WARSZAWSKI WSPÓLNICY

cyberbezpieczeństwo

Warszawa, listopad 2014 r.

Spis treści

Ochrona przed zagrożeniami z cyberprzestrzeni 3
Cyberbezpieczeństwo w praktyce 7
Europejskie podejście do cyberbezpieczeństwa 11
Ściganie przestępstw popełnionych w cyberprzestrzeni 16
Ochrona tajemnicy przedsiębiorstwa w świecie cyfrowym 20
Przeszukania na odległość – jeszcze nie teraz 24
Zabezpieczenie dowodów elektronicznych w postępowaniu karnym 27
Konkluzje 35
Autorzy 36
Praktyka prawa nowych technologii 38
Praktyka karna 39
O kancelarii 40
O EFICOM 41

Ochrona przed zagrożeniami z cyberprzestrzeni

Piotr Rutkowski

Niepożądanym skutkiem szybkiego rozwoju coraz bardziej użytecznych usług i aplikacji w sieciach łączności elektronicznej są liczne nowe okazje do naruszania norm, które przez wieki wypracowała cywilizacja, by dać społeczeństwom pewność bezpiecznego życia. W usieciowionym społeczeństwie spójny niegdyś system norm i wartości coraz bardziej się relatywizuje, co ma związek z łatwością tworzenia nowych relacji i możliwością konfrontacji z normami i systemami wartości istniejącymi w innych kręgach kulturowych.

Bezpieczeństwo w internecie, zwane cyberbezpieczeństwem, stało się problemem ze względu na złożone oddziaływanie przynajmniej trzech niezależnych czynników: (i) z sieci korzystają także nieuczciwe osoby, (ii) rośnie nasze uzależnienie od wielu ważnych dla nas procesów zachodzących w internecie, (iii) w bardzo złożonym technicznie systemie nieuniknione jest istnienie słabych punktów, z których mogą skorzystać osoby mające wobec nas złe zamiary.

Z okazji do popełniania czynów kryminalnych z wykorzystaniem cyberprzestrzeni korzystają nie tylko pojedynczy przestępcy. Coraz szerszą działalność w wirtualnej przestrzeni podejmuje też przestępczość zorganizowana, z którą przeważnie trudniej jest walczyć. Zasięg nielegalnych działań może być ogromny, prowadząc do kradzieży pieniędzy z wielu milionów kart płatniczych oraz oszustw na ogromną skalę. Media wciąż dostarczają przykładów takich przestępstw, niekiedy bardzo pomysłowych. Cyberprzestrzeń inspiruje też środowiska o poglądach skrajnych, które nie stronią od planowania akcji o charakterze cyberterrorystycznym. Nie trzeba wreszcie wielkiej wyobraźni, by przyjąć, że niektóre ataki na systemy informacyjne mogą być sponsorowane przez wrogie rządy. Oficjalne raporty bezpieczeństwa odnotowują przypadki szpiegostwa skierowanego na wykradanie tajemnic firm technologicznych lub eksplorującego możliwość ataku na obiekty infrastruktury krytycznej.

Wymuszona współpraca

Opublikowana na początku 2013 roku unijna strategia bezpieczeństwa cybernetycznego[1] całościowo ujmuje problematykę zagrożeń z cyberprzestrzeni, postulując przede wszystkim uruchomienie mechanizmów współpracy i wymiany informacji. Z zestawienia zagadnień w tym

[1] Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, JOIN(2013)1 final.

dokumencie wynika, że nawet w przypadku cyberprzestępstw już penalizowanych w systemie prawa karnego jest to wyzwanie wielowątkowe, czyli koncepcyjnie trudne, a na dodatek różnie traktowane w poszczególnych jurysdykcjach. Ponadto należy się liczyć z tym, że wymiana informacji o zagrożeniach systemów informacyjnych identyfikowanych jako wrażliwe z punktu widzenia państwa lub poszczególnych sektorów gospodarki będzie budziła opór.

Strategii towarzyszył projekt dyrektywy w sprawie cyberbezpieczeństwa[2], jednak debata nad nim się przeciąga. Poprzedni Parlament Europejski wniósł wiele poprawek na etapie pierwszego czytania, a na efekty przyjęcia i wdrożenia dyrektywy trzeba będzie poczekać, ponieważ projektowany okres transpozycji wynosi 18 miesięcy.

Tymczasem brak mechanizmów skutecznej współpracy pomiędzy państwem a sektorem prywatnym w zakresie cyberprzestępstw jest jednym z najważniejszych i jednocześnie najtrudniejszych do rozstrzygnięcia zagadnień bezpieczeństwa we współczesnym świecie. W Stanach Zjednoczonych po atakach terrorystycznych 11 września społeczna akceptacja dla wymiany informacji o zagrożeniach była bardzo duża. Znamienne jest, że osiągnięto stan, w którym dbałość o interesy akcjonariuszy spółki giełdowej oceniano przez pryzmat jej polityki bezpieczeństwa. Wdrożone wówczas mechanizmy dobrowolnej wymiany informacji są jednak obecnie krytykowane nie tylko ze względu na wątpliwości co do zakresu uprawnień państwa wywołane ujawnieniem istnienia systemu PRISM posiadanego przez NSA. W wielu przypadkach te dobrowolne mechanizmy okazały się nieskuteczne, bo nie powstrzymały rosnącej fali cyberprzestępstw, które zdarzają się pomimo jasnych sygnałów ostrzegawczych.

Spektakularnym przykładem takiego zaniechania była ubiegłoroczna kradzież danych 40 mln kart płatniczych w Stanach Zjednoczonych w okresie świątecznego szczytu zakupowego. Zlekceważono wyraźne sygnały ostrzegawcze, bo dotyczyły mikropłatności. Na domiar złego nie zadziałały procedury wymiany informacji[3].

Między innymi z powodu słabości systemu wymiany informacji w lipcu 2014 roku Kongres Stanów Zjednoczonych przyjął trzy ustawy wprowadzające szereg zmian wzmacniających i formalizujących zasady współpracy z sektorem prywatnym w sprawach cyberbezpieczeństwa[4]. Komentarze na temat wprowadzanych zmian pokazują, że to zaledwie kolejny etap dyskusji o przeciwdziałaniu zagrożeniom z cyberprzestrzeni, która powinna doprowadzić do współpracy wszystkich zainteresowanych.

Ryzyko cyberwojny

Prognozowany od jakiegoś czasu znaczny wzrost zagrożeń z cyberprzestrzeni jest być może nieuchronnym skutkiem kryzysu w stosunkach międzynarodowych spowodowanego zaangażowaniem Rosji w działania separatystów na Krymie i we wschodniej Ukrainie. Konflikt ten ma cechy wojny hybrydowej. Zmobilizowaniu armii na

[2] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii, COM(2013)48.

[3] Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It, http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

[4] H.R.3696 – National Cybersecurity and Critical Infrastructure Protection Act of 2014

granicy spornego obszaru i potyczkom zbrojnym prowadzonym przez nieregularne oddziały towarzyszy ostra wojna propagandowa i nasilenie ataków w cyberprzestrzeni.

Rosjanie otwarcie grożą odwetem za sankcje nakładane na nią przez Unię Europejską, Stany Zjednoczone, Kanadę i Australię. Doświadczenie wcześniejszych konfliktów z sąsiadami (Gruzją w 2008 roku i Estonią w 2007 roku) dowodzi, że Rosjanie chętnie używają ataków w cyberprzestrzeni jako wspomagającego środka odwetowego. Podczas wojny w Gruzji cyberataki wspomagały bezpośrednio operacje wojskowe. W Estonii nie doszło do zaangażowania oddziałów zbrojnych, ale dzięki cyberatakom uzyskano przede wszystkim efekt psychologiczny. Blokada systemów rządowych i bankowych miała pokazać „nie jesteście bezpieczni". Zaatakowana Estonia już wtedy była jednak członkiem NATO. Mimo że Rosjanie starali się przedstawić ataki cybernetyczne jako spontaniczną akcję niezorganizowanej formalnie grupy patriotycznych hakerów, wydarzenia te sprowokowały dowództwo NATO do ustanowienia Centrum Kompetencyjnego ds. Obrony Cybernetycznej (NATO Cooperative Cyber Defence Centre of Excellence) z siedzibą w Tallinie.

W tegorocznym sprawozdaniu składanym przez amerykańskie agencje wywiadowcze przed Kongresem[5] szef wspólnoty wywiadowczej James R. Clapper umieścił ryzyka związane z cyberprzestrzenią na czele listy najważniejszych źródeł zagrożeń globalnych. Zwrócił przy tym uwagę na istotną rozbieżność poglądów dotyczących stosowania prawa międzynarodowego do cyberprzestrzeni. Po jednej stronie sporu znajdują się Stany Zjednoczone i Unia Europejska, a po drugiej m.in. Rosja i Chiny. Rosja przy wsparciu Chin i niektórych innych państw, posługując się hasłami suwerenności narodowej w sprawach kontroli treści, próbuje w ostatnich latach forsować na różnych forach umowy, by uprzedzić planowane objęcie cyberprzestrzeni dotychczasowym dorobkiem prawa międzynarodowego, w tym Kartą Narodów Zjednoczonych. Przykładem tego rodzaju działań było promowanie zmiany regulaminu telekomunikacyjnego przy okazji konferencji Międzynarodowego Związku Telekomunikacyjnego w Stambule w 2012 roku.

Pomijając jednak debatę o zarządzaniu światowym internetem i swobodach obywatelskich, kwestia stosowania prawa międzynarodowego do cyberprzestrzeni ma też znaczenie dla międzynarodowego prawa wojennego. Biorąc bowiem pod uwagę potencjalne szkody, które mógłby wywołać atak z cyberprzestrzeni na nowoczesne systemy energetyczne, infrastrukturę wodną, gazową czy systemy zarządzania transportem, należałoby takie działania traktować jako akty agresji prowadzące do wojny w rozumieniu prawa międzynarodowego. Wiele krajów tworzy obecnie specjalne tajne oddziały wojskowe do walki w cyberprzestrzeni.

[5] Statement for the Record Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, James R. Clapper, Director of National Intelligence http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

W tym kontekście, biorąc pod uwagę rozważania o ewentualności globalnej cyberwojny, warto przytoczyć pogląd zaprezentowany ostatnio[6] przez Center for Strategic and International Studies (CSIS), jeden z najbardziej renomowanych waszyngtońskich think tanków, znany w Polsce z udziału Zbigniewa Brzezińskiego. Otóż z amerykańskiego punktu widzenia gwarantem bezpieczeństwa międzynarodowego wciąż pozostaje doktryna odstraszania oparta o zdolność użycia broni jądrowej i rakiet dalekiego zasięgu. Eksperci CSIS uważają, że ryzyko wywołania wojny o zasięgu globalnym może powstrzymać przede wszystkim utrzymanie przeciwnika w przeświadczeniu, że w odwecie zostanie użyta przeciw niemu najgroźniejsza niszcząca broń ofensywna. Tymczasem nawet bolesny w skutkach atak z cyberprzestrzeni nie wywołałby dzisiaj najprawdopodobniej odwetowej reakcji z użyciem rakiet strategicznych.

Takie podejście pokazuje, że odpowiedzialność za działania zapewniające gotowość i odporność systemów informacyjnych na ataki spoczywa przede wszystkim na podmiotach, które nimi zarządzają. To one będą na pierwszej linii ataku i muszą mu zaradzić, nie oczekując natychmiastowej odsieczy.

Zamiast ograniczać się do myślenia, jakimi coraz bardziej złożonymi metodami technicznymi i prawnymi powstrzymywać cyberataki na konkretne systemy, definiowane w teoretycznych założeniach jako krytyczne, właściwiej byłoby rozważać, jak jaśniej zdefiniować żywotne interesy państwa i obywateli, by zaplanować skontrowanie przeciwników. Trzeba zrozumieć, gdzie i jakimi metodami przeciwnik może zadziałać, by nam zaszkodzić lub osiągnąć własną korzyść. To przeważnie nie jest równoznaczne z rzuceniem wszystkich sił na budowanie murów obronnych.

Wszelkie rozważania na temat rozwiązań prawnych, które zapewniłyby bezpieczeństwo użytkowania technologii informacyjnych, ale równocześnie sprzyjałyby ich rozwojowi, muszą brać pod uwagę, że okazje do cyberprzestępstw mogą być obecnie łatwo wykorzystywane w dużej skali, a motywy atakujących mogą być złożone i z perspektywy atakowanego niełatwe do zdiagnozowania, szczególnie jeżeli zleceniodawcą jest wrogi rząd.

Powyższe rozważania obrazują skalę zagrożeń, z których muszą sobie dziś zdawać sprawę przedsiębiorcy prowadzący choćby część działalności w internecie. Nawet jeśli nie zarządzają infrastrukturą krytyczną, która mogłaby stać się obiektem ataku wrogich rządów, mogą znaleźć się na celowniku zorganizowanych grup przestępczych czy paść ofiarą hakera, który znajdzie lukę w ich systemie zabezpieczeń. Stawką może być bezpieczeństwo obywateli, wynik finansowy przedsiębiorstwa lub wizerunek i wiarygodność przedsiębiorcy. Każdy atak może być dotkliwy w skutkach. Dlatego nikt nie może sobie pozwolić na to, by bagatelizować zagrożenia płynące z cyberprzestrzeni.

[6] 2015 Global Forecast, Center for Strategic & International Studies http://issuu.com/csis/docs/141110_cohen_globalforecast2015_web?e=2586794/10140596

Cyberbezpieczeństwo w praktyce

Rozmowa z Anną Katarzyną Nietykszą, prezesem grupy Eficom-Sinersio oraz Dominiką Stępińską-Duch i Januszem Tomczakiem z praktyki karnej kancelarii Wardyński i Wspólnicy

Jak istotny jest problem cyberbezpieczeństwa w Państwa działalności?

Anna Katarzyna Nietyksza: Grupa Eficom zakupiła ostatnio spółkę – właściciela dwóch data centers, dostarczających chmurę obliczeniową. Oznacza to konieczność zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Jesteśmy do tego autoryzowanym doradcą i wiemy, jak ważne jest bezpieczeństwo informacji poufnych. Dostarczamy cyberbezpieczne rozwiązania technologiczne w ramach budowanej bezpiecznej platformy Cloud Computing oraz Wirtualnego Data Center. Dodatkowo jako partner firm technologicznych sprzedajemy rozwiązania cyberbezpieczeństwa dla banków i innych firm. Jako Eficom z kolei doradzamy, jak pozyskać fundusze UE na cyberbezpieczeństwo, prowadzimy szkolenia w zakresie bezpiecznego wykorzystania internetu i przechowywania danych. Z opinii grupy roboczej ds. ataków cybernetycznych w UE, której jestem członkiem, wynika, że przedsiębiorcy powinni być prawnie zobowiązani nie tylko do stosowania bezpiecznych i odpornych technologii informacyjnych i komunikacyjnych, ale także do szkolenia personelu w zakresie polityki cyberbezpieczeństwa.

Dominika Stępińska-Duch: Również dla prawników cyberbezpieczeństwo zyskuje na znaczeniu. Coraz więcej spraw karnych zawiera w sobie elementy związane z cyberprzestępczością. Nasi klienci coraz częściej padają ofiarą kradzieży danych czy to wskutek działalności podmiotów zewnętrznych, czy to przez nieostrożność swoich pracowników bądź współpracowników. W obecnym świecie informacja staje się kluczową wartością, tymczasem informacje te są często przechowywane w systemach komputerowych bez należytych zabezpieczeń. Dlatego należy podnosić poziom świadomości klientów w tym obszarze.

Janusz Tomczak: Prawnik świadczący pomoc prawną przed sądem czy w prokuraturze funkcjonuje dziś w realiach gospodarki cyfrowej. Elektroniczny charakter różnych zdarzeń zmienia m.in. całą kwestię gromadzenia dowodów. Dziś, gdy komunikacja w dużej mierze odbywa się mailowo, właściwie w każdej sprawie mamy do czynienia z kwestią wydobywania

ewentualnych dowodów z systemów elektronicznych naszych klientów. Prawidłowe zabezpieczenie tego rodzaju dowodów wymaga zarówno określonej wiedzy, jak i specjalistycznego sprzętu, co niemal zawsze oznacza konieczność zatrudnienia firmy zewnętrznej. Bez znajomości zagadnień związanych z cyberbezpieczeństwem prawnik nie byłby dziś w stanie pomagać swoim klientom.

Na ile istotne są kwestie cyberbezpieczeństwa w dzisiejszej gospodarce?

AKN: Zagrożenie wzrasta wraz ze wzrostem naszej zależności od internetu i technologii cyfrowych. Według ostatniego sprawozdania opracowanego przez firmę Symantec całkowita liczba naruszeń ochrony danych na świecie wzrosła w 2013 r. o 62%, co oznacza ujawnienie ponad 552 mln zapisów obejmujących imię i nazwisko, datę urodzenia, numer dowodu tożsamości, dokumentację medyczną czy informacje finansowe. Każdego roku na całym świecie ofiary cyberataków tracą około 290 mld EUR, co czyni tę przestępczość bardziej dochodową od światowego handlu marihuaną, kokainą i heroiną łącznie. W maju 2014 r. baza danych zawierająca dane osobowe 145 mln posiadaczy kont w witrynie eBay została skradziona podczas pojedynczego ataku. Zgodnie z badaniem przeprowadzonym w 2013 r. przez Uniwersytet Kent na temat bezpieczeństwa cybernetycznego w ciągu zaledwie jednego roku (2012–2013) włamano się na konta internetowe ponad 9 milionów dorosłych mieszkańców Wielkiej Brytanii, a 8% mieszkańców Zjednoczonego Królestwa wskutek cyberprzestępczości straciło pieniądze, przy czym w wypadku 2,3% straty przekraczały 10 tys. GBP. To dane dotyczące Wysp Brytyjskich, ale dotyczą nas wszystkich. Internet nie zna granic.

Jakie obszary działalności gospodarczej są szczególnie zagrożone?

JT: Naruszenia i nieprawidłowości związane z ochroną danych w systemie komputerowym można zauważyć wszędzie tam, gdzie istnieją przepływy finansowe, gdzie mamy do czynienia z wartościami materialnymi.

AKN: Celem ataków cybernetycznych są sieci rządowe, transportowe i telekomunikacyjne oraz podmioty świadczące usługi, od których zależy nasze zdrowie i bezpieczeństwo. Każdego roku w Europie ataki cybernetyczne powodują ogromne straty gospodarcze. Szacunki dotyczące kosztów muszą uwzględniać utratę własności intelektualnej i danych szczególnie chronionych, koszty utraconych korzyści, w tym koszty zakłóceń w zatrudnieniu i świadczeniu usług, szkody dla wizerunku marki i reputacji przedsiębiorstwa, kary i płatności wyrównawcze dla klientów (za niedogodności lub pośrednie straty) bądź odszkodowania umowne (np. za opóźnienia), koszty środków zaradczych i ubezpieczenia, koszty strategii łagodzących i usuwania szkód wynikających z ataków cybernetycznych, straty handlowe i utratę konkurencyjności, zakłócenia obrotu handlowego oraz utratę miejsc pracy.

Zgodnie z opublikowanym przez rząd brytyjski badaniem na temat przypadków naruszenia bezpieczeństwa informacyjnego z 2014 r. w 2013 r. tego rodzaju naruszeń doświadczyło 81% dużych przedsiębiorstw oraz 60% MŚP. W tym samym sprawozdaniu rządowym oszacowano, że przeciętny koszt najpoważniejszego naruszenia bezpieczeństwa cybernetycznego może sięgać nawet 1,4 mln EUR w wypadku wielkich organizacji i 140 tys. EUR w wypadku MŚP.

Mówimy o zagrożeniach zewnętrznych. A jak istotne są zagrożenia płynące z wewnętrznych struktur organizacji?

JT: Co najmniej równie istotne.

DSD: Każdy człowiek, każdy uczestnik obrotu gospodarczego powinien mieć świadomość, że wszelkie informacje, które zamieścił w jakimkolwiek systemie elektronicznym, na zawsze w tym systemie pozostają.

JT: Trzeba też pamiętać, że szereg naruszeń może mieć charakter nieświadomy i nieintencjonalny. Pracownicy, którzy przegrywają dane na nośniki mobilne, wchodzą na niezabezpieczone strony internetowe albo nieostrożnie posługują się swoimi środkami komunikacji elektronicznej, mogą nieświadomie, nieumyślnie narażać swojego pracodawcę na bardzo poważne konsekwencje.

DSD: Każde skorzystanie przez pracownika z prywatnego telefonu czy też prywatnego adresu mailowego, który nie posiada takich zabezpieczeń, jakie powinny mieć systemy internetowe przedsiębiorstwa, już jest narażeniem spółki na niebezpieczeństwo.

AKN: Trzeba też pamiętać, że każda zmiana systemu informatycznego bez back-upu grozi wywróceniem się przedsiębiorstwa, tak jak się to stało z PKP. Dlatego też należy dbać o właściwe przechowywanie wszystkich danych.

Jakiego rodzaju skutki niosą za sobą incydenty komputerowe?

AKN: Cyberprzestępcy polują głównie na nasze pieniądze, ale również na reputację i markę firm, dane klientów. Szczególnie narażone są firmy giełdowe, gdyż udostępniają mnóstwo danych, a ich wartość zależy w ogromnym stopniu od wizerunku. Motywy ataków cybernetycznych mogą być różne, od bardzo osobistych, takich jak odwet na osobie lub przedsiębiorstwie, po szpiegostwo gospodarcze i państwowe oraz wojnę cybernetyczną między krajami.

JT: Trzeba pamiętać, że cyberprzestępstwa to także przestępstwa bardzo pospolite, takie jak kradzież środków, popełniane przy wykorzystaniu sieci komputerowych.

Niektóre takie zdarzenia mogą nawet nie mieć poważnych skutków materialnych, ale za to mogą nieść ze sobą bardzo poważne skutki reputacyjne. Nagłośnienie dziury w systemie może całkowicie pogrzebać wiarygodność instytucji finansowej, która jest faktycznie podmiotem zaufania publicznego.

DSD: W swojej praktyce mieliśmy do czynienia z sytuacją, w której środki przepływające przez taką instytucję trafiały z automatu na rachunki innych podmiotów. System nie był wystarczająco szczelny i dane na którymś etapie były podmieniane.

JT: Zdarzają się też incydenty, np. różnego rodzaju ataki hakerskie, które są wprawdzie dolegliwe, ale nie niosą ze sobą innych skutków czy konsekwencji. Nie ma w nich chęci wyrządzenia szkody, tylko chęć wypunktowania luki w systemie.

Trzeba jednak powiedzieć, że w cyberprzestrzeni dzieje się coraz ciekawiej w negatywnym znaczeniu tego słowa. Ostatnio jedna z gazet donosiła, że dochodzi do nielegalnego obrotu bronią w sieci przy wykorzystaniu wirtualnych nielegalnych walut. Mogłoby się to wydawać egzotyczną ciekawostką, ale podano, że wartość tej nielegalnej waluty to 8 mln USD. Jest to więc konkretna kwota.

Czy można dziś mówić o bezpieczeństwie obrotu prawnego/gospodarczego bez zapewnienia bezpieczeństwa w cyberprzestrzeni?

AKN: Nasza gospodarka w coraz większym stopniu staje się gospodarką cyfrową, uzależnioną od internetu. Wdrożenie bezpiecznych rozwiązań technologicznych do przesyłu i przechowywania danych jest w mojej opinii kluczowe do zapewnienia nie tylko bezpiecznego obrotu, ale również ciągłego wzrostu gospodarczego.

JT: Zauważmy, że w systemie informatycznym są i księgi wieczyste, i Krajowy Rejestr Sądowy, a na nich właśnie opiera się bezpieczeństwo obrotu. Dziś notariusz nie musi już iść do sądu wieczystoksięgowego. Wystarczy, że spojrzy w komputer i na tej podstawie informuje stronę aktu notarialnego, że księga wieczysta jest czysta, choć tak naprawdę nie ma żadnych narzędzi, by zweryfikować, że dane zawarte w systemie są w chwili weryfikacji zgodne z rzeczywistością. Każde potencjalne zagrożenie dla takiego systemu stanowi więc ogromne zagrożenie dla bezpieczeństwa obrotu gospodarczego i prawnego.

Czy organy ścigania i regulatorzy przykładają wystarczającą wagę do zagadnień związanych z cyberbezpieczeństwem?

AKN: Nadal brakuje wyspecjalizowanych ekspertów i biegłych potrafiących oceniać skutki ataków cybernetycznych, paraliżu systemów, szkód finansowych i utraty marki.

DSD: Jednak w Polsce nie jest tak źle, jak można by się spodziewać. Pracownicy organów ścigania są coraz lepiej wykształceni w obszarze nie tylko prawnym, ale również informatycznym. Spraw jest coraz więcej, więc zdobywają doświadczenie. Często jednak nie mają narzędzi pozwalających na szybką i sprawną reakcję, a niestety w sieci wszystko dzieje się szybciej niż w świecie realnym.

JT: W sferze publicznej jest trochę lepiej, bo problem jest rozpoznany i podejmuje się próby zabezpieczenia funkcjonowania instytucji publicznych, czym się zajmują stosowne agencje. Duży nacisk kładzie się na prewencję. Natomiast w sferze prywatnej mamy raczej do czynienia z reakcją na poszczególne incydenty niż z prewencją. Na dodatek w sferze tejże reakcji mamy do czynienia z nierównościami. Wprawdzie w policji istnieją wydziały do walki z przestępczością komputerową, ale ich działalność jest w głównej mierze skoncentrowana na przestępczości niezwiązanej z obrotem gospodarczym. Do tego dochodzi kwestia dostępności środków, którymi dysponuje policja w swojej codziennej działalności, i możliwości szybkiego reagowania.

DSD: Jest coraz lepiej. W policji jest coraz więcej ludzi, którzy wiedzą, o co chodzi, którzy specjalizują się w tym obszarze i mają instrumenty prawne, które nie wiążą im rąk. Nie zawsze jednak mają środki do tego, aby swoją wiedzę zastosować w praktyce. Bo jeżeli dochodzenie toczy się na koszt Skarbu Państwa, to nie ma wystarczających środków na to, żeby szybko, sprawnie i profesjonalnie zabezpieczyć dowody.

A jakie są największe wyzwania na przyszłość?

AKN: W dobie dynamicznie rosnącej gospodarki cyfrowej niezbędne są nowe narzędzia i rozwiązania, które zapewnią bezpieczeństwo danych, przesyłu, sieci i urządzeń mobilnych oraz przedsiębiorstw i konsumentów. Konieczne są także szkolenia i kampania edukacyjna, które mogą być

sfinansowane dzięki funduszom strukturalnym.

JT: Ważne jest też to, żeby korzystając z udogodnień cyfrowego świata pamiętać o potencjalnych słabych punktach. Cyfryzacja ksiąg wieczystych to bardzo wygodne rozwiązanie, ale obecna technologia pozwala wprowadzić w błąd notariusza, który bada stan nieruchomości w momencie podpisywania aktu notarialnego. Skuteczny atak na system elektroniczny pozwoliłby wyświetlić na komputerze notariusza dowolne treści, obracając w gruzy cały obrót nieruchomościami. Cały czas pojawiają się więc nowe zagrożenia dla obrotu, stąd konieczność jego ochrony i stosowania zabezpieczeń w ogóle.

Europejskie podejście do cyberbezpieczeństwa

Krzysztof Wojdyło

Wszystko wskazuje na to, że w najbliższych latach czekają nas bardzo istotne zmiany w zakresie regulacji związanych z cyberbezpieczeństwem. W polskim prawie pojawi się kilka nowych rozwiązań, mających swe źródło przede wszystkim w prawie europejskim. Kierunek zmian jest bardzo wyraźny – podmioty z sektora prywatnego mają stać się współodpowiedzialne za bezpieczeństwo cyberprzestrzeni.

Proponowane rozwiązania, przynajmniej w warstwie podstawowych założeń, bardzo przypominają zmiany, które towarzyszyły wprowadzaniu w życie przepisów dotyczących przeciwdziałania praniu pieniędzy. Wtedy również zaangażowano podmioty sektora prywatnego. Uznano bowiem, że skala zjawiska jest tak wielka, że jedynie zaangażowanie sektora prywatnego pozwoli na skuteczną walkę z tym przestępstwem. W przypadku cyberprzestępczości jest podobnie. Skala wyzwań przekracza możliwości organów ścigania najpotężniejszych nawet państw świata.

Wystarczy sobie wyobrazić skuteczny atak na system telefonii komórkowej, paraliżujący na kilka dni działanie sieci. Odciąłby on nas od bardzo wielu funkcjonalności, bez których trudno już nam sobie wyobrazić codzienne życie. Nie moglibyśmy korzystać z bankowości elektronicznej, używać programów geolokalizacyjnych, a nawet zadzwonić na numer alarmowy 112. Nie zdajemy sobie też na ogół sprawy, jak wiele urządzeń jest obecnie automatycznie sterowanych z urządzeń mobilnych. Wiele z nich służy do sterowania systemami transportu, energetyki czy płatności.

Konieczność zaangażowania sektora prywatnego w walkę z cyberprzestępczością wynika też z tego, że państwo, tracąc kilkanaście lat temu monopol na budowę sieci telekomunikacyjnych i świadczenie

usług, oddało też prawie całkowicie sektorowi prywatnemu inicjatywę w zakresie rozwoju nowych technologii. Kompetencje w sprawach technologii bezpieczeństwa są w tej chwili również w sektorze prywatnym.

Odpowiednie dokumenty europejskie podkreślają, że dziś niezakłócony dostęp do sieci teleinformatycznych jest tak samo niezbędny jak dostęp do wody czy energii. W obliczu krytycznego znaczenia sieci oraz rosnącej liczby cyberataków stało się oczywiste, że niezbędne są skoordynowane działania zmierzające do zapewnienia europejskiej cyberprzestrzeni należytego poziomu cyberbezpieczeństwa.

Strategia

Skuteczna ochrona krytycznej europejskiej infrastruktury teleinformatycznej przed cyberprzestępczością jest jednym z filarów Europejskiej Agendy Cyfrowej[7] – podstawowego dokumentu określającego strategiczne cele Unii Europejskiej w obszarze gospodarki cyfrowej. Strategia przewiduje szereg działań legislacyjnych, które mają przyczynić się do stworzenia ogólnoeuropejskiej infrastruktury cyberbezpieczeństwa. Wspomniane działania są wielowymiarowe. Część z nich zmierza do stworzenia nowych ogólnoeuropejskich organów odpowiedzialnych za wzmocnienie współpracy i wymianę informacji, służących zapewnieniu odpowiedniego poziomu cyberbezpieczeństwa, w tym skuteczniejszemu reagowaniu na incydenty. Inne z kolei mają nałożyć na podmioty z sektora publicznego oraz prywatnego nowe obowiązki związane z cyberbezpieczeństwem. Tym samym Europejska Agenda Cyfrowa proponuje poprawę systemu ochrony cyberprzestrzeni poprzez zaangażowanie do tego działania bardzo szerokiego grona podmiotów, w tym z sektora prywatnego.

Europejski system cyberbezpieczeństwa ma się opierać na stworzeniu nowych mechanizmów wymiany informacji i współpracy między odpowiednio umocowanymi instytucjami państwowymi i organizacjami sektorowymi oraz na określeniu dla instytucji europejskich zajmujących się różnymi aspektami bezpieczeństwa mandatu umożliwiającego skuteczne gromadzenie informacji i wypracowanie mechanizmów wspólnego reagowania na nowe rodzaje zagrożeń z cyberprzestrzeni.

Przegląd ostatnich inicjatyw europejskich w tym zakresie prowadzi do wniosku, że kluczowe są w tej chwili następujące zagadnienia:

- stworzenie efektywnych mechanizmów wymiany informacji z zakresu cyberbezpieczeństwa pomiędzy państwami członkowskimi oraz uruchomienie mechanizmów reagowania;
- koordynacja ustawodawstw karnych w odniesieniu do cyberprzestępczości;
- zapewnienie odpowiedniego poziomu cyberbezpieczeństwa u dostawców podstawowych usług cyfrowych oraz operatorów infrastruktury krytycznej.

Instytucje

ENISA

Już w 2004 r. na podstawie rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. powołano do życia Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA). Zakres działania ENISA został rozszerzony na

[7] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r.

ENISA to agencja unijna mająca swoją siedzibę główną w Heraklionie na Krecie. Została ona pierwotnie powołana przede wszystkim do prowadzenia prac analitycznych oraz badawczych, które będą podstawą do konstruowania polityk cyberbezpieczeństwa w ramach Unii Europejskiej oraz pozwolą wypracować dobre praktyki, wymagania, a jeżeli to możliwe również standardy w zakresie bezpieczeństwa informacji. ENISA jest również zobowiązana do wspierania zarówno instytucji unijnych, jak i organów poszczególnych państw w konstruowaniu skutecznych rozwiązań zapewniających cyberbezpieczeństwo. Jednym z ważniejszych przejawów aktywności ENISA w ostatnich latach było przeprowadzenie kilku międzynarodowych ćwiczeń ochrony cyberprzestrzeni i wypracowanie dzięki temu metodologii dla takich przedsięwzięć.

Zgodnie ze znowelizowaną dyrektywą 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (tzw. dyrektywa ramowa pakietu regulacyjnego dla sieci i usług łączności elektronicznej) ENISA jest również organem, do którego powinny trafiać informacje o incydentach naruszenia bezpieczeństwa oraz integralności sieci telekomunikacyjnych. Informacje o incydentach przesyłają odpowiednie organy państw, które z kolei pozyskują te informacje od dostawców sieci oraz usług telekomunikacyjnych. W Polsce takim organem jest Prezes Urzędu Komunikacji Elektronicznej.

CERT

Jednym z kluczowych zadań europejskiej polityki cyberbezpieczeństwa jest powołanie w poszczególnych państwach członkowskich zespołów szybkiego reagowania na zagrożenia w cyberprzestrzeni – Computer Emergency Response Team. W Polsce działa Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL (zajmujący się ochroną sieci rządowych), CERT zorganizowany wiele lat temu w NASK oraz kilka CERT-ów w sektorze prywatnym, np. w Orange. Projekt dyrektywy o bezpieczeństwie sieci oraz informacji (więcej o projekcie w dalszej części tekstu) zakłada obligatoryjne powołanie przez wszystkie państwa członkowskie CERT-ów zajmujących się wskazanymi w dyrektywie sektorami gospodarki. Podstawowym celem CERT-ów jest gromadzenie informacji o zagrożeniach, wczesne reagowanie na incydenty w cyberprzestrzeni oraz opracowywanie rozwiązań mających na celu zapobieganie atakom w przyszłości.

Europejskie Centrum Cyberprzestępczości (EC3)

Europejska Agenda Cyfrowa zobowiązywała organy Unii Europejskiej do powołania ogólnoeuropejskiej platformy do walki z cyberprzestępczością. 11 stycznia 2013 r. przy EUROPOL-u zaczęło działać Europejskie Centrum Cyberprzestępczości (EC3). Podstawową rolą EC3 jest zapewnienie współpracy i wymiany informacji pomiędzy organami policyjnymi państw członkowskich. EC3 wspomaga organizacyjnie działania przeciw przestępczości zorganizowanej i identyfikuje nowe rodzaje przestępstw w cyberprzestrzeni. Centrum świadczy również usługi laboratoryjne związane z cyberprzestępczością.

Nowe przestępstwa

Walka z cyberprzestępczością wymaga również zagwarantowania, aby, przynajmniej na poziomie ustawodawstw państw członkowskich, ujednolicone zostały przepisy karne odnoszące się do cyberprzestępstw. Taki cel przyświeca dyrektywie Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW. Dyrektywa musi zostać implementowana do 4 września 2015 r.

Ważnym elementem dyrektywy jest również wprowadzenie odpowiedzialności osób prawnych, w których imieniu działali sprawcy cyberprzestępstw. Warto podkreślić, że znaczna część rozwiązań postulowanych przez dyrektywę jest już w tej chwili zawarta w polskich przepisach prawa karnego.

Obowiązki

Dostawcy usług telekomunikacyjnych

Do podejmowania określonych działań związanych z cyberbezpieczeństwem zobowiązani zostali w pierwszej kolejności dostawcy publicznie dostępnych usług telekomunikacyjnych oraz operatorzy publicznych sieci telekomunikacyjnych. Trzeba pamiętać, że w wielu państwach członkowskich przedsiębiorcy telekomunikacyjni mają obowiązek podejmować określone działania w sytuacjach szczególnych zagrożeń, a także współpracować z instytucjami właściwymi w sprawach bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. W wyniku nowelizacji dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) doprecyzowano obowiązki w zakresie stosowania rozwiązań technicznych i organizacyjnych, które zapewnią bezpieczeństwo i integralność sieci telekomunikacyjnych. Wprowadzono też zupełnie nowe obowiązki informacyjne. Operatorzy i dostawcy usług muszą informować Prezesa Urzędu Komunikacji Elektronicznej o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług. Ma to być podstawą do zbudowania ogólnoeuropejskiego systemu wymiany informacji o naruszeniach bezpieczeństwa. Trzeba zaznaczyć, że obowiązki informacyjne obejmują nie tylko incydenty związane z domniemanymi cyberprzestępstwami, ale wszelkie istotne przerwy i awarie systemów komunikacyjnych. Obowiązki wynikające z przywołanej dyrektywy zostały implementowane w Dziale VIIa ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Nadchodząca zmiana

Bardzo istotne znaczenie dla europejskiego systemu cyberbezpieczeństwa będzie miała dyrektywa o bezpieczeństwie sieci i informacji (Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union[8]).

Projekt dyrektywy w wersji zaproponowanej przez Komisję zawierał kilka bardzo istotnych i rewolucyjnych rozwiązań. Przede wszystkim zaproponowano rozszerzenie obowiązków związanych z cyberbezpieczeństwem na szereg nowych podmiotów z sektora

[8] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

prywatnego. Można się było spodziewać, że obowiązki informacyjne wzorowane na powinnościach sektora telekomunikacji obejmą podmioty zarządzające różnymi rodzajami infrastruktury krytycznej, ale projektowane rozwiązania poszły dalej. Przyjęto bowiem założenie, że celem ewentualnych ataków z cyberprzestrzeni jest nie tylko infrastruktura, ale wszelkie systemy informacyjne, nie tylko w sektorach klasyfikowanych tradycyjnie jako krytyczne. Stąd zakres podmiotowy uregulowań w projekcie dyrektywy obejmował między innymi portale internetowe przetwarzające duże ilości wrażliwych danych o użytkownikach, media społecznościowe, dostawców usług cloud computingu, platformy z aplikacjami, dostawców rozwiązań płatniczych, firmy zajmujące się organizacją transportu, logistyką, dostawców usług energii elektrycznej, banki i firmy z sektora ochrony zdrowia (obowiązki tych podmiotów miałyby być analogiczne do tych, które już teraz spoczywają na dostawcach sieci oraz usług telekomunikacyjnych).

W zamyśle Komisji podmioty te powinny zostać zobowiązane, pod groźbą sankcji, do stosowania rozwiązań technicznych oraz organizacyjnych gwarantujących bezpieczeństwo sieci oraz kontrolowanych i używanych przez siebie systemów informatycznych. Dodatkowo miały zostać zobowiązane do zgłaszania odpowiednim organom w swoich macierzystych państwach incydentów mających znaczący wpływ na bezpieczeństwo ich systemów. Odpowiednie organy mają otrzymać uprawnienie do ujawnienia takich incydentów opinii publicznej, jeżeli uznają, że leży to w interesie publicznym. Organy nadzoru będą również uprawnione do żądania przeprowadzenia audytów bezpieczeństwa przez podmioty szczególnie narażone na cyberataki.

Niezależnie od opisanych powyżej obowiązków projekt dyrektywy przewiduje również rozwiązania zmierzające do skutecznego stworzenia przestrzeni dla skoordynowanej europejskiej polityki cyberbezpieczeństwa. Państwa członkowskie mają zostać zobligowane do stworzenia strategii w zakresie bezpieczeństwa sieci i informacji, powołania CERT-ów oraz organów odpowiedzialnych za bezpieczeństwo sieci oraz informacji. Organy te powinny stworzyć ogólnoeuropejską sieć wymiany informacji na temat cyberbezpieczeństwa i przesyłać sobie nawzajem m.in. ostrzeżenia o zagrożeniach.

Powyższe propozycje wzbudzają szereg kontrowersji, głównie jeżeli chodzi o zakres podmiotowy. Wielu krytyków zarzucało propozycji Komisji zbytnie rozszerzenie katalogu podmiotów zobowiązanych do realizacji dodatkowych obowiązków. W pierwszym czytaniu Parlament Europejski zaproponował szereg zmian do projektu dyrektywy. Wiele z nich skutkuje zmniejszeniem rygoryzmu pierwotnej wersji dyrektywy. Zmiany wprowadzone przez Parlament przewidują, że obowiązki wymiany informacji nie będą obejmować organów administracji publicznej, zostawiając kwestie zabezpieczeń systemów rządowych uznaniu państw członkowskich. Zaproponowano także zwolnienie z obowiązkowych zgłoszeń incydentów wielu kategorii podmiotów prywatnych, które w pierwotnej wersji dyrektywy były do tego zobowiązane (dotyczy to m.in. platform e-commerce, dostawców usług cloud computingu czy wyszukiwarek internetowych).

Na tym etapie trudno jeszcze przewidzieć, jaki kształt będzie miała ostatecznie dyrektywa o bezpieczeństwie sieci i informacji. Dotychczasowe prace nad tym aktem

prawnym pokazały niewątpliwie, że ścierają się ze sobą dwie wizje. Pierwsza, której wyraz dał Parlament Europejski, zakłada nałożenie dodatkowych obowiązków notyfikacyjnych na relatywnie niewielką grupę podmiotów z sektora prywatnego świadczących usługi o krytycznym znaczeniu dla współczesnych gospodarek (m.in. dostawców energii, banki, podmioty z sektora ochrony zdrowia). Parlament opowiedział się natomiast przeciwko nakładaniu nowych obowiązków na podmioty świadczące szeroko rozumiane usługi cyfrowe (m.in. dostawców cloud computingu, instytucje pośredniczące w płatnościach internetowych, wyszukiwarki internetowe). W tym zakresie stanowisko Parlamentu wydaje się sprzeczne z podejściem prezentowanym przez Komisję Europejską. Należy się spodziewać, że to właśnie zakres podmiotowy nowej regulacji będzie osią sporu dotyczącego kształtu przyszłej europejskiej polityki cyberbezpieczeństwa.

Parlament Europejski przedstawił swoje stanowisko w odniesieniu do dyrektywy w marcu 2014 r. Od tego czasu byliśmy świadkami kilku spektakularnych cyberataków na podmioty świadczące usługi cyfrowe (m.in. na dostawców cloud computingu). Czas pokaże, na ile te zdarzenia będą miały wpływ na ostateczny kształt dyrektywy.

Ściganie przestępstw popełnionych w cyberprzestrzeni

Aleksandra Stępniewska

Pojęcie cyberprzestrzeni, jako „miejsca między komputerami", pojawiło się w literaturze fantastycznej na początku lat 80. ubiegłego wieku. Cyberprzestrzeń od początku była także przedstawiana jako swoiste pole bitwy o informację i wpływy. W ten sposób m.in. obrazował cyberprzestrzeń William Gibson w kultowej cyberpunkowej powieści „Neuromancer" (1984). Jego wizja, choć w szczegółach pozostaje w sferze fikcji, w swoich fundamentach niewiele się różni od dzisiejszej rzeczywistości.

Powiązanie biznesowej i instytucjonalnej aktywności z cyberprzestrzenią, lub wręcz umiejscowienie w niej tych aktywności, w naturalny sposób uzależnia jednostki, przedsiębiorców i struktury państwowe od prawidłowego i niezakłóconego funkcjonowania sieci i systemów

komputerowych. Jednocześnie dane umieszczone w cyberprzestrzeni są narażone na ciągłe ataki. Cyberprzestrzeń może bowiem jawić się jako obszar niepodlegający właściwości organów ścigania jakiegokolwiek państwa, dając sprawcom przestępstw poczucie bezkarności. Przeświadczenie o niewielkiej skuteczności wymiaru sprawiedliwości w ściganiu i karaniu cyberprzestępców skutkuje także małym odsetkiem zgłoszeń o możliwości popełnienia przestępstwa właściwym organom.

Tymczasem cyberprzestrzeń i przestępstwa popełniane przy jej wykorzystaniu lub w jej obszarze bynajmniej nie są wyjęte spod jurysdykcji państw, czyli ich kompetencji do stosowania obowiązującego prawa celem jego egzekwowania. Cyberprzestępstwa są bowiem popełniane przez osoby realnie istniejące, a ich skutki realizują się w otaczającej nas rzeczywistości i mają materialny wymiar. Zgodnie zaś z ogólnie przyjętymi zasadami prawa karnego odpowiedzialności karnej podlega ten, kto popełnił czyn zabroniony pod groźbą kary na podstawie przepisów prawa obowiązujących w miejscu popełnienia konkretnego czynu (art. 1 polskiego Kodeksu karnego).

Utrudnieniem w ściganiu i karaniu cyberprzestępstw są jednak kłopoty z określeniem miejsca popełnienia cyberprzestępstwa. Od tego miejsca zależy zaś, jakie prawo będzie miało zastosowanie i gdzie to przestępstwo powinno być ścigane, czyli organy jakiego państwa organy będą władne, by wymierzyć sprawiedliwość. Tymczasem charakterystyczną cechą przestępstw popełnianych w sieci i przy użyciu systemów informatycznych jest ich transgraniczność i tzw. wielomiejscowość. Niejednokrotnie sprawca, znajdując się na terytorium państwa A, korzysta z sieci informatycznej zlokalizowanej w państwie B, by umieścić dane w formie strony internetowej na serwerze komputerowym istniejącym w państwie C, przy czym strona z zamieszczonymi na niej danymi jest dostępna właściwie na całym świecie. Wedle tego schematu popełniane są przestępstwa związane z rozpowszechnianiem nielegalnych treści, stalkingiem czy naruszaniem praw autorskich.

Podobny schemat dotyczy przestępstw, w których sieć komputerowa lub system komputerowy są środowiskiem lub celem zamachu, czyli tzw. przestępstw stricte komputerowych. Są to przestępstwa hackingu (art. 267 k.k.), naruszenia integralności informacji (art. 268 k.k.) lub naruszenia integralności systemu komputerowego na skutek wykorzystania złośliwego oprogramowania, tzw. ataki typu *denial of service* (DoS – art. 269 k.k.). W tych sytuacjach osoba znajdująca się fizycznie w państwie A, lecz działająca za pomocą systemu informatycznego zlokalizowanego w państwie B, wprowadza do systemu informatycznego znajdującego się na terytorium państwa C dane zakłócające funkcjonowanie tego systemu lub zmierzające do wykradzenia z niego danych. Terytorialny zasięg cyberprzestępstwa może też skutecznie poszerzyć wprowadzanie robaków lub wirusów mających na celu przekształcenie komputera w tzw. *zombie* i włączenie go tym samym do *botnetu*, czyli sieci zainfekowanych komputerów mających na celu zainfekowanie dalszych, docelowych systemów.

Podstawową zasadą rządzącą możliwością stosowania prawa karnego i ścigania przestępstw na konkretnym terytorium państwowym jest tzw. zasada terytorialności. Jej wyrazem na gruncie prawa polskiego jest art. 5 k.k., który stanowi, że polskie przepisy

karne stosuje się do sprawcy, który popełnił przestępstwo na terytorium Polski lub na pokładzie polskiego statku morskiego lub powietrznego. Za miejsce popełnienia czynu zabronionego polski Kodeks karny uważa miejsce, w którym sprawca działał lub zaniechał działania, do którego był obowiązany, a także miejsce, w którym wystąpił lub według zamiaru sprawcy miał wystąpić skutek stanowiący element konstytutywny przestępstwa (art. 6 k.k.). Tak sformułowane zasady kompetencji polskich organów ścigania i wymiaru sprawiedliwości upoważniają do ścigania i ukarania czynów zabronionych popełnionych w sieci lub przy jej wykorzystaniu wówczas, gdy sprawca fizycznie działał na terytorium Polski, nawet gdy skutek nastąpił poza jej granicami, a także wówczas, gdy sam skutek nastąpił na terytorium Polski, choć sprawca działał w innym państwie.

Przepisy te nie obejmują jednak sytuacji, gdy sprawca, działając poza granicami Polski, dopuszcza się tzw. przestępstwa formalnego, czyli takiego, które zostaje popełnione w związku z oznaczonym zachowaniem, ale niekoniecznie wywołuje określony naganny skutek. Dotyczy to m.in. przestępstw rozpowszechniania nielegalnych treści za pomocą internetu. Tak ujęte zasady nie uprawniają też do ścigania cyberprzestępstw wówczas, gdy tylko jeden z elementów schematu działania sprawcy znajduje się na terytorium Polski, tj. w sytuacji, gdy sprawca, działając w innym państwie, korzysta z sieci informatycznej zlokalizowanej na terytorium Polski, lecz skutek przedsięwzięcia w jego zamierzeniu ma nastąpić w państwie trzecim.

Remedium na tego rodzaju sytuacje stanowi w niektórych systemach prawnych, np. we Francji lub Belgii, tzw. teoria związku, która upoważnia organy ścigania do działania nawet wówczas, gdy tylko jeden z elementów faktycznych całego łańcucha przestępczego ma miejsce na terytorium tego państwa. Rozwiązanie to jednak nie znajduje zastosowania w polskim systemie.

Aby wypełnić tę lukę, stosuje się więc inne zasady ustalania właściwości polskich organów wymiaru sprawiedliwości. Należą do nich m.in. zasada personalna, która uprawnia do ścigania sprawcy przestępstwa popełnionego w całości poza granicami Polski przez obywatela polskiego, lub tzw. zasada ochronna względna uprawniająca do ścigania cudzoziemca, który za granicą popełnił przestępstwo kierowane przeciwko istotnym interesom Rzeczypospolitej Polskiej lub jej obywatelom, w tym osobom prawnym.

Warunkiem ścigania w tych przypadkach jest jednak to, aby popełnione przestępstwa stanowiły także przestępstwa zgodnie z prawem państwa, gdzie zostały popełnione. Nadto w oznaczonych w ustawie przypadkach ściganie przez polskie organy wymiaru sprawiedliwości na podstawie polskiej ustawy karnej jest możliwe nawet wówczas, gdy warunek podwójnej karalności nie jest spełniony. Dotyczy to m.in. przestępstw przeciwko bezpieczeństwu Rzeczypospolitej Polskiej, jej funkcjonariuszom lub istotnym interesom gospodarczym. Nietrudno sobie przy tym wyobrazić, że w każdym z tych scenariuszy cyberprzestrzeń może być wykorzystana jako *modus operandi* przestępstwa, a systemy informatyczne, np. z zakresu infrastruktury krytycznej państwa (energetyka, transport), mogą być celem działań przestępnych.

Jako że cyberprzestępczość ma silny wymiar transgraniczny, kwestia kompetencji państw do ścigania i karania przestępstw popełnianych w sieci pozostaje także w orbicie zainteresowania instytucji

ponadkrajowych. Zasady jurysdykcji krajowej zawiera zarówno Konwencja Rady Europy o cyberprzestępczości, jak i – na poziomie Unii Europejskiej – dyrektywa 2013/40 Parlamentu Europejskiego i Rady dotycząca ataków na systemy informatyczne. Zasadniczo reguły obowiązujące na gruncie polskiej ustawy są zbieżne z tymi wskazanymi w obu powołanych aktach. Dotyczy to terytorialności oraz zasady personalnej. Jednocześnie dyrektywa daje państwom możliwość uznania ich jurysdykcji także wówczas, gdy sprawca cyberprzestępstwa ma jedynie miejsce stałego pobytu na terytorium danego państwa lub gdy przestępstwo przyniosło korzyść osobie prawnej, mającej siedzibę na terytorium konkretnego państwa.

Wielomiejscowość cyberprzestępstw wymaga przyjęcia szeregu różnorodnych kryteriów, według których organy wymiaru sprawiedliwości mogą ustalać swoją kompetencję do ścigania cyberprzestepstwa. Należą do nich działanie sprawcy, skutek działania, obywatelstwo, interes państwa lub inny związek z konkretnym terytorium państwowym. Z jednej strony zatem wielomiejscowość cyberprzestępstw może ułatwiać ich ściganie i karanie, bowiem organy kilku państw mogą równolegle prowadzić postępowania, uznając swoją właściwość. Okoliczność ta jednak może rodzić istotne problemy natury prawnej, a także technicznej. Prowadzenie równoległych postępowań przygotowawczych lub sądowych w odniesieniu do tego samego czynu i osoby będzie bowiem skutkować naruszeniem podstawowej zasady *ne bis in idem*, zakazującej podwójnego lub wielokrotnego ścigania i skazania tej samej osoby za ten sam czyn. Ponadto prowadzenie postępowań w zakresie tego samego czynu przeciwko tej samej osobie przez różne ośrodki jest sprzeczne z zasadą ekonomiki postępowania, prowadząc do marnotrawienia środków finansowych, technicznych, osobowych oraz czasu.

W celu przeciwdziałania negatywnym skutkom podwójnych postępowań decyzja ramowa Rady 2009/948 w sprawie zapobiegania konfliktom jurysdykcyjnym w sprawach karnych i w sprawie rozstrzygania takich konfliktów zobowiązuje organy państw UE do współpracy. Ma ona polegać przede wszystkim na wymianie informacji w razie podejrzenia, że w dwóch lub kilku państwach członkowskich prowadzone są postępowania w odniesieniu do tego samego przestępstwa, a także na wypracowywaniu porozumień dotyczących przekazania ścigania i całego postępowania karnego organom jednego z państw. W motywach decyzji wskazane są przy tym kryteria, które mogą decydować o tym, gdzie ostatecznie postępowanie powinno się toczyć. Należą do nich m.in. miejsce, w którym większość przestępnego działania została zrealizowana lub w którym przestępne działanie wywołało większą szkodę, miejsce ujęcia sprawcy lub jego stałego pobytu, narodowość sprawcy lub lokalizacja jego istotnych interesów, istotne interesy pokrzywdzonych przestępstwem lub świadków, a także dopuszczalność dowodów.

Kryteria te pozwalają skoncentrować ściganie cyberprzestępstwa tam, gdzie może być to najbardziej optymalne. W tym kontekście jako istotne jawią się te, które biorą pod uwagę interesy pokrzywdzonego oraz kwestie dowodowe. Pierwsze dowody na popełnienie cyberprzestępstwa będą bowiem w głównej mierze pochodzić od pokrzywdzonego, tj. ich materialnym substratem będą kopie dysków lub zabezpieczone dane z systemu informatycznego, z którego pokrzywdzony korzystał. Biorąc jednak pod uwagę wielomiejscowość cyberprzestępstw,

postępowanie dowodowe niejednokrotnie będzie także wymagało współpracy z organami wymiaru sprawiedliwości innych państw w ramach tzw. pomocy prawnej.

Cyberprzestrzeń, choć z pozoru nieuchwytna, nie jest więc obszarem wyjętym spod prawa. Wachlarz zasad powalających na stosowanie krajowych przepisów prawa nie pozostawia wątpliwości, że cyberprzestępstwa mogą być skutecznie ścigane i karane, nawet jeśli praktyka tych działań wciąż pozostawia sporo do życzenia.

Ochrona tajemnicy przedsiębiorstwa w świecie cyfrowym

Janusz Tomczak

Odpowiedź na pytanie, czym jest tajemnica przedsiębiorstwa, jest dość intuicyjna. Czytelnik zapewne wie albo się domyśla, że chodzi o takie informacje, które mają kluczowe znaczenie dla działalności danego przedsiębiorstwa oraz w istocie odróżniają je od innych przedsiębiorstw na rynku i decydują o jego wartości.

Ustawa o zwalczaniu nieuczciwej konkurencji z 1993 r. definiuje tajemnicę przedsiębiorstwa jako „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności”[9].

Stworzenie katalogu wszelkich możliwych zagadnień/informacji, które mogą stanowić tajemnicę przedsiębiorstwa, byłoby niemożliwe. To głównie przedsiębiorca decyduje o tym, jakie informacje chce w sposób szczególny chronić i które nie powinny być upubliczniane. Czasem też bywa inaczej, jak w przypadku informacji wpływających na kurs akcji spółek notowanych na giełdzie, kiedy to ustawodawca nakazuje przedsiębiorcy – emitentowi określony sposób postępowania z tym, co ustawa o obrocie instrumentami finansowymi nazywa informacją poufną[10].

Prawna ochrona informacji

System prawny chroni informacje w różnoraki sposób – zarówno za pomocą norm o charakterze administracyjnym (np. ustawa o ochronie informacji niejawnych, regulacje dotyczące tajemnic zawodowych, tajemnica telekomunikacyjna), jak i za pomocą przepisów stricte karnych (Rozdział XXXIII Kodeksu karnego, Przestępstwa przeciwko

[9] Art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji z 16 kwietnia 1993 r.

[10] Art. 154 ustawy o obrocie instrumentami finansowymi z 29 lipca 2009 r.

ochronie informacji). Niektóre z nich mogą posłużyć do działań służących ochronie prawnej przedsiębiorcy, którego tajemnica została naruszona (przepisy Kodeksu karnego). Kompleksowa (z pozoru) regulacja poświęcona ochronie tejże tajemnicy została jednak zawarta we wspomnianej ustawie z 1993 r. Jej poświęcony jest niniejszy tekst.

W świetle jej przepisów tym, co czyni informację tajemnicą, są dwa elementy: (i) nieujawnienie do wiadomości publicznej, (ii) działania, jakie przedsiębiorca podejmuje w celu zachowania informacji w poufności.

Jest oczywiste, że przepis chroni przedsiębiorcę „aktywnego", a więc takiego, który definiuje informacje, które są dla niego ważne i cenne, które nie mogą być rozpowszechnione i które należy chronić. Stara rzymska zasada prawna „Chcącemu nie dzieje się krzywda" rozumiana dosłownie zdaje się niewystarczająca. System prawny udziela ochrony temu, kto nie tylko podejmuje działania w celu zachowania poufności, ale też podejmuje w tym celu działania niezbędne.

Sposób zapewnienia poufności

W literaturze przedmiotu podkreśla się, że zapewnienie poufności winno dokonywać się poprzez instrumenty prawne oraz ochronę fizyczną czy też techniczną. Praktyka bez wątpienia również idzie w tym kierunku.

Każde z podejmowanych działań musi uwzględniać specyfikę prowadzonej działalności, a w konsekwencji potencjalne zagrożenia dla informacji będących przedmiotem ochrony. Zagrożenia mogą płynąć nie tylko od osób czy podmiotów zewnętrznych wobec organizacji. Ich źródłem może być też niestety sama organizacja, a konkretnie osoby w niej ulokowane. Pamiętać przy tym należy, że nie każdy wyciek informacji będzie konsekwencją zaplanowanych, bezprawnych w swym założeniu działań. Bez trudu można znaleźć w praktyce przykłady wycieków danych, których przyczyną była zwykła nieostrożność lub głupota. Parę lat temu w wielu firmach praktycznie każdy zainteresowany pracownik mógł skopiować i wynieść listę klientów, wraz z danymi o obrotach i preferowanym asortymencie. Zidentyfikowanie osoby, która to zrobiła, było praktycznie niemożliwe. Dziś to się zmienia.

Nowoczesne przedsiębiorstwo wykorzystuje szereg instrumentów prawnych, by swoich pracowników, współpracowników i kontrahentów zmusić do przestrzegania zasad ochrony informacji. Wykorzystuje przy tym zakazy konkurencji, umowy o pracę, umowy o zachowaniu w poufności, regulaminy wewnętrzne itp. Bardzo istotne są obowiązkowe szkolenia, ułatwiające budowanie świadomości zasad zachowania bezpieczeństwa i ich korzyści dla osiągania wspólnych celów przedsiębiorstwa. Przedsiębiorcy wprowadzają też zasady organizacyjne sprzyjające zachowaniu bezpieczeństwa oraz wewnętrzne systemy nadzoru i kontroli.

Wykładnia wspomnianego przepisu prowadzi jednak do wniosku, że bardzo pomocne we wdrażaniu polityki bezpieczeństwa może być zastosowanie różnego rodzaju środków technicznych. Mogą one na przykład chronić przed fizycznym dostępem osób niepowołanych do informacji stanowiących tajemnicę, uwierzytelniać osoby uprawnione do dostępu do informacji, uwierzytelniać samą informację, jej autentyczność i integralność. Jest oczywiste, że określona grupa osób musi mieć dostęp do ważnych informacji. Przyjmuje się, że „ze stanem poufności będziemy mieli do czynienia tylko

wtedy, gdy przedsiębiorca kontroluje liczbę i charakter osób mających dostęp do określonych informacji"[11].

Wyzwania związane z cyfryzacją

Świat, w którym spisane na papierze cenne formuły lekarstw lub strategiczne plany spoczywały na dnie najlepiej zabezpieczonych sejfów, odszedł albo odchodzi dość szybko do historii. Zapewne większość informacji stanowiących tajemnicę przedsiębiorstw zapisana jest już w formie elektronicznej. Możliwość przekazywania tych informacji w formie cyfrowej to z jednej strony szansa i motor rozwoju gospodarczego, z drugiej zaś niebezpieczeństwo, które należy za każdym razem oceniać i któremu należy przeciwdziałać.

„Niezbędne działania w celu zachowania poufności informacji" w świecie cyfrowym to stosowanie elektronicznych zabezpieczeń na wielu płaszczyznach dostępu do informacji.

Trzeba wyraźnie podkreślić, że w świetle komentowanej ustawy istnienie zabezpieczeń adekwatnych do zagrożeń to obowiązek, gdyż informacje stanowiące tajemnicę przedsiębiorstwa są elementem majątku przedsiębiorstwa. Piecza nad majątkiem stanowi obowiązek kierownictwa przedsiębiorstwa. Niezabezpieczenie cennej informacji pozbawia ją przymiotu tajemnicy, a więc także ochrony prawnej.

Zabezpieczenie przed cyberprzestępczością

Głównym zagrożeniem dla informacji elektronicznych jest cyberprzestępczość. Każde przedsiębiorstwo obecnie winno dysponować systemem zabezpieczeń swoich danych przechowywanych cyfrowo.

Pod obco brzmiącym terminem „cyberprzestępczość" kryją się działania często nieróżniące się w swej naturze od pospolitych przestępstw. Kradzież, zniszczenie mienia, paserstwo znajdują obecnie swoje odpowiedniki w świecie cyfrowym. Tym, co odróżnia te pospolite w swej naturze zdarzenia, to szybkość zdarzeń, często anonimowość, a także konieczność dysponowania zaawansowaną techniką. Zmienia się instrumentarium; coraz bardziej inteligentne oprogramowanie, które służy wykradzeniu informacji, zniszczeniu systemu, nielegalnemu dostępowi czy też powielaniu utworów, pojawia coraz częściej i szybciej.

Mamy do czynienia z nowymi rodzajami zagrożeń w działalności przedsiębiorców. Pojawia się potrzeba ochrony informacji, które kiedyś nie sprawiały problemów, jak na przykład prywatność klientów przedsiębiorcy.

Równolegle systematycznie rośnie oferta produktów i usług informatycznych służących przeciwdziałaniu incydentom informatycznym.

Można w tym obszarze wyróżnić:

- działania służące kontroli użytkowników systemu informatycznego polegające na monitorowaniu ich aktywności, dostępu, możliwości instalowania lub uruchamiania nowego oprogramowania;
- działania służące zapewnieniu bezpieczeństwa danych polegające na zabezpieczeniu sieci przed atakami, porządkowaniu i ewidencjonowaniu posiadanych informacji oraz ich dodatkowym zabezpieczaniu, np. szyfrowaniu w razie potrzeby;
- działania służące zapewnieniu ciągłości funkcjonowania infrastruktury technicznej.

Trudności dowodowe

Konsekwencją cyfryzacji kluczowych dokumentów firmy jest rosnące znaczenie

[11] Arkadiusz Michalak, Komentarz do ustawy o zwalczaniu nieuczciwej konkurencji 2010, uwaga 11 do art. 11.

w strukturach przedsiębiorstw komórek odpowiedzialnych za bezpieczeństwo systemów informatycznych oraz bezpieczeństwo danych. Właściwa kontrola nad procesami informatycznymi w przedsiębiorstwie ma znaczenie również z punktu widzenia skuteczności kroków prawnych podejmowanych przeciwko sprawcom potencjalnych naruszeń. Trzeba móc udowodnić przed sądem fakt naruszenia, jego sposób i wskazać tropy prowadzące do sprawcy.

Na chwilę obecną niewątpliwie najszersze możliwości zabezpieczenia dowodów elektronicznych mają organy ścigania, w ramach przysługujących im uprawnień w postępowaniu karnym. Możliwość dochodzenia roszczeń z tytułu naruszenia tajemnicy przedsiębiorstwa na drodze cywilnej to wieloletnia batalia sądowa, która nie daje gwarancji sukcesu (głównie z uwagi na model postępowania dowodowego).

Okazuje się jednak, że zapotrzebowanie na dowody w sprawach cyberprzestępstw sprzyja też rozwojowi nowego rynku usług. Pojawiły się specjalistyczne przedsiębiorstwa zajmujące się odzyskiwaniem danych na nośnikach cyfrowych, a także zabezpieczaniem ich dla celów postępowań dowodowych.

Ustawa o zwalczaniu nieuczciwej konkurencji w analizowanym kontekście zawiera jeden przepis karny, który stanowi, że: „Kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej".

Orzecznictwo i praktyka są jednak ubogie w stosowaniu tego przepisu. Stosunkowo niewielkie sankcje i trudne do wykazania przesłanki skutecznie zniechęcają organy ścigania do jego stosowania. Konieczność wykazania związku pomiędzy poważną szkodą a wykorzystywaniem we własnej działalności cudzych tajemnic stanowi przeszkodę niemal nie do pokonania. Zdarzenia polegające na zaplanowanych cyberatakach nakierowanych na wykradzenie tajemnic przedsiębiorstwa, w założeniu z zamiarem późniejszego wykorzystania w działalności innego przedsiębiorcy, wpisywałyby się idealnie w cel tej regulacji.

Postawić należy pytanie, czy wykazanie szkody jest w tym momencie warunkiem koniecznym. Czy regulacja dotycząca włamania do systemu informatycznego z art. 267 Kodeksu karnego (przestępstwo ścigane na wniosek pokrzywdzonego) zawiera w sobie wystarczającą dozę represji i w sposób należyty chroni dobro prawne, którym jest tajemnica przedsiębiorstwa.

Moim zdaniem czyny polegające na cyberatakach nakierowanych na wykradzenie istotnych danych przedsiębiorcy w celu ich dalszego, nielegalnego wykorzystania nie znajdują adekwatnego remedium w środkach ochrony prawnej. Ustawodawca winien zadać sobie pytanie, czy stworzona 21 lat temu ustawa jest adekwatna do rzeczywistości, która zmienia się w cybertempie.

Przeszukania na odległość – jeszcze nie teraz

Magdalena Gutowska

Idzie nowe – 28 października 2014 r. Prezydent podpisał ustawę o ratyfikacji Konwencji Rady Europy o cyberprzestępczości oraz ustawę o ratyfikacji Protokołu dodatkowego do Konwencji dotyczącego penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych.

Konwencja jest pierwszym międzynarodowym aktem prawnym, który dotyka problemu przestępstw popełnianych w internecie lub przy jego wykorzystaniu. Została ona sporządzona w Budapeszcie 23 listopada 2001 roku. Jej sygnatariuszami jest obecnie 49 państw.

Chociaż Polska była jednym z pierwszych państw sygnatariuszy Konwencji, na jej ratyfikację trzeba było czekać 10 lat (licząc od wejścia w życie Konwencji w 2004 roku). Prace nad dostosowaniem polskiego prawa do wymagań stawianych przez Konwencję toczą się jednak już od dawna.

Nowe przestępstwa internetowe

Dzięki wdrażaniu Konwencji w Kodeksie karnym znalazły się takie przestępstwa jak niszczenie danych informatycznych, zakłócenie systemu komputerowego czy wytwarzanie programów komputerowych w celu popełniania innych przestępstw. Nie ma zatem już wątpliwości, że są to czyny przestępne podlegające karze.

Niestety, chociaż Polska miała stosunkowo dużo czasu na przygotowanie kompleksowych, spójnych i przemyślanych regulacji, nie udało się uniknąć błędów i niespójności.

Przykładem niedoskonałości regulacyjnej jest np. przestępstwo wytwarzania „narzędzi hakerskich", które może budzić bardzo poważne wątpliwości. Zgodnie z Kodeksem karnym przestępstwem jest bowiem „wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia" przestępstw takich jak np. bezprawne uzyskanie informacji czy zakłócanie systemu komputerowego.

Wydaje się, że autor regulacji nie wziął pod uwagę istnienia programów, które mogą mieć podwójne zastosowanie. Program wyszukujący luki w systemie zabezpieczeń może bowiem służyć zarówno usunięciu tych luk (jeśli jest używany przez uprawnionych administratorów systemu), jak też ich wykorzystaniu w celu uzyskania nieuprawnionego dostępu (gdy posługują się nim hakerzy). Ten przykład obnaża niefortunność sformułowania „przystosowane do popełnienia przestępstwa" – program przystosowany do popełnienia przestępstwa nie musi bowiem być w tym celu wykorzystywany. Tymczasem, posuwając rzecz

do absurdu, użyte sformułowanie mogłoby prowadzić do karalności udostępniania takich programów w celach naukowych bądź szkoleniowych.

Kłopot z ustaleniem miejsca popełnienia przestępstwa

Poważnym niedociągnięciem Konwencji, a także związanych z jej wdrożeniem regulacji krajowych, jest część dotycząca jurysdykcji, która zupełnie nie spełnia swojego zadania, tzn. nie dostosowuje przepisów do specyfiki przestępstw popełnianych w internecie lub przy jego użyciu. Przepisy jurysdykcyjne zawierają bowiem jedynie ogólne zasady odnoszące się do miejsca popełnienia przestępstwa. Nie rozjaśniają przy tym zupełnie problemów związanych z ustaleniem miejsca popełnienia przestępstwa internetowego. Wobec tego jurysdykcja państwowa, a następnie właściwość miejscowa prokuratury i sądów, będą wciąż uzależnione od sposobu pojmowania internetu jako miejsca popełnienia przestępstwa.

Miejscem popełnienia przestępstwa mogłoby być bowiem: a) miejsce, w którym sprawca znajdował się, uzyskując dostęp do sieci, b) miejsce zlokalizowania serwera, c) miejsce położenia komputera, dzięki któremu sprawca uzyskał dostęp do innych komputerów, przy których użyciu popełnił przestępstwo – warianty można mnożyć.

Nie ma jasnej odpowiedzi, jakie miejsce należy uznać za miejsce popełnienia przestępstwa wirtualnego, które dodatkowo bardzo często ma charakter transgraniczny. Dlatego też przestępcy mogą wyszukiwać jurysdykcje, w których system wykrywania przestępstw oraz ich sprawców jest mniej skuteczny. Jest to jedna z głównych słabości systemu represji karnej w wymiarze międzynarodowym.

Niedostatki regulacji dotyczących przeszukania

Konwencja reguluje także kwestie związane z przeszukaniem systemu informatycznego, danych w nim przechowywanych oraz nośnika służącego do przechowywania danych informatycznych. Nakazuje ona państwom, aby przyjęły środki prawne przewidujące odpowiednie uprawnienia dla organów realizujących takie przeszukania.

Obecnie obowiązujące przepisy krajowe na szczeblu ustawowym ograniczają się jednak wyłącznie do stwierdzenia, że do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego należy odpowiednio stosować przepisy o zatrzymaniu rzeczy i przeszukaniach. Ta formuła rodzi zarówno duże pole do nadużyć, jak też może uzasadniać bierność organów wobec braku odpowiednich uregulowań dostosowanych do specyfiki prowadzenia przeszukań sieci komputerowych.

Dokonując zmiany przepisów krajowych oraz dostosowując je do wymagań Konwencji, ustawodawca krajowy nie odniósł się do kwestii **realizacji przeszukań na odległość** – poprzez dostęp do sieci informatycznej. Instrument ten, którego stosowanie postulują biegli z zakresu informatyki śledczej, mógłby znacznie ułatwić i usprawnić gromadzenie dowodów. Budzi on jednak znaczne kontrowersje, bowiem stanowi poważną ingerencję w strefę prywatną obywateli.

Walka z czasem – zanim znikną dowody

Pozytywnie za to należy ocenić wprowadzenie do Kodeksu postępowania karnego

możliwości niezwłocznego zabezpieczenia danych informatycznych przez urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną na okres nieprzekraczający 90 dni. Ta regulacja też jest wynikiem dostosowania polskiego prawa do Konwencji. Instrument ten pozwala wydłużyć okres dostępności danych telekomunikacyjnych, które zgodnie z przepisami ustawy Prawo telekomunikacyjne są usuwane po 12 miesiącach.

Współpraca międzynarodowa

Konwencja ustanawia też zasady współpracy pomiędzy państwami, które ratyfikowały Konwencję, poprzez udzielenie wzajemnej pomocy prawnej przy ściganiu i prowadzeniu postępowań w sprawie cyberprzestępstw. Jak już wskazano, przy tym typie przestępstw bardzo często występuje element transgraniczny, np. wykorzystanie zagranicznych serwerów.

W Konwencji przewidziano jednak możliwość odmowy udzielenia pomocy prawnej przez stronę wezwaną, gdy wniosek dotyczy przestępstwa, które jest przez nią uważane za polityczne lub związane z przestępstwem politycznym. Odmowa udzielenia pomocy jest także możliwa, gdy realizacja wniosku może stanowić zagrożenie dla suwerenności, bezpieczeństwa, porządku publicznego lub innych podstawowych interesów państwa będącego stroną Konwencji.

Sama idea ustanowienia podstawy prawnej dla współpracy pomiędzy stronami przy prowadzeniu czynności śledczych lub gromadzenia dowodów odnoszących się do przestępstw związanych z systemami i danymi informatycznymi zasługuje na uznanie. Jednakże istnieje ryzyko, że przesłanka „zagrożenia innych podstawowych interesów" może być nadużywana, skutecznie paraliżując wzajemną współpracę pomiędzy państwami.

Należy tu wskazać, że istnieje wiele dwu- i wielostronnych umów międzynarodowych, które umożliwiają sięganie po pomoc międzynarodową w sprawach karnych. Jednakże z uwagi na niedoskonałości systemowe pomoc taka może trwać miesiącami lub latami. Zawarta w Konwencji instytucja pomocy prawnej wpisała się w ten schemat. Nie zawiera ona bowiem żadnych mechanizmów gwarantujących usprawnienie systemu pomocy prawnej i jego dostosowanie do specyfiki cyberprzestępstw. Krokiem naprzód byłoby chociażby umożliwienie współpracy na polu transgranicznych przeszukań prowadzonych zdalnie, ale Konwencja nie przewiduje takiej możliwości. W tej sferze nadal zatem istnieje duże zapotrzebowanie na dodatkową regulację.

Wsparcie specjalistów

Konwencja przewiduje także obowiązek wyznaczenia punktu kontaktowego dostępnego 24 godziny na dobę przez 7 dni w tygodniu, który będzie zapewniał natychmiastową pomoc na potrzeby prowadzenia czynności śledczych lub postępowań odnoszących się do cyberprzestępstw. Dlatego właśnie w 2010 roku został utworzony Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Służby Kryminalnej Komendy Głównej Policji. Może on nie tylko samodzielnie prowadzić czynności dochodzeniowo-śledcze, ale też oferować wsparcie jednostkom policji i prokuraturom, które nie mają pracowników wyspecjalizowanych w ściganiu sprawców cyberprzestępstw.

Konwencja stawia też duży nacisk na wykrywanie oraz ściganie sprawców

przestępstw związanych z pornografią dziecięcą popełnianych w internecie lub przy jego wykorzystaniu.

Łatwiej zapobiegać niż ścigać

Inicjatywy podejmowane na potrzeby walki z cyberprzestępczością zasługują na uznanie, ale nie da się uniknąć pytania o ich skuteczność. Zgodnie z raportem przygotowanym przez Symantec Corporation[I] liczba cyberataków ukierunkowanych w 2013 roku była o 91% większa niż w roku 2012, liczba naruszeń danych w tym samym okresie wzrosła o 62%, a jeden na 392 e-maile zawierał tzw. phishing attack, czyli próbę wyłudzenia danych osobowych.

Zgodnie z komunikatem Komisji Europejskiej każdego dnia w sieci krąży około 150 tys. wirusów komputerowych i codziennie zagrożonych zostaje 148 tys. komputerów[II].

Czy zatem pomimo wprowadzenia instrumentów do walki z cyberprzestępstwami, ich wykrywania i zwalczania, nie pozostajemy ciągle w tyle za ich sprawcami? Działając wyłącznie w reakcji na popełnione przestępstwo, służby ścigania stoją na straconej pozycji. Cała nadzieja na walkę z cyberprzestępczością tkwi w prewencji.

I http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

II http://europa.eu/rapid/press-release_IP-13-94_pl.htm.

Zabezpieczenie dowodów elektronicznych w postępowaniu karnym

Ludwina Klein

Pojęcie dowodu elektronicznego

W obowiązujących przepisach, nie tylko w zakresie postępowania karnego, brak jest definicji legalnej dowodu elektronicznego. Zgodnie ze stanowiskiem Ministra Sprawiedliwości zaprezentowanym 30 marca 2009 r. na potrzeby postępowania karnego pod pojęciem „dowodu elektronicznego" należałoby rozumieć informację, która może mieć znaczenie dowodowe w procesie karnym, zapisaną, przesłaną lub przechowywaną w formie elektronicznej[12]. Dowodem elektronicznym nie są zatem nośniki informacji takie jak twardy dysk komputera, pamięć wewnętrzna telefonu komórkowego, karta pamięci czy płyta CD, ale zapisane na nich dane niosące ze sobą określone informacje. Oczywiście nośniki te

[12] Odpowiedź sekretarza stanu w Ministerstwie Sprawiedliwości – z upoważnienia ministra – na interpelację nr 7857 w sprawie postępowania z dowodami elektronicznymi.

mogą również stanowić dowód w postępowaniu karnym, ale będzie to „tradycyjny" dowód rzeczowy.

Bez wątpienia część dowodów elektronicznych, takich jak e-mail, sms czy tekst stworzony w jednym z edytorów tekstu, będzie miała charakter dokumentów. Zgodnie z art. 115 § 14 Kodeksu karnego „dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne". Jednakże, jak wskazał Sąd Najwyższy, zacytowany powyżej przepis „wskazuje jedynie, jakie dokumenty znajdują się pod ochroną prawa karnego, a więc określa przedmiot ochrony prawnej przy przestępstwach skierowanych przeciwko wiarygodności dokumentów. Określony przedmiot nie musi być jednak dokumentem w rozumieniu karnoprawnym, aby być dowodem z dokumentu w rozumieniu karnoprocesowym"[13]. Pojęcie dokumentu w znaczeniu procesowym jest szersze i obejmuje nie tylko dokumenty wskazane w ustawowym określeniu tego pojęcia w materialnym prawie karnym[14]. Dokumentem w znaczeniu procesowym jest zatem każdy przedmiot lub zapis na nośniku informacji, zawierający treść wyrażoną słowami lub znakami graficznymi, która znalazła się tam w wyniku aktu woli jego wystawcy[15].

Dowód elektroniczny może przybrać również postać danych cyfrowych (tzw. logów komputerowych), przedstawiających przykładowo historię logowań z danego adresu IP na dany serwer. Dowody takie stanowią odrębną kategorię niematerialnych źródeł dowodowych[16].

Status dowodów elektronicznych w postępowaniu karnym

Aby dowód elektroniczny mógł stanowić dowód w postępowaniu karnym, musi być on odpowiednio zabezpieczony, uwierzytelniony i przeanalizowany przez specjalistów. Wyniki pierwszych czynności wykonanych przez organy prowadzące postępowanie przygotowawcze, które mają na celu zabezpieczenie dowodów elektronicznych w sprawie, oraz nośników, na których zostały one zapisane, mają istotne znaczenie dla osiągnięcia celów postępowania karnego. Popełnione w tym zakresie błędy mogą uniemożliwić późniejsze wydanie opinii przez biegłego i tym samym zaprzepaścić szanse na wykrycie sprawcy. Mimo to procedury zabezpieczania dowodów elektronicznych w ramach postępowania karnego nie doczekały się do tej pory szczególnej regulacji prawnej. W Kodeksie postępowania karnego (k.p.k.) brak jest unormowań szczególnych, odnoszących się bezpośrednio do problematyki dowodów elektronicznych. Wyjątek stanowią art. 218 k.p.k. w zakresie, w jakim dotyczy on korespondencji przesłanej pocztą elektroniczną, wykazów połączeń telekomunikacyjnych lub innych przekazów

[13] Wyrok Sądu Najwyższego z 3 marca 2011 r., sygn. akt V KK 311/2010, Lexis.pl nr 2508614.
[14] Wyrok Sądu Najwyższego z 29 listopada 1972, sygn. akt III KR 217/72, OSNPG 1973/6, poz. 82, str. 15.
[15] A. Gaberle, Dowody w sądowym postępowaniu karnym. Teoria i praktyka, Warszawa 2010, str. 255, cytowany w uzasadnieniu wyroku Sądu Najwyższego z 3 marca 2011 r., Nb 2.
[16] Tak M. Rusinek, Pozyskanie danych elektronicznych [w:] Tajemnica zawodowa i jej ochrona w polskim procesie karnym, Oficyna 2007.

informacji, oraz art. 218a k.p.k., który reguluje kwestię tymczasowego zabezpieczenia danych informatycznych przez urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną[17]. W pozostałym zakresie do dowodów cyfrowych odpowiednie zastosowanie znajdują przepisy dotyczące dowodów rzeczowych oraz dokumentów.

Przepisy regulujące zasady gromadzenia dowodów, które znajdą odpowiednie zastosowanie do dowodów elektronicznych, zostały zamieszczone w szczególności w rozdziałach 25 i 26 Kodeksu postępowania karnego. Z mocy art. 236a k.p.k. przepisy rozdziału 25 dotyczące zatrzymania rzeczy i przeszukania stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną. Natomiast zgodnie z art. 241 k.p.k. przepisy rozdziału 26 dotyczące kontroli i utrwalania rozmów stosuje się odpowiednio do kontroli oraz do utrwalania przy użyciu środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. Oznacza to, że także w odniesieniu do dowodów elektronicznych możliwe jest zarządzenie wydania i zatrzymanie danych informatycznych czy też korespondencji elektronicznej wraz z załączonymi do niej plikami, jak również przeszukanie urządzenia, na którym takie dane są przechowywane, lub systemu informatycznego.

Tymczasowe zabezpieczanie danych informatycznych

Wspomniane powyżej zabezpieczenie danych informatycznych na podstawie art. 218a k.p.k. jest swego rodzaju środkiem tymczasowym, poprzedzającym ewentualne żądanie wydania i zatrzymanie tych danych na podstawie art. 217 w zw. z art. 236a k.p.k. lub na podstawie art. 218 k.p.k.[18]

Obowiązek niezwłocznego zabezpieczenia danych informatycznych przechowywanych w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym ciąży na urzędach, instytucjach i podmiotach prowadzących działalność telekomunikacyjną. Zabezpieczenie następuje na podstawie postanowienia sądu lub prokuratora, w którym określony jest czas jego trwania. Dopuszczalne jest kilkukrotne wydanie postanowienia o zabezpieczeniu w odniesieniu do tych samych danych, jednak łączny czas ich zabezpieczenia nie może przekroczyć 90 dni[19]. Po upływie okresu zabezpieczenia wskazanego w postanowieniu zabezpieczenie upada. Organ, który nakazał zabezpieczenie danych, powinien wydać postanowienie o ich zwolnieniu spod zabezpieczenia, jeżeli po ich zabezpieczeniu okaże się, że nie mają one znaczenia dla postępowania karnego.

Sposoby zabezpieczania danych informatycznych w urządzeniach zawierających te dane oraz w systemach i na nośnikach informatycznych, w tym danych

[17] Przepis ten stanowi implementację art. 16 i 17 Konwencji Rady Europy o cyberprzestępczości z 23 listopada 2001 r.

[18] J. Skorupka, Komentarz do art. 236a k.p.k. [w:] Kodeks postępowania karnego. Komentarz, wydanie 15, C.H.Beck 2014.

[19] J. Skorupka, Komentarz do art. 218a k.p.k. [w:] Kodeks postępowania karnego. Komentarz, wydanie 15, C.H.Beck 2014.

przesyłanych pocztą elektroniczną, zwanych dalej „danymi zapisanymi", jak również wymogi dotyczące przechowywania zabezpieczonych danych określa rozporządzenie Ministra Sprawiedliwości z 28 kwietnia 2004 r.

Przewiduje ono w szczególności, że zabezpieczenia danych zapisanych dokonuje się przy użyciu środków technicznych, w sposób umożliwiający ich późniejsze odtworzenie przy użyciu urządzeń odtwarzających. Zabezpieczenia danych zapisanych dokonuje osoba upoważniona przez podmiot obowiązany do ich zabezpieczenia, przy użyciu środków technicznych tego podmiotu, w urządzeniach zawierających przedmiotowe dane, w systemie lub na nośniku informatycznym. W przypadku zabezpieczenia danych zapisanych na nośniku informatycznym osoba dokonująca tego zabezpieczenia zapisuje lub oznacza na tym nośniku:

- sygnaturę akt sprawy, w której czynność ta została zlecona,
- swoje imię, nazwisko i stanowisko służbowe,
- dane dotyczące podstawy zabezpieczenia,
- czas dokonania zabezpieczenia.

Z czynności zabezpieczenia danych zapisanych osoba dokonująca zabezpieczenia sporządza notatkę, w której zamieszcza:

- datę i miejsce sporządzenia notatki,
- sygnaturę akt sprawy,
- swoje imię, nazwisko i stanowisko służbowe,
- dane dotyczące podstawy zabezpieczenia,
- imię i nazwisko użytkownika systemu lub sieci albo nazwę podmiotu będącego użytkownikiem, w stosunku do którego zarządzono zabezpieczenie danych zapisanych,
- czas dokonania zabezpieczenia danych zapisanych,
- dane identyfikujące miejsce zabezpieczenia danych zapisanych,
- inne dane dotyczące dokonywanej czynności (w miarę potrzeby).

Rozporządzenie przewiduje, że zabezpieczone dane zapisane przechowuje się w warunkach zabezpieczających przed ich utratą, zniekształceniem lub nieuprawnionym ujawnieniem oraz zniszczeniem lub uszkodzeniem nośnika informatycznego.

Należy tu zauważyć, że obecnie wielu użytkowników korzysta z tzw. dynamicznych adresów IP, które nie są im przypisane na stałe, ale zmieniają się z każdym uruchomieniem modemu lub komputera. Dlatego też formułując wniosek o udostępnienie danych osobowych użytkownika, któremu przypisano ustalony przez wnioskodawcę adres IP, konieczne jest wskazanie konkretnej daty i godziny, w której nastąpiło logowanie na serwerze dostawcy usług internetowych, ponieważ tylko na tej podstawie dostawca ten jest w stanie ustalić, kto w danym momencie korzystał z danego adresu IP.

Odpowiednie stosowanie przepisów o zatrzymaniu rzeczy i przeszukaniu oraz o kontroli i utrwalaniu rozmów

Jak już zasygnalizowano, z mocy art. 236a k.p.k. przepisy rozdziału 25 dotyczące zatrzymania rzeczy i przeszukania stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku

znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.

Krąg podmiotów, na których ciąży obowiązek wydania danych, jest szerszy od tego wskazanego w art. 218a k.p.k. i obejmuje zarówno dysponenta, tj. osobę upoważnioną do rozporządzania systemem (np. administratora sieci), jak i użytkownika, czyli osobę używającą urządzenia zawierającego dane informatyczne lub systemu informatycznego (np. posiadacza komputera czy konta poczty elektronicznej). W literaturze słusznie wskazuje się, że w razie żądania wydania danych powinny one być w zasięgu określonej osoby. Nie muszą jednak znajdować się na terytorium Polski, gdyż mogą znajdować się np. w skrzynce pocztowej utworzonej na serwerze zagranicznym[20].

Zatrzymania dowodów elektronicznych można dokonać na kilka sposobów, w tym w jeden ze sposobów określonych w art. 19 Konwencji Rady Europy o cyberprzestępczości z 23 listopada 2001 r., tj. przez:

- zajęcie lub zabezpieczenie w podobny sposób systemu informatycznego lub jego części albo nośnika służącego do przechowywania danych informatycznych,
- wykonanie i zachowanie kopii danych informatycznych,
- zachowanie całości odpowiednich przechowywanych danych informatycznych (zablokowanie),
- uczynienie niedostępnymi lub usunięcie danych informatycznych z danego systemu informatycznego.

W celu odnalezienia danych informatycznych organ uprawniony do przeszukania może nie tylko poszukiwać nośnika tych danych, ale także przeprowadzić przeszukanie (z pomocą stosownego oprogramowania) systemu informatycznego, jego części, urządzenia lub nośnika zawierającego dane.

Z kolei odpowiednie stosowanie kontroli korespondencji i przesyłek, a także billingów, może polegać na żądaniu wydania zapisów wiadomości poczty elektronicznej lub wykazu połączeń dokonywanych w sieci w ramach użytkowania adresu elektronicznego[21].

Odpowiedniemu stosowaniu podlegają także przepisy dotyczące ochrony informacji niejawnych oraz informacji objętych tajemnicą zawodową (w tym obrończą) lub inną tajemnicą prawnie chronioną. Jeżeli zatem dane informatyczne zawierają informacje chronione tajemnicą, o której mowa w art. 225 k.p.k., należy postępować w taki sposób, aby były one dostępne jedynie osobom do tego uprawnionym.

Jeżeli natomiast chodzi o odpowiednie stosowanie przepisów rozdziału 26 dotyczących kontroli i utrwalania rozmów do kontroli oraz do utrwalania przy użyciu środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną, w literaturze słusznie wskazuje się, że w praktyce znajdą one zastosowanie jedynie do korespondencji e-mailowej znajdującej się w fazie transmisji, ponieważ do wiadomości takich utrwalonych na serwerze odbiorcy lub nadawcy stosuje się przepisy rozdziału 25. Nie ulega wątpliwości, że na podstawie art. 241 k.p.k. wolno kontrolować informacje przekazywane w sieci

[20] J. Skorupka, Komentarz do art. 236a k.p.k. [w:] Kodeks postępowania karnego. Komentarz, wydanie 15, C.H. Beck 2014.

[21] P. Hofmański (red.), Kodeks postępowania karnego. Komentarz do art. 1-296. Tom I. Wydanie 4, C.H. Beck 2011.

internet na czacie, czyli „na żywo"[22]. Natomiast inne przekazy informacji, o których mowa w przedmiotowym przepisie, to w szczególności faks, telefaks, telegraf, telewizja kablowa, przekaz radiowy oraz przekaz internetowy.

Wytyczne dotyczące zasad zabezpieczania dowodów elektronicznych przez policję

Pewne ogólne zasady postępowania z dowodami elektronicznymi przez funkcjonariuszy policji w trakcie wykonywanych przez nich czynności-dochodzeniowo śledczych reguluje § 69 wytycznych Komendanta Głównego Policji z dnia 15 lutego 2012 r.[23] oraz dodatkowe wytyczne dotyczące zasad zabezpieczania dowodów elektronicznych przekazane komórkom dochodzeniowo-śledczym w jednostkach policji przez Biuro Służby Kryminalnej KGP w sierpniu 2013 r.[24]

Zgodnie ze wspomnianymi powyżej źródłami czynności związane z zabezpieczeniem dowodów elektronicznych, w tym przeszukanie systemu informatycznego, powinny być dokonywane przy udziale biegłego. Podczas przeszukania niedopuszczalne jest umożliwienie dysponentowi lub użytkownikowi bezpośredniego dostępu do urządzeń lub systemów informatycznych. Dowód elektroniczny powinien zostać właściwie zabezpieczony zarówno w sensie prawnym, jak i technicznym. Poza sporządzeniem dokumentacji procesowej, tj. – w zależności od dokonywanych czynności – przed sporządzeniem protokołów oględzin, protokołów przeszukania osoby, miejsca, rzeczy i systemu informatycznego oraz protokołów zatrzymania rzeczy i danych informatycznych (art. 143 § 1 pkt 3 i pkt 6 k.p.k.) konieczne jest prawidłowe zabezpieczenie dowodu pod względem technicznym, w sposób uniemożliwiający dostęp do niego osobom trzecim.

Prowadzący przeszukanie ma prawo żądać od dysponenta lub użytkownika systemu informatycznego ujawnienia hasła lub haseł umożliwiających dostęp do systemu, chyba że dysponentem lub użytkownikiem jest oskarżony/podejrzany albo osoba, której przysługiwałoby prawo do odmowy zeznań albo do uchylenia się od odpowiedzi na pytanie w postępowaniu karnym, na potrzeby którego dowód jest zabezpieczany. Podczas przeszukania systemu informatycznego w przypadku, gdy zasoby przeszukiwanego systemu lub połączonego z nim innego komputera są zaszyfrowane i niemożliwe jest zapoznanie się z nimi bez podania hasła lub klucza prywatnego, można użyć urządzeń lub programów komputerowych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym. Niedopuszczalne jest przy tym użycie takich urządzeń lub programów należących do osoby, u której czynność jest dokonywana, nawet za zgodą tej osoby. Jeżeli policjant dokonuje zatrzymania oryginalnego nośnika danych informatycznych, może on uwzględnić wniosek dysponenta tych danych o pozostawienie mu kopii plików niezbędnych do prowadzonej działalności, o ile posiadanie treści utrwalonych w tych plikach nie jest zabronione. Co istotne, prowadzącym czynności policjantom wyraźnie zaleca się, oczywiście w zależności od okoliczności, podjęcie właściwych działań zmierzających

[22] *Tamże.*

[23] Wytyczne nr 3 Komendanta Głównego Policji z dnia 15 lutego 2012 r. w sprawie wykonywania czynności dochodzeniowo-śledczych przez policjantów.

[24] Przestępczość gospodarcza – stanowisko Biura Służby Kryminalnej KGP, Kwartalnik Prawno-Kryminalistyczny Szkoły Policji w Pile nr 19/2014, str. 65-70.

do ustalenia sieciowych śladów działania sprawcy, takich jak zwrócenie się do operatorów telekomunikacyjnych czy dostawców internetu.

Z kolei szczegółowe wskazówki odnośnie do zabezpieczania komputerów i innych nośników danych cyfrowych (a nie samych danych stanowiących dowody elektroniczne) znajdują się w opracowaniu przygotowanym przez Katedrę Kryminalistyki Szkoły Policji w Pile, który zawiera swego rodzaju instrukcję „*step-by-step*" (26 kroków)[25]. Zawarto tam również wyraźne zalecenie, aby przeprowadzający czynności funkcjonariusze policji nie próbowali sami badać komputera, zabezpieczonych urządzeń oraz zawartości nośników danych, z uwagi na to, że każde włączenie komputera po zakończeniu zabezpieczenia powoduje powstanie śladów wskazujących na naruszenie integralności materiału badawczego.

Dobre praktyki w zakresie zabezpieczania dowodów elektronicznych przez informatyków

Stowarzyszenie Instytut Informatyki Śledczej opracowało praktyki dotyczące zabezpieczania dowodów elektronicznych, które powinny być stosowane przez informatyków śledczych dokonujących czynności zabezpieczenia urządzeń posiadających nośnik elektroniczny oraz komponentów elektronicznych, aby zarówno one, jak i zapisane na nich dane mogły stanowić wiarygodny dowód w postępowaniu, w którym mają być wykorzystane. Zasady w nich sformułowane służą zapewnieniu autentyczności i integralności dowodów elektronicznych. Odnoszą się one zarówno do zabezpieczenia samych dowodów elektronicznych, jak i nośników, na których zostały one zapisane.

Zgodnie ze wspomnianymi praktykami, aby prawidłowo zabezpieczyć przechowywane na nośnikach elektronicznych informacje, należy przestrzegać następujących wytycznych:

- Dowód powinien być zachowany w stanie z chwili zabezpieczenia, z dokładnym odnotowaniem daty i czasu. Sama czynność zabezpieczania powinna odbyć się w obecności świadków.
- Zabezpieczany sprzęt i nośniki powinny być prawidłowo oznakowane, opisane i ewentualnie oplombowane. W zależności od sprawy, numery seryjne wszystkich urządzeń wchodzących w skład systemu powinny zostać odnotowane (ze względu na możliwość ich późniejszej zamiany). W sprawach, w których może to być konieczne, należy fotograficznie udokumentować wszystkie elementy i połączenia wchodzące w skład danego systemu.
- Jedyną możliwością autentyfikacji materiału, zakładając możliwość stwierdzenia późniejszych zmian, jest wyliczenie w momencie zabezpieczania sumy kontrolnej nośnika. Możliwość ponownego wyliczenia tej samej sumy w późniejszych etapach postępowania oraz porównanie jej z sumą z zabezpieczenia pozwala na stwierdzenie, czy materiał nie został zmieniony.
- Badania powinny być prowadzone wyłącznie na kopii (utworzonej na zasadzie równości z oryginałem), tak aby nie naruszyć wartości dowodowej oryginału i umożliwić inne badania na tym samym materiale. Z tego samego

[25] L. Bieliński, W. Miś, Kryminalistyczno-procesowe zabezpieczanie śladów na miejscu zdarzenia, Szkoła Policji w Pile, Zakład Kryminalistyki, lipiec 2009 r.

powodu badania na oryginale powinny być prowadzone z użyciem technik uniemożliwiających zmiany zapisów zawartych na badanym nośniku[26].

Jak to wygląda w praktyce

Aktualna praktyka podmiotów zaangażowanych w czynności związane z zabezpieczaniem dowodów elektronicznych w postępowaniu karnym, tj. głównie funkcjonariuszy policji i informatyków, wydaje się wskazywać, że mimo braku szczegółowej regulacji ustawowej czynności te wykonywane są w sposób poprawny i profesjonalny. Zmiana podejścia, zwłaszcza funkcjonariuszy policji, z całą pewnością wynika w znacznej mierze ze zdobytych doświadczeń, które pokazały konsekwencje najmniejszych nawet błędów. Trudno też nie docenić roli opisanych wytycznych opracowanych specjalnie na użytek policjantów dokonujących zabezpieczenia dowodów elektronicznych.

Niestety nadal wiele do życzenia pozostawia tempo podejmowania działań w zakresie zabezpieczenia dowodów elektronicznych przez organy ścigania. Czas reakcji na zawiadomienie o zdarzeniu, którego wyjaśnienie wymaga zabezpieczenia tego typu dowodów, jest nadal zbyt długi. Przyczyną takiego stanu rzeczy może być generalna niechęć organów ścigania do podejmowania działań, które generują dodatkowe koszty, a taką decyzją jest niewątpliwie decyzja o powołaniu biegłego. W sprawach bardziej skomplikowanych, w których konieczne jest podjęcie próby odzyskania utraconych danych lub odzyskania danych ze zniszczonych nośników, koszty te mogą być znaczne.

[26] http://www.siis.org.pl/najlepsze-praktyki/zabezpieczanie.html

Konkluzje

1. Nie ma dziś bezpieczeństwa obrotu prawnego bez bezpieczeństwa informatycznego.
2. Kluczowe kwestie związane z cyberprzestępczością i cyberbezpieczeństwem wciąż nie zostały należycie potraktowane przez ustawodawcę na poziomie unijnym i krajowym.
3. Z punktu widzenia ustawodawców, prawników i organów ścigania głównym wyzwaniem jest transgraniczność cyberprzestępstw. Główne narzędzia prawne do walki z zagrożeniami z cyberprzestrzeni znajdują się w obszarze prawa karnego, a doświadczenia unijne pokazują, że obszar ten jest najtrudniejszy do zharmonizowania na poziomie poszczególnych państw członkowskich.
4. Problemem jest współpraca między poszczególnymi państwami w sprawach karnych (tzw. pomoc prawna), a także szybkość reakcji organów ścigania (brak powszechnych praktyk, dostępnego instrumentarium).
5. W tych warunkach remedium na bolączki w sferze prywatnej stanowi prężnie rozwijający się rynek usług z zakresu cyberbezpieczeństwa.
6. Z prawnego punktu widzenia cyberbezpieczeństwo jest problemem zarówno prawa publicznego, jak i prywatnego, przy czym propozycje regulacji i działań adresowanych do instytucji publicznych nie mogą być tożsame z działaniami adresowanymi do podmiotów prywatnych.
7. Wobec braku spójnych uregulowań i powszechnych praktyk prawnicy muszą patrzeć na zagadnienia cyberbezpieczeństwa przez pryzmat konkretnych spraw. Dla każdego przypadku należy indywidualnie ocenić możliwości dowodzenia, sposób i szybkość reakcji oraz adekwatność dostępnych środków prawnych w stosunku do zdarzeń, z którymi mierzy się klient.

Autorzy

Magdalena Gutowska jest aplikantem adwokackim w praktyce postępowań sądowych i arbitrażowych oraz praktyce karnej kancelarii Wardyński i Wspólnicy. Zajmuje się sprawami z zakresu prawa karnego, w tym karnego gospodarczego, wdrażaniem i monitorowaniem funkcjonowania procedur *compliance* oraz postępowaniami sądowymi i arbitrażowymi powstałymi na tle stosunków handlowych.

E-mail: magdalena.gutowska@wardynski.com.pl

Ludwina Klein jest aplikantem adwokackim w praktyce postępowań sądowych i arbitrażowych oraz praktyce karnej kancelarii Wardyński i Wspólnicy. Specjalizuje się w prowadzeniu sporów przed sądami arbitrażowymi oraz powszechnymi. Występuje w postępowaniach arbitrażowych prowadzonych w oparciu o regulaminy wiodących instytucji arbitrażowych takich jak ICC, SCC, czy SAKiG. Ma doświadczenie w zakresie sporów posttransakcyjnych, dotyczących nieruchomości oraz powstałych na tle długoterminowych umów kooperacyjnych. Zajmuje się także sprawami z zakresu prawa karnego gospodarczego.

E-mail: ludwina.klein@wardynski.com.pl

Anna Katarzyna Nietyksza od 1998 roku Prezes Zarządu EFICOM SA obecnie Grupy Kapitałowej Eficom-Sinersio, notowanej na NewConnect GPW. Członek Europejskiego Komitetu Ekonomiczno-Społecznego, Grupy Agenda Cyfrowa i Energetyka, III instytucji w UE, opiniującej wszystkie akty prawne i regulacje UE. Sprawozdawca Opinii Nt Rynku Telekomunikacyjnego UE i Gospodarki Cyfrowej, członek Grup ds. Cyberbezpieczeństwa, Big Data, Cloud Computing, ekspert ds. funduszy UE i government relations. Prezes Eurocloud Polska, Członek Rady Eurocloud Europe, Rady Izby Francuskiej, Przewodnicząca Komitetu Gospodarki Innowacyjnej Kigeit.

Piotr Rutkowski jest doradcą kancelarii ds. nowych technologii. Zajmuje się uwarunkowaniami prawnymi, regulacyjnymi i technologicznymi innowacyjnych sektorów gospodarki. Od 1990 roku prowadzi własną firmę konsultingową Rotel, specjalizując się w problematyce strategii i regulacji rynku telekomunikacyjnego, zastosowaniach nowych technologii, bezpieczeństwie, ochronie infrastruktury krytycznej, zarządzaniu ryzykiem oraz współpracy sektora prywatnego i publicznego.

E-mail: piotr.rutkowski@wardynski.com.pl

Dominika Stępińska-Duch jest adwokatem, partnerem kancelarii Wardyński i Wspólnicy. Zajmuje się praktyką rozwiązywania sporów i arbitrażu oraz praktyką karną. Odpowiada również za obszar cyberbezpieczeństwa w praktyce prawa nowych technologii. Prowadzi spory sądowe, w szczególności z zakresu prawa karnego gospodarczego. Ocenia ryzyko odpowiedzialności karnej wynikające ze zdarzeń gospodarczych, np. przyjmowanie/dawanie „prowizji" za udzielanie zleceń/kontraktów (m.in. prywatna korupcja). Zajmuje się wdrażaniem i monitorowaniem funkcjonowania procedur *compliance*.

E-mail: dominika.stepinska-duch@wardynski.com.pl

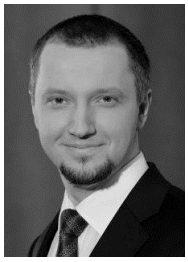
Aleksandra Stępniewska jest adwokatem w praktyce rozwiązywania sporów i arbitrażu oraz praktyce karnej kancelarii Wardyński i Wspólnicy.

Zajmuje się głównie sprawami z zakresu prawa karnego, w tym karnego gospodarczego, a także wdrażaniem i monitorowaniem funkcjonowania procedur *compliance*.

E-mail: aleksandra.stepniewska@wardynski.com.pl

Janusz Tomczak, adwokat, partner kancelarii Wardyński i Wspólnicy, jest odpowiedzialny za praktykę karną, zajmuje się także praktyką rozwiązywania sporów i arbitrażu. Odpowiada za obszar cyberbezpieczeństwa w praktyce prawa nowych technologii. Reprezentuje polskich i zagranicznych klientów indywidualnych oraz instytucjonalnych w postępowaniach karnych, karnych gospodarczych i cywilnych. Bierze udział w postępowaniach mających na celu wyeliminowanie albo ograniczenie negatywnych konsekwencji przestępstw gospodarczych. Ocenia ryzyko odpowiedzialności karnej wynikające ze zdarzeń gospodarczych, np. przyjmowanie/dawanie „prowizji" za udzielanie zleceń/kontraktów (m.in. prywatna korupcja).

E-mail: janusz.tomczak@wardynski.com.pl



Krzysztof Wojdyło jest adwokatem w praktykach: nowych technologii, postępowań regulacyjnych oraz usług płatniczych. Zajmuje się regulacjami dotyczącymi elektronicznych instrumentów płatniczych, obrotu wierzytelnościami i przeciwdziałania praniu brudnych pieniędzy. Uczestniczy w dużych i nowatorskich projektach z zakresu szeroko rozumianego prawa finansowego Regularnie doradza największym polskim oraz zagranicznym instytucjom finansowym.

E-mail: krzysztof.wojdylo@wardynski.com.pl

Praktyka prawa nowych technologii

Dla nas nowe technologie to przede wszystkim nowe wyzwania prawne. W wielu przypadkach musimy zmagać się z wątpliwościami dotyczącymi kwalifikacji prawnej innowacyjnych produktów lub usług albo wręcz z brakiem odpowiednich regulacji. Zapewnienie klientom bezpieczeństwa prawnego w takich okolicznościach wymaga od prawników doświadczenia, kreatywności i rozumienia otoczenia biznesowego.

Dlatego stworzyliśmy w kancelarii interdyscyplinarną praktykę prawa nowych technologii, która skupia wysokiej klasy prawników, specjalistów w wybranych dziedzinach prawa. Wspierają nas współpracujący z kancelarią eksperci dysponujący szeroką wiedzą techniczną.

Staramy się na bieżąco reagować na potrzeby naszych klientów, tworząc wysoce wyspecjalizowane usługi prawne adresowane do poszczególnych segmentów rynku nowych technologii. Świadczymy kompleksowe doradztwo regulacyjne, podatkowe oraz transakcyjne.

Praktyka prawa nowych technologii zapewnia kompleksowe doradztwo w następujących obszarach: biomedycyna i nowoczesna żywność, crowdfunding, cyberbezpieczeństwo, e-commerce, finansowanie nowych technologii, gaming, nowe rozwiązania płatnicze, nowe technologie w pozyskiwaniu energii, ochrona prywatności, prace badawcze, projekty partnerstwa publiczno-prywatnego, przemysł kreatywny, technologie informacyjne, telekomunikacja.

Anna Pompe
adwokat, wspólnik

E-mail: anna.pompe@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00

Krzysztof Wojdyło
adwokat

E-mail: krzysztof.wojdylo@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00

Joanna Prokurat
doradca podatkowy

E-mail: joanna.prokurat@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00

Piotr Rutkowski
doradca ds. nowych technologii

E-mail: piotr.rutkowski@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00

Praktyka karna

W związku z coraz silniejszą ingerencją prawa karnego w stosunki między przedsiębiorcami wyodrębniliśmy praktykę specjalistów zajmujących się prawem karnym gospodarczym.

Obok doświadczenia w sprawach karnych mamy szeroką wiedzę na temat funkcjonowania podmiotów gospodarczych oraz różnych obszarów prawa gospodarczego. Umożliwia nam to pełną analizę zagadnień związanych z przestępczością gospodarczą i zapobieganiem ryzyku odpowiedzialności karnej.

Dążymy do zapewnienia przedsiębiorcom pełnej ochrony prawnej w kontaktach z organami ścigania, strzegąc takich wartości jak tajemnice przedsiębiorstwa, bezpieczeństwo obrotu gospodarczego i bezpieczeństwo funkcjonowania organów podmiotów gospodarczych.

Reprezentujemy klientów we wszystkich rodzajach postępowań karnych i na wszystkich ich etapach postępowań karnych.

Pomagamy minimalizować ryzyko odpowiedzialności karnej oraz ograniczać skutki przestępstw godzących w przedsiębiorców.

Przygotowujemy programy badania zgodności (*internal compliance programmes*) służące usprawnieniu funkcjonowania podmiotów gospodarczych oraz zapewnieniu przestrzegania powszechnie obowiązujących przepisów w ich codziennej działalności, w tym szybkiemu wykrywaniu nieprawidłowości.

Doradzamy przedsiębiorcom w tzw. postępowaniach wewnętrznych, służących zdiagnozowaniu przyczyny wykrytych nieprawidłowości, które mogą nosić znamiona przestępstw, i usunięciu ich skutków.

Zapewniamy pełną pomoc prawną z zakresu prawa karnego również poza granicami Polski.

Dominika Stępińska-Duch
adwokat, partner

E-mail: dominika.stepinska-duch@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00

Janusz Tomczak
adwokat, partner

E-mail: janusz.tomczak@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00

O kancelarii

Kancelaria Wardyński i Wspólnicy jest jedną z największych niezależnych polskich firm prawniczych. Biura kancelarii znajdują się w Warszawie, Poznaniu, Wrocławiu, Krakowie oraz Brukseli.

Kancelaria specjalizuje się m.in. w następujących dziedzinach: arbitraż, bankowość i finansowanie projektów, fuzje i przejęcia, nieruchomości, obsługa korporacyjna firm, podatki i spory podatkowe, prawo konkurencji, prawo Unii Europejskiej, prawo farmaceutyczne, prawo morskie, prawo ochrony środowiska, prawo pracy, projekty infrastrukturalne oraz PPP, rozwiązywanie sporów, doradztwo dla sektora energetycznego, rynki kapitałowe, technologie, media i telekomunikacja, upadłości i postępowania naprawcze, własność intelektualna i zamówienia publiczne.

Kancelaria jest właścicielem portalu **Co do zasady** przeznaczonego dla przedsiębiorców i prawników. Piszemy prosto o skomplikowanych zagadnieniach prawnych mogących mieć przełożenie na działalność gospodarczą. Portal Co do zasady powstał z połączenia Portalu Procesowego i Portalu Transakcyjnego.

Publikacje autorstwa prawników kancelarii są też prezentowane w aplikacji **Wardyński+**, pierwszej polskojęzycznej aplikacji o tematyce prawnej na iPada i Androida. Aplikację można pobrać nieodpłatnie w App Store i Google Play.

www.wardynski.com.pl

www.codozasady.pl

Wardyński+

O EFICOM

EFICOM SA specjalizuje się w regulacjach i funduszach UE. Dostarczyła do tej pory ponad 250 mln pln dotacji dla swoich klientów. EFICOM jest notowany na rynku NewConnect, jest Autoryzowanym Doradcą, wprowadził na NewConnect 7 spółek.

Grupa EFICOM kupiła spółkę Sinersio, dostawcę chmury obliczeniowej, zainwestowała już ponad 5 mln pln w 9 start-upów internetowych, platformę cloud computing, komputerowych sieci neuronowych i wyszukiwarek semantycznych poprzez fundusz Microbiolab, który kontroluje.

Grupa Kapitałowa EFICOM - Sinersio przekształca się aktualnie w dostawcę chmury obliczeniowej wspieranego przez fundusze UE, na dynamicznie rosnącym rynku Cloud Computing w Europie Centralnej przedstawiającym ogromny potencjał wzrostu, napędzany gospodarką cyfrową, rozwojem rynku telekomunikacyjnego, E-commerce i rynkiem Big Data. Planuje też oferować rozwiązania cyberbezpieczeństwa. Nowe inwestycje EFICOM Sinersio będą wspierane przez fundusze UE i środki pozyskane od inwestorów.

Wardyński i Wspólnicy
Al. Ujazdowskie 10
00-478 Warszawa

Tel.: 22 437 82 00, 22 537 82 00
Faks: 22 437 82 01, 22 537 82 01

E-mail: warsaw@wardynski.com.pl