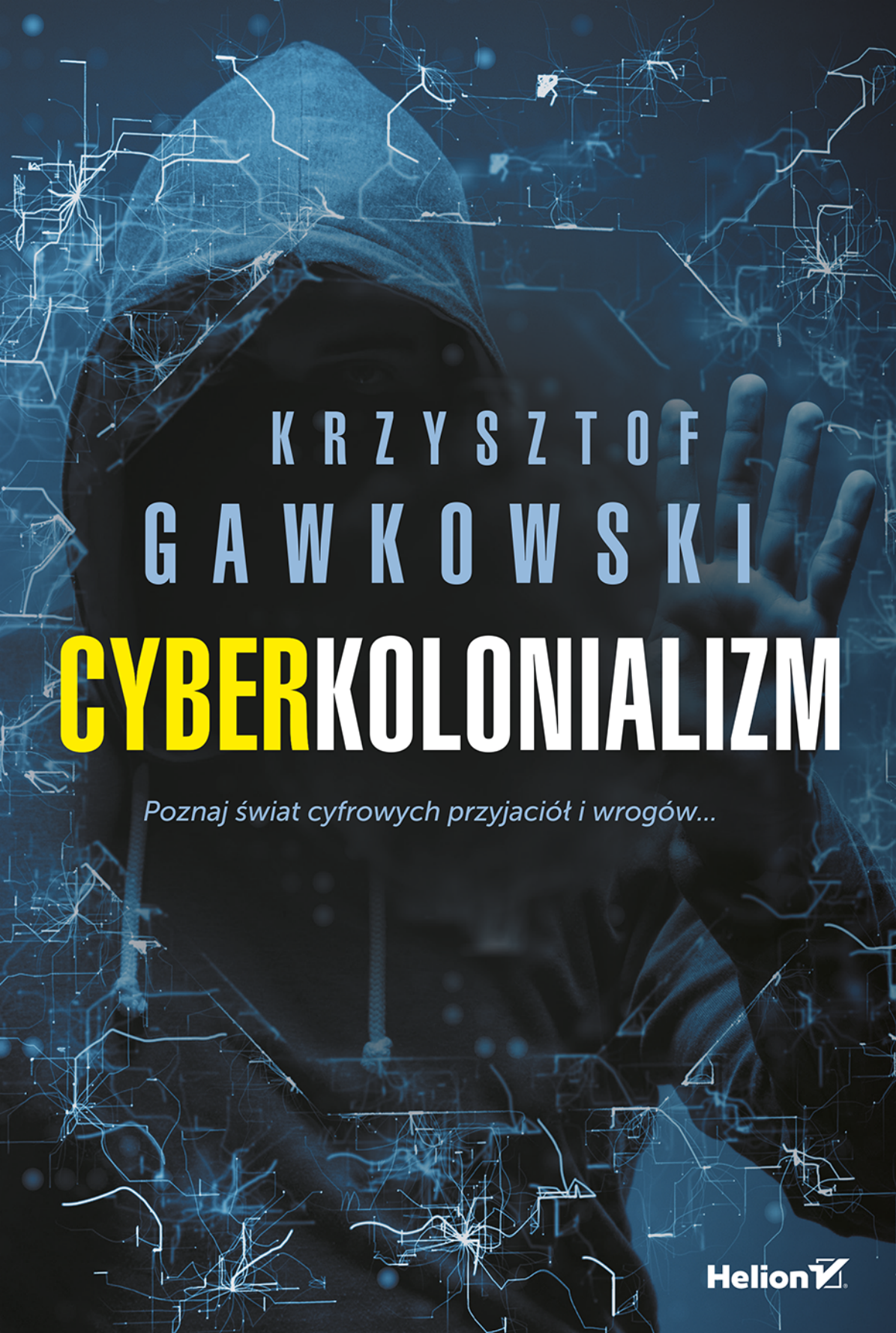

KRZYSZTOF
GAWKOWSKI
CYBERKOLONIALIZM
Poznaj świat cyfrowych przyjaciół i wrogów...
Helion

Recenzje naukowe: prof. Vladimir G. Lebedev, prof. Paweł Soroka
Opieka redakcyjna: Ewelina Burska
Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki
Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/cyberk
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-4801-1

Printed in Poland.

Spis treści

Rozdział 5.

Prawne regulacje dotyczące internetu

Powinniśmy zakładać, że każda służba wywiadu, nie tylko nasza, ale każda europejska służba wywiadu, każda azjatycka służba wywiadu [...] będzie dążyć do tego, by spróbować zrozumieć świat oraz co się dzieje w światowych stolicach.

BARACK OBAMA[1]

Podejmując temat regulacji prawnych dotyczących sieci, należy zwrócić uwagę na fakt, że sam dostęp do niej stał się obecnie jednym z podstawowych praw obywatelskich, przynajmniej w krajach rozwiniętych. Nie wszystkie państwa uregulowały to w sposób równie bezpośredni jak Grecja, która w 2008 roku wprowadziła odpowiedni zapis do swojej konstytucji[2]. Estonia np. zasygnalizowała to prawo poprzez ustawę o bibliotekach publicznych i ustawę o dostępie do informacji publicznych[3]. Na tej podstawie każdy obywatel zyskał tam prawo dostępu do informacji za pomocą dostępu do sieci w publicznych bibliotekach. Jeszcze inaczej sformułowała ten przepis Finlandia, nakładając na operatorów telekomunikacyjnych obowiązek zapewnienia określonej minimalnej prędkości dostępu do internetu dla abonentów usługi powszechnej[4]. Rada Konstytucyjna Francji dała wyraz swojemu przekonaniu o niezbywalności prawa obywatela do korzystania z zasobów sieci, przeciwstawiając się ustawie przewidującej możliwość kary dożywotniego lub przynajmniej długotrwałego zakazu korzystania z internetu osobom naruszającym za jego pośrednictwem prawa autorskie i argumentując, że porozumiewanie się online stanowi obecnie istotny sposób komunikowania się i wymiany poglądów, a to jedne z podstawowych praw człowieka[5].

Polska należy do państw, które dotychczas nie sformułowały prawa dostępu do sieci w sposób kategoryczny i jednoznaczny, kolejne rządy podejmują jednakże rozmaite inicjatywy mające na celu rozwój społeczeństwa informacyjnego i przeciwdziałanie informacyjnemu wykluczeniu obywateli. Rozpoczynając od programów edukacyjnych w szkołach, poprzez umożliwienie mieszkańcom dostępu do Wi-Fi w miejscach publicznych, kończąc na projektach wspierających

informatyzację najmniej rozwiniętych w tym zakresie regionów i określonych grup społecznych — m.in. w bieżącym roku podjęto decyzję o sfinansowaniu w ramach Programu Operacyjnego Polska Cyfrowa przyłączenia do najnowocześniejszej sieci internetowej ponad 1,3 mln gospodarstw domowych dotychczas pozbawionych dostępu do internetu, na co przeznaczono około 3 mld złotych[6].

Oficjalne strategie informatyzacji kraju

W 1991 roku, na zlecenie rządu, Polskie Towarzystwo Informatyczne opracowało raport omawiający zagrożenia i szanse rozwoju informatyki w Polsce, w 1998 roku, podczas II Kongresu Informatyki Polskiej, powstał *Pakt na rzecz budowy społeczeństwa informacyjnego*, a w roku 2000, jako konsekwencja paktu, powstała sejmowa uchwała w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce. W pierwszej kolejności powstał dokument programowy *Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce*, a w 2001 roku pojawiła się strategia *ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 – 2006*[7]. W 2002 roku zaktualizowano tę strategię, a w 2003 roku powstała, opracowana przez Komitet Badań Naukowych, *Strategia informatyzacji Rzeczypospolitej Polskiej — ePolska*[8]. W roku 2004 zaprezentowano dwa kolejne dokumenty określające przyszłość informatyzacji kraju: *Plan działań na rzecz rozwoju elektronicznej administracji (eGovernment) na lata 2005 – 2006* oraz raport *Proponowane kierunki rozwoju społeczeństwa informacyjnego w Polsce do 2020 r.*[9] W 2005 roku powstała kolejna strategia[10], a lata 2006 i 2007 przyniosły nowe rozporządzenia zatwierdzające plany informatyzacji na lata 2006 i 2007 – 2010[11]. W 2008 roku powstała strategia rozwoju sięgająca roku 2013[12], a w 2013 przyjęto długookresowy plan, obejmujący działania w tym zakresie aż po rok 2030[13]. Informatyzacja polskiego społeczeństwa jest również od czasu wstąpienia kraju do UE współfinansowana przez unijne programy operacyjne[14].

Wiele kwestii związanych z cyberprzestrzenią regulują także różne przepisy odnoszące się do konkretnych dziedzin. I tak np. poszczególne ustawy regulują kwestie handlu w internecie, prasy internetowej, prawa autorskiego, nieuprawnionego dostępu do danych komputerowych itp.

W internecie obowiązuje też tzw. niepisane prawo — zespół norm społecznych akceptowanych przez dużą część użytkowników sieci i wymaganych przez nich od całości społeczeństwa sieciowego, czyli netykieta.

Nadzór nad domenami

Działania ściśle związane z uporządkowaniem sieci regulowane są na poziomie globalnym. Za przyznawanie nazw *domen* internetowych, ustalanie ich struktury i ogólny nadzór nad działaniem serwerów DNS (ang. *Domain Name System* — system nazw domenowych) na świecie odpowiada, zarejestrowana w stanie Kalifornia jako prywatna organizacja non profit, Internetowa Korporacja ds. Nadanych Nazw i Numerów (ang. *the Internet Corporation for Assigned Names and Numbers* — ICANN). Została powołana w 1998 roku i rząd USA przekazał jej czasowo prawo nadzoru nad systemem DNS, przydziałem puli adresów IPv4 i IPv6 dla tzw. *Regional Internet Registries* (RIR) oraz rejestracją numerów portów[15]. Warto również wspomnieć o organizacji IANA (ang. *Internet Assigned Numbers Authority*), instytucji będącej grupą roboczą Internet Engineering Task Force i stanowiącej autonomiczną część ICANN-y[16].

Wspomniane organizacje przyznają jednak tylko domeny najwyższej klasy (takie jak *.pl*, *.gov*, *.com*, *.eu*), rozdzielając je pomiędzy kraje i instytucje, które mogą później przekazać nadzór nad częścią lub całością swoich domen innym podmiotom (tak jak rząd polski, który powierzył Naukowej i Akademickiej Sieci Komputerowej całkowity nadzór nad domeną *.pl* oraz obsługę rejestrowania domen *gov.pl*, *com.pl*, *biz.pl*, *net.pl*, *org.pl* i niektórych domen lokalnych, jak *waw.pl*). Innymi instytucjami zajmującymi się przyznawaniem i rejestracją konkretnych domen są rząd USA (*.mil* i *.gov*), rządy poszczególnych krajów, czasem za pośrednictwem innych organizacji (domeny narodowe), Verisign Global Registry Services (*.net*, *.com*), Public Interest Registry (*.org*), NeuLevel (*.biz*), Institute of Electrical and Electronics Engineers — IEEE (*.aero*), Afilias Limited (*.info*), Global Name Registry (*.name*), EURid — rejestracja i nadzór nad domeną (*.eu*).

Inne regulacje międzynarodowe dotyczące cyberprzestrzeni

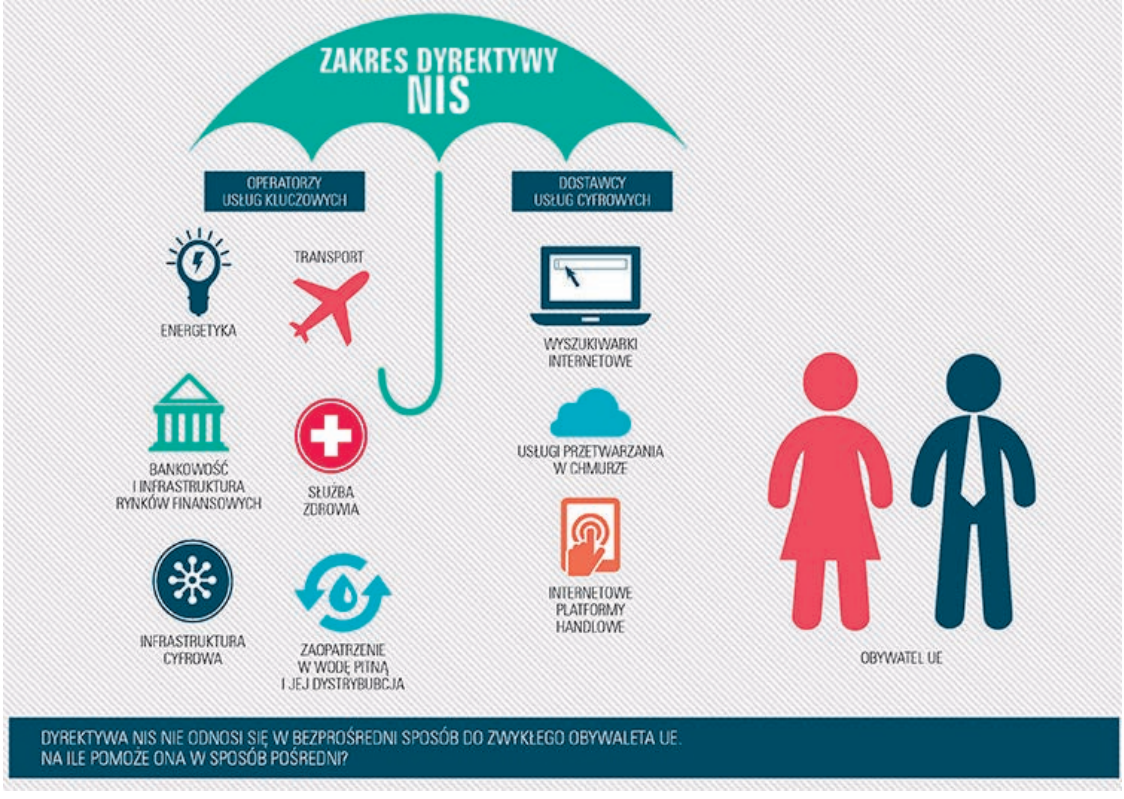
Sieć internetowa w założeniu miała być ogólnodostępna i poddana jak najmniejszym ograniczeniom, dlatego dotyczące jej międzynarodowe regulacje prawne skupiają się głównie na bezpieczeństwie cyberprzestrzeni i ustanowieniu ram prawnych działania instytucji czuwających nad tym bezpieczeństwem. Jednym z najistotniejszych aktów prawnych w tym zakresie jest przyjęta przez Parlament Europejski *Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na*

terytorium Unii (2016/1148/UE), zwana też dyrektywą NIS[17], która weszła w życie w sierpniu 2016 roku i na której implementację państwa członkowskie miały dwadzieścia jeden miesięcy[18] (rysunek 5.1).

Dyrektywa NIS nie odnosi się w sposób bezpośredni do bezpieczeństwa obywateli Unii Europejskiej, ale odnosi się do dwóch typów podmiotów — dostawców usług cyfrowych (dostawców internetowych platform handlowych, wyszukiwarek internetowych i usług przetwarzania w chmurze) oraz operatorów usług kluczowych (przedstawicieli takich sektorów jak: ochrona zdrowia, energetyka, transport, infrastruktura cyfrowa, infrastruktura rynków finansowych czy bankowość)[19], których bezpieczeństwo ma jednakże istotny wpływ na bezpieczeństwo wszystkich obywateli. Do obowiązków wspomnianych grup będzie należało zgodne z wytycznymi raportowanie o istotnych incydentach dotyczących naruszenia bezpieczeństwa oraz korzystanie z technicznych i organizacyjnych środków ochrony, dostosowanych do poziomu ryzyka (rysunek 5.2).

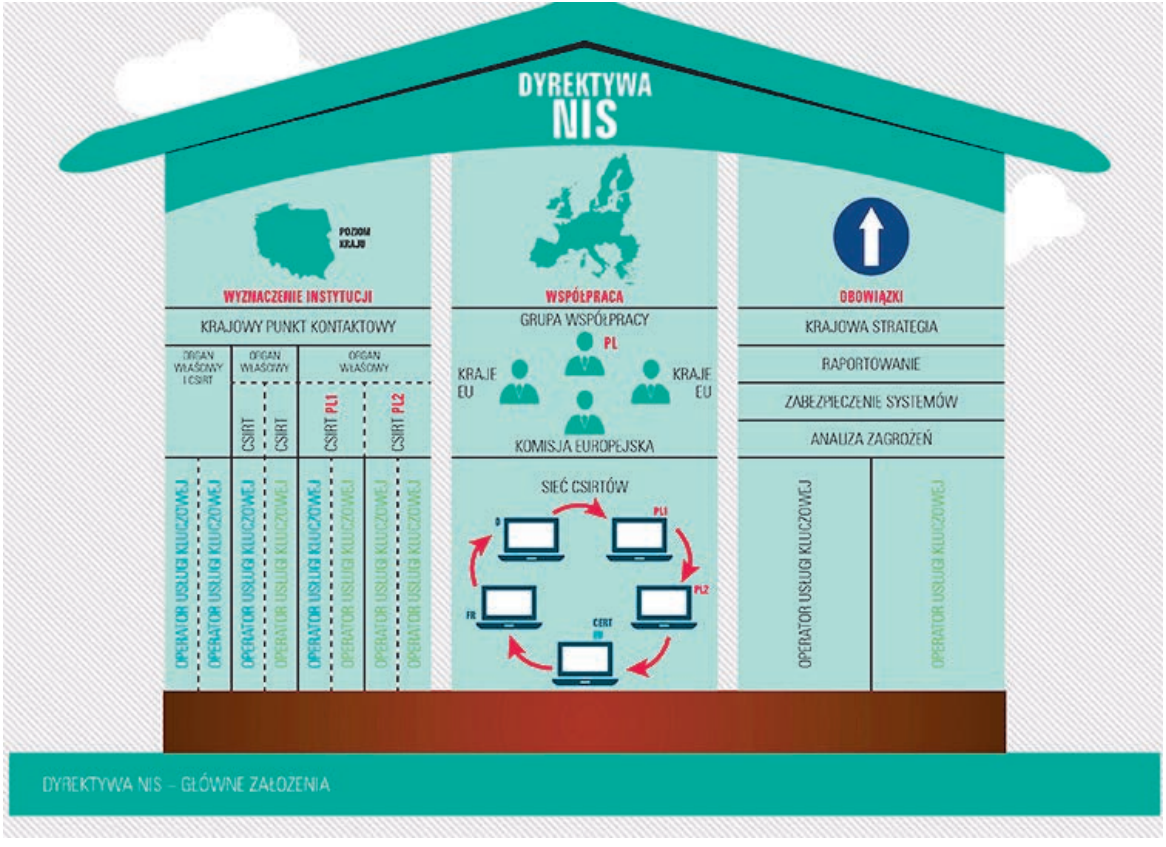
Zgodnie z NIS dostawcy usług cyfrowych wybierani mają być bezpośrednio przez UE, a operatorzy usług kluczowych — samodzielnie przez państwa członkowskie. NIS wskazuje jednak sektory, z których operatorzy mają być wyłonieni, i określa przebieg sześciostopniowego procesu ich identyfikacji, który ma być przeprowadzony wraz z implementacją dyrektywy lub bezpośrednio po niej. Wyznaczono również inne obowiązki państw członkowskich, które powinny wskazać organy mające nadzorować operatorów usług kluczowych i dostawców usług cyfrowych, wyznaczyć punkty kontaktowe (po jednym w każdym kraju) mające uczestniczyć w Grupie Współpracy (tj. zespole międzynarodowym zajmującym się np. zbieraniem cyklicznych raportów czy wymianą dobrych praktyk), a także powołać zespoły reagowania na incydenty bezpieczeństwa komputerowego (ang. *Computer Security Incident Response Team* — CSIRT[20]). W tym zakresie Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) stanowić będzie dla nich rodzaj sekretariatu.

Określenia „CSIRT"[21] używa się w Europie zamiast zastrzeżonego prawnie przez USA akronimu CERT (*Computer Emergency Response Team* — zespół szybkiego reagowania na zagrożenia komputerowe) i oznacza ono grupę ekspertów w dziedzinie bezpieczeństwa informatycznego, która współpracuje ze sobą, świadcząc usługi w zakresie likwidacji incydentów i umożliwienia normalnego użytkowania systemów po usunięciu incydentów oraz usługi prewencyjne i szkoleniowe.



Rysunek 5.1. *Zakres dyrektywy NIS*

Źródło: D. Byrska, K. Gawkowski, D. Liszowska, *Unia Europejska — geneza, funkcjonowanie wyzwania* [w:] K. Gawkowski, *Cyberbezpieczeństwo w UE*, Wydawnictwo Exante, Wrocław, 2017, s. 91.



Rysunek 5.2. *Główne założenia dyrektywy NIS*

Źródło: D. Byrska, K. Gawkowski, D. Liszowska, op. cit., s. 92.

CSIRT-y dostosowują usługi do swoich kompetencji i wybranej grupy użytkowników (np. CSIRT dla sektora akademickiego, CSIRT komercyjny, CSIRT sektora ochrony informacji i infrastruktury, CSIRT sektora rządowego, CSIRT wewnętrzny, CSIRT sektora wojskowego, CSIRT krajowy, CSIRT sektora małych i średnich przedsiębiorstw, CSIRT dostawcy). Z danych amerykańskich badaczy[22] wynika, że zestaw świadczonych usług powinien być określony przez zasoby, zestawy umiejętności i możliwości współpracy, dzięki którym zespół będzie działał poprawnie. Wybór usług powinien przede wszystkim wspierać i umożliwiać osiąganie celów biznesowych środowiska, dla którego działa CSIRT, lub jego organizacji macierzystej. Wybór usług nie jest więc narzucony i jest uzależniony jedynie od możliwości (zasobów, umiejętności, liczebności) zespołów. Usługi są zatem różnorodne i różnie nazywane. ENISA podejmuje próby usystematyzowania zakresu oferowanych przez CSIRT-y usług, zarówno podstawowych, jak i dodatkowych, oraz określenia ich ogólnego zakresu. W publikacji z 2006 roku dzieli je na usługi reagowania, usługi zapobiegania, obsługę artefaktów oraz zarządzanie jakością zabezpieczeń. W publikacji z 2016 roku wyróżniane są usługi takie jak: alerty i ostrzeżenia, obsługa incydentów, zarządzanie lukami w zabezpieczeniach, obsługa artefaktów, usługi proaktywne — takie jak ogłoszenia, aktualności technologiczne, audyty bezpieczeństwa lub oceny, konfiguracja i konserwacja narzędzi, aplikacji i infrastruktury zabezpieczeń, rozwój narzędzi bezpieczeństwa, usługi wykrywania włamań, rozpowszechnianie informacji związanych z bezpieczeństwem, usługi zarządzania jakością bezpieczeństwa — takie jak ocena ryzyka, planowanie ciągłości działań biznesowych i odzyskiwania danych, doradztwo w zakresie bezpieczeństwa, budowanie świadomości, edukacja/szkolenia, ocena lub certyfikacja produktu.

Dyrektywa NIS z pewnością w dużym stopniu przyczyni się do ujednolicenia zasad ochrony struktur teleinformatycznych (ITC) i infrastruktury krytycznej w całej Europie oraz do opracowania indywidualnych polityk ochrony cyberprzestrzeni kraju, zobowiązuje bowiem wszystkie państwa członkowskie Unii Europejskiej do opracowania i przyjęcia krajowych strategii cyberbezpieczeństwa. Wiele jednak wskazuje, że wytyczne nie zostały dopracowane tak, jak tego oczekiwali specjaliści od cyberochrony, np. progi istotności incydentów, które mają być raportowane przez dostawców usług kluczowych, ustalają samodzielnie państwa członkowskie, choć powinny być one jednakowe dla wszystkich państw i jasno określone przez grupę niezależnych specjalistów przy UE. Ponadto operatorzy powiadamiać będą o zaistniałych incydentach tylko kraje, w których mieszczą się ich siedziby, co oznacza, że pozostałe kraje działania

operatorów międzynarodowych liczyć mogą w kwestii informacji o ewentualnych zagrożeniach jedynie na uzyskanie informacji za pośrednictwem państw poinformowanych. Brak jest także możliwości określenia zasięgu geograficznego incydentu lub zasięgu zakłócenia funkcjonowania usługi albo zasięgu wpływu incydentu na działalność gospodarczą i społeczną oraz liczbę użytkowników, których incydent dotyczył, operatorzy zwolnieni są z obowiązku raportowania o incydencie, co przyczynia się do możliwości przeoczenia lub zlekceważenia istotnych sygnałów o możliwości wystąpienia w Europie poważniejszych cyberzagrożeń.

Prawne wyzwania dotyczące regulacji cyberprzestrzeni

Powszechny dostęp obywateli do sieci niesie ogromne korzyści dla edukacji i gospodarki krajów zinformatyzowanych, stwarza też jednak wiele zagrożeń. Pierwszym dylematem, jaki nasuwa się przy okazji rozważań na temat umożliwienia każdemu zainteresowanemu dostępu do otwartych sieci (Wi-Fi, hotspot), np. w bibliotekach, środkach transportu, na dworcach, w kawiarniach itp., jest kwestia odpowiedzialności za naruszenia prawa za pomocą tych sieci. Kto poniesie karę za popełnione w ten sposób cyberprzestępstwa: właściciel sieci czy właściciel komputera (zidentyfikowany dzięki IP)? A jeśli nie uda się odszukać właściciela komputera? Czy wtedy do odpowiedzialności nie zostanie pociągnięty dostarczyciel „narzędzia zbrodni", choćby właściciel dworcowej kafejki czy kierownictwo biblioteki? Fiński sąd orzekł, że nie można ukarać właściciela sieci, nie mając dowodu, że to on naruszył prawo, jednak sądy innych państw czasem rozstrzygają inaczej — takie wyroki zapadały już m.in. w USA, Wielkiej Brytanii czy Niemczech[23], zwłaszcza w przypadkach naruszenia prawa autorskiego.

Podobnie przedstawia się problem odpowiedzialności za naruszenia prawa w przypadku innego rodzaju pośredników — dostawców stron internetowych. Kto powinien odpowiadać za zniesławienie osoby przez użytkownika portalu lub za zamieszczone w tym portalu nieprawdziwe informacje: użytkownik (często trudny do wytropienia) czy właściciel lub administrator portalu? Tutaj znów brak jednolitych i jednoznacznych rozstrzygnięć, a kwestie te pozostawiane są do indywidualnej interpretacji sądów. Z punktu widzenia osoby poszkodowanej portal pozwalający na umieszczenie obraźliwych treści na jej temat powinien ponieść karę. Z punktu widzenia właścicieli portali internetowych wygląda to jednak inaczej, gdyż nie zawsze są w stanie rozstrzygnąć, czy informacja zamieszczana przez użytkownika jest prawdziwa, czy użytkownik ma prawo do jej

upowszechniania itp. Często nie są też w stanie fizycznie kontrolować każdej informacji pojawiającej się w portalu i obawiają się posądzenia o cenzurowanie internetu — użytkownicy sieci bardzo tego nie lubią.

Zaprezentowane przykładowe argumenty dają wyobrażenie o sytuacji pośredników. Czy jednak wystarczą one, by przekonać użytkownika, który został znieważony lub którego dziecko zostało zalane falą hejtu, do zaakceptowania bezkarności pośrednika w takiej sytuacji? Po czyjej stronie powinien opowiedzieć się sędzia, komu przyznać słuszność? Czy wolno pozostawić to przypadkowi? Znalezienie właściwych odpowiedzi na powyższe pytania to duże wyzwanie, a obecnie w tego typu sprawach możemy zaobserwować duże rozbieżności nawet w orzecznictwie tej samej instancji rozstrzygającej.

Europejski Trybunał Praw Człowieka w sprawie serwisu Index.hu, który przegrał w węgierskim sądzie sprawę o naruszenie dóbr opisywanej spółki, mimo że jej nazwa pojawiła się jedynie w komentarzach internautów dosyć szybko przez portal usuniętych, wydał wyrok stanowiący, że „co do zasady" serwis internetowy nie ponosi odpowiedzialności za treść komentarzy. W przypadku serwisu Delfi, który przegrał w estońskim sądzie dosyć podobną sprawę, lecz negatywne komentarze usunął dopiero po upływie dwóch miesięcy, Trybunał uznał jednak, że w pewnych sytuacjach odstępstwo od tej zasady jest dopuszczalne, i wydał wyrok uznający odpowiedzialność serwisu za naruszenie prawa[24]. Zdaniem ekspertów z „Gazety Prawnej" obecnie wpływ na wyrok mają takie czynniki jak wielkość portalu (liczba pracowników odpowiedzialnych za kontrolowanie treści pojawiających się w komentarzach), zawartość komentarzy (szczególnie w przypadku pojawienia się gróźb karalnych i mowy nienawiści) oraz czas ich usunięcia[25].

Na mocy obecnie obowiązującego prawa komentarze naruszające jego przepisy powinny być usuwane natychmiast po zgłoszeniu administratorowi/właścicielowi portalu, że są bezprawne. Pośrednik musi więc, jeszcze przed rozstrzygnięciem sądowym podjąć decyzję, czy komentarz/artykuł rzeczywiście narusza regulacje prawne i należy go usunąć, czy też jest jedynie np. zgodną z prawem krytyką i usunięcie go naruszy prawo do wolności słowa komentującego, a to nie zawsze jest łatwe zadanie. Zwłaszcza że autor usuniętych/zablokowanych treści lub komentarzy może nie zgodzić się z opinią, że naruszają one czyjeś dobro, i dochodzić swoich praw w sądzie. I nie usuwając komentarza, niejednokrotnie może mieć rację. Tak było w przypadku portalu, który nie zgodził się na usunięcie krytycznego komentarza na temat firmy usługowej zamieszczonego przez niezadowolonego klienta tejże firmy. Sprawa trafiła do sądu, który przyznał rację

właścicielom portalu i autorowi komentarza, argumentując: „Niewątpliwie treść wpisu jest krytyczna, ale — podzielając pogląd Sądu Najwyższego wyrażony w wyroku z 18 stycznia 2013 r., IV CSK 270/12 — stwierdzić trzeba, że nikt nie może oczekiwać od innych wyłącznie afirmacji swojej osoby lub postępowania. [...] Choć niejednokrotnie trudność sprawia wyznaczenie granicy pomiędzy formułą dopuszczalną a taką, którą należy uznać za niemożliwą do akceptacji, to jednak omawiany wpis z całą pewnością nie przekracza formuły dopuszczalnej. Gdyby podzielić poglądy powódki domagającej się usunięcia wpisu, byłoby to równoznaczne z przyjęciem koncepcji, zgodnie z którą dopuszczalne są jedynie wypowiedzi i oceny pozytywne, co w oczywisty sposób sprzeciwiałoby się wolności słowa”[26].

Równie trudnym wyzwaniem dla prawodawców jest znalezienie proporcji między wspomnianą już wolnością słowa i prawem obywateli do informacji a ograniczaniem naruszania dóbr osobistych użytkowników (i nie tylko) oraz innych niezgodnych z prawem, szkodliwych i niepożądanych społecznie treści w sieci. Internet z założenia stanowi wolne medium — ponadnarodowe, ponadwyznaniowe, ponadpolityczne itd. Każdy użytkownik chce mieć w nim prawo głosu i prawo dostępu do informacji (najlepiej z wielu różnych źródeł, bo to pozwala oddzielić fakty od propagandy i cudzych interpretacji) oraz prawo do zapoznawania się z osiągnięciami kultury i nauki (bo sieć to najpowszechniejsze medium edukacyjne, a dla wielu osób być może jedyne). Użytkownicy marzą o internecie niezawisłym, otwartym, nieocenzurowanym. Są jednak wyjątki. Właściciele praw autorskich do utworów rozpowszechnianych — bez ich zgody — w sieci nie popierają internetu bez ograniczeń. Obliczają (realne lub życzeniowe) kwoty utraconych zysków z tytułu dystrybucji należących do nich utworów udostępnianych w różnych portalach i żądają surowych kar dla sprawców tych strat oraz wymagają od pośredników, czyli dostawców umożliwiających użytkownikom dostęp do sieci, by tropili nielegalne udostępnienia i blokowali wytropione lub wskazane przez właścicieli praw strony internetowe. Od prawodawców wymagają zaś kar nie zawsze proporcjonalnych do przewinień — jak wspomniany już dożywotni zakaz korzystania z internetu dla osób rozpowszechniających cudze utwory.

Osoby zapoznające się z dostępnymi w portalach utworami często są zupełnie nieświadome, że ktoś mógłby je uznać za przestępców: skoro coś jest dostępne w ogólnodostępnym miejscu, to dlaczego przestępstwem miałoby być obejrzenie, wysłuchanie czy wykorzystanie tego lub podzielenie się tym z innymi? Również osoby udostępniające jako pierwsze utwór muzyczny, film czy

program w przeważającej większości nie robią tego z przyczyn komercyjnych, nie czerpią z tego jakichkolwiek zysków. Nie zawsze też właściciel praw autorskich czy twórca rzeczywiście dużo na tym traci: po pierwsze nie udowodniono, że np. osoby oglądające film w sieci wybrałyby się na niego do kina, gdyby nie miały możliwości obejrzenia go na ekranie komputera (zresztą prawdziwi kinomani często w ogóle nie uznają oglądania filmów na małym ekranie, zwłaszcza w jakości, jaką oferują często nielegalne kopie najnowszych ekranizacji), po drugie często do sieci trafiają filmy (książki, utwory muzyczne, programy etc.), których czas świetności już minął i tylko niewielka grupa spośród osób pobierających je z sieci byłaby gotowa zapłacić za nie w sklepie (np. za wiele już razy oglądany w telewizji film czy piosenkę będącą przebojem wakacji 15 lat temu). Należy się więc zastanowić, czy ich wykroczenia są na tyle poważne, by szpiegować ich w sieci i surowo karać. W tej kwestii podzielone są nawet opinie autorów nielegalnie udostępnianych utworów. Wielu z nich cieszy popularność wśród internautów — niektórzy udostępniają im swoje utwory zupełnie za darmo lub korzystają z narzędzi umożliwiających współfinansowanie ich pracy przez osoby zainteresowane (np. poprzez portale crowdfundingowe) albo legalny zakup utworów przez internet za stosunkowo niewielką kwotę. Pomysł ten podchwycili też niektórzy wydawcy, oferując legalne utwory, do których posiadają prawa autorskie, w rozsądnych cenach tam, gdzie dotąd pojawiały się one nielegalnie (np. w źle ocenianym przez innych wydawców portalu Chomikuj.pl).

Być może zamiast tracić czas i energię, polując na (często nieświadome swojej winy) osoby korzystające bezprawnie ze znalezionych w sieciowych zasobach utworów, warto byłoby wypracować proste rozwiązania prawne, jednoznaczne i zrozumiałe dla każdego oraz proste narzędzia do sygnalizowania, że utwór jest legalny, umożliwiające sprawdzenie tego, ale np. za jego obejrzenie czy wysłuchanie lub skorzystanie z niego wprowadzić opłaty (przelewem internetowym czy SMS-em), choćby jakąś symboliczną kwotę, z której powodu nie warto narażać się na nieprzyjemności. Jeśli skala wykorzystania w sieci nielegalnych utworów jest rzeczywiście tak ogromna, jak uważają właściciele praw autorskich (raport firmy Deloitte podaje, że z nielegalnych źródeł treści korzysta w Polsce co drugi internauta w wieku od 15 do 75 lat, i wycenia straty dla Skarbu Państwa z tego tytułu na 836 mln złotych tylko w 2016 roku[27]), to zysk z tych niewielkich opłat powinien być zupełnie zadowalający. Zwłaszcza że Polacy bardzo często płacą za korzystanie z tych treści, nie zawsze przy tym wiedząc, że zasilają budżety serwisów pirackich (wydają na to 900 mln rocznie[28]), co utwierdza ich w przekonaniu, że te treści legalnie kupują, a nie kradną — z raportu PwC

wynika, że co trzeci respondent wskazał nielegalny serwis jako serwis oferujący wyłącznie legalny dostęp[29].

Znalezienie rozwiązań prawnych umożliwiających internautom rozpoznanie treści i serwisów legalnych (pośród treści serwisów powszechnie dostępnych), a także legalny zakup tych treści za niewygórowaną cenę zaoszczędziłoby pośrednikom nieprzyjemnych obowiązków: naruszania prywatności osób korzystających z ich portali i decydowania, czy strona, której zablokowania domaga się np. któryś z wydawców, rzeczywiście narusza przepisy prawa autorskiego. Nie zapominaj też, że w sieci nic nie ginie — zablokowana strona istnieje w niej nadal i nadal jest możliwość jej odszukania. Niektórzy właściciele praw autorskich żądają więc, żeby karać również osoby, które takie strony odwiedzają (nawet przypadkowo, bo np. wyświetliła je przeglądarka internetowa) lub pobierają z nich dane. Zapewne nie zawahaliby się oni również przed ukaraniem osób, dla których internet stanowi jedyny dostęp do dóbr nauki i kultury. Tymczasem osoby z najuboższych warstw społecznych, którym brakuje często nawet środków na życie, mając dostęp do sieci (w bibliotekach, szkołach, firmach), mogą uniknąć wykluczenia informacyjnego, jeszcze bardziej obniżającego ich pozycję w nowoczesnym społeczeństwie.

Z raportu przygotowanego na zlecenie Komisji Europejskiej przez firmę Ecorys w 2015 roku (i nieudostępnionego, choć jego sporządzenie kosztowało 360 tys. euro) wynika, że internauci bez względu na zasobność portfeli nie są skłonni płacić zbyt wysokich kwot za treści dostępne w sieci: „średnia deklarowana kwota, jaką skłonni byli zapłacić za film wynosiła 6,90 euro. W przypadku książek ta średnia wyniosła 15,80 euro, dla muzyki 0,90 euro, a dla gier 8,40 euro”[30]. W raporcie tym, udostępnionym dopiero po dwóch latach od sporządzenia przez Julię Redę z Partii Piratów, niemiecką eurodeputowaną do Parlamentu Europejskiego, pojawia się też inna istotna informacja: „Zasadniczo wyniki nie pokazują mocnych statystycznych dowodów na przesunięcie sprzedaży w wyniku naruszenia praw autorskich”[31].

Fakt, że zablokowane strony nadal istnieją w sieci, ma jeszcze inny, znacznie bardziej negatywny wymiar. Są bowiem w internecie treści, które zdaniem przeważającej części internautów powinny z niego zniknąć, np. pornografia dziecięca czy samouczki terrorystyczne. W tym jednakże przypadku prawo powinno jasno i bardzo precyzyjnie określać zakres takich treści (zdefiniowanych jako niewłaściwe nie uznaniowo przez ustawodawcę, ale w sposób demokratyczny, na podstawie wyników sondaży społecznych) i przewidywać usuwanie ich z sieci, a nie tylko maskowanie ich.

Internet a prawne ramy prywatności

Szerokie możliwości nadużywania prawa stwarza także obowiązkowa retencja danych przez operatorów telekomunikacyjnych, tj. zbieranie i zatrzymywanie przez określony czas informacji dotyczących połączeń elektronicznych wszelkiego typu i udostępnianie ich w celu walki z przestępczością. W Polsce, inaczej niż w wielu innych krajach, do uzyskania tego rodzaju danych przez upoważnione służby (w naszym kraju wyjątkowo liczne) nie jest konieczny nakaz sądu czy prokuratora, dlatego nikt właściwie nie sprawuje kontroli nad celowością pobierania tych informacji przez przedstawicieli służb i sposobem ich wykorzystania. Zmiana wprowadzona w tym zakresie tzw. ustawą inwigilacyjną[32] obejmuje jedynie konieczność składania do właściwego sądu okręgowego, w odstępach półrocznych, zbiorowych sprawozdań podsumowujących liczbę pobrań danych (z wyłączeniem tzw. danych abonenckich, niepodlegających sprawozdawczości), rodzaj danych i kwalifikację prawną czynów skłaniającą do ich pobrania. Sąd zaś może[33] zapoznać się z materiałami uzasadniającymi kontrolę. Raporty przekazywane do sądów nie zawierają uzasadnienia rzeczywistej konieczności pobrania tych danych, dostarczane są w formie prostych tabel weryfikowanych jedynie przez instytucje, które je sporządzają. Jeszcze mniej informacji zawierają raporty sądów, składane raz do roku ministrowi sprawiedliwości, obejmujące liczbę przypadków pozyskania danych przez poszczególne organy i rodzaj tych danych. Na ich podstawie minister raz w roku sporządza raport przedstawiany parlamentowi i opinii publicznej, zawierający jedynie zagregowaną dla wszystkich rodzajów danych i wszystkich rodzajów służb całkowitą liczbę przypadków pozyskiwania danych, co stanowi niekorzystną zmianę w stosunku do wcześniejszych przepisów[34]. Uchylony przez wprowadzenie ustawy inwigilacyjnej przepis ustawy — Prawo telekomunikacyjne zobowiązywał bowiem Urząd Komunikacji Elektronicznej do przedstawiania Komisji Europejskiej corocznego raportu, dostępnego dla obywateli w ramach danych publicznych, obejmującego oprócz całkowitej liczby zapytań także ich podział na kategorie danych i rodzaj służb o nie występujących oraz tzw. wiek danych (czas od ich zarejestrowania do zapytania) i liczbę zapytań o dane abonenckie.

Co więcej, opinia publiczna była o liczbie i rodzajach zapytań od poszczególnych służb informowana także przez Fundację Panoptykon, zbierającą dane do swoich raportów od poszczególnych służb. Było to możliwe, ponieważ zbierane przez nią dane były przekazywane w ramach dostępu do informacji publicznej. Obecnie większość służb odmawia przekazywania danych, zasłaniając się zapisem nowej ustawy głoszącym, że sprawozdania mają być przekazywane

sądom „z zachowaniem przepisów o ochronie informacji niejawnych", co pozwala im na wygodną interpretacją, że są to dane niejawne, choć nie zostało to wprost zapisane w ustawie[35].

Tak więc to, co dzieje się z Twoimi danymi, jest jeszcze bardziej nieprzejrzyste niż poprzednio. Nawet jako zwykły obywatel masz prawo czuć się zaniepokojony faktem, że władze Twojego kraju traktują Cię jak potencjalnego przestępcę, gromadząc Twoje dane na wszelki wypadek, że nikt nie kontroluje faktycznej potrzeby pobierania informacji naruszających Twoje prawo do prywatności przez upoważnione służby. A służby te do samego tylko Facebooka w pierwszej połowie 2018 roku wystąpiły z nakazem udostępnienia danych użytkowników ponad tysiąc razy[36]. Jak wygląda udostępnienie danych? W sieci można się natknąć na przykłady wydruków sprzed kilku lat[37], zawierających oprócz aktualnych danych z profilu także m.in. skasowane przez użytkownika posty i zdjęcia, informacje o usuniętych już znajomych, a także informacje o wydarzeniach, w których uczestniczył, i grupach, do których należał lub został zaproszony. Do tego wszystkie polubienia, wyświetlenia profili czy fanpage'y i zdjęć oraz uruchomienia aplikacji. Jeśli dorzucimy dane, które można zebrać np. od Google, historię odwiedzonych stron, wyszukiwania itd. i operatora telekomunikacyjnego sieci, w której mamy telefon, numery, pod które dzwonimy, numery rozmów przychodzących, treść wiadomości, miejsca logowania, to mamy niezły obraz historii naszego życia oraz naszych relacji służbowych i towarzyskich. W 2016 roku Policja i inne służby pobrały nasze bilingi i dane o logowaniu się telefonów 1 147 092 razy[38], w roku 2017 było ich już ponad 1,5 mln, a specjaliści Polskiego Instytutu Cyberbezpieczeństwa szacują, że w roku 2018 możemy przekroczyć 2 mln zapytań.

Pobrane i sprawdzane dane w niektórych przypadkach mogą też naruszać tajemnice lub prawo do prywatności innych osób, powiązanych z osobą inwigilowaną: w przypadku dziennikarzy — ich źródła informacji, w przypadku lekarzy — ich pacjentów, w przypadku prawników — klientów itd. Mimo negatywnej opinii wielu osób i instytucji (np. Naczelnej Rady Adwokackiej, Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych[39]) i wieloletnich dyskusji poświęconych temu zagadnieniu retencja danych nadal jest dla rządzących (bez względu na opcję polityczną) czymś oczywistym i nic nie wskazuje na to, by z własnej inicjatywy zechcieli z niej zrezygnować. Przeciwnie — nowa ustawa o Policji uwzględnia również, prowadzoną za zgodą sądu, tzw. kontrolę operacyjną, czyli kontrolę informacji przekazywanych przy użyciu sieci telekomunikacyjnych, podsłuchiwanie rozmów telefonicznych, sprawdzanie

listów i przesyłek itp. W sytuacjach uznanych przez Policję za pilne wystarczy jedynie pisemna zgoda prokuratora. Fundacja Panoptykon dodaje, że prawdopodobnie władze korzystają również z danych zebranych o nas przez prywatne sieci medyczne, takie jak Medicover, Enel-Med czy LUX MED[40]. Mogą też, na podstawie art. 20 ust. 3 ustawy o Policji, uzyskać dostęp do naszych danych stanowiących tajemnicę bankową, skarbową, zawodową, ubezpieczeniową[41] itd. To jeszcze nie wszystko — ustawa inwigilacyjna wprowadziła dodatkowe ułatwienie dla służb w pobieraniu danych internetowych na nasz temat: mogą teraz pobierać je bezpośrednio od firm, przy udziale tzw. bezpiecznego łącza, nie angażując w to pracowników firm lub angażując tylko niezbędnych[42]. W ustawie zastrzeżono przy tym co prawda, że nie wolno w ten sposób pobierać treści naszych e-maili, ale nie zawsze łatwe jest od strony technicznej oddzielenie danych użytkownika od treści jego korespondencji, a ponadto przy bezpośrednim pobieraniu danych przez służby pracownicy firm nie są w stanie skontrolować przestrzegania tego zapisu.

Choć w polskim systemie prawnym nie funkcjonuje takie pojęcie jak legalny *hacking* (ang. *lawful hacking*), to właśnie z tym zjawiskiem mamy do czynienia w przypadku niektórych zmian wprowadzonych w 2016 roku i funkcjonującej już wcześniej kontroli operacyjnej[43]. Kontrola ta wszak umożliwia uzyskiwanie i utrwalanie treści rozmów, korespondencji i danych z urządzeń i systemów teleinformatycznych, a także obrazu i dźwięku z miejsc niepublicznych[44]. Przeciwnicy takich rozwiązań podkreślają, że system prawny nie uwzględnił bardzo istotnych praw inwigilowanych obywateli: „wymogu (w ramach tzw. procedury następczej) informowania podmiotów inwigilowanych o niejawnym pozyskaniu informacji na ich temat, [...] procedury dającej prawo zaskarżania przez ww. podmioty czynności operacyjno-rozpoznawczych; [...] uzależnienia zgody na kontrolę operacyjną od niemożności uzyskania danych w inny, mniej *inwazyjny* sposób (zasada proporcjonalności)”[45].

Służbom zarzuca się też często nadużywanie swoich uprawnień. Kontrowersje wzbudzają zmiany wprowadzone w polskim prawie wraz ze zmianą ustawy antyterrorystycznej i zezwalające na działania w ramach tzw. oceny bezpieczeństwa i blokady dostępności. Ocena bezpieczeństwa umożliwia służbom bezpieczeństwa testowanie sieci teleinformatycznych (tzw. testowanie penetracyjne), a więc m.in. tworzenie i stosowanie hakerskich narzędzi, łamanie zabezpieczeń sieci czy stosowanie inżynierii społecznej w celu pozyskania potrzebnych danych. Niebezpieczeństwo dla praw obywatelskich stanowi w jej przypadku m.in. brak doprecyzowania, jakiego rodzaju dane wolno służbom gromadzić. Blokada

dostępności polega na uniedostępnianiu danych w celu: przeciwdziałania terroryzmowi, wykrywania przestępstw o charakterze terrorystycznym i przeciwdziałania im. Zdaniem przeciwników tego rozwiązania przesłanki pozwalające na zablokowanie treści w internecie są zbyt ogólne, a uprawnienia służb mogą naruszać prawo obywateli do wolności wypowiedzi[46]. Polską ustawę antyterrorystyczną krytykuje również najnowszy raport Amnesty International: „W ustawie zawarto szerokie definicje terroryzmu i *zdarzeń o charakterze terrorystycznym* oraz odpowiadające im przepisy. Nowe prawo dotyka przede wszystkim cudzoziemców. Ustawa zezwala na niejawną inwigilację, w tym zakładanie podsłuchu, monitoring komunikacji online, inwigilację sieci i urządzeń telekomunikacyjnych bez autoryzacji sądu przez 3 miesiące, po których inwigilacja może zostać przedłużona nakazem sądowym. Wystarczającym usprawiedliwieniem koniecznym do wykorzystania tych środków prawnych jest *obawa*, a nie uzasadnione podejrzenie, że dana osoba może być zaangażowania w działania terrorystyczne”[47].

Lawful hacking nie tylko w Polsce budzi sprzeciw — w 2016 roku głośny był konflikt między firmą Apple a FBI[48]. Federalne Biuro Śledcze zażądało od firmy Apple złamania zabezpieczeń do iPhone’a terrorysty, który w San Bernardino zabił kilkanaście osób — Syeda Rizwana Farooka. Ponieważ od 2014[49] roku dane (SMS-y, fotografie itp.) na iPhone’ach Apple’a są szyfrowane (na co istotny wpływ miały sensacyjne informacje Snowdena) i dostęp do nich możliwy jest tylko po wpisaniu przez właściciela hasła, a kilkakrotne wpisanie niewłaściwego hasła powoduje skasowanie danych, amerykańscy śledczy zażądali od twórców oprogramowania ominięcia tego systemu ochrony danych. Firma odmówiła. Sprawa skończyła się w sądzie. Przedstawiciele Federalnego Biura Śledczego argumentowali swoje stanowisko potrzebą walki z terroryzmem. Jednak szefowie Apple’a byli nieugięci. Przekazali FBI dostępne w chmurze kopie telefonu zabójcy, ale w kwestiach zabezpieczeń odmówili. Opublikowali m.in. list otwarty w tej sprawie, w którym napisali: „Teraz rząd Stanów Zjednoczonych poprosił nas o coś, czego nie mamy i czego stworzenie byłoby bardzo niebezpieczne. Poprosili nas o zbudowanie do iPhone’a tylnych drzwi”. Dyrektor generalny firmy Apple podkreślał w swoich wypowiedziach, że żądanie stworzenia tylnej furtki do zabezpieczeń urządzenia, z którego korzystał Farook, a co za tym idzie, do wszystkich produkowanych przez firmę urządzeń, stanowi niebezpieczny precedens. „Rząd zwraca się do Apple’a o zhakowanie naszych własnych użytkowników i podważenie dekad rozwoju zabezpieczeń chroniących naszych klientów” — uzasadniał odmowę. Jakiś czas później FBI zrezygnowało z dalszego prowadzenia sprawy sądowej, informując, że złamało zabezpieczenia „przy pomocy

osób trzecich". Mówiono, że śledczym udało się to dzięki fachowcom z izraelskiej firmy Cellebrite. I tym razem FBI odmówiło pomocy firmie Apple, nie zgadzając się na udostępnienie jej informacji, w jaki sposób włamano się do iPhone'a. Szefowie Apple'a zapowiedzieli więc, że poszukają luki w systemie zabezpieczeń na własną rękę i zaktualizują oprogramowanie. Pozostali przy stanowisku, że ich decyzja była słuszna. Opinię tę podzielili inni (w przeważającej większości) producenci oprogramowania i duża część społeczeństwa, choć Barack Obama podkreślał, że prawo do prywatności danych na urządzeniach mobilnych nie może przesłaniać innych racji. Czy miał rację? FBI nie poinformowało, czy jakiekolwiek istotne dane znaleziono w telefonie terrorysty — który już dokonał ataku (więc cokolwiek to było, nie zapobiegło śmierci obywateli) — będącym pretekstem do złamania zabezpieczenia chroniącego prywatne dane wszystkich innych użytkowników urządzeń tego typu przed cyberprzestępcami, i nie zgodziło się na przekazanie producentom informacji, jak lepiej zabezpieczyć te dane, kiedy już taką informację zdobyło (powiększając tym samym grono przeciwników „legalnego hackingu").

Z negatywnym oddźwiękiem społecznym spotkało się również działanie firmy Amazon, która w czasie sporu pomiędzy FBI a szefami Apple'a dyskretnie, nie informując o tym użytkowników, usunęła podczas jednej z aktualizacji oprogramowania w swoich produktach możliwość szyfrowania danych z poziomu urządzenia[50].

Tymczasem polskie władze planują inwigilację mieszkańców na jeszcze większą skalę; np. ustawa o Komisji Nadzoru Finansowego (KNF) wprowadziła istotne zmiany bardzo niebezpieczne dla naszego prawa do prywatności. Fundacja Panoptykon, która złożyła już w tej sprawie petycję, ostrzegała jeszcze na etapie tworzenia ustawy: „W obecnym brzmieniu projekt umożliwia przewodniczącemu KNF dostęp do treści rozmów bez żadnej zewnętrznej kontroli: tak daleko idących uprawnień nie mają nawet służby takie jak Policja czy ABW. Zaproponowaliśmy, żeby przewodniczący KNF musiał w tym celu uzyskać zgodę sądu — i to tylko pod warunkiem, że inne środki okażą się nieskuteczne. [...] Wzmocnienia wymaga też system kontroli nad pozyskiwaniem przez przewodniczącego KNF bilingów i innych danych niezawierających treści rozmów. Uważamy, że najpełniejszą ochronę przed nadmierną ingerencją w prywatność zapewni konieczność każdorazowego uzyskania uprzedniej zgody sądu. [...] W obecnym brzmieniu projektu Komisja może podjąć decyzję o wpisaniu strony internetowej na listę ostrzeżeń publicznych w drodze uchwały (i to nawet przed złożeniem zawiadomienia do prokuratury!), a operatorzy internetowi muszą

automatycznie zablokować do dostęp do tej strony. Rodzi to ogromne ryzyko pomyłek i arbitralności”[51]. Ponieważ ustawodawca nie uwzględnił tych zastrzeżeń, Fundacja skierowała pismo w tej sprawie do Rzecznika Praw Obywatelskich, który na skutek tej interwencji zwrócił się z prośbą o wyjaśnienia do Ministra Rozwoju i Finansów i zasugerował konieczność zmian prawnych[52]. W odpowiedzi na zarzuty przedstawione przez Rzecznika podsekretarz stanu w Ministerstwie Finansów „zadeklarował, że jeszcze w tym roku zaproponuje wprowadzenie nadzoru nad kontrowersyjnymi uprawnieniami Szefa KNF. Mechanizm ma być analogiczny do tego, jaki sąd sprawuje nad działaniami CBA”[53].

Czy na pewno do takiego „bezpieczeństwa” dążymy? Czy chcemy, by bez naszej wiedzy i zgody inne osoby, kiedy tylko zechcą, zaglądały nam do komputerów, kart zdrowia, historii zakupów, umów bankowych czy ubezpieczeniowych i sypialni, bo ewentualnie moglibyśmy być o coś podejrzani? Czy ustawa inwigilacyjna nie oznacza przypadkiem, że jeśli krzywo spojrzymy na dzielnicowego, to ten może nam się odwdzięczyć, szukając na nas „haka” w kilku tomach zebranych (pod byle pretekstem) informacji na nasz temat? Czy już wkrótce będzie wolno uznaniowo zablokować naszą stronę internetową lub nasz artykuł, tylko dlatego, że komuś się nie spodobały? Czy możemy mieć pewność, że do takiej blokady nie wystarczy prosta argumentacja typu: nie podoba mu się działanie Rady Ministrów = jest przeciwko Radzie Ministrów = jest opozycjonistą = może być wrogo nastawiony do polityków partii rządzących = stanowi zagrożenie dla ich bezpieczeństwa = jest potencjalnym zamachowcem? Czy dużo brakuje do ocenzurowania w internecie treści „niepoprawnych politycznie” (gdyż przykładowo mogłyby mieć niekorzystny wpływ na wychowanie i edukację młodzieży) albo komentarzy krytycznych (bo potencjalnie mogą naruszyć czyjeś dobra osobiste) itp.? Czy nie znaleźliśmy się niebezpiecznie blisko granicy, w której prywatność już nie istnieje, bo zrezygnowano z niej „dla wyższych celów”, np. wybranego poziomu bezpieczeństwa? Czy nie masz wrażenia, że historia zatoczyła koło? Ideę poświęceń „dla wspólnego dobra” już kiedyś usiłowano narzucić światu, wszyscy znamy efekty. A przecież wtedy nie było jeszcze tak doskonałych narzędzi inwigilacyjnych...

Z raportu organizacji Freedom House (*Freedom on the Net 2016*) wynika, że 67% wszystkich użytkowników internetu na świecie jest poddawanych inwigilacji, a 27% mieszka w krajach, w których aresztowano ludzi za publikowanie, share’owanie albo nawet polubienie czegoś na Facebooku[54]. Jeśli nie chcesz godzić się potulnie na taką sytuację i na życie wszechstronnie upublicznione — możesz zacząć działać: uświadamiać znajomych, pisać petycje i brać udział

w protestach przeciwko ograniczaniu Twoich praw, dopóki jeszcze oficjalnie za takie uznawane są wolność słowa, prawo do prywatności, prawo do nienaruszalności korespondencji, wolny internet itp.

Ochrona danych

Władze nie tylko chętnie same pozyskują informacje na temat obywateli, ale także słabo chronią dostęp do tych informacji na forum międzynarodowym. Najlepszy przykład stanowić może Safe Harbour, czyli system „bezpiecznego" przekazywania danych do USA (choć w tym przypadku można mówić o lekkomyślności całej Unii Europejskiej, nie tylko naszego kraju). Jak podało w 2014 roku Ministerstwo Administracji i Cyfryzacji, „Komisja Europejska sama przyznaje, iż w momencie negocjacji zasad *bezpiecznej przystani* nie była w stanie przewidzieć skali, jaką może osiągnąć inwigilacja przez agencje wywiadowcze danych przekazywanych w Internecie w związku z działalnością gospodarczą (takie dane są przekazywane w ramach *bezpiecznej przystani*). Dostrzega ona także zagrożenie w postaci dostępu do danych przez organy amerykańskie poza niezbędnym i proporcjonalnym, ze względu na bezpieczeństwo narodowe, porządek publiczny oraz egzekwowanie prawa, zakresem. Te trzy przesłanki interpretowane są przez stronę amerykańską szeroko. Przekazywanie danych amerykańskim służbom przez podmioty certyfikowane odbywa się bez żadnej kontroli ze strony europejskiej"[55]. Wiemy jednak, że przecież to nie jedyne umowy dotyczące przekazywania informacji o obywatelach, przy których podpisywaniu poświęcono zbyt mało uwagi ochronie danych. Podobnie przedstawia się sytuacja z danymi o transakcjach finansowych przekazywanymi na podstawie porozumienia SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) czy danymi pasażerów linii lotniczych przekazywanymi na podstawie porozumienia w sprawie PNR (*Passenger Name Records*). W ramach tych drugich oprócz typowych danych teleadresowych i numeru karty kredytowej zbierane są też informacje „o rezerwacjach hotelowych, wynajmie samochodu czy zakupie biletu kolejowego, jeśli tylko strona linii lotniczych oferuje taką możliwość. Dane PNR mogą też zawierać wrażliwe informacje, takie jak dane o stanie zdrowia albo fakt rezerwowania pokoju z podwójnym łóżkiem (co może zdradzać relacje intymne)"[56].

RODO

Dostęp do naszych danych mają wszakże nie tylko rządy, służby specjalne i inne organizacje państwowe. Ogromnymi zasobami takich danych dysponują liczne firmy prywatne (ubezpieczyciele, sieci medyczne, banki, sklepy itd.) oraz hakerzy i nielegalni handlarze danych. Technologie teleinformatyczne umożliwiły nie tylko bezproblemowe kopiowanie i przesyłanie ogromnych ilości takich danych, ale także tworzenie w sieci licznych baz danych i e-handel nimi. Poszczególne państwa na różne sposoby starają się ukrócić proceder nieuczciwego pozyskiwania danych, nielegalnej ich sprzedaży i niewłaściwego ich wykorzystania, nie przynosi to jednak spektakularnych efektów. Problemem tym zajmuje się również prawodawstwo unijne. To właśnie najnowsze w tym zakresie rozporządzenie UE wprowadza do europejskich systemów prawnych wiele oczekiwanych przez obywateli zmian. Nie tylko przyczynia się bowiem do ujednolicenia przepisów w krajach europejskich i uregulowania przekazywania danych do państw trzecich, ale też stawia wiele konkretnych wymogów właścicielom i administratorom baz zawierających dane osobowe. Trudno dziś wyrokować, czy przyniesie ono realne zmiany, niemniej jednak stanowi w dziedzinie ochrony danych osobowych milowy krok we właściwym kierunku. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE1 (zwane RODO lub GDRP) weszło w życie w maju 2016 roku, jednak w poszczególnych państwach unijnych obowiązywać zaczęło w maju 2018 roku, po upływie okresu niezbędnego na dostosowanie się podmiotów przetwarzających dane osobowe do jego wymogów.

Przetwarzanie danych to — w myśl obowiązujących przepisów — dowolne operacje (zwłaszcza te wykonywane w systemach informatycznych) na danych, takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. Przepisy o ochronie danych osobowych wchodzą w zakres różnego rodzaju aktów prawnych, takich jak Kodeks pracy, ustawa o świadczeniu usług drogą elektroniczną, ustawa — Prawo telekomunikacyjne czy ustawa o usługach detektywistycznych[57], najistotniejsze regulacje w tym zakresie wprowadza jednak ustawa ochronie danych osobowych, która w obecnym brzmieniu musi być dostosowana do zapisów zawartych w RODO.

Rozporządzenie to obejmie nie tylko podmioty unijne, ale także podmioty spoza UE „będą miały obowiązek zapewnienia zgodności z Rozporządzeniem w zakresie przetwarzania danych osobowych osób przebywających na terenie

UE wtedy, gdy czynność przetwarzania wiąże się z: oferowaniem towarów lub usług takim osobom w UE, niezależnie, czy wymaga się od tych osób zapłaty; lub monitorowaniem ich zachowania, o ile do tego zachowania dochodzi w UE”[58]. Ponadto rozporządzenie przewiduje, że przetwarzanie danych będzie oparte na przynajmniej jednej ze wskazanych w nim podstaw prawnych, a więc jest niezbędne do wykonania umowy zawartej z osobą, której dane są przetwarzane, do wywiązania się administratora z obowiązków narzuconych prawem lub zadania realizowanego w interesie publicznym, do ochrony żywotnych interesów albo osoby, której dane dotyczą, albo innych osób fizycznych, ewentualnie wynika z uzasadnionych interesów realizowanych przez przetwarzającego dane lub przez stronę trzecią (i ten zapis przedstawia najszersze pole interpretacji do nadużyć), albo osoba, której dane dotyczą, wyraziła zgodę (w sposób mający charakter świadomego działania) na ich przetwarzanie w określonym (jasno, z góry) celu (lub w różnych, wyszczególnionych odrębnie celach). Co ważne, zgoda taka musi być dobrowolna, nie można więc (co jest obecnie powszechną praktyką) uzależnić od niej wykonania umowy (jeśli do celów wykonania umowy nie jest niezbędne przetwarzanie danych w tym zakresie czy celu) ani wyciągnąć w stosunku do odmawiającego jej udzielenia innych negatywnych konsekwencji. Zgoda pozyskana w sposób niezgodny z przepisami będzie nieważna, a kara za łamanie tego przepisu przez przedsiębiorcę wynosi „do 20 000 000 euro lub [...] do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot będzie wyższa”[59]. Osoba udzielająca zgody na przetwarzanie jej danych musi też otrzymać na temat celów i zakresu tego przetwarzania jasne, zrozumiałe informacje (zasada przejrzystości). Ponadto zakres pozyskiwanych danych musi być adekwatny do określonego celu i ograniczony do niezbędnego minimum pozwalającego ten cel zrealizować.

Przetwarzanie danych powinno być realizowane w taki sposób, by wykluczyć możliwość nieautoryzowanego usunięcia lub zmodyfikowania ich (zasada integralności) albo niezgodnego z prawem udostępnienia lub przekazania innym podmiotom (zasada poufności). Niezbędne środki do realizacji tych zasad powinny być wprowadzane na wszystkich etapach działań przetwarzającego dane — już od momentu planowania aplikacji, procedur, poprzez wdrażanie ich, aż po ich wycofywanie (tzw. zasada *security by design*, nazywana też zasadą bezpieczeństwa w fazie projektowania, i tzw. *zasada security by default*, określana jako zasada bezpieczeństwa w ustawieniach domyślnych). Administrator danych musi również być w stanie wykazać, że spełnia wymogi RODO (zasada rozliczalności).

Osoby fizyczne, których dane są przetwarzane, mają w myśl nowego rozporządzenia prawo m.in. do wglądu w dane, do sprzeciwu wobec ich przetwarzania, do żądania ich sprostowania lub przeniesienia, a także do bycia zapomnianym. Na administratorach danych spoczywa zaś obowiązek informowania tych osób o celach przetwarzania, o danych administratora oraz o innych odbiorcach danych osobowych, o sposobie przetwarzania i czasie przechowywania tych danych oraz o przekazywaniu ich poza UE, jeśli taka okoliczność zachodzi. RODO sugeruje też podmiotom administrującym danymi ich anonimizację, czyli opracowanie ich w taki sposób, aby nie można ich było przypisać do osoby, oraz pseudonimizację, czyli oddzielenie danych osobowych od danych personalnych pozwalających na ich identyfikację. Rodzi to jednak pewne niebezpieczeństwa — dane anonimowe nie podlegają przepisom o ochronie danych w ramach RODO, choć przecież przy dużej ilości zgromadzonych danych istnieje możliwość ustalenia tożsamości osób, których dotyczą, podobnie jak istnieje możliwość powiązania danych osobowych z personaliami, nawet jeśli teoretycznie są przechowywane osobno, skoro są w posiadaniu tego samego administratora.

Bardzo istotną zmianą wprowadzaną przez RODO jest natomiast to, że osoba, której dane są przetwarzane dla innych celów, będzie mogła wyłączyć je spod profilowania, będzie miała prawo nie wyrazić na nie zgody, otrzyma „prawo do tego, by nie podlegać decyzji, która ocenia jej czynniki osobowe, opierając się wyłącznie na przetwarzaniu zautomatyzowanym", tym bardziej że „tego typu decyzje mogą wywoływać skutki prawne lub w podobny sposób znacząco wpływać na sytuację osoby, której dane dotyczą"[60]. Rozporządzenie jest też pierwszym aktem prawnym, który wprowadza w Polsce zasady *privacy by design* (tj. zasadę prywatności w fazie projektowania) i *privacy by default* (tj. zasadę prywatności w ustawieniach domyślnych).

LUDZKOŚĆ OD WIELU TYSIĘCY LAT PRZEKSZTAŁCA I ZMIENIA OTACZAJĄCĄ JĄ PRZESTRZEŃ.

Jednak nawet XIX-wieczna rewolucja przemysłowa nie przyczyniła się w tak dużym stopniu do zmiany codziennego życia, ewolucji struktur społecznych czy uwarunkowań psychologicznych, jak współczesny postęp cybernetyczno-internetowy. Nowoczesna technologia już dawno przekroczyła granice wieku użytkownika, a teraz mierzy się z granicą czasu. Zaledwie 2 procent ludzi na świecie, którzy mają dostęp do komputera, smartfona czy internetu, deklaruje, że mogłoby bez nich żyć. W której grupie jesteś Ty?

Dobrodziejstwa technologiczne otoczyły życie człowieka jak pajęczyna, z której już dziś niezwykle trudno jest się wydostać, a za kilka lat może to być całkiem niemożliwe. Rozwój nowoczesnych technologii niesie ze sobą wiele korzyści, ale jeszcze więcej zagrożeń. Rodzi również pytania o kondycję ludzkości, o wszechobecną możliwość manipulacji. Polityka, bezpieczeństwo, nasza prywatność i anonimowość — to zagadnienia, które Krzysztof Gawkowski porusza w swojej książce. Przeczytaj i dowiedz się, gdzie czają się niebezpieczeństwa i jak się przed nimi chronić. Naucz się, jak nie dać się pochłonąć i oszukać w cyfrowym świecie.

CYBERKOLONIALIZM TO KSIĄŻKA O BLISKIEJ PRZYSZŁOŚCI, KTÓRA NA PEWNO ZMIENI TWOJE ŻYCIE. MOŻE SAM ZOSTANIESZ CYFROWYM REWOLUCJONISTĄ?

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-4801-1
9 788328 348011
INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 44,90 zł