Kwiecień 2018

INSTYTUT KOŚCIUSZKI

BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI

Paweł Opitek

Clarifying Lawful Overseas Use Data Act – nowy model pozyskiwania danych cyfrowych w sprawach karnych

autor

Paweł Opitek – Doktor nauk prawnych, prokurator del. do Prokuratury Krajowej, ekspert Instytutu Kościuszki ds. Cyberbezpieczeństwa, członek Strumienia Blockchain/DLT i Waluty Cyfrowe przy Ministerstwie Cyfryzacji, Polskiego Towarzystwa Kryminalistycznego oraz Centrum Technologii Blockchain przy Uczelni Łazarskiego. Zajmuje się cyberprzestępczością, m.in. kartami płatniczymi, kryptowalutami, dowodami cyfrowymi oraz hakingiem. Bada metody dydaktyczne prawa nowych technologii. Prelegent na krajowych i międzynarodowych konferencjach naukowych, autor książek, publikacji i specjalistycznych opracowań z zakresu prawa i kryminalistyki. Wykładowca Krajowej Szkoły Sądownictwa i Prokuratury. Ukończył studia dziennikarskie oraz studium pedagogiki i psychologii.

Skuteczne uzyskiwanie danych cyfrowych w postępowaniu karnym coraz częściej stanowi nieodłączny warunek ustalenia sprawcy przestępstwa i udowodnienia mu winy. *Modus operandi* osób podejrzanych powiązane jest w jakiś sposób z użyciem telefonu, Internetu czy chmury obliczeniowej, a to powoduje, że zaciera się granica pomiędzy cyberprzestępstwami, a pozostałą grupą nadużyć penalizowanych w kodeksie karnym. Każdy rodzaj przestępstwa może w mniejszym lub większym stopniu dotyczyć cyberprzestrzeni. Z drugiej strony, gromadzenie śladów binarnych przez prokuratora napotyka na poważne trudności, a często jest wręcz niemożliwe, m.in. z tego powodu, że serwery wykorzystywane przez figuranta zlokalizowane są w innym kraju aniżeli miejsce popełnienia zbrodni. Poza tym uzyskanie informacji wymaga spełnienia żmudnych procedur, jest znacznie rozciągnięte w czasie, a nigdy nie ma pewności, czy pomoc prawna zostanie efektywnie zrealizowana. Ostatecznie, natychmiastowa reakcja na przestępstwo i związana z nią konieczność zabezpieczenia dowodów cyfrowych staje się nie lada wyzwaniem dla policji i innych służb. Przykładowo, średni czas realizacji wniosku o pomoc prawną w zakresie zabezpieczenia danych gromadzonych przez popularnego Facebooka wynosi od 8 do nawet kilkunastu miesięcy. Dochodzą do tego kolejne problemy: ponieważ dane składowane w chmurze mogą być transferowane z jednej szerokości geograficznej do drugiej (w zależności od bieżącej polityki firmy),

ISSN 1689-9873

aktualny dzisiaj nakaz ich wydania jutro może okazać się całkowicie bezużyteczny. Globalne firmy branży IT świadczą usługi w różnych krajach, a więc podlegają różnym jurysdykcjom. W procedurze uzyskiwania danych cyfrowych na potrzeby postępowania karnego należy zatem brać pod uwagę zarówno prawo obowiązujące w państwie-wnioskodawcy, jak i przepisy właściwe dla miejsca składowania informacji. W praktyce rodzi to wiele niejasności i trudności interpretacyjnych, łącznie z brakiem współpracy pomiędzy państwami w ściganiu najpoważniejszych przestępstw.

Dotychczasowa współpraca międzynarodowa w zakresie pozyskiwania danych oparta była na tzw. MLAT (ang. *Mutual Legal Assistance Treaties*), tj. systemie umów bilateralnych: kiedy zagraniczne służby chciały zgromadzić dane cyfrowe znajdujące się na terenie Stanów Zjednoczonych, musiały uzyskać amerykański nakaz sądowy. W odwrotnej sytuacji, to Amerykanie musieli przejść całą procedurę udostępniania e-dowodów zgodnie z prawem państwa ulokowania serwerów. Dzisiaj „system MLAT" stał się zbyt wolny i trudno przypuszczać, aby zmieniły to podejmowane na różnych szczeblach działania w kierunku poprawy jego wydajności.

Opisana sytuacja powoduje, że rodzina państw demokratycznych pracuje nad budową sprawnego mechanizmu pozyskiwania danych cyfrowych przez organy ochrony prawa. Z perspektywy polskiej szczególnie ważne jest zacieśnianie współpracy pomiędzy Stanami Zjednoczonymi i Unią Europejską, czemu służyć ma zaplanowane w dniach 22-23 maja 2018 r. spotkanie UE-USA w Sofii. Ostatecznym celem omawianych działań jest wypracowanie wspólnej polityki międzynarodowej poprzez aktualizację obowiązujących przepisów lub wprowadzenie całkiem nowych rozwiązań. Nie jest to zadanie łatwe, szczególnie, że „lawful hacking" stoi zawsze w kontrze do takich wartości, jak prawo do prywatności, tajemnica korespondencji czy wolność Internetu. Z drugiej strony, problem udostępniania danych cyfrowych na potrzeby walki z przestępczością stał się na tyle istotny, że ostatnimi czasy podjęto konkretne działania celem jego rozwiązania.

7 lutego 2018 r. weszła w życie nowelizacja Kodeksu postępowania karnego wdrażająca do prawa polskiego dyrektywę Parlamentu Europejskiego i Rady Europy z 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (END). W relacjach z państwami Unii Europejskiej (z wyjątkiem Danii i Irlandii) zastępuje on (z pewnymi wyjątkami) tradycyjną instytucję pomocy prawnej i umożliwia sprawniejsze przeprowadzenie lub uzyskanie dowodów (także cyfrowych) na terytorium innego państwa członkowskiego. Nowa procedura została już zastosowana z pozytywnym rezultatem w czynnościach zabezpieczenia i gromadzenia dowodów przeciwko zatrzymanemu w marcu 2018 r. sławnemu hakerowi „Argamedonowi". Chociaż END stanowi znaczny postęp w walce z cyberprzestępczością, to jednak przewidziany w nim maksymalny okres przekazania dowodu do 120 dni i tak jest zbyt długi. Dlatego Unia Europejska pracuje nad kolejnymi zmianami w prawie ułatwiającymi dostęp organom ścigania do informacji cyfrowych zgromadzonych za granicą (m.in. do końca 2019 r. ma zostać opracowany kolejny protokół do Konwencji budapesztańskiej o cyberprzestępczości). 26 lutego 2018 r. odbyło się posiedzenie Radu UE dotyczące wstępnych ustaleń w tym zakresie. Głównym celem jest szybsze i skuteczniejsze uzyskiwanie danych poprzez zintensyfikowanie współpracy z krajami trzecimi i dostawcami usług internetowych, którzy są aktywni na europejskim rynku. W najdalej idącej wersji zmian, firmy działające w UE będą zobowiązane do przekazywania danych przechowywanych poza Europą nawet wtedy, jeśli mogłoby to w jakiś sposób naruszyć zagraniczne przepisy. Zmiany dotyczące uzyskiwania i zabezpieczania e-dowodów konsultowane są na bieżąco ze środowiskami eksperckimi (m.in. Cloud Evidence Group), podmiotami ochrony danych osobowych, przemysłem i organizacjami społecznymi.

Ponieważ najwięksi globalni gracze na rynku usług cyfrowych mają siedzibę w Stanach Zjednoczonych i podlegają prawu amerykańskiemu, dlatego rozwój sytuacji za Oceanem ma bezpośredni wpływ na procesy zachodzące w UE. W tym kontekście rewolucyjna może okazać się, podpisana 27 marca 2018 r. przez prezydenta Donalda Trumpa, ustawa *Clarifying Lawful Overseas Use Data Act* (tzw. CLOUD Act). Zakreśla ona na jakich zasadach organy ścigania mogą uzyskiwać dostęp do danych cyfrowych gromadzonych przez dostawców usług internetowych i zlokalizowanych w obcych jurysdykcjach aniżeli siedziba organu wydającego nakaz.

CLOUD Act jest wspólna inicjatywą Republikanów i Demokratów, którzy, przy wsparciu m.in. Departamentu Sprawiedliwości i Białego Domu, utworzyli ponadpartyjną koalicję na rzecz wprowadzenia ustawy w życie. Znamienne jest, iż projekt został poparty przez światowych gigantów na rynku usług cyfrowych: Microsoft, Facebook, Google, Apple i Oath; we wspólnym oświadczeniu z 6 lutego 2018 r. stwierdzili oni, że najlepszą drogą unikania sporów jest współpraca międzynarodowa, a CLOUD Act jest „logicznym rozwiązaniem dla pozyskiwania przez rządy danych cyfrowych". Na blogu Microsoftu podpis prezydenta Trumpa pod ustawą skwitowano jako ważny krok w stronę ochrony prywatności indywidualnych użytkowników Internetu, zażegnanie międzynarodowych konfliktów o stosowanie prawa i zapewnienie większego bezpieczeństwa użytkownikom sieci.

CLOUD Act jest wspólna inicjatywą Republikanów i Demokratów, którzy, przy wsparciu m.in. Departamentu Sprawiedliwości i Białego Domu, utworzyli ponadpartyjną koalicję na rzecz wprowadzenia ustawy w życie.

Nietrudno odgadnąć, że pojawiły się także głosy sprzeciwu, jakoby CLOUD Act zniweczył ochronę prywatności na całym świecie; pisano o poświęceniu interesu indywidualnych osób dla dobra rządu i biznesu. Propagatorom nowego prawa zarzucono zbytnią ingerencję władzy wykonawczej w prawa człowieka i tajemnicę korespondencji. Miało nawet dojść do obejścia IV Poprawki do Konstytucji Stanów Zjednoczonych, która gwarantuje nietykalność „osobistą i materialną". W piśmie z 19 marca 2018 r. skierowanym do członków Kongresu, przedstawiciele organizacji pozarządowych (m.in. European Digital Rights i Panoptykon Foundation) wyrazili głębokie zaniepokojenie sposobem procedowania nad CLOUD Act z pominięciem rzeczowej i szczegółowej dyskusji i bez konsultacji społecznych.

Przechodząc do oceny rozwiązań przyjętych w *Clarifying Lawful Overseas Use Data Act*, należy najpierw pochylić się nad tłem ich wprowadzenia oraz merytoryczną treścią przepisów.

CLOUD Act jest pokłosiem sprawy United States v. Microsoft (zwanej „Microsoft Ireland" lub sprawą „o suwerenność danych") zawisłej przed amerykańskim sądem. Wszystko zaczęło się w 2013 r., kiedy Departament Sprawiedliwości zwrócił się do Microsoftu o ujawnienie treści korespondencji przesłanej pocztą elektroniczną i zapisanej na serwerach firmy zainstalowanych w Irlandii. Dane miały być wykorzystane jako kluczowy dowód w śledztwie dotyczącym handlu narkotykami. Microsoft odmówił ich wydania podnosząc, że amerykański nakaz jest sprzeczny z przepisami obowiązującymi w miejscu ulokowania serwera, a dla uzyskania danych amerykańskie organy ścigania powinny postarać się o pozwolenie w myśl irlandzkiego prawa. Sąd Najwyższy Stanów Zjednoczonych przychylił się do takiego stanowiska, ale wskazał równocześnie na konieczność przystosowania obowiązujących przepisów do realiów współczesnej gospodarki i wezwał Kongres do zaktualizowania ustawy o ochronie danych. Nie gwarantował tego pochodzący z 1986 r. *Electronic Communications Privacy Act* jako anachroniczny w konfrontacji z nowoczesnym rynkiem usług cyfrowych. Sprawa „Microsoft Ireland" nie została zakończona. W tym roku Sąd Najwyższy musi odpowiedzieć na pytanie, czy władze Stanów Zjednoczonych mogą zmusić Microsoft do wydania na potrzeby toczącego się śledztwa kluczowych danych cyfrowych zapisanych na serwerach ulokowanych w Europie? Wyrok, jakikolwiek będzie, nie rozwiąże jednak problemu i dopiero CLOUD Act stanowi odpowiedź na wyzwania związane ze zwalczaniem transgranicznej przestępczością zorganizowanej, której skuteczność zależy od efektywnej współpracy z firmami prywatnymi.

Clarifying Lawful Overseas Use Data Act wprowadza dwa podstawowe rozwiązania:

1) umożliwia amerykańskim organom ścigania (agencjom federalnym i lokalnym departamentom policji) dostęp do danych cyfrowych przechowywanych przez firmy amerykańskie za granicą i dotyczących osób fizycznych niezależne od tego, gdzie mieszkają, gdzie wytworzone przez nich informacje są przechowywane i niezależnie od reżimu prawnego obowiązującego w miejscu lokalizacji danych,

2) pozwala prezydentowi na zawieranie umów (ang. *executive agreements*) dających państwu obcemu prawo uzyskiwania z pominięciem drogi sądowej danych cyfrowych znajdujących się na serwerach firm amerykańskich w każdym zakątku globu

(z wyjątkiem obywateli Stanów Zjednoczonych, gdzie podstawę inwigilacji nadal będzie stanowił nakaz sądowy).

Nowe prawo przewiduje jednakże mechanizmy blokujące dostęp do danych na dwóch poziomach: *in abstracto* oraz *in concreto*. W pierwszym przypadku Kongres, zanim podpisany zostanie *executive agreement*, przeprowadza audyt, czy kraj-strona umowy podziela wartości demokratycznego państwa prawnego i posiada system zapewniający faktyczną ochronę praw i wolności obywatelskich. Kontrola *in concreto* daje firmom możliwość blokowania lub modyfikowania wniosków o wydanie danych w sytuacji, gdy np. stanowiłoby to pogwałcenie prawa innego kraju lub zagroziło jego suwerenności. Zastrzeżenia takie powinny być zgłaszane w ciągu 14 dni od otrzymania wniosku i ostatecznie amerykański sąd rozstrzyga, kto w sporze ma rację.

CLOUD Act dotyczy przestępstw o najpoważniejszym ciężarze gatunkowym: aktów terroryzmu czy pornografii dziecięcej. Nie zmieni się zatem charakterystyczna dla Stanów Zjednoczonych wstrzemięźliwość w realizacji wniosków o pomoc prawną w sprawach karnych, które są odrzucane (pozostawione bez biegu), jeśli wartość szkody nie przekracza 5 tys. dolarów czy dotyczy innych przestępstw o mniejszym ciężarze gatunkowym. Warto dodać, że dzisiaj warunkiem uzyskania od strony amerykańskiej odpowiedzi jest szczegółowe opisanie i udokumentowanie wniosku, gdyż za Oceanem funkcjonuje zakaz tzw. *fishing expeditions*, czyli poszukiwania dowodów w miejscach, co do których nie ma pewności, że zawierają jakiekolwiek dane istotne dla śledztwa. Jeszcze trudniejsze jest realizowanie jakichkolwiek wniosków dotyczących wolności słowa (I poprawka do Konstytucji) czy też spraw drobnych przestępstw ze względu na regułę *de minimis* wynikającą z obowiązującej w prawie amerykańskim zasady oportunizmu.

CLOUD Act dotyczy przestępstw o najpoważniejszym ciężarze gatunkowym: aktów terroryzmu czy pornografii dziecięcej.

Wprowadzenie *Clarifying Lawful Overseas Use Data Act* jest właściwym krokiem w kierunku walki z szeroko pojętą cyberprzestępczością:

1) umożliwia skuteczne pozyskiwanie w krótkim czasie dowodów cyfrowych w sprawach o najpoważniejsze przestępstwa,

2) wytycza standardy ochrony prywatności użytkowników cyberprzestrzeni,

3) formułuje dla firm międzynarodowych zasady, na jakich mogą udzielać informacji organom ochrony prawa,

4) wspiera międzynarodową współpracę w sprawach karnych i ujednolica normy prawne w zakresie pozyskiwania danych,

5) wpływa korzystnie na rozwój nowoczesnych technologii, gdyż niejasne prawo prowadziło do sporów i konfliktów między firmami i rządami poszczególnych państw, których finał nierzadko znajdował się w sądzie.

Doprecyzowując temat wprowadzenia CLOUD Act w aspekcie praw człowieka, zauważyć należy, że prawo do poszanowania życia prywatnego nie ma charakteru ostatecznego. Chociaż przyznanie służbom kompetencji do uzyskiwani treści korespondencji (e-maili, zapisu rozmów na portalach społecznościowych) rodzi groźbę nadmiernej kontroli, jest warunkiem koniecznym do zwalczania współczesnych form przestępczości. Europejski Trybunał Praw Człowieka niejednokrotnie wskazywał, że tego typu działania muszą mieć jasno opisaną procedurę stosowania, dotyczyć określonych kategorii czynów czy obejmować osoby, co do których istnieje realne i udokumentowane podejrzenie popełnienia przestępstwa. Zadaniem ustawodawcy jest, aby wskazane zalecenia wprowadzić w międzynarodowym modelu uzyskiwania danych cyfrowych. Standardy ochrony praw człowieka w UE, a więc także w Polsce, są na wysokim poziomie i w przyszłości należy spodziewać się podobnych rozwiązań. Bardziej niepokojące są działania podmiotów komercyjnych, które dysponują ogromnymi bazami danych cyfrowych dotyczących indywidualnych osób. O tym, że pozostają one bez należytego nadzoru świadczy chociażby niedawna afera Cambridge Analytica: poprzez tzw. wyciek

informacji do firmy prywatnych trafiło ponad 87 mln danych użytkowników Facebooka wykorzystanych następnie do celów komercyjnych oraz w akcjach opartych na manipulacji społecznej.

Standardy ochrony praw człowieka w UE, a więc także w Polsce, są na wysokim poziomie (...). Bardziej niepokojące są działania podmiotów komercyjnych, które dysponują ogromnymi bazami danych cyfrowych dotyczących indywidualnych osób.

Warto zastanowić się jeszcze nad wpływem nowych rozwiązań na rachunek ekonomiczny firm działających na rynku usług cyfrowych, szczególnie w branży *cloud computing*. Sektor prywatny skorzystałby zapewne na harmonijnej kooperacji z podmiotami publicznymi w zakresie polityki rozporządzania danymi cyfrowymi. Zasoby przeznaczane dotychczas na rozwiązywanie sporów prawnych i analizowanie odmiennych jurysdykcji pod kątem podejmowanych działań mogłyby zostać przerzucone w kreatywne obszary rozwoju firmy. Poza tym wspólne ramy polityki ochrony danych osobowych zwiększają zaufanie pomiędzy sektorem publicznym i prywatnym, co wpływa korzystnie na środowisko funkcjonowania biznesu.

Jednakże CLOUD Act i podobne rozwiązania prawne mogą generować dodatkowe koszty związane z koniecznością inwestycji we własną infrastrukturę IT. Dostawcy usług internetowych będę zobowiązani w dość krótkim czasie do udzielenia wielu odpowiedzi na zapytania o udostępnienie danych cyfrowych. Oczywistym jest, że bardziej efektywny system zwiększy ilość wniosków zagranicznych służb kierowanych do podmiotów prywatnych. Dostawcy spoza UE będą musieli rozważyć, czy efektywne współdziałanie w przekazywaniu danych nie rodzi konieczności tworzenia specjalnych oddziałów firm na Starym Kontynencie. Szczególnie, że do takich rozwiązań zmierza tzw. dyrektywa NIS oraz transponująca ją niebawem na grunt polski ustawa o cyberbezpieczeństwie.

Budowa nowego modelu dostępu do danych cyfrowych w sprawach karnych może spowodować przetasowania na rynku usług *cloud computing*. Jeśli technologiczni giganci oraz mniejsze przedsiębiorstwa, celem uniknięcia obowiązku udostępniania danych, zaczną w jakimś zakresie emigrować do krajów nieimplementujących planowanych rozwiązań, będzie chodzić zapewne o państwa niedemokratyczne, a nawet autorytarne. Działania takie mogą przybierać zawoalowany charakter, opierać się na zaawansowanych rozwiązaniach teleinformatycznych i wyrafinowanych interpretacjach prawnych. Wszystko po to, aby zwiększyć konkurencyjność firmy na rynku i przedstawić ofertę wzmożonej ochrony danych cyfrowych przed możliwości pozyskiwania ich dla toczącego się śledztwa. Ponieważ część klientów ceni sobie nade wszystko całkowitą prywatność w sieci i jest gotowa dużo za nią zapłacić, nie można wykluczyć, że część firm poszuka terytoriów nieuczestniczących w reformach rynku i niezwiązanych międzynarodowymi umowami do udostępniania danych cyfrowych.

Budowa nowego modelu dostępu do danych cyfrowych w sprawach karnych może spowodować przetasowania na rynku usług cloud computing.

Na chwilę obecną w przypadku Polski i innych krajów Unii Europejskiej korzyści z wprowadzenia CLOUD Act mają czysto potencjalny charakter. Będzie tak aż do czasu ratyfikowania *executive agreement* pomiędzy Stanami Zjednoczonymi i UE w zakresie implementacji postanowień *Clarifying Lawful Overseas Use Data Act*. Podobna umowa ustanawiająca ramy prawne dla wniosków o wydanie danych cyfrowych od amerykańskich potentatów rynku internetowego została już zawarta pomiędzy Amerykanami i Wielką Brytanią. W tym kierunku zmierzają prace Komisji Europejskiej, a podjęta inicjatywa legislacyjna nosi wymowny tytuł: „Improving cross-border access to electronic evidence in criminal matters". Najbliższe lata pokażą, czy słuszne postulaty znajdą odzwierciedlenie w ułatwieniu organom ścigania dostępu do dowodów cyfrowych, a więc przyznaniu walce z cyberprzestępczością jeszcze skuteczniejszych narzędzi.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki jest niezależnym, pozarządowym instytutem naukowo-badawczym (Think Tank) o charakterze non profit, założonym w 2000 r. Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego. Instytut Kościuszki pragnie być liderem pozytywnych przemian, tworzyć i przekazywać najlepsze rozwiązania, również na rzecz sąsiadujących krajów budujących państwo prawa, społeczeństwo obywatelskie i gospodarkę wolnorynkową.

Instytut Kościuszki jest organizatorem Europejskiego Forum Cyberbezpieczeństwa oraz Polskiego Forum Cyberbezpieczeństwa – pierwszych w Polsce oraz jednych z nielicznych w Europie corocznych konferencji poświęconych strategicznym wyzwaniom płynącym z cyberprzestrzeni i dotyczących cyberbezpieczeństwa. Więcej: http://cybersecforum.eu/.

Instytut Kościuszki jest wydawcą European Cybersecurity Journal (ECJ). ECJ to anglojęzyczny kwartalnik ekspercki poświęcony cyberbezpieczeństwu. Zawiera artykuły wiodących analityków i liderów opinii, ekskluzywne wywiady z decydentami oraz monitoring regulacji dotyczących kluczowych aspektów związanych z cyberprzestrzenią. Więcej: http://cybersecforum.eu/czym-jest-ecj/.

Biuro w Krakowie: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: instytut@ik.org.pl

Dalsze informacje i komentarze: Magdalena Bujak, magdalena.bujak@ik.org.pl, tel. +48 12 200 23 69