i będą wiedzieli, że rząd, po pierwsze, zamierza rozszerzyć czas przechowywania danych ponad wymagania dyrektywy, a po drugie, nie ma zamiaru zwracać dodatkowych kosztów z tego wynikających".

Podsekretarz stanu w MS Andrzej Grzelak odpowiedział posłom: „Jeśli chodzi o rekompensaty, zdaniem rządu decydowanie o rekompensatach przez prawo unijne nie bardzo znajduje podstawę, dlatego też stanowisko Polski jest takie, żeby to regulować prawem wewnętrznym. Jest oczywiste, że pewne funkcje państwa, zwłaszcza te, które dotyczą bezpieczeństwa obywateli, są obowiązkiem tego państwa i w związku z tym państwo powinno ponosić koszty. Ale trzeba zwrócić uwagę i na to, że polskie prawo telekomunikacyjne w stosunku do praw telekomunikacyjnych innych państw zawiera dosyć daleko idące regulacje i dostosowanie się do dyrektywy nie będzie więc zbyt wielkie. W związku z tym, na wniosek Komitetu został powołany specjalny zespół, który ma przede wszystkim ustalić, na ile zwiększą się te dane, które operatorzy będą musieli przetrzymywać w stosunku do tego obowiązku, który wynika z ustawy. Zespół ten ma też oszacować koszty, a potem trzeba będzie się zastanowić, jak z tymi kosztami postąpić. Ale traktujemy to jako wewnętrzną sprawę Polski". I dalej: "operatorzy przetrzymują dane ze względów gospodarczych, bo np. muszą wystawiać faktury, i na ogół przetrzymują je właśnie przez taki okres, o jakim jest tu mowa. Zaś kwestia wydłużania tych okresów jest w tej chwili płynna, dlatego że to jest projekt dyrektywy i tekst wciąż jest doskonalony. Co do 12 i 6 miesięcy stanowisko jest oczywiste".

Odpowiedź ministra uzupełnił przedstawiciel Ministerstwa Sprawiedliwości Cezary Michalczuk, prokurator w Departamencie Współpracy Międzynarodowej w MS: „...tak jak powiedział pan poseł Tadeusz Iwiński, faktem jest, że ta dyrektywa dotyka bardzo drażliwych kwestii, a mianowicie głównie ochrony tajemnicy korespondencji, a tym samym praw człowieka i podstawowych wolności, czyli wolności człowieka od ingerencji państwa w jego prywatne komunikaty. Od razu chcę zaznaczyć, że ta dyrektywa nie porusza materii treści komunikatów. W przepisach dyrektywy wyraźnie wyłączone są

[9] Ibidem

komunikaty, zarówno elektroniczne, czyli e-mailowe, jak i rozmowy telefoniczne. Nie będzie tak, że jakiekolwiek państwo będzie zobowiązywało swoich operatorów do przechowywania treści połączeń między mną a moim kolegą, bo to ingeruje w tajemnicę korespondencji, a naruszenie tajemnicy korespondencji podlega przepisom prawa karnego. W każdym państwie zresztą jest tak samo. Dyrektywa w razie jej przyjęcia, bo jest to póki co kwestia dyskusyjna, czy będzie przyjęta, czy nie, ponieważ nie ma zgodności w Radzie UE co do tego, będzie zobowiązywała państwa członkowskie do nakazania operatorom przechowywania takich danych, jak np. kto dzwonił, kto jest abonentem, który się łączył, jakie są dane osobowe tego człowieka, jakie są dane abonenta, do którego wykonywano połączenie, czyli z kim było połączenie. Będzie określane również, jak długo trwało połączenie między nimi, o której godzinie i w której minucie to połączenie zostało zainicjowane i kiedy zakończone. Będzie możliwe ustalenie urządzenia, które było wykorzystane, czyli, czy to był telefon komórkowy, czy stacjonarny, czy internet. Ostatnia informacja będzie dotyczyć miejsca, czyli tak zwanej danej lokalizacyjnej". I dalej: „(...) przestępcy wykorzystują coraz częściej instytucję tzw. połączeń nieodebranych, tzn. połączenie jest inicjowane, ale rozłączone przez samego dzwoniącego przed uzyskaniem połączenia. Obecnie te dane nie są przechowywane, bo są zbędne dla operatorów. Jest to niezmiernie ważne, bo jedna z bomb w Londynie została detonowana właśnie na podstawie wysłania z komórki sygnału do drugiej komórki, która znajdowała się w pociągu i której mechanizm elektryczny zainicjował wybuch bomby. Potem było możliwe ustalenie, skąd nadany był sygnał. I znowu, mamy kamerę w metrze londyńskim wychwytującą osobę, która dzwoniła, i mamy w ten sposób sprawcę. Dla potrzeb prokuratury i sądów w kwestiach dowodowych i wykrywczych jest to sprawa zupełnie priorytetowa".

W kolejnym fragmencie czytamy: „Oczywiście kwestia bardzo drażliwa – z wiadomych przyczyn mogą tu być poniesione pewne koszty, więc w państwach unijnych trwa dyskusja na ten temat, czy jest to zasadne. Natomiast niektóre państwa mają te regulacje, i to o wiele dalej idące. Przykładem jest Wielka Brytania. Pan poseł Tadeusz Iwiński słusznie powiedział, że w Wielkiej Brytanii debata była toczona i faktycznie ten projekt nie przeszedł. Ale był to projekt, który drastycznie wydłużał okresy przechowywania danych, bodajże z półtora roku do 4 lat, o ile pamiętam, i na to nie było zgody. Natomiast samej zasady się nie kwestionuje, bo w Wielkiej Brytanii jak również w Irlandii priorytetem jest walka z przestępczością. Podobne myślenie jest w innych państwach, takie mamy sygnały w MS, bo mamy kontakt z naszymi odpowiednikami w innych państwach".

Kolejne uwagi Posła Andrzeja Gałażewskiego: „Dzisiaj przyjmując ten projekt, usztywniamy stanowisko rządu, bo akceptujemy projekt. Rząd ma obowiązek prezentować takie stanowisko, jakie będzie mu sugerowała Komisja. W związku z tym, jeżeli na posiedzeniach będziecie państwo prezentować inne stanowisko, będziecie występować ze stanowiskiem odmiennym od tego, które dzisiaj przyjmiemy. A my dyskutujemy o zupełnie innym projekcie niż te nowe projekty, o których przed chwilą pan powiedział, i przyjmujemy stanowisko. To jest problem, który może spowodować pewien konflikt między Komisją a MS, ponieważ, rozumiem, że się zmieniają projekty i co dwa tygodnie są inne, ale państwo przedstawiliście konkretny projekt do zaopiniowania i my ten zaopiniujemy, czyli ten, w którym będą ramy ustanowione 12 i 6 miesięcy oraz będzie powiedziane, że dodatkowe koszty, w przypadku Polski dotyczące szczególnie internetu, będą musiały być pokrywane przez państwa członkowskie".

Poseł Piotr Gadzinowski (SLD) o swojej wizycie w w Hongkongu w Urzędzie Antykorupcyjnym: „Podstawowym problemem tego urzędu może nie jest to, że ogranicza wolności obywatelskie, że przechowuje wiedzę, ale że ta wiedza wypływa. I tutaj jest podobna sytuacja. Bo możemy zrezygnować z pewnej swojej suwerenności czy z pewnej prywatności na rzecz walki z terroryzmem, ale jakie mamy gwarancje, że ta wiedza o naszej prywatności, która może być wykorzystana przeciwko nam, nie wypłynie. Że nasze rozmowy, które nie będą związane z działalnością terrorystyczną, mogą być np. wykorzystane w kwestiach obyczajowych, biznesowych, rodzinnych i innych, nie znajdą się w mediach"

Posłanka Grażyna Ciemniak (SLD): „Myślę, że dyskutujemy o tym, bo nikt nie neguje potrzeby wprowadzenia regulacji, ale nie może być tak, jak niektórzy sugerowali w swoich wypowiedziach, że prawo prawem, ale życie może nieco inaczej wyglądać. Stąd moje pytanie, jakie techniczne możliwości zabezpieczenia są czy będą, że te dane znajdujące się w załączniku załączonym do projektu dyrektywy, w którym jest wyspecyfikowanych kilkadziesiąt danych, w zależności od tego, jakim źródłem jest odbiorca połączenia, będą chronione? Że będą przetrzymywane, ale nie będzie miał do nich dostępu operator, tylko ta instytucja czy osoba, która będzie wyznaczona, aby móc te

dane w celu ścigania pozyskać. Kto w Polsce ustali sposób zabezpieczenia, o którym mowa w art. 3 w pkt 1 i 2 dyrektywy? Bo na pewno wprowadzenie tych zabezpieczeń jest trudne, ale musimy wiedzieć, kto je ustali, w jakim trybie i kto będzie później kontrolował. Te pytania zadał również pan poseł Tadeusz Iwiński, ale nie usłyszeliśmy odpowiedzi"...

Podsekretarz stanu w MS Andrzej Grzelak odpowiadając na pytania i wątpliwości stwierdził m.in.: „Jeżeli chodzi o uwagi i wątpliwości pana posła Piotra Gadzinowskiego dotyczące gwarancji, że prywatność nie zostanie naruszona dalej, niż to jest niezbędnie potrzebne przy wykorzystywaniu tych możliwości, z dyrektywy wynikałoby, że korzystać z tego będzie mógł tylko prokurator i sąd i to w sprawach wszczętych. Nawiązując również do wątpliwości pani poseł, trzeba by powiedzieć, że operator, z którego powodu jakieś informacje znalazłyby się poza tymi dwoma podmiotami, popełnia przestępstwo. Z tego punktu widzenia jest to bezpieczeństwo instytucjonalne – że tylko prokurator i tylko sąd, i tylko w sprawach wszczętych, które się toczą, i w żadnych innych. A więc to nie jest dostęp do informacji w ogóle przez jakiekolwiek inne organy..."

Pan Cezary Michalczuk uzupełnił: „Odnosząc się jeszcze do tego udostępniania danych, o które pytał pan poseł Piotr Gadzinowski – jak już powiedział pan minister, prokuratura wszczyna jakieś postępowanie lub jest ono prowadzane przez sąd na etapie postępowania sądowego i konieczne jest zasięgnięcie informacji o określonych danych od operatora. Wtedy takich informacji na postanowienie prokuratora się zasięga. Robione jest to teraz i będzie robione w przyszłości. Nie ma możliwości, żeby Służby Specjalne, czy osoby powołane do ścigania w jakichś kwestiach obyczajowych miały jakiekolwiek uprawnienia do żądania takich danych od operatorów telekomunikacyjnych. Jest to absolutnie wykluczone. Gwarancja jest tu w ramach postępowania karnego, które jest toczone, i tę gwarancję prawidłowości prowadzenia daje prokurator albo sąd. Jeżeli to zakwestionujemy, to musimy zakwestionować kompetencje sądu i prokuratora do prowadzenia postępowań karnych w ogóle. Na pewno nie jest celem gromadzenie danych w celu udostępniania prasie czy szantażowania kogokolwiek. Nie. Postępowanie karne jest wszczęte i od tego momentu uruchamiają się wszystkie regulacje Kodeksu postępowania karnego, a tam zabezpieczeń nałożonych i na prokuratora, i również na sąd, bo łącznie z kontrolą instancyjną decyzji wydawanych przez prokuraturę i przez sąd, jest dużo. Padło pytanie dotyczącego tego, co będzie, jeżeli te dane wypłyną w jakiś sposób. Jeżeli dane gromadzone przez operatora wypłynęłyby od operatora i dostały się do prasy czy w inne niepowołane ręce, to sankcji i obwarowań w takich przypadkach jest kilka, również obecnie. Przede wszystkim z ustawy – Prawo komunikacyjne wynika, że Prezes Urzędu Regulacji Telekomunikacji i Poczty ma uprawnienie do tego, by podmioty, które złamały tajemnicę telekomunikacyjną, były odpowiedzialne za to nawet do utraty koncesji. Więc żaden podmiot prowadzący usługi na rynku telekomunikacyjnym nie zaryzykuje umyślnego upłynnienia posiadanych danych z obawy przed utratą koncesji do świadczenia usług. To najbardziej trafia w operatów i uważam, że jest wystarczającym środkiem powstrzymującym takie ewentualne zapędy z ich strony".

Warto przestudiować pełny zapis stenograficzny z obrad komisji. Komisja powołała trzyosobowy zespół, który został zobligowany do przygotowania na kolejne posiedzenie projekt opinii na temat stanowiska Rządu odnośnie dyrektywy.

Poseł Michał Wójcik (PiS) na kolejnym posiedzeniu Komisji[10] zabrał głos: „Zostałem wyznaczony do zabrania głosu w tej sprawie. Po burzliwej dyskusji, która odbyła się na ostatnim posiedzeniu Komisji do Spraw Unii Europejskiej, została powołana grupa w składzie trzech osób. Grupa spotkała się wczoraj i wypracowaliśmy kompromisową, moim zdaniem, opinię, pomimo tego, że stanowisko jednej z osób było takie, że ta dyrektywa nie obejmuje jednak wszystkich obszarów, które powinny zostać objęte tą materią, wokół której toczy się dyskusja. Generalnie grupa przyjęła, że popiera stanowisko rządu w sprawie dyrektywy, a nasze wątpliwości rozwiała opinia przedstawiona przez Ministerstwo Sprawiedliwości. Nie wiem, czy jest potrzeba, aby ją przedstawiać, bo zawiera się na pięciu stronach. Podkreślę jeszcze raz, że popieramy stanowisko rządu w tym zakresie i taką rekomendację dzisiaj przedstawiamy Komisji. Niemniej zwracamy uwagę, co zostało zawarte w naszej opinii nr 4, którą otrzymaliście państwo w materiałach, na kilka ważnych elementów". I dalej: „Pierwsza sprawa to potrzeba zapewnienia ochrony dóbr osobistych i pewnych wolności konstytucyjnych. Druga – w

[10] Dyskusja była kontynuowana w czasie obrad Komisji do Spraw Unii Europejskiej /nr 4/ z dnia 24 listopada 2005. Zapis stenograficzny tego posiedzenia Komisji dostępny jest również na stronach Sejmu w formie Biuletynu (http://orka.sejm.gov.pl/Biuletyn.nsf/0/0F2E0FD39FB8F2C9C12570CF004CD083?OpenDocument)

związku z tym, że zostanie powołany specjalny zespół składający się z przedstawicieli organów ścigania, branży łączności elektronicznej oraz organów ochrony danych, rząd powinien zwrócić uwagę na dwie bardzo ważne kwestie. Przede wszystkim na to, aby, może nie tą dyrektywą, ale zintensyfikować prace tej grupy wokół pewnych usług tzw. nierejestrowalnych. Tych usług na dzisiaj, jak pani poseł wczoraj zasygnalizowała, jest 40-50 proc. Ta grupa powinna więc się zająć również tym obszarem nie objętym dyrektywą. I po drugie, aby zachować pewną równowagę pomiędzy ochroną danych osobowych a potrzebą uzyskania dostępu do tych danych. Krótko mówiąc, chodzi o to, żeby w jakiś dziwny sposób treści objęte tą usługą nie przedostawały się w niepowołane ręce. Zasadniczo, jeszcze raz mówię, popieramy stanowisko, jakie rząd zamierza zająć wobec tej dyrektywy".

Powyżej przedstawiłem jedynie fragmenty, by pokazać, iż dyskusja w Sejmie, w związku z kształtowaniem stanowiska Rządu w sprawie dyrektywy toczyła się. Zadziwiające, że w tym czasie o sprawie nie informowały „media głównego nurtu".

15 lat retencji

Przemysław Gosiewski podczas konferencji prasowej, która miała miejsce 29 listopada 2005 roku stwierdził, iż Prawo i Sprawiedliwość oczekuje, że bilingi telekomunikacyjne będą w Polsce przechowywane przez 15 lat. Tłumaczył to koniecznością zwiększenia skuteczności ścigania przestępstw. Stwierdził, że Konstytucja RP pozwala ograniczać wolności i prawa obywatelskie ze względy na bezpieczeństwo państwa i właśnie mamy do czynienia z taką sytuacją. Wobec tego PiS chce zmian w ustawie Prawo telekomunikacyjne i chce głosować nad nowelizacją ustawy jak najszybciej, by nowe przepisy weszły w życie 31 grudnia 2005 roku. Zdaniem Gosiewskiego: gdyby nie bilingi - nie mielibyśmy ważnej wiedzy w takich sprawach jak afera Rywina, informacji dotyczących łódzkiej ośmiornicy, mafii paliwowej, czy na temat łowców skór. Jak stwierdził podczas konferencji (emitowanej m.in. przez TVN24) - w tej kwestii raczej nie ma większych kontrowersji społecznych...

Dziennikarze zadali przewodniczącemu klubu PiS pytania o wycieki danych od operatorów telekomunikacyjnych. Poseł Gosiewski odpowiedział wówczas, że takimi sprawami powinna skutecznie zajmować się Agencja Bezpieczeństwa Wewnętrznego. Pytany o koszt infrastruktury zabezpieczającej dane (wedle wyliczeń Polskiej Izby Informatyki i Telekomunikacji: procedura wydawania poświadczenia bezpieczeństwa przemysłowego jest nie tylko skomplikowana, ale i kosztowna. Wydanie tylko przez ABW certyfikatu kosztuje ok. 9 000 złotych. Cała zaś procedura związana z przemysłowym certyfikatem bezpieczeństwa to koszty liczone w dziesiątkach tysięcy) stwierdził, że wedle jego wiedzy nie trzeba ponosić dziś żadnych nowych nakładów na infrastrukturę. Uznał również, że w chwili obecnej ważniejsze jest skuteczne ściganie przestępstw niż liczenie kosztów, jakie się z tym wiążą.

Jeden z dziennikarzy zapytał o VoIP[11]: czy rozszerzony wymóg przechowywania danych dotyczy również firm, które świadczą usługi dostępu do internetu? Poseł Gosiewski: Jeżeli kwestie dotyczące zbierania materiału dowodowego będą tego wymagały to warto się nad nimi pochylić. Sprawność prowadzenia postępowań karnych wymaga, by zbierać informacje o konkretnych połączeniach telefonicznych, a co za tym idzie informacje o tym, gdzie się dana osoba znajdowała.

Gosiewski stwierdził, że w tych sprawach nie możemy oglądać się na przepisy Unii Europejskiej, w której okresy przechowywania danych telekomunikacyjnych są obecnie znacznie krótsze.

W tym czasie media informowały o sprawie "wycieku z ERY". Jak pisała Rzeczpospolita w dniu 29 listopada, według Ryszarda Pospieszyńskiego, członka zarządu Polskiej Telefonii Cyfrowej związanego z francuską spółką Vivendi, z siedziby spółki miało wypłynąć kilka tysięcy stron tajnych dokumentów. Chodziło o informacje ze specjalnego departamentu Ery, tzw. działu ds. współpracy z organami ścigania. Dział udostępnia służbom billingi, pośredniczy w zakładaniu podsłuchów. W ubiegłym tygodniu Pospieszyński złożył w Agencji Bezpieczeństwa Wewnętrznego zawiadomienie o popełnieniu przestępstwa. Dzień wcześniej zawiadomił o tym Wojskowe Służby Informacyjne. Podobno obecna dyrekcja (związana z konkurującą frakcją w stosunku do tej, reprezentowanej przez Pospieszyńskiego) m.in. zlecała kopiowanie danych o klientach Ery, którymi w ostatnich latach interesowały się służby specjalne.

[11] Voice over IP

W dniu następnym, tj. 30 listopada, Rzeczpospolita pisze w artykule „Sprawdzają przecieki z Ery” (z nadtytułem: „AFERA Co się dzieje z tajnymi danymi”): "W zawiadomieniu do ABW oskarżono o kopiowanie danych abonentów Krzysztofa Bondaryka, który odpowiada za współpracę ze służbami (m.in. przy zakładaniu podsłuchów i sprawdzaniu billingów). Bondaryk to były szef delegatury UOP w Białymstoku. W 1996 r. odwołał go minister spraw wewnętrznych Zbigniew Siemiątkowski. Według Bondaryka - z powodów politycznych. Za rządu AWS Krzysztof Bondaryk był wiceministrem w MSWiA. Odszedł w 1999 r. - "Gazeta Wyborcza" zarzucała mu wtedy nadużycia przy archiwizowaniu dokumentów związanych z lustracją".

A skoro mowa o Gazecie Wyborczej – poinformowała ona pierwszego grudnia o wycieku danych z Telekomunikacji Polskiej. Ktoś wykradł bazę danych z numerami telefonów – w tym numerów zastrzeżonych - oraz adresów abonentów TP S.A. Wszystko trafiło do Internetu i przechowywane jest na amerykańskim serwerze[12]. Telekomunikacja wezwała listownie zarówno prowadzącego serwer, jak i autora strony do jej natychmiastowego usunięcia...

W Unii przed rozstrzygnięciem

Co zostało już wcześniej wspomniane - Komisja Parlamentu Europejskiego LIBE zaakceptowało propozycję Komisji z pewnymi istotnymi zmianami. Istnieje gigantyczna presja Prezydencji Brytyjskiej, która chce przyjęcia dyrektywy jeszcze przed końcem roku. Dyrektywa dotyczy podstawowych praw i wolności obywatelskich. Nie ma zgody w krajach członkowskich w odniesieniu do podstawowych zagadnień, których ma dotyczyć dyrektywa. Innymi słowy: projekt nowej regulacji wzbudza olbrzymie kontrowersje.

W Holandii trwa dyskusja pomiędzy odpowiednim ministerstwem a tamtejszym Senatem. W swoim liście senacka Komisja Sprawiedliwości i Spraw Wewnętrznych w ostrych słowach skrytykowała propozycje Komisji (Europejskiej). Wedle holenderskiej senackiej komisji wiele z projektowanych zapisów dyrektywy jest niepotrzebnych. Skrytykowano również wyniki raportu KPMG (przywoływanego przez Komisję).

Mamy wystąpienia Europejskiego Inspektora Ochrony Danych Osobowych (EDPS[13]). Zdaniem Petera Hustinx (pełniącego funkcję inspektora europejskiego, a wcześniej szefa holenderskiego urzędu ds ochrony danych) projektowane regulacje mają bezpośredni wpływ w sferę prywatności obywateli UE i muszą przestrzegać fundamentalnych praw człowieka. Dysponujemy bogatym orzecznictwem Europejskiego Trybunału Praw Człowieka dotyczącym tych zagadnień. Jak powiedział Hustinx - nowe regulacje, które będą osłabiać ochronę nie tylko są nie akceptowalne, ale również nielegalne.

Zgodnie z treścią wypowiedzi publikowanych w tym czasie - jeśli Parlament Europejski i Rada zdecydują, że legislacja dotycząca zbierania i przechowywania danych telekomunikacyjnych jest konieczna by walczyć z przestępczością i terroryzmem, wówczas – zdaniem EDPS - taka legislacja musi uwzględniać odpowiednie terminy przechowywania danych (zdaniem inspektora europejskiego dłuższe okresy niż 6-12 miesięcy są nie do zaakceptowania), należy ograniczyć rodzaje danych zbieranych w wykonaniu takiego prawa, a także zagwarantować bezpieczeństwo danych zgromadzonych. Osoba, której dane dotyczą musi mieć możliwość dochodzenia swoich praw a zbierający te dane muszą zagwarantować efektywność ich realizacji.

Najlepiej jednak zapoznać się z treścią opinii opublikowanych na stronie EDPS[14]. W jednej z nich Inspektor stwierdził, że wciąż nie jest przekonany do konieczności zatrzymywania danych telekomunikacyjnych oraz lokalizacyjnych, w calach egzekwowania prawa, w takim kształcie jak zaproponowała to Komisja[15]. EDPS wskazuje również na konieczność poszanowania Europejskiej Deklaracji Praw Człowieka.

W opinii Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zatrzymywania danych przetwarzanych w związku ze

[12] Dostępnym pod domeną www.ksiazka-telefoniczna.com
[13] European Data Protection Supervisor
[14] http://www.edps.eu.int/12_en_opinions.htm
[15] "is as yet not convinced of the necessity of the retention of traffic and location data for law enforcement purposes, as established in the proposal"

świadczeniem publicznie dostępnych usług łączności elektronicznej zmieniającej dyrektywę 2002/58/WE (COM(2005) 438 wersja ostateczna) czytamy: „EIOD uznaje wagę dysponowania przez organy ścigania Państw Członkowskich wszelkimi niezbędnymi instrumentami prawnymi, służącymi w szczególności do walki z terroryzmem i innymi poważnymi przestępstwami. Należna dostępność pewnych danych dotyczących ruchu oraz danych dotyczących lokalizacji związanych z publicznymi usługami łączności elektronicznej może być dla tych organów ścigania kluczowym narzędziem i może przyczynić się do zapewnienia fizycznego bezpieczeństwa ludności. Ponadto należy zauważyć, że nie łączy się to automatycznie z koniecznością wprowadzenia nowych instrumentów, jak przewidziano w omawianym wniosku". I dalej: „Jest również oczywiste, że wniosek ma znaczny wpływ na kwestie ochrony danych osobowych. Jeżeli rozważa się wniosek wyłącznie z perspektywy ochrony danych osobowych, dane dotyczące ruchu oraz dane dotyczące lokalizacji nie powinny w ogóle być zatrzymywane do celów ścigania przestępstw. Właśnie z powodów ochrony danych dyrektywa 2002/58/WE ustanawia zasadę prawną przewidującą, że dane dotyczące ruchu muszą zostać usunięte, gdy tylko ich przechowywanie przestaje być niezbędne do celów ściśle związanych z komunikacją (w tym naliczania płatności). Wyjątki od tej zasady prawnej są obwarowane ścisłymi ograniczeniami".

2 grudnia odbyło się spotkanie Rady – a więc przedstawicieli rządów państw członkowskich, na którym doszło do zawarcia "kompromisu" w sprawie retencji danych. Gazeta Wyborcza relacjonowała to spotkanie w wydaniu z 4 grudnia: „Polski rząd zgłaszał w piątek swoje wątpliwości w sprawie projektu nowego prawa. Najważniejsza z nich dotyczyła okresu przechowywania danych przez operatorów telekomunikacyjnych. Polski rząd nie chce, żeby w tekście dyrektywy pojawiał się maksymalny okres przechowywania danych. Dlaczego? - W Sejmie pojawiła się inicjatywa poselska, by w prawie telekomunikacyjnym wprowadzić 15-letni obowiązek przechowywania danych - wyjaśniał wiceminister sprawiedliwości Andrzej Grzelak. - Nie tylko zresztą Polska uważa, że proponowane dwa lata to za mało - stwierdził Grzelak"

Data retention is no solution

58257 osób z całej unii podpisało petycję [16] w sprawie prac nad dyrektywą pozwalającą na gromadzenie danych telekomunikacyjnych, a podpisali się pod następującymi stwierdzeniami:

„Jestem przekonany, że:

- Spisywanie rozmów jest narzędziem, które głęboko narusza prywatność życia każdego z nas;

- Gromadzenie osobistych i prywatnych informacji o wszystkich obywatelach jest nielegalne w świetle art. 8 Europejskiej Konwencji Praw Człowieka, gdyż drastycznie wykracza poza zakres odpowiedni dla swego celu;

- Bezpieczeństwo uzyskane w wyniku spisywania rozmów może okazać się iluzoryczne, gdyż jest bardzo prawdopodobne, że informacje o powiązaniach i kontaktach jednej osoby mogą zostać przypisane do działań podjętych przez kogoś innego lub przez automatyczny proces, który nie ma żadnego związku z działaniem danej osoby;

- metody używane do wdrożenia tej polityki są nielegalne, gdyż rządy części państw członkowskich, w których ich własne parlamenty odrzuciły projekty odpowiednich ustaw próbują teraz przepchnąć je w skali całej Unii Europejskiej pod pretekstem ujednolicenia metod w skali kontynentu oraz współpracy międzynarodowej.

Wzywam Komisję Europejską oraz Parlament Europejski do bardzo krytycznego przebadania propozycji powszechnego spisywania rozmów oraz potwierdzenia zasad ochrony praw człowieka, w tym ochrony prywatności, zwłaszcza w obecnych trudnych czasach".

[16] Podpisy pod petycją były zbierane w ramach kampanii „Data retention is no solution” (gromadzenie danych nie jest rozwiązaniem). Strona internetowa kampanii dostępna jest pod adresem: www.dataretentionisnosolution.com

Zbliżał się czas ostatecznej rozgrywki. Organizacje broniące w Unii Europejskiej praw człowieka podjęły ostatnią próbę wpłynięcia na treść przyjmowanych regulacji, adresując 5 grudnia do Posłów Parlamentu Europejskiego list otwarty:

Do Posłów Parlamentu Europejskiego

My niżej podpisani wzywamy do odrzucenia europejskiej Dyrektywy w sprawie zatrzymywania danych przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej zmieniającej dyrektywę 2002/58/WE (COM(2005) 438 wersja ostateczna).

Przyjęcie tej dyrektywy spowoduje nieodwracalne zmiany systemu ochrony praw obywatelskich w obrębie Wspólnoty Europejskiej. Będzie też niekorzystnie wpływać na ochronę praw konsumentów, oraz stworzy bezprecedensowe bariery dla konkurencyjności Europy na rynkach światowych.

Brzemienne konsekwencje Dyrektywy

W społeczeństwie informacyjnym każde działanie człowieka pozostawia elektroniczne ślady (transaction logs). Każdy nasz ruch, każde nasze działanie i wzajemne relacje może być zarejestrowane zarówno w rejestrach publicznych jak i prywatnych. W związku z tym w Unia Europejskiej przyjęto pewne standardy dotyczące ochrony prywatności, zmierzające do ograniczenia przetwarzania danych osobowych. Teraz składająca się z przedstawicieli rządów Rada UE żąda, by Parlament Europejski całkowicie zmienił swe stanowisko i doprowadził do tego, by Europa zaczęła przewodzić Światu w powszechnej inwigilacji obywateli.

Na mocy regulacji Unii Europejskiej wiele z rejestrów już w tej chwili dostępnych jest dla odpowiednich służb egzekwujących prawo (law enforcement purposes), tak długo, jak operatorzy telekomunikacyjni przetwarzają zgromadzone dane dla celów biznesowych. Władze odpowiedzialne za sprawy wewnętrzne oraz wymiar sprawiedliwości naciskają jednak, by tak dostępnych danych było więcej.

Nowa dyrektywa przewiduje, że zbierane i przechowywane będą dane na temat każdej aktywności wszystkich uczestników komunikacji elektronicznej. Taki zbiór danych komunikacji elektronicznej (communications traffic data) pozwoli każdemu na dostęp i analizę: kto z kim i kiedy kontaktował się w sposób elektroniczny, a także gdzie przebybwał. Dane te będą przechowywane kilka miesięcy, a nawet przez lata.

Podczas niedawnego posiedzenia Rady (the Justice and Home Affairs Council), które miał miejsce w dniach 1 i 2 grudnia 2005 roku utrzymywano, że Parlament Europejski jakoby zgodził się na przechowywanie i gromadzenie takich informacji dla celów przeciwdziałania niejasno określonej przestępczości rozumianej szeroko, mimo iż
wcześniej dwukrotnie Parlament sprzeciwiał się takiej polityce.

Wzywamy członków Parlamentu Europejskiego do odrzucenia tej polityki z następujących przyczyn:

1. ***Dyrektywa wkracza w sferę prywatności wszystkich Europejczyków.*** *Dyrektywa wymaga gromadzenia wszelkich danych w bardzo szerokim znaczeniu (danych dotyczących wielu czynności wykonywanych za pomocą elektronicznych środków komunikacji). Tego typu polityka, dająca przyzwolenie na powszechne gromadzenie informacji tylko dlatego, że mogą być one interesujące dla państwa, nigdy nie była wcześniej prowadzona w UE.*

2. ***Zaproponowana dyrektywa jest niezgodna z prawem.*** *Proponując nieuzasadnione i tak szerokie zbieranie wrażliwych informacji o obywatelach pozostaje w sprzeczności z postanowieniami Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Zbierane będą informacje o poglądach politycznych, religijnych, medycznych, także tajemnice adwokackie i te pozostające pod ochroną prawa prasowego. Wszystko to będzie gromadzone i przechowywane, gotowe do użycia, oraz - być może - nadużywania.*

3. ***Dyrektywa uderza w prywatność konsumentów.*** *Ponad 58 tysięcy Europejczyków podpisało się już pod petycją przeciwko Dyrektywie. Jak wynika z badań w Niemczech: 78% obywateli tego kraju nie zgadza się z polityką gromadzenia o nich informacji. Jeśli dane będą gromadzone przez lata -*

Dyrektywa będzie miała znaczny wpływ na obniżenie aktywności konsumentów dokonujących obecnie transakcji drogą elektroniczną.

4. ***Dyrektywa uderza w Europejskich przedsiębiorców oraz godzi w ich konkurencyjność na rynkach globalnych****. Konieczność zbieranie i przechowywania danych tworzy nowe koszty liczone w setkach milionów Euro rocznie. Te nowe obciążenia dotyczą wyłącznie europejskiej branży IT: USA, Kanada, oraz Rada Europy odrzuciły wcześniej propozycje retencji danych.*

5. ***Nowa dyrektywa wymaga stanowienia w krajach członkowskich bardziej restrykcyjnego prawa.*** *Gdy raz zostanie wdrożona okaże się, iż nie jest skutecznym rozwiązaniem w walce z poważną przestępczością. W związku z tym pojawią się głosy, że należy dalej, w sposób drakoński, zaostrzać prawo, w tym postulaty:*

- wcześniejszej identyfikacji tych wszystkich, którzy zechcą skorzystać z kawiarni internetowych, publicznych telefonów, otwartych sieci bezprzewodowych (wireless hotspots), oraz klientów usług przedpłacanych (pre-paid),

- wprowadzenia zakazu wykorzystywania środków międzynarodowej komunikacji takich jak webmail (jak na przykład Hotmail czy Gmail), oraz zablokowania możliwości użycia usług oferowanych przez operatorów spoza Unii Europejskiej.

Nieusprawiedliwione działania

Proponowana polityka zbierania danych telekomunikacyjnych pozostawia na uboczu powyższe zastrzeżenia i zmierza głównie do harmonizacji działań na rzecz zwiększenia inwigilacji, jednocześnie nie przedstawiając propozycji mechanizmów obrony przed nadużyciami zgromadzonych danych. Budzi ona w Europie silny opór, a argumenty jej przeciwników są rozsądne i wyważone. Ich pomijanie jest niewytłumaczalne, gdyż tylko z ich uwzględnieniem można uratować Europę przed nielegalnymi konsekwencjami do jakich prowadzą forsowane propozycje.

Ich pomysłodawcy twierdzą, że zbieranie danych telekomunikacyjnych jest zjawiskiem powszechnym w Europie. W rzeczywistości jedynie pięć państw wprowadziło w tym zakresie pewne zasady, a jeszcze mniej wprowadziło praktykę dotyczącą zbierania danych komunikacji internetowej.

Jednocześnie Rada (rządy państw członkowskich) żąda, by Parlament Europejski zatwierdził rozwiązania, które proponowane wcześniej w krajach członkowskich poniosły porażkę. Dla przykładu Prezydencja Brytyjska forsuje swoją politykę, która jednak została odrzucona przez Parlament Wielkiej Brytanii. Teraz Rada stara się "wyprostować" wcześniejszą decyzję parlamentu krajowego.

Decydująca chwila

Z racji tego, że Unia Europejska wkroczyła na drogę wprowadzania tej bezprecedensowej polityki, obecnie stanęliśmy wobec bardzo ważnej decyzji: czy chcemy doprowadzić do uruchomienia łańcucha wydarzeń na końcu którego znajduje się społeczeństwo inwigilowane.

Takie zasady raz wprowadzone zwykle stopniowo same się rozrastają. Jak zauważył Europejski Inspektor Ochrony Danych osobowych w swojej opinii nawet przetwarzanie obecnie istniejących danych może prowadzić do zwiększenia popytu na dostęp do nich i chęć ich wykorzystywania w gospodarce, przez organy władzy państwowej i służby wywiadowcze. Zapowiedzią tego procesu jest to, że ograniczenia wypracowane w czasie posiedzenia Komisji Wolności Obywatelskich zostały zepchnięte na bok w trakcie tajnych pertraktacji z Radą.

Chociaż Rada twierdzi, że gromadzone dane będą wykorzystywane jedynie do celów walki z terroryzmem, to jednak odrzuciła propozycje zmierzające do legalnego ograniczenia wykorzystywania takich danych jedynie w takim celu. Dlatego jeśli nawet dostęp do gromadzonych danych nie będzie ograniczony przez Parlament jedynie do listy poważnych przestępstw, nic nie zapobiegnie stopniowemu rozszerzaniu stosowania nowych przepisów na coraz to dalsze obszary: już teraz wojownicy własności intelektualnej (Copyright Industry) zabiega, by uzyskać dostęp do gromadzonych informacji w celu zwalczania wymiany plików w internecie.

Wszelki zwrot ponoszonych przez operatorów kosztów będzie miał charakter jedynie czasowy. Koszty i obowiązki wynikające z realizowania forsowanej obecnie polityki będą przedstawione jako "koszty związane z prowadzeniem działalności gospodarczej", ale w rzeczywistości przenoszone będą na barki konsumentów jako "koszty komunikacji w ramach Unii Europejskiej"

Jedynym wyjściem z tego zaklętego kręgu jest już teraz przerwanie łańcucha przyszłych wydarzeń i podążenie za przykładem innych państw na świecie, odrzucając tą politykę na samym początku tej drogi.

Obietnice nie wystarczą

Zarówno Europejski Inspektor Ochrony Danych Osobowych jak również Grupa Robocza ds art. 29 (the Article 29 Working Party of European Privacy Commissioners), podobnie zresztą jak sam Parlament Europejski, niejednokrotnie już głosili, że nie będzie w przyszłości tego typu regulacji, pozwalających na zatrzymywanie sygnałów telekomunikacyjnych. Ich wezwania do utworzenia odpowiednich standardów i niezbędnej ochrony przed nadużywaniem informacji gdzieś przepadły. Głos organizacji zabiegających o prawa człowieka, ale również głos branży ICT nie został wysłuchany.

Polityka taka jest kontynuowana jedynie dzięki temu, iż mają miejsce jakieś tajne ustalenia, porozumienia zawierane są bez wcześniejszego badania ich konsekwencji. Znów projekt został wprowadzony na szybką ścieżkę legislacyjną. Wszystko dlatego, że Rada obawia się otwartej i demokratycznej dyskusji dotyczącej tych właśnie zagadnień. Jednocześnie w Unii Europejskiej nie ma podobnych regulacji, które w państwach członkowskich konstytucyjnie gwarantują krajowym parlamentom możliwość przebadania danej sprawy.

Unia Europejska powinna pójść za przykładem otwartych i demokratycznych państw, w których dane zbierane i przechowywane są tylko i jedynie dla jasno określonych potrzeb i celów, a dostęp do nich jest przyznawany na mocy decyzji sądu.

My, niżej podpisani wzywamy Posłów Parlamentu Europejskiego do uwzględnienia wskazanych zagrożeń dla europejskich swobód obywatelskich, dla konsumentów oraz gospodarki, a także do odrzucenia Dyrektywy w sprawie zatrzymywania danych telekomunikacyjnych.

Gus Hosein, Privacy International and Sjoera Nas, European Digital Rights

Tak brzmiał list, który trafił do skrzynek eurodeputowanych kilka dni przed głosowaniem nad kształtem dyrektywy pozwalającej na zbieranie danych telekomunikacyjnych. Pod tym listem podpisało się ponad osiemdziesiąt organizacji pozarządowych z całej Europy, w tym z Polski: Internet Society Poland oraz Helsińska Fundacja Praw Człowieka.

W Polsce szybka ścieżka

6 grudnia 2005 roku zakończyło się w Komisji Infrastruktury pierwsze czytanie rządowego projektu ustawy o zmianie ustawy - Prawo telekomunikacyjne (druk nr 51). Celem tego projektu złożonego jeszcze przez poprzedni rząd jest "pełniejsze dostosowanie przepisów ustawy do pakietu dyrektyw o łączności elektronicznej". Puls Biznesu z dnia następnego (str. 9) cytuje wypowiedź wiceminister transportu i budownictwa odpowiedzialnej za telekomunikację, Anny Streżyńskiej: „Nowelizacja zawiera najpilniejsze zmiany związane z zastrzeżeniami Komisji Europejskiej. Sprawa jest pilna z uwagi na konsekwencje, które nam grożą, jeśli się tych zmian nie wprowadzi".

Nikt nie miał wątpliwości, że sprawa jest pilna. Czego dotyczył projekt rządowy, który wpłynął do Sejmu 19 października? Była tam mowa m.in. wykreślenie art. 55 (ze względu na przekroczenie art. 13 dyrektywy ramowej; chodziło o prowadzenie księgowości przez przedsiębiorstwa udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej), zmiany w art. 71 (ze względu na uwagi Komisji Europejskiej w odniesieniu do ograniczeń przenoszalności numerów także użytkowników końcowych usługi przedpłaconej świadczonej w ruchomej publicznej sieci telekomunikacyjnej, chodzi o pre-paidy), zmiany w art. 98, 178, 201, 202, 203, 204 - zmiany o charakterze legislacyjnym, związane ze zmianami w art. 206 ust. 2a (wykreślenie zdania "decyzji nadaje się rygor natychmiastowej wykonalności), art. 139

(zapewnienie dostępu do infrastruktury telekomunikacyjnej bez względu na pozycję operatora na rynku).

Jak wspomniałem - Komisji Infrastruktury zakończyło pierwsze czytanie nowelizacji prawa telekomunikacyjnego w dniu 6 grudnia. Dnia następnego projekt trafił do podkomisji i tam właśnie została zaproponowana poprawka zobowiązująca do 15 letniego okresu przechowywania danych telekomunikacyjnych dla potrzeb bezpieczeństwa państwa i porządku publicznego. Prace legislacyjny toczyły się niezwykle szybko. Podkomisja miała wypracować stanowisko, a 9 grudnia (czyli w piątek), sprawa znów miała trafić do komisji stałej do drugiego czytania. A następnie projekt miał być głosowany w Sejmie. Wszystko w tydzień.

Wspólny przekaz

Relacjonując stanowiska polskich prawników (tych konkretnie, którzy w tych gorących dniach grudnia zdecydowali się publicznie wypowiedzieć w sprawie retencji danych) warto w pierwszej kolejności przytoczyć słowa dr hab. Andrzej Adamski[17], prof. UMK Toruń, który poproszony o wypowiedź związaną z pracami nad dyrektywą, napisał: „Retencja danych transmisyjnych jest koncepcją realizowaną na szczeblu Unii Europejskiej dwutorowo - w ramach I i III filara. W obu przypadkach wiąże się z pamiętnymi zamachami terrorystycznymi z 11 września 2001 r. (Nowy Jork i Waszyngton) i 11 marca 2004 r. (Madryt), które dały silny impuls polityczny do wzmocnienia bezpieczeństwa publicznego. Refleksem pierwszego z tych wydarzeń jest art. 15 Dyrektywy 2002/58/WE z dnia 12 lipca 2002 r. o przetwarzaniu danych osobowych i ochronie prywatności w sektorze komunikacji elektronicznej. Przepis ten zezwala na odstępstwo od jednej z fundamentalnych zasad ochrony danych osobowych (polegającej w dziedzinie telekomunikacji na usuwaniu bądź anonimizacji danych o ruchu po zakończeniu korzystania z usługi przez usługobiorcę). Dopuszcza bowiem możliwość gromadzenia i przechowywania danych w innym celu niż ten, dla którego są one przetwarzane, tj. ze względu na bezpieczeństwo państwa, zapobieganie przestępczości i ściganie przestępstw. Upoważnia przy tym państwa członkowskie do ustanowienia instytucji retencji danych w ustawodawstwie wewnętrznym, pod warunkiem respektowania zasad prawa wspólnotowego - przede wszystkim zasady proporcjonalności.

Zasadę tę rażąco narusza proponowany przez PiS 15-letni okres przechowywania danych osobowych, jakimi są dane o ruchu telekomunikacyjnym. Nie jest to bowiem niezbędny, właściwy i proporcjonalny w państwie demokratycznym środek „zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych”. Rząd żadnego innego państwa członkowskiego UE, łącznie z tymi które mają u siebie poważne problemy z terroryzmem (Hiszpania) i przestępczością zorganizowaną (Włochy), nie odważyłby się wystąpić z podobną propozycją. I to nie z obawy przez utratą poparcia własnych obywateli, zaliczonych bez wyjątku do kategorii osób podejrzanych i poddanych permanentnej inwigilacji, lecz by się nie ośmieszyć w oczach obywateli i rządów innych europejskich demokracji.

Projekt ustawy, która przewiduje wprowadzenie tak monstrualnego, jak na warunki państwa demokratycznego okresu retencji danych w Polsce jest sprzeczny zarówno z Europejską Konwencją Praw Człowieka (art.8), jak i Konstytucją RP (art. 31 ust 3.). Akceptacja tego rozwiązania przez ustawodawcę może przynieść Polsce więcej szkód niż korzyści".

W tym miejscu również warto przytoczyć słowa referatu wygłoszonego w roku 2004 przez prof. Adamskiego na konferencji CERT Secure 2004. Referat zatytułowany był: „Problem retencji danych o ruchu na tle przepisów ustawy - Prawo telekomunikacyjne[18]”. Można tam min. przeczytać:

„Gromadzenie i przechowywanie danych stanowiących „prawdziwą kopalnię wiedzy o życiu prywatnym i zawodowym użytkowników sieci telekomunikacyjnych” dla potrzeb ewentualnych postępowań karnych jest uznawane za nielegalne. Narusza bowiem zasadę proporcjonalności ingerencji państwa w prawa i wolno ci obywatelskie, gwarantowane przez Europejską Konwencję Praw Człowieka (art. 8) oraz ustawy zasadnicze większości krajów europejskich, w tym Konstytucją RP (art. 31 ust. 3). Trzeba w związku z tym przypomnieć, że na naruszenie zasady proporcjonalności - w odniesieniu do nadmiernego gromadzenia informacji o obywatelach - powołuje się uzasadnienie

[17] autor licznych artykułów i opracowań, w szczególności: A. Adamski, Prawo karne komputerowe, C.H.Beck 2000.
[18] http://www.cert.pl/PDF/secure2004/adamski.pdf

wyroku Trybunału Konstytucyjnego z dnia 20 listopada 2002 r., który za niezgodne z konstytucją uznał „nałożenie na obywateli powszechnego obowiązku ujawniania majątku w deklaracjach podatkowych" przez ustawę z dnia 26 września 2002 r. o jednorazowym opodatkowaniu nieujawnionego dochodu oraz o zmianie ustawy – Ordynacja podatkowa i ustawy – Kodeks karny skarbowy (zawekowaną przez Prezydenta RP i uchyloną następnie wspomnianym Wyrokiem Trybunału Konstytucyjnego)

Alternatywnym dla retencji danych i zgodnym z zasadą proporcjonalności rozwiązaniem, które uwzględnia m.in. Konwencja Rady Europy o cyberprzestępczości oraz znowelizowane niedawno przepisy kodeksu postępowania karnego, jest instytucja „zabezpieczenia danych" (preservation of data)..."

Zbierając informacje na temat retencji danych oraz procesu legislacyjnego dotyczącego tej problematyki poprosiłem również inne osoby zajmujące się problematyką ochrony danych osobowych, ochroną prywatności i prawem telekomunikacyjnym o wypowiedzi.

Dr Arwid Mednis[19], który m.in. reprezentował Polskę w Komitecie ds. Ochrony Danych Osobowych w Radzie Europy w Strasbourgu, w latach 1998-2000 był przewodniczącym tego Komitetu, stwierdził w nadesłanej do mnie wypowiedzi: „W kwestii retencji danych w telekomunikacji Polska i Unia to jakby dwa odrębne światy. W Unii w związku z projektem Dyrektywy toczy się zażarta dyskusja przede wszystkim nad okresem przechowywania danych: czy mają to być 3 miesiące, 6 czy 12. Polskie władze w tej dyskusji nie biorą udziału, tak jakby to nas w ogóle nie dotyczyło. W kraju natomiast min. L. Dorn wychodząc naprzeciw postulatom organów ścigania postuluje przechowywanie danych przez 15 lat! Brak jakiejkolwiek publicznej dyskusji, wypowiedzi właściwych organów (GIODO, URTiP) a przecież rzecz dotyczy jednego z podstawowych praw obywatelskich. Wydaje się, że dla wielu osób w Polsce zagadnienie jest proste: trzeba walczyć z przestępcami a dane od operatorów to znakomity oręż, więc prawo do prywatności musi ustąpić.

Nikt nie zadaje sobie pytania: kto i w jaki sposób ma przechowywać dane, jak je zabezpieczyć przed dostępem osób nieuprawnionych (znane są przypadki, gdy mafia była zainteresowana bilingiem). Czy państwo weźmie na siebie odpowiedzialność za brak odpowiednich zabezpieczeń u operatora? Problemem nie jest sam fakt przechowywania, tylko potencjalny dostęp do tych danych i możliwość ich użycia dla innych celów. Ryzyko wzrasta wraz z wydłużeniem okresu przechowywania danych. A może to ma być remedium na opieszałość organów ścigania, które nie są w stanie zabezpieczyć dowodów w krótkim czasie?"

Dr Maciej Rogalski, radca prawny z ukończoną aplikacją sędziowską, pełniący funkcję Wiceprezesa ds. telekomunikacji oraz Członka Rady Polskiej Izby Informatyki i Telekomunikacji nadesłał następującą wypowiedź: „Wątpliwości budzi przede wszystkim sposób procedowania nad wprowadzeniem nowych regulacji do Prawa telekomunikacyjnego. Nie jest praktycznie uwzględniane w procesie legislacyjnym, że prace w zakresie retencji danych są prowadzone na poziomie UE. Z pewnością polski rząd musiał zająć stanowisko w zakresie regulacji przygotowywanych na poziomie UE. Nie było słychać o protestach w zakresie proponowanych przez UE czasookresów. Powstać może więc niebezpieczna sytuacja, że uregulowania na poziomie krajowym będą znacznie odbiegać od uregulowań na poziomie UE.

W procesie przygotowywania tych regulacji powinny być uwzględnione obowiązujące już w Polsce akty prawne w zakresie ochrony i przechowywania danych osobowych, a w szczególności ustawę o ochronie danych osobowych, która formułuje zasadę proporcjonalności i adekwatności przechowywania danych osobowych. Dane należy gromadzić w sposób proporcjonalny i adekwatny do celu dla jego są gromadzone. Powinna być przeprowadzona szczegółowa analiza wykazująca na konieczność przyjęcie określonego okresu przechowywania danych telekomunikacyjnych.

Można odnieść wrażenie, że nie zostały przeprowadzone w wystarczającym stopniu analizy, przede wszystkim o charakterze statystycznym, potwierdzające tezę o konieczności przechowywania danych przez tak długi okres czasu. Postulat ten nabiera szczególnego znaczenia w kontekście przyjętych w projektach UE maksymalnych okresów przechowywania danych, które wynoszą 2 lata. Trzeba

[19] Autor licznych publikacji na temat ochrony danych osobowych, m.in.: A. Mednis, Ustawa o ochronie danych osobowych. Komentarz, Wydawnictwo Prawnicze 1999.

pamiętać także, że regulacje te stworzone zostały przede wszystkich dla zwalczania terroryzmu i przyjęte okresy przechowywania tych danych dla tak poważnego celu okazały się wystarczające".

Również autor niniejszej kroniki, czyli Piotr Waglowski [20] (chociaż bez tytułu doktorskiego) do wspólnego przekazu dołączając swoje „trzy grosze" pisał w serwisie http://prawo.vagla.pl obok powyżej przedstawionych wypowiedzi ekspertów: „W Unii Europejskiej nowe prawo uchwalane jest coraz częściej bez szerszych konsultacji społecznych, zbyt często z wykorzystaniem "szybkiej ścieżki legislacyjnej". Jeśli chodzi o retencje danych telekomunikacyjnych - z sygnałów płynących z Unii można wywnioskować, że Parlamentarzyści nie zdają sobie sprawy z konsekwencji wynikających z przyjmowanych właśnie regulacji. Dokonano „politycznej sprzedaży" prawa do prywatności, swobody działalności gospodarczej oraz praw konsumentów, w imię obrony „Świętego Grala" walki z terroryzmem i przestępczością. Jednak wprowadzane właśnie „nowe standardy" prawne nie gwarantują uzyskania celu, który - w zamyśle lobujących za nimi sił - mają realizować.

Pierwszą i podstawową koniecznością staje się wprowadzenie systemowej standardu kontroli nad wykorzystywaniem gromadzonych przez państwa informacji o obywatelach. Nowe zasady przewidują nieograniczone w żaden poważny sposób możliwości zbierania i wykorzystywania takich informacji. Gwałci się w ten sposób zasadę proporcjonalności. Mówimy o informacji na temat każdego sposobu komunikowania się, a przecież tajemnica komunikowania się należy do podstawowych praw człowieka. Musi nim być zwłaszcza w czasie, gdy podobno budujemy społeczeństwo informacyjne. Jeśli powszechnie i bez systemowej kontroli zbierane będą informacje dotyczące komunikacji obywateli, nie możemy już dziś mówić o jakiejkolwiek ochronie tajemnicy dziennikarskiej, tajemnicy adwokackiej czy o tajemnicy przedsiębiorstwa. W chwili obecnej ochrona gromadzonych przez państwo informacji o obywatelach jest iluzoryczna – co dobitnie pokazują ostatnie przypadki wycieków danych z Telekomunikacji Polskiej, historia 12 dysków twardych, które wyniesiono z Ministerstwa Spraw Zagranicznych, znalezione na śmietniku informacje o tysiącu klientach jednego z banków. Gromadzone bez żadnej kontroli dane telekomunikacyjne staną się wygodnym narzędziem w rękach zorganizowanych grup przestępczych, będą wykorzystywane dla doraźnych celów politycznych. Chodzi o to, że cyfrowe zapisy dotyczące komunikacji elektronicznej nie mogą stanowić dowodu na istnienie jakichkolwiek faktów. Łatwość, z jaką można manipulować elektronicznymi zapisami, spowoduje, że pojawią się zaraz informacje o rozmowach czy komunikacji elektronicznej, która nigdy nie miała miejsca. Przykładem na tego typu działania może być lista pochodząca z Instytutu Pamięci Narodowej, którą ktoś anonimowo opublikował w internecie. Pojawiły się na tej „liście agentów" takie postaci jak Kaczor Donald, czy Myszka Micky.

Koszty gromadzenia danych telekomunikacyjnych zostaną z pewnością przeniesione na końcowych klientów operatorów telekomunikacyjnych. W efekcie klienci ci będą finansowali „mechanizm" powszechnej inwigilacji, który nie będzie skuteczny (terroryści i zorganizowana przestępczość doskonale potrafi zadbać o poufność swojej komunikacji), będzie mógł być wykorzystywany do bliżej nieokreślonych w tej chwili celów (np. dla potrzeb szantażu). W efekcie nowe prawo będzie godziło w szarych obywateli, którzy nie mają większych szans na obronę swoich interesów.

Zasmuca też sposób, w jaki przygotowywane i forsowane jest w dzisiejszych czasach prawo. Politycy nie mający większego pojęcia na temat tego, nad czym w danej chwili głosują, muszą bazować na opinii „ekspertów". Eksperci zaś – co wynika z kampanii informacyjnej jaką prowadzą w tej chwili różne organizacje pozarządowe w Unii Europejskiej – również nie mają świadomości konsekwencji przyjęcia któregoś z możliwych rozwiązań. To wszystko jednak nie przeszkadza temu, by wprowadzić kolejny projekt prawa na szybką ścieżkę legislacyjną, by ograniczyć debatę publiczną – co przejawia się w Polsce m.in. w ten sposób, że projektowane zmiany nie zostały podane do publicznej wiadomości, nawet po ich przegłosowaniu w podkomisji sejmowej, by ignorować niezależne raporty, lub niewygodne stanowiska. Sposób, w jaki wprowadzane są właśnie w tej chwili nowe regulacje wiele mówi o społeczeństwie obywatelskim, które właśnie tworzymy".

Warto porozmawiać

[20] Przy dorobku innych badaczy skromnie będzie wyglądał przypis odnoszący się do publicystycznej wszak, nie zaś naukowej, pozycji: P. Waglowski, „Prawo w sieci. Zarys regulacji Internetu", Helion 2005.

9 grudnia na konferencji prasowej posła Przemysława Gosiewskiego, szef Klubu PiS poinformował, że Klub PiS może rozmawiać o okresie, w jakim te dane będą przechowywane: „jeśli będzie wolą Sejmu znalezienia kompromisu, to PiS jest otwarty na dyskusję" - powiedział Gosiewski.

Dzień wcześniej sejmowa Komisja Infrastruktury zaakceptowała nowe propozycję zmian do Prawa telekomunikacyjnego, a jak pisze Rzeczpospolita (9.12.2005): nikt nie głosował przeciw. Jedynie czterech posłów wstrzymało się od głosu. Art. 165 ustawy Prawo telekomunikacyjne został zmieniony[21] nie tylko w taki sposób, że zastąpiono okres 12 miesięcy okresem 15 lat. Po ustaleniu nowego okresu przepis zmieniano znacznie bardziej. Operator już nie będzie anonimizował danych (na konieczność anonimizacji danych zwracał uwagę m.in. Europejski Inspektor Ochrony Danych Osobowych, o czym mowa była wyżej), tylko będzie przekazywał je do odpowiedniego urzędu...

W dyskusji na liście dyskusyjnej ISOC Polska[22] można było przeczytać w tych dniach: "Ta dyrektywa Wielkiego Brata ma 5 lat i kilkanaście tygodni. Jest to Wańka Wstańka lobby bezpieczeństwa publicznego, która została już wielokrotnie odrzucona. I właśnie dlatego pojawiła się teraz w trybie nagłym w Brukseli. Ministrowie kilku poważnych, naprawdę demokratycznych krajów europejskich, którym własne parlamenty odmówiły takich środków przenieśli ja do Brukseli licząc, że wykręcą się w ten sposób przed własną opinią publiczną. Później się będą tłumaczyć, że trzeba zaimplementować, bo Bruksela się domaga. Ta manipulacja w jakieś części się udaje. Mimo że sprawa ma wiele lat, pierwsza propozycja jest jeszcze sprzed zamachu 11 września, tylko niewielka część posłów europejskich ma wystarczająca wiedzę by świadomie głosować".

W Unii Europejskiej dwie główne siły parlamentarne, które forsują nowe regulacje, tj EPP[23], czyli chrześcijańscy demokraci oraz PSE[24] czyli socjaliści - „dogadały się" nad głowami reszty Parlamentu i postanowiły przeforsować dyrektywę w proponowanym przez siebie kształcie. Pytani o sprawę Eurodeputowani niezbyt wiele wiedzieli o sprawie. Po co mają wiedzieć skoro ich klubowi eksperci mówią im kiedy i jak trzeba głosować. Pytani o sprawę eksperci również nie do końca wiedzieli czego

---

[21] Zmieniany przepis ustawy Prawo telekomunikacyjne brzmiał:
Art. 165. 1. Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych jest obowiązany, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, dane te przechowywać przez okres 12 miesięcy. Po upływie tego okresu, dane transmisyjne są usuwane lub anonimizowane przez operatora publicznej sieci telekomunikacyjnej lub dostawcę publicznie dostępnych usług telekomunikacyjnych, którzy je przechowują.
2. Przetwarzanie danych transmisyjnych, niezbędnych dla celów naliczania opłat abonenta i opłat z tytułu rozliczeń operatorskich, jest dozwolone:
1) po uprzednim poinformowaniu abonenta lub użytkownika końcowego o rodzaju danych transmisyjnych, które będą przetwarzane przez dostawcę publicznie dostępnych usług telekomunikacyjnych oraz o okresie tego przetwarzania;
2) tylko do końca okresu, o którym mowa w art. 108 ust. 2.
3. Dostawca publicznie dostępnych usług telekomunikacyjnych jest obowiązany poinformować abonenta lub użytkownika końcowego o rodzaju danych transmisyjnych, które będą przetwarzane oraz o okresie tego przetwarzania dla celów marketingu usług telekomunikacyjnych lub świadczenia usług o wartości wzbogaconej.
4. Dostawca publicznie dostępnych usług telekomunikacyjnych może przetwarzać dane transmisyjne, o których mowa w ust. 3, w zakresie i przez czas niezbędny dla celów marketingu usług telekomunikacyjnych lub świadczenia usług o wartości wzbogaconej, jeżeli abonent lub użytkownik końcowy wyraził na to zgodę.
5. Do przetwarzania danych transmisyjnych, zgodnie z ust. 1-4, uprawnione są podmioty działające z upoważnienia operatorów publicznych sieci telekomunikacyjnych i dostawców publicznie dostępnych usług telekomunikacyjnych, zajmujące się naliczaniem opłat, zarządzaniem ruchem w sieciach telekomunikacyjnych, obsługą klienta, systemem wykrywania nadużyć finansowych, marketingiem usług telekomunikacyjnych lub świadczeniem usług o wartości wzbogaconej. Podmioty te mogą przetwarzać dane transmisyjne wyłącznie dla celów niezbędnych przy wykonywaniu tych działań.
[22] Internet Society Poland, http://www.isoc.org.pl
[23] European People's Party
[24] Party of European Socialists

w istocie dotyczy ta dyrektywa. Im wytyczne przekazywali szefowie klubów, w szczególności, że mają rekomendować innym posłom konieczność jej przegłosowania.

Ze względu na uzyskany przez chrześcijańskich demokratów i socjalistów „kompromis" - Alexander Nuno Alvaro (ALDE[25]), twórca projektu raportu głosowanego wcześniej przez komisję LIBE, a jednocześnie jego sprawozdawca, rozważał usunięcie swojego nazwiska z nazwy raportu. Ale to jest jedynie smaczek całej tej polityki. W pewnym momencie nie było jasne, czy ALDE zgłosi w ogóle do głosowania treść propozycje LIBE, tak, by była głosowana w całości. Z drugiej strony sporu parlamentarnego miały stanąć propozycje Komisji wspierane przez EPP oraz PSE. A co by było, gdyby raport LIBE nie został zgłoszony do głosowania? To bardzo ważne, w jaki sposób konstruowane są w Parlamencie Europejskim głosowania. Ważna jest kolejność i zakres głosowanych poprawek. Raport Alexandera Alvaro zmieniony przez LIBE został jednak "zatabletowany".

W Rzeczpospolitej (10.12.05 Nr 288) przy artykule Sławomira Wikariaka pt. „Bezpieczeństwo państwa kontra swobody obywatelskie" zacytowano wypowiedź autora niniejszej kroniki, Piotra Waglowskiego[26]: „Dla mnie nie jest istotne, czy dane będą przechowywane kilka miesięcy czy kilkanaście lat. Liczy się to, w jaki sposób będą wykorzystywane. Jeśli godzimy się na gromadzenie informacji na temat obywateli, to trzeba stworzyć mechanizmy, które zabezpieczą przed wykorzystywaniem ich z naruszeniem praw człowieka. Bez tego możemy zapomnieć o ochronie tajemnicy dziennikarskiej, adwokackiej czy tajemnicy przedsiębiorstwa. Prokuratura nie będzie już musiała prosić sądu o zwolnienie z tajemnicy np. dziennikarza, skoro dowie się z billingów, kto był jego informatorem. Pojawia się też pytanie, kto zagwarantuje, że dane nie wyciekną z samej firmy telekomunikacyjnej. Niedawno "Rz" informowała o tym, że mogły być wynoszone z Ery GSM. Skąd pewność, że następnym razem nie trafią do zorganizowanych grup przestępczych?"

Retencja – decydujące starcie

W Unii Europejskiej głosowanie w sprawie dyrektywy o retencji danych zostało przesunięte na środę 14 grudnia i w ten sposób termin rozstrzygnięcia europejskiego pokrył się z terminem głosowania nad poprawkami do Prawa telekomunikacyjnego w polskim Parlamencie.

W tym czasie znane są już propozycje nowelizacji polskiej[27]. Rządowi zależy na tym, by nowelizacja prawa telekomunikacyjnego w tym zakresie zaczęła funkcjonować od 1 stycznia. Jak wspomniałem wyżej - posłowie „dorzucili" do rządowego projektu (złożonego jeszcze przez poprzedni rząd) dodatkowe zapisy związane z retencją, jednak te regulacje wzbudzają ostre sprzeciwy zarówno środowisk walczących o prawa człowieka, jak i środowisk operatorów telekomunikacyjnych. Grupa posłów postanowiła złożyć do Prezydium Sejmu wniosek o odroczenie prac nad nowelizacją prawa telekomunikacyjnego, gdyż sprawę uznali za kontrowersyjną, a publicznej debaty nie udało się przeprowadzić. Wobec takiego odroczenia – rządowi nie udałoby się przyjąć ustawy przed końcem roku. Pojawiło się też pewne rozwiązanie tego problemu: potrzebne Polsce przepisy powinny zostać przyjęte podczas następnego posiedzenia Sejmu, ale retencja danych, czyli nowelizacja art. 165 ust. 1 ustawy - Prawo telekomunikacyjne - powinna – wedle tych propozycji z nowelizacji zostać usunięta.

---

[25] Alliance of Liberals and Democrats for Europe

[26] Wówczas jako członka Zarządu Internet Society Poland

[27] Propozycja ta brzmiała:

"*w art. 165 ust. 1 otrzymuje brzmienie:*

"1. Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych jest obowiązany, z uwagi na realizację przez uprawnione organy zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, dane te przechowywać przez okres 15 lat. Obowiązek uważa się za wykonany w przypadku zapewnienia przez zaprzestającego działalności operatora publicznej sieci telekomunikacyjnej lub dostawcę publicznie dostępnych usług telekomunikacyjnych przechowywania danych transmisyjnych przez innego operatora operatora publicznej sieci telekomunikacyjnej lub dostawcę publicznie dostępnych usług telekomunikacyjnych. Po upływie tego okresu, dane transmisyjne są usuwane lub anonimizowane przez operatora publicznej sieci telekomunikacyjnej lub dostawcę publicznie dostępnych usług telekomunikacyjnych, którzy je przechowują.";"

Przechodząc do prac w Unii Europejskiej warto zauważyć, że 12 grudnia do Eurodeputowanych swoją odezwę skierowały organizacje takie jak ECCA[28], ECTA[29], ETNO[30], EuroISPA[31] oraz GSM Europe[32]. Innymi słowy - duzi gracze włączyli się w do bitwy. Organizacje te wspierają i rekomendują te same rozwiązania, które wspierane są w pewnej części przez organizacje zabiegające o poszanowanie praw człowieka (aczkolwiek zapewne zupełnie z innych powodów) [33] . Swoje rekomendacje Eurodeputowanym przedstawił również The Foundation for a Free Information Infrastructure (FFII)[34].

W Polsce swoją opinię na temat prac nad retencją przedstawiła również Polska Izba Informatyki i Telekomunikacji[35] (wcześniej cytowałem również list do Eurodeputowanych sygnowany przez Internet Society Poland oraz Helsińską Fundację Praw Człowieka). PIIT zwraca uwagę na konieczność uwzględnienia w polskim procesie legislacyjnym prac Unii (tj. uwzględnić przewidywany okres retencji danych nie dłuższy niż 2 lata), postuluje uwzględnienie obowiązujących już w Polsce aktów prawnych w zakresie ochrony i przechowywania danych osobowych, a w szczególności zapisów ustawy o ochronie danych osobowych, która formułuje zasadę proporcjonalności i adekwatności przechowywania danych osobowych w stosunku do rzeczywistych potrzeb. PIIT sygnalizuje również, że okres 15-lat retencji powinien być szczegółowo uzasadniony oraz przeanalizowany, co do kosztów, użyteczności oraz możliwości zapewnienia ochrony przed nieuprawnionym dostępem oraz zniszczeniem. PIIT odniosła wrażenie, że „nie zostały przeprowadzone w wystarczającym stopniu analizy, przede wszystkim o charakterze statystycznym, potwierdzające tezę o konieczności przechowywania danych przez tak długi okres czasu". Wreszcie PIIT wskazała na konieczność oszacowania kosztów wprowadzenia takiej regulacji oraz określenia jej wpływu na poziom cen dla użytkowników usług telekomunikacyjnych: „Według propozycji unijnych operatorzy realizujący obowiązki na rzecz Państwa w zakresie retencji danych powinny mieć zwracane ponoszone koszty z budżetu Państwa. Konieczne jest więc oszacowanie, w jakim stopniu może być obciążony budżet Państwa w tym zakresie po przyjęciu takich zapisów w dyrektywie".

Na posiedzeniu Rady Ministrów w dniu 13 grudnia rząd zaakceptował swoje stanowisko do poselskiego projektu ustawy o zmianie ustawy Prawo Telekomunikacyjne (druk nr 103):

„W projekcie poselskim zapisano, że operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych, przetwarzający dane transmisyjne dotyczące abonentów i użytkowników końcowych, jest obowiązany do ich przechowywania przez 15 lat. Jest to związane z realizacją zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Rząd uważa, że nowelizacja jest zasadna i celowa. Proponuje jednak skrócenie okresu przechowywania danych do co najmniej 5 lat. Tym bardziej, że jest to zgodne z analogicznymi pracami prowadzonymi w krajach Unii Europejskiej".

Nadeszła środa, 14 grudnia 2005 roku. Na godzinę 11:30 (do 11:50) przewidziano głosowanie w Parlamencie Europejskim w sprawie przyjęcia raportu „Report: Alexander Nuno Alvaro" (retencja danych). W Polsce właśnie rozpoczął się drugi punkt porządku obrad Sejmu RP dotyczący drugiego czytania ustawy nowelizującej Prawo telekomunikacyjne (tam również znajduje się przywoływany wcześniej zapis dot. retencji danych)...

W Polsce, wobec zgłoszonych przez posłów poprawek w czasie drugiego czytania ustawy w Sejmie, projekt nowelizacji Prawa telekomunikacyjnego trafił ponownie do komisji infrastruktury w celu przygotowania sprawozdania. Wśród poprawek - kilka klubów zgłosiło propozycje dotyczące retencji

---

[28] ECCA, European Cable Communication Association
[29] ECTA, European Competitive Telecommunications Association
[30] ETNO, European Telecommunications Network Operators' Association
[31] EuroISPA, the European Internet Services Providers Association
[32] GSM Europe, the European Interest Group of the GSM Association
[33] W swojej rekomendacji dotyczącej przyszłego głosowania w Parlamencie Europejskim (Voting recommendation) duzi, komercyjni gracze proponują Posłom Europejskim odrzucenie poprawek od 47 do 92, przyjęcie zaś poprawek 1 do 46 (draft Alvaro report) oraz poprawki nr 93.
[34] FFII prosi Eurodeputowanych o głosowanie za przyjęciem poprawek 47 oraz 93.
[35] Opinia dostępna jest na stronach Polskiej Izby Informatyki i Telekomunikacji pod adresem: http://www.piit.org.pl

danych. Poza propozycją rządową (o której wyżej) jest m.in. poprawka całkowitego wykreślenia z nowelizacji ustawy propozycji w zakresie retencji danych (jest też taka, która mówi o 2 latach gromadzenia danych).

W Unii dyrektywę przyjęto dokładnie w tym samym czasie. Przeszły propozycje Komisji i Rady, wspierane głosami dwóch największych ugrupowań Parlamentarnych EPP (European People's Party), czyli chrześcijańskich demokratów oraz PSE (Party of European Socialists) czyli socjalistów. Po zakończeniu głosowania (378 głosów za propozycją, 197 przeciw, przy 30 głosach wstrzymujących się) Alexander Nuno Alvaro w geście protestu wycofał swoje nazwisko z oficjalnych dokumentów odwołujących się do raportu LIBE. Dane telekomunikcyjne mają być zbierane od sześciu miesięcy do dwóch lat (przy czym kraje członkowskie mogą uzyskać zgodę na dłuższy okres przechowywania danych, jeśli w odpowiedni sposób to uzasadnią). Jeśli chodzi o zwrot kosztów na rzecz operatorów: kraje członkowskie mogą przewidzieć taką możliwość w swoim prawie krajowym, nie wprowadzono jednak takiej zasady.

Po głosowaniu w czasie drugiego czytania w polskim Sejmie zebrała się Komisja Infrastruktury. W czasie obrad Komisji posłowie zgodzili się na dwuletni okres retencji oraz wprowadzili dodatkowo zapisy zobowiązujące ministra właściwego do spraw łączności do ustalenia trybu i zasad przechowywania danych transmisyjnych zapewniających bezpieczeństwo i poufność danych. Chodziło o określenie szczególnych wymogów bezpieczeństwa, jakie musiałby spełnić operator telekomunikacyjny przechowujący zgromadzone dane.

Jak donosiła tego dnia Gazeta.pl[36]: "Komisja Europejska poinformowała w środę o pozwaniu Polski przed Europejski Trybunał Sprawiedliwości. Powód? Abonenci sieci telefonicznych wciąż nie mają prawa do zachowania numeru przy zmianie operatora". To jeden z elementów nowelizacji, którym tego dnia zajmował się polski Parlament...

Czy złamano procedurę przyjmowania prawa?

Dzień po europejskim głosowaniu serwisy informacyjne[37] podały, iż irlandzki Minister Sprawiedliwości Michael McDowell ma zamiar argumentować przed Europejskim Trybunałem Sprawiedliwości, że podczas procesu prawodawczego organy Unii Europejskiej złamały prawo przyjmując dyrektywę o retencji danych. Jego zdaniem przyjęcie dyrektywy w ramach procedur pierwszego filaru jest naruszeniem prawa, gdyż regulacje związane ze ściganiem przestępstw (dyrektywa ma za zadanie - wedle inicjatorów procesu prawodawczego - dawać narzędzia do walki z poważną przestępczością i terroryzmem) powinny być przyjmowane w procedurze trzeciego filaru unijnego. Oznacza to, że kompetencje w tym zakresie powinna mieć wyłącznie Rada, a do podjęcia decyzji wymagana jest jednomyślność wszystkich jej członków - a więc rządów państw tworzących UE. W związku z tym, że Irlandia nie zgadza się na przyjęte właśnie normy, i w procedurze trzeciego filaru z pewnością zgłosiłaby swoje veto (blokując decyzję Rady) - teraz podjęto konsultacje z irlandzkim prokuratorem generalnym dotyczące możliwości zaskarżenia dyrektywy do Europejskiego Trybunału Sprawiedliwości.

Również Minister sprawiedliwości Słowacji podzielił stanowisko, zgodnie z którym naruszono zasady proceduralne, chociaż Słowacja zgodziła się z treścią przyjętej właśnie dyrektywy (wcześniej Słowacja należała do grupy trzech państw, które głosowały przeciwko propozycjom w ramach prac Rady).

Jeszcze Senat i Prezydent

Po kilku dniach Senat podjął uchwałę w sprawie ustawy o zmianie ustawy - Prawo telekomunikacyjne oraz ustawy - Kodeks postępowania cywilnego. Senat wprowadził zmiany w stosunku do projektu nowelizacji ustawy Prawo telekomunikacyjne jaki „wyszedł" z Sejmu. W uchwale Senatu z dnia 22 grudnia 2005 r. poza innymi zmianami znalazły się te, które dotyczą kontrowersyjnej nowelizacji art. 165 ust. 1 ustawy Prawo telekomunikacyjne[38]. Zrezygnowano z delegacji do określenia w drodze rozporządzenia szczególnych wymogów bezpieczeństwa gromadzenia i przechowywania danych.

---

[36] http://gospodarka.gazeta.pl/gospodarka/1,33181,3067887.html
[37] http://euobserver.com/9/20548
[38] Senat zdecydował się na dokonanie następujących zmian:
W art. 1 w pkt 8, w ust. 1 zdanie drugie otrzymuje brzmienie:

W uzasadnieniu do poprawek senackich czytamy: "Poprawka nr 3 precyzyjnie wskazuje obowiązek, zaprzestającego działalności operatora lub dostawcy usług, przekazania danych transmisyjnych do przechowywania innemu operatorowi lub dostawcy usług.

Poprawka nr 4 powoduje zastąpienie upoważnienia dla ministra do wydania rozporządzenia klauzulą nakazującą przechowującemu dane transmisyjne dołożenie szczególnej staranności przy przechowywaniu tych danych, tak aby zapewnić ich bezpieczeństwo, poufność oraz ochronę interesów osób, których dane dotyczą. Zdaniem Senatu, regulowanie zasad przechowywania danych transmisyjnych w formie aktu wykonawczego jest zbędne, ponieważ dane te są objęte tajemnicą telekomunikacyjną, nie mniej jednak, ze względu na znaczenie tych danych, Senat proponuje nałożenie na operatorów obowiązku dochowania szczególnej staranności".

W opinii Biura Legislacyjnego Senatu z dnia 19 grudnia 2005[39] (a więc opinii, na podstawie której Senat dokonał swoich poprawek) czytamy: „W związku z dodaniem do przepisu nakładającego obowiązek przechowywania danych transmisyjnych przez okres 2 lat, upoważnienia ministra do wydania rozporządzenia określającego zasady i tryb przechowywania tych danych, powstaje wątpliwość w jaki sposób operatorzy mają przechowywać dane w okresie od wejścia w życie ustawy do dnia wydania wspomnianego rozporządzenia. Ponieważ wydanie rozporządzenia ma charakter obligatoryjny należy dodać przepis przejściowy nakazujący stosowanie, do momentu wydania rozporządzenia, dotychczasowych zasad przechowywania. Należy nadmienić, iż dane te są już chronione przez ustawę jako tzw. „tajemnica telekomunikacyjna"".

Po przyjęciu poprawek Senackich przez Sejm w Gazeta.pl[40] można było przeczytać: „W ten sposób zniknął zapis, zgodnie z którym minister transportu i budownictwa miał określić w rozporządzeniu zasady i tryb przechowywania danych. - To wymagałoby gruntownego pochylenia się przez urzędników nad tą materią, ale PiS uznał, że nie ma na to czasu. Ostateczny zapis może doprowadzić do konfliktów między operatorami a służbami, bo określenie "dołożenie szczególnej staranności" nie jest specjalnie precyzyjne - powiedział nam Piotr Rutkowski, niezależny konsultant na rynku telekomunikacyjnym".

Prezydent podpisał ustawę nowelizującą Prawo telekomunikacyjne (Dz. U. z 2006 r. nr 12, poz. 66), a ta w dniu 9 lutego 2006 roku, weszła w życie.

Memento - Greek Watergate

Jeszcze przed wejściem w życie omawianej nowelizacji liczne media [41] poinformowały o spektakularnym skandalu: ktoś przez rok podsłuchiwał rozmowy prowadzone przez telefony komórkowe greckiego premiera Kostasa Karamanlisa i wielu członków jego gabinetu.

Rzecznik greckiego rządu Teodoros Rusopulos powiedział, że prokuratorzy wszczęli dochodzenie w sprawie naruszenia prywatności łączności telefonicznej. Bierze się pod uwagę także ewentualne zarzuty szpiegostwa. Podsłuchiwano rozmowy telefoniczne ok. 100 osób, w tym polityków opozycji i przedsiębiorców. Podsłuchiwano rozmowy premiera, ale też rozmowy szefa greckiego MSZ Petrosa

---

"Obowiązek uważa się za wykonany w przypadku gdy zaprzestający działalności operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przekaże do przechowywania dane transmisyjne innemu operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych.";
w art. 1 w pkt 8, w ust. 1 zdanie czwarte otrzymuje brzmienie:
"Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych przechowujący dane transmisyjne jest obowiązany dołożyć szczególnej staranności w celu ochrony bezpieczeństwa i poufności tych danych oraz interesów osób, których dane dotyczą.";

[39] http://www.senat.gov.pl/k6/dok/opinia/2005/003/029.htm

[40] http://gospodarka.gazeta.pl/gospodarka/1,33181,3088957.html

[41] O sprawie pisały liczne serwisy, w tym PAP, Independent UK, CNET News.com, Reuters.uk, International Herald Tribune, grecki serwis Kathimerini, Guardian Unlimited, Scotsman, BBC News, Forbes, United Press International... Linki do tych źródeł zgromadzone są pod adresem http://prawo.vagla.pl/node/5991

Moliwiatisa również były przez kogoś monitorowane. Na liście podsłuchiwanych numerów był też jeden należący do ambasady USA w Atenach. Podsłuchy trwały od roku 2004, i miały się zacząć tuż przed olimpiadą. Całość zakończyła się w marcu 2005, gdy grecka grupa telefonii komórkowej Vodafone ujawniła sprawę (i chciałoby się dodać: do momentu, gdy sprawę wszczęcia przed rokiem dochodzenia przez organa ścigania ujawnił dziennik "Ta Nea").

Serwis Scotsman [42] pisze, że podsłuch był możliwy dzięki nielegalnie zainstalowanemu oprogramowaniu u operatora Vodafone Greece. To pokazuje coś, na co zwracali uwagę liczni komentatorzy przez cały czas trwania batalii związanej z procesem legislacyjnym dotyczącym retencji danych: „realizowanie" zadań na rzecz bezpieczeństwa państwa i porządku publicznego etc.. daje de facto więcej narzędzi przeróżnym mafiom, wywiadom i zorganizowanej przestępczości i nie jest rozwiązaniem problemu...

Zakończenie

Po tej, subiektywnej wszak, relacji - warto wskazać czytelnikowi inne materiały poświęcone poruszanej tu tematyce. W ostatnich latach w Polsce toczy się burzliwa debata dotycząca kształtu regulacji prawnych związanych z przepływem informacji (i szerzej – społeczeństwa informacyjnego). Na uwagę zasługują na przykład pionierska wówczas publikacja „Internet a prawo[43]", autorstwa prof. Barty oraz prof. Markiewicza, która – jak się dziś wydaje – rozpoczęła na dobre tą dyskusję. Podobnie można powiedzieć o materiałach z konferencji „Internet – problemy prawne", która odbyła się w katolickim Uniwersytecie Lubelskim dnia 2 grudnia 1998 r., a której efektem była książka o tym samym tytule[44].

Szczególnie zaś – ze względu na tematykę poruszaną w tym opracowaniu – pragnę przywołać publikację[45], która była efektem konferencji naukowej nt. „Społeczeństwo inwigilowane w państwie prawa? Granice ingerencji w sferę praw jednostki". Konferencja odbyła się w dniach 26-27 marca 2003 r. Jej organizatorami byli pracownicy naukowi Katedry Prawa Karnego i Polityki Kryminalnej oraz Katedry Kryminalistyki UMK wraz ze studentami skupionymi w kołach naukowych: Homo Homini, Prawa Karnego Komputerowego, Studenckiego Koła Naukowego Prawa Porównawczego i Studenckiego Koła Naukowego Kryminalistyki. Wówczas to uczestnicy konferencji starali się podjąć odpowiedzi na nurtujące wszystkich pytania: Co to jest inwigilacja?, Jakie są jej korzenie i jakimi metodami jest lub może być prowadzona?, Na ile państwo może ingerować w prawa człowieka?. Czy w tym zakresie jesteśmy dostatecznie chronieni? oraz wiele innych – pisała we wprowadzeniu do książki „Społeczeństwo inwigilowane w państwie prawa" Violetta Kwiatkowska Darul, opiekun Studenckiego Koła Naukowego Kryminalistyki.

Analizując zaś problematykę „retencji danych" – chociaż, jak zauważył jeden z dyskutantów na forum grupy pl.soc.prawo, działającej w ramach Usenetu: to niefortunne określenie, gdyż w żaden sposób nie kojarzy się niewtajemniczonym z potencjalnymi naruszeniami praw obywatelskich – poza przywołanymi w niniejszym opracowaniu materiałami warto też zwrócić uwagę, iż oceniać ją (problematykę właśnie) należy na gruncie dorobku wielu autorów zajmujących się prawem telekomunikacyjnym[46], ochroną informacji[47] (w tym informacji niejawnych), dostępem do informacji[48],

---

[42] http://thescotsman.scotsman.com/international.cfm?id=172412006

[43] J. Barta, R. Markiewicz, Internet a prawo, TAiWPN UNIVERSITAS, 1998; Ośrodek krakowski powinien być reprezentowany w tym wyliczeniu również publikacją P. Podrecki (red), Prawo Internetu, LexisNexis 2004...

[44] Ośrodek lubelski reprezentowany jest w dyskursie m.in. przez publikacje konferencyjne takie jak: R. Skubisz (red), Internet - problemy prawne, POLIHYMNIA, 1999; Następnie: R. Skubisz (red), INTERNET 2000 Prawo - ekonomia - kultura, Oficyna Wydawnicza VERBA, 2000; T. Zasępa (red), Internet - fenomen społeczeństwa informacyjnego, Edycja Świętego Pawła 2001; T. Zasępa, R. Chmura (red) Internet i nowe technologie ku społeczeństwu przyszłości, Edycja Świętego Pawła, 2003.

[45] P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński (red), "Społeczeństwo inwigilowane w państwie prawa", Wydawnictwo UMK Toruń 2003.

[46] Dorobek w zakresie prawa telekomunikacyjnego reprezentowany być może np. przez takie publikacje jak: S. Piątek, Prawo telekomunikacyjne Wspólnoty Europejskiej, C.H. Beck 2003; W. Gromski, J. Kolasa, A. Kozłowski, K. Wójtowicz, Europejskie i polskie prawo telekomunikacyjne, LexisNexis, 2004; A. Krasuski, Prawo telekomunikacyjne. Komentarz, LexisNexis 2005; S. Piątek, Prawo telekomunikacyjne. Komentarz, C.H. Beck 2005, co jednak w żaden sposób nie wyczerpuje długiej listy wartych polecenia publikacji.

czy wreszcie (a może – przede wszystkim) ochroną danych osobowych [49]. Z racji ram tego opracowania pozwoliłem sobie jedynie na zasygnalizowanie tego dorobku w taki oto sposób licząc, że autorzy innych opracowań, artykułów i analiz nie będą mi mieli za złe, iż nie wspomniałem o ich pracach. Jest ich wielu. Proszę niniejszym o wybaczenie.

[47] Np. B. Kunicka-Michalska, Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości, C.H. Beck, 2000; B. Fischer, Przestępstwa komputerowe i ochrona informacji, Kantor Wydawniczy Zakamycze 2000;. W tym nurcie chciałbym zasygnalizować potężny dorobek Wyższej Szkoły Policji w Szczytnie, w szczególności publikacje konferencyjne J. Kosiński, A. Misiuk, P. Ciszek (red. naukowa), Przestępczość teleinformatyczna, Wyd. Wyższej Szkoły Policji, Szczytno 2003 czy J. Kosiński (red) Przestępczość teleinformatyczna, Wyd. Wyższej Szkoły Policji, Szczytno 2004...

[48] M. Bernaczyk, M. Jabłoński, K. Wygoda, Biuletyn Informacji Publicznej. Informatyzacja administracji, Wydawnictwo Uniwersytetu Wrocławskiego 2005; T. R. Aleksandrowicz, Komentarz do ustawy o dostępie do informacji publicznej, LexisNexis, 2004; M. Butkiewicz, Internet w instytucjach publicznych, Difin, 2006;

[49] Wskazując przykładowo: R. Szałowski, Prawna ochrona informacji niejawnych i danych osobowych, Difin 2000; P. Fajgielski, Ochrona danych osobowych w telekomunikacji - aspekty prawne, Lubelskie Towarzystwo Naukowe, 2003; G. Sibiga, Postępowanie w sprawach ochrony danych osobowych, Dom Wydawniczy ABC, 2003; R. Markiewicz, P. Fajgielski, J. Barta, Ochrona danych osobowych - Komentarz, Kantor Wydawniczy Zakamycze, 2004;