KOMISJA
EUROPEJSKA

Bruksela, dnia 25.1.2017 r.
COM(2017) 41 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY EUROPEJSKIEJ I RADY

Czwarte sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa

Czwarte sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa

I. WPROWADZENIE

Niniejsze sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa jest czwartym comiesięcznym sprawozdaniem i obejmuje działania w dwóch głównych dziedzinach: *zwalczanie terroryzmu i przestępczości zorganizowanej oraz środków, które je wspierają; oraz wzmocnienie naszej obrony i rozwijanie odporności wobec wymienionych zagrożeń.* Niniejsze sprawozdanie skupia się na czterech kluczowych obszarach: systemach informacyjnych i interoperacyjności, ochronie celów miękkich, zagrożeniach cybernetycznych oraz ochronie danych w kontekście dochodzeń w sprawach karnych.

Grudniowy zamach na kiermaszu bożonarodzeniowym w Berlinie ujawnił ponownie poważne słabości w naszych systemach informacyjnych. Należy im pilnie zaradzić, w szczególności na szczeblu UE, aby wspomóc krajowe organy ochrony granic i organy ścigania w terenie oraz umożliwić im skuteczne wykonywanie ich trudnych obowiązków. Fakt, że różne systemy informacyjne nie są ze sobą powiązane - co pozwala napastnikom na posługiwanie się różnymi tożsamościami i niezauważone przemieszczanie się, w tym przekraczanie granic - oraz że informacje nie są systematycznie wprowadzane przez państwa członkowskie do odpowiednich baz UE, to słabości w praktycznej realizacji unii bezpieczeństwa, którym trzeba szybko zaradzić. Ponadto konieczne są dalsze prace w odniesieniu do środków egzekwowania prawa na granicach oraz powrotów osób, których wnioski o udzielenie azylu zostały odrzucone[1].

Jeśli chodzi o ochronę celów miękkich, Komisja przyspieszy prace prowadzone w celu umożliwienia ekspertom z państw członkowskich wymiany najlepszych praktyk i uzgodnienia standardowych wytycznych.

Zagrożenia cybernetyczne, którym musi sprostać UE, są szeroko komentowane w mediach i w niniejszym sprawozdaniu przedstawiono szereg działań prowadzonych już w tej dziedzinie. Dotyczą one zarówno prewencji - w drodze współpracy z odpowiednią gałęzią przemysłu w celu uwzględniania bezpieczeństwa na etapie projektowania oraz wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji - jak i propagowania współpracy między państwami członkowskimi oraz współpracy z organizacjami międzynarodowymi i partnerami dotyczącej reagowania w momencie ataku cybernetycznego. W nadchodzących miesiącach Komisja oraz Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa ustalą, jakie działania są konieczne do zapewnienia skutecznej reakcji na te zagrożenia na poziomie UE, opierając się na strategii Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego z 2013 r.

Ochrona prywatności osób fizycznych oraz ochrona danych osobowych to szczególnie istotne prawa podstawowe, które stanowią jeden z fundamentów wszelkich działań zmierzających do stworzenia prawdziwej unii bezpieczeństwa. Wspólny wysoki poziom ochrony danych zapewnia dyrektywa o ochronie danych w obszarze działań policji i

[1] W nadchodzących tygodniach Komisja przedstawi zmieniony plan działania w zakresie powrotów, zob. Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady Europejskiej i Rady w sprawie zapewnienia pełnej operacyjności Europejskiej Straży Granicznej i Przybrzeżnej, COM(2017)42.

wymiaru sprawiedliwości w sprawach karnych przyjęta w kwietniu 2016 r., która tym samym ułatwi sprawną wymianę odpowiednich danych między organami ścigania państw członkowskich. Komisja rozpoczęła również przegląd dyrektywy o prywatności i łączności elektronicznej w ramach swojego pakietu dotyczącego danych, aby rozszerzyć zakres dyrektywy na wszystkich dostawców usług łączności elektronicznej oraz ujednolicić jej postanowienia z ogólnym rozporządzeniem o ochronie danych. Wniosek ma na celu zapewnienie prywatności w łączności elektronicznej, a równocześnie określenie powodów, dla których można przewidzieć ograniczenia zakresu rozporządzenia o prywatności i łączności elektronicznej, w tym ze względu na bezpieczeństwo narodowe lub dochodzenia w sprawach karnych.

II. WZMOCNIENIE SYSTEMÓW INFORMACYJNYCH I INTEROPERACYJNOŚCI

W orędziu o stanie Unii wygłoszonym przez przewodniczącego Jeana-Claude'a Junckera we wrześniu 2016 r. oraz w konkluzjach Rady Europejskiej z grudnia 2016 r. podkreślono, jak istotne znaczenie ma likwidacja niedociągnięć w zarządzaniu informacjami oraz poprawa **interoperacyjności istniejących systemów informacyjnych oraz połączeń międzysystemowych**. Niedawne wydarzenia ujawniły pilną potrzebę wzajemnego połączenia istniejących baz danych UE, również po to, aby dać organom ochrony granic i organom ścigania w terenie narzędzia niezbędne do wykrywania oszustw dotyczących tożsamości. Na przykład sprawca, który przeprowadził zamach terrorystyczny w Berlinie w grudniu 2016 r., posługiwał się przynajmniej 14 różnymi tożsamościami i mógł przemieszczać się niezauważony pomiędzy państwami członkowskimi. Wyraźnie widać, że należy umożliwić równoczesne przeszukiwanie istniejących i przyszłych systemów informacyjnych UE pod kątem identyfikatorów biometrycznych, aby odebrać terrorystom i przestępcom taką możliwość.

W związku z tym Komisja rozpoczęła w kwietniu 2016 r. prace nad swoim projektem w sprawie „sprawniejszych i bardziej inteligentnych systemów informacyjnych do celów zarządzania granicami i zapewnienia bezpieczeństwa”[2]. Podczas tych prac stwierdzono niedociągnięcia w funkcjonowaniu istniejących systemów, luki w strukturach zarządzania danymi w UE, problemy wynikające ze skomplikowanej architektury różnie zarządzanych systemów informacyjnych oraz z fragmentaryzacji, której przyczyną jest fakt, że istniejące systemy były projektowane pojedynczo, a nie jako elementy większej całości. W ramach tego procesu Komisja uruchomiła **Grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności** we współpracy z agencjami UE, państwami członkowskimi i odpowiednimi zainteresowanymi podmiotami. W dniu 21 grudnia 2016 r.[3] w sprawozdaniu przewodniczącego określono **wstępne ustalenia** grupy, które obejmują priorytetowy wariant stworzenia jednego portalu służącego do wyszukiwania, który pozwoliłby organom ścigania i organom zarządzania granicami na jednoczesne przeszukiwanie istniejących unijnych baz danych i systemów informacyjnych. We wstępnym sprawozdaniu podkreślono również znaczenie jakości danych - ponieważ skuteczność systemów informacyjnych zależy od jakości i

[2] Komunikat „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” COM(2016)205 final.

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

formatu wprowadzonych do nich danych - oraz zalecono poprawę jakości danych w systemach UE poprzez zautomatyzowaną kontrolę jakości danych.

Komisja szybko podejmie działania następcze w związku z propozycją stworzenia jednego portalu służącego do wyszukiwania i wspólnie z agencją UE ds. zarządzania operacyjnego wielkoskalowymi systemami informatycznymi, eu-LISA, rozpocznie prace nad stworzeniem portalu umożliwiającego równoległe przeszukiwanie wszystkich odpowiednich istniejących systemów UE. Do czerwca powinno być gotowe powiązane badanie, które posłuży jako podstawa do opracowania i testowania prototypu portalu przed końcem roku. Komisja uważa, że równocześnie Europol powinien kontynuować swoje prace nad interfejsem systemu, który pozwoliłby funkcjonariuszom pierwszej linii kontroli w państwach członkowskich na automatyczne sprawdzanie baz Europolu równocześnie ze sprawdzaniem ich własnych krajowych systemów.

Prace w kierunku interoperacyjności systemów informacyjnych mają na celu przezwyciężenie obecnej fragmentaryzacji unijnych struktur związanych z zarządzaniem danymi w celu kontrolowania granic i zapewnienia ich bezpieczeństwa oraz wyeliminowanie powiązanych nieuwzględnionych kwestii. Kiedy bazy danych korzystają ze wspólnego repozytorium danych dotyczących tożsamości - jak przewiduje proponowany system wjazdu/wyjazdu UE oraz proponowany unijny system informacji o podróży oraz zezwoleń na podróż – dana osoba może być zarejestrowana tylko pod jedną tożsamością w różnych bazach danych, co zapobiega posługiwaniu się różnymi fałszywymi tożsamościami. Pierwszym krokiem, który zasugerowano we wstępnych ustaleniach grupy ekspertów wysokiego szczebla, było zwrócenie się przez Komisję do eu-LISA o przeanalizowanie technicznych i operacyjnych aspektów wdrażania wspólnego serwisu kojarzenia danych biometrycznych. Taki serwis mógłby umożliwić przeszukiwanie różnych baz danych zawierających dane biometryczne, co mogłoby ujawnić fałszywe tożsamości, jakimi posługuje się dana osoba w innych systemach. Ponadto grupa ekspertów wysokiego szczebla powinna obecnie ocenić, czy rozszerzenie **wspólnego repozytorium tożsamości** przewidzianego przez system wjazdu/wyjazdu UE i ETIAS na inne systemy jest konieczne, technicznie wykonalne i proporcjonalne. Oprócz danych biometrycznych przechowywanych w serwisie kojarzenia danych biometrycznych, takie wspólne repozytorium tożsamości mogłoby również obejmować alfanumeryczne dane dotyczące tożsamości. Grupa powinna przedstawić swoje ustalenia w tej kwestii w sprawozdaniu końcowym do końca kwietnia 2017 r.

Niedawne wydarzenia zagrażające bezpieczeństwu uwypuklają potrzebę ponownego zbadania kwestii **obowiązkowego udostępniania informacji** pomiędzy państwami członkowskimi. Wniosek Komisji z grudnia 2016 r. dotyczący wzmocnienia **systemu informacyjnego Schengen** przewiduje - po raz pierwszy - obowiązek dokonywania przez państwa członkowskie wpisów dotyczących osób, które mają powiązania z działalnością terrorystyczną. Ważne jest, żeby współprawodawcy podjęli teraz działania zmierzające do szybkiego przyjęcia proponowanych środków. Komisja jest gotowa zbadać, czy ustawowy obowiązek udostępniania informacji powinien zostać wprowadzony w odniesieniu do innych unijnych baz danych.

III. OCHRONA CELÓW MIĘKKICH W EUROPIE PRZED ATAKAMI TERRORYSTYCZNYMI

Zamach w Berlinie to najnowszy atak skierowany przeciwko tak zwanym miękkim celom w UE. Zazwyczaj są nimi obiekty cywilne, w których zbiera się wielu ludzi (np.

przestrzenie publiczne, szpitale, szkoły, stadiony sportowe, ośrodki kultury, kawiarnie i restauracje, centra handlowe i węzły komunikacyjne). Przez swój charakter te miejsca są szczególnie narażone na ataki i trudne do ochrony, charakteryzuje je również duże prawdopodobieństwo masowych ofiar w ludziach w przypadku ataku. Z tych względów terroryści często je wybierają. Zagrożenie kolejnymi atakami na cele miękkie, w tym na transport, pozostaje wysokie, co potwierdzają dostępne analizy, w tym sprawozdanie Europolu na temat zmian w sposobie działania Państwa Islamskiego[4].

W Europejskiej agendzie bezpieczeństwa z 2015 r. oraz w komunikacie z 2016 r. w sprawie unii bezpieczeństwa podkreślono potrzebę intensywniejszych działań w celu poprawy bezpieczeństwa oraz potrzebę wykorzystywania innowacyjnych narzędzi i technologii wykrywania zagrożeń w celu ochrony celów miękkich. Komisja działała na rzecz wspierania państw członkowskich w wymianie najlepszych praktyk oraz zachęcania ich do takiej wymiany w zakresie opracowywania lepszych narzędzi służących zapobieganiu atakom na cele miękkie oraz reagowania na takie ataki. W wyniku tych działań powstały podręczniki operacyjne oraz materiały zawierające wytyczne. Obecnie Komisja jest w trakcie opracowywania w ścisłej współpracy z ekspertami państw członkowskich, kompleksowego podręcznika dotyczącego procedur i modeli ochrony różnych celów miękkich (np. centrów handlowych, szpitali, wydarzeń sportowych i kulturalnych). Celem jest wydanie w 2017 r. wytycznych dla państw członkowskich dotyczących ochrony celów miękkich, opierających się na najlepszych praktykach stosowanych w państwach członkowskich.

Równocześnie Komisja zorganizuje w lutym wspólnie z organami krajowymi pierwsze warsztaty dotyczące ochrony celów miękkich, w celu wymiany informacji i opracowania najlepszych praktyk, które będą dotyczyć złożonej kwestii ochrony celów miękkich oraz bezpieczeństwa publicznego i ochrony. Komisja finansuje również projekt pilotażowy prowadzony przez Belgię, Niderlandy i Luksemburg w ramach Funduszu Bezpieczeństwa Wewnętrznego, którego celem jest stworzenie regionalnego centrum doskonałości w dziedzinie specjalnych interwencji wymiaru sprawiedliwości. Będzie ono oferowało szkolenia dla funkcjonariuszy policji w służbach pierwszego reagowania w przypadku ataku.

Interwencje w przypadku ataków na cele miękkie stanowią podstawowy element działań Komisji w zakresie ochrony ludności. W grudniu Komisja zapowiedziała, jakie działania planuje podjąć z państwami członkowskimi w celu ochrony obywateli UE oraz zmniejszania podatności na zagrożenia w bezpośrednim następstwie ataku terrorystycznego. Działania te poprawią koordynację pomiędzy wszystkimi podmiotami zaangażowanymi w zarządzanie skutkami ataków. Komisja zobowiązała się do wspierania wysiłków państw członkowskich poprzez ułatwianie wspólnych szkoleń i ćwiczeń oraz poprzez zapewnienie stałego dialogu za pośrednictwem krajowych punktów centralnych i grup ekspertów. Komisja będzie również wspierać rozwój wyspecjalizowanych modułów w zakresie reagowania na zamachy terrorystyczne w ramach Unijnego Mechanizmu Ochrony Ludności oraz inicjatywy służące wymianie zdobytych doświadczeń i podnoszeniu świadomości społecznej.

---

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited (Zmiany w sposobie działania Państwa Islamskiego (IS) - ponowna analiza)*, listopad 2016 r. – Publiczna Informacja Europolu, dokument dostępny na stronie: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

Wraz z państwami członkowskimi Komisja zbada również możliwości zmobilizowania środków UE w celu wsparcia budowania odporności oraz wzmocnienia zabezpieczenia potencjalnych celów miękkich. Państwa członkowskie mogłyby również wnioskować o finansowanie z Europejskiego Banku Inwestycyjnego (EBI) (w tym z Europejskiego Funduszu na rzecz Inwestycji Strategicznych) zgodnie z polityką UE i grupy EBI. Każdy projekt podlegałby normalnym procedurom decyzyjnym określonym w przepisach.

Jeśli chodzi o szczególne cele miękkie związane z transportem publicznym, takie jak ogólnodostępne części portów lotniczych lub stacji kolejowych, podczas poświęconych temu tematowi warsztatów zorganizowanych przez Komisję w listopadzie 2016 r. podkreślono konieczność pogodzenia potrzeb w zakresie bezpieczeństwa z wygodą pasażerów oraz usługami transportowymi. We wnioskach podkreślono znaczenie budowania kultury bezpieczeństwa, obejmującej nie tylko personel, ale również pasażerów, znaczenie lokalnych ocen ryzyka stanowiących podstawę ustalania odpowiednich środków zaradczych oraz potrzebę wzmocnienia komunikacji pomiędzy wszystkimi zainteresowanymi stronami.

IV. WYZWANIA ZWIĄZANE Z ZAGROŻENIAMI CYBERNETYCZNYMI

Cyberprzestępczość oraz ataki cybernetyczne to jedne z najważniejszych zagrożeń, w obliczu których stoi Unia. Działanie na szczeblu UE może przyczynić się do wzmocnienia naszej zbiorowej odporności. Każdego dnia wydarzenia naruszające bezpieczeństwo cybernetyczne poważnie szkodzą wielu ludziom i powodują znaczne szkody dla europejskiej gospodarki i przedsiębiorstw. Ataki cybernetyczne stanowią jeden z podstawowych elementów zagrożeń hybrydowych - precyzyjnie zaplanowane w tym samym czasie co przemoc fizyczna, na przykład terroryzm, mogą mieć niszczycielski wpływ. Mogą również przyczyniać się do destabilizacji kraju i podważenia jego instytucji politycznych oraz podstawowych procesów demokratycznych. Ponieważ w coraz większym stopniu polegamy na technologiach internetowych, nasza infrastruktura krytyczna (od szpitali po elektrownie jądrowe) będzie w coraz większym stopniu podatna na zagrożenia.

Strategia Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego z 2013 r. stanowi część podstawowej odpowiedzi politycznej na zagrożenia bezpieczeństwa cybernetycznego. Głównym instrumentem jest dyrektywa w sprawie bezpieczeństwa sieci i informacji (NIS)[5], przyjęta w lipcu zeszłego roku. Określa ona podwaliny lepszej współpracy na szczeblu UE oraz większej odporności cybernetycznej dzięki wspieraniu współpracy i wymiany informacji między państwami członkowskimi i propagowaniu współpracy operacyjnej w związku z konkretnymi incydentami zakłócającymi bezpieczeństwo cybernetyczne, a także za pośrednictwem wymiany informacji o zagrożeniach. Aby zapewnić spójne wdrażanie w różnych sektorach i w różnych państwach, Komisja zorganizuje w lutym pierwsze spotkane grupy współpracy NIS z państwami członkowskimi.

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

W kwietniu 2016 r. Komisja i Wysoki Przedstawiciel przyjęli wspólne ramy w zakresie przeciwdziałania zagrożeniom hybrydowym[6], w których zaproponowano 22 działania operacyjne służące podnoszeniu świadomości, budowaniu odporności, lepszemu reagowaniu na kryzysy oraz zacieśnieniu współpracy pomiędzy UE a NATO. W odpowiedzi na wezwanie Rady Komisja i Wysoki Przedstawiciel przedstawią do lipca 2017 r. sprawozdanie, w którym ocenią osiągnięte postępy.

Komisja propaguje i wspiera również innowacje technologiczne, w tym poprzez wykorzystywanie unijnych środków na badania służące tworzeniu nowych rozwiązań i nowych technologii, które mogą przyczynić się do wzmocnienia naszej odporności wobec ataków cybernetycznych (np. projekty dotyczące uwzględniania bezpieczeństwa na etapie projektowania). W lecie ubiegłego roku uruchomiliśmy z przedstawicielami przemysłu partnerstwa prywatne dotyczące bezpieczeństwa cybernetycznego[7] na kwotę 1,8 mld EUR.

W sektorze transportu cyfryzacja staje się głównym czynnikiem umożliwiającym niezbędną transformację obecnego systemu transportu. Szybkie tempo cyfryzacji przynosi wiele korzyści, ale sprawia także, że transport staje się bardziej podatny na zagrożenia w kontekście bezpieczeństwa cybernetycznego. Podejmowanych jest wiele działań, które mają złagodzić te zagrożenia na różnych szczeblach, szczególnie w transporcie lotniczym, ale również morskim, rzecznym, kolejowym oraz drogowym[8]. Wyzwaniem pozostaje dalsze doprecyzowanie, zharmonizowanie oraz uzupełnienie działań różnych zainteresowanych stron zaangażowanych we wzmacnianie różnych aspektów odporności cybernetycznej.

Biorąc pod uwagę szybko zmieniający się charakter zagrożeń, w nadchodzących miesiącach Komisja oraz Wysoki Przedstawiciel ustalą, jakie działania są konieczne do zapewnienia skutecznej reakcji na te zagrożenia na poziomie UE, opierając się na strategii Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego z 2013 r.

V. OCHRONA DANYCH OSOBOWYCH PRZY JEDNOCZESNYM WSPIERANIU SKUTECZNYCH DOCHODZEŃ W SPRAWACH KARNYCH

Dyrektywa o ochronie danych w obszarze działań policji i wymiaru sprawiedliwości w sprawach karnych[9] stanowi jeden z podstawowych elementów walki z terroryzmem i

---

6 JOIN (2018)18.

7 Ogłoszone w komunikacie dotyczącym wzmacniania europejskiego systemu odporności cybernetycznej z 2016 r., COM(2016)410 final.

8 Przykładem są tu międzynarodowe wytyczne, takie jak te opracowane przez Międzynarodową Organizację Morską lub w drodze niedawno przyjętej rezolucji ICAO, ze wspólną inicjatywą UE i USA; informowanie o incydentach (Europejska Agencja Bezpieczeństwa Lotniczego opracowuje obecnie model pozwalający szybciej reagować), oraz uwzględnianie bezpieczeństwa cybernetycznego na etapie projektowania, stosowane do nowych tworzonych systemów, takich jak centralny plan zarządzania ruchem lotniczym opracowywany przez Wspólne Przedsięwzięcie SESAR.

9 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych

poważną przestępczością. W oparciu o wspólną normę ochrony danych określoną w dyrektywie, organy egzekwowania prawa w państwach członkowskich będą mogły w łatwy sposób wymieniać odpowiednie dane, podczas gdy dane ofiar, świadków i podejrzanych o popełnienie przestępstw będą należycie chronione.

Ponadto, aby zapewnić wysoki poziom poufności komunikacji zarówno dla osób fizycznych, jak i dla przedsiębiorstw oraz równe warunki działania dla wszystkich uczestników rynku, jak określono w strategii jednolitego rynku cyfrowego z kwietnia 2015 r., Komisja przyjęła dnia 11 stycznia[10] projekt dotyczący **rozporządzenia o ochronie prywatności** (zastępującego dyrektywę 2002/58/WE). Podobnie jak dotychczasowa dyrektywa, zmienione rozporządzenie o prywatności i łączności elektronicznej doprecyzowuje ogólne rozporządzenie o ochronie danych[11] oraz określa ramy regulujące ochronę prywatności i danych osobowych w sektorze łączności elektronicznej.

Dzięki zmienionemu rozporządzeniu wszystkie dane łączności elektronicznej, nawet jeśli jest to komunikacja dodatkowa, są uważane za poufne – niezależnie od tego, czy komunikacja odbywa się za pośrednictwem tradycyjnych usług telekomunikacyjnych czy innych tzw. usług OTT, które mają podobny zakres (np. Skype i WhatsApp) i z których wielu użytkowników korzysta wymiennie z usługami normalnych operatorów telekomunikacyjnych[12]. Zobowiązania nałożone na usługodawców - oprócz poszanowania wyborów klientów dotyczących prywatności podczas wykorzystywania, przechowywania i przetwarzania ich danych - obejmują również wymóg mianowania przedstawiciela w państwie członkowskim w przypadku dostawców usług z siedzibą poza UE . Pozwoli to państwom członkowskim na łatwiejszą współpracę organów ścigania i organów wymiaru sprawiedliwości z dostawcami usług w celu dostępu do dowodów elektronicznych (zob. poniżej).

Podobnie jak w obecnych przepisach o ochronie prywatności w sieci, dostęp organów ścigania i organów wymiaru sprawiedliwości do odpowiednich informacji elektronicznych niezbędnych do prowadzenia dochodzeń w sprawach karnych będzie regulowany za pomocą wyłączenia określonego w art. 11 proponowanego rozporządzenia o prywatności i łączności elektronicznej[13]. Przepis ten przewiduje możliwość ograniczenia poufności komunikacji w prawie UE lub prawie krajowym, gdy

---

oraz uchylająca decyzję ramową Rady 2008/977/WSiSW. Dyrektywa, obowiązująca od dnia 5 maja 2016 r., ma zostać transponowana przez państwa członkowskie do dnia 6 maja 2018 r. Komisja powołała wraz z państwami członkowskimi grupę ekspertów, która będzie stanowić forum wymiany poglądów na temat transpozycji dyrektywy o ochronie danych w obszarze działań policji.

10 Rozporządzenie o prywatności i łączności elektronicznej COM(2017) 10.

11 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych), które wejdzie w życie dnia 15 maja 2018 r.

12 Jest to zgodne z podejściem przyjętym we wniosku dotyczącym dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej, przedstawionym przez Komisję w dniu 14 września 2016 r. (pakiet Telecoms), COM(2016)590 final.

13 Zob. art. 11 ust. 1, klauzula „zatrzymywania danych", niezmieniona w stosunku do art. 15 dyrektywy o prywatności i łączności elektronicznej oraz dostosowana do wymogów ogólnego rozporządzenia o ochronie danych. Takie ograniczenie musi przestrzegać idei praw podstawowych oraz być niezbędne, odpowiednie i proporcjonalne.

jest to niezbędne i proporcjonalne, w celu ochrony bezpieczeństwa narodowego, obrony, ochrony bezpieczeństwa publicznego i zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych i wykonywania kar. Przepis ten ma szczególne znaczenie dla krajowych przepisów dotyczących **zatrzymywania danych**, tj. dla nakładania na dostawców usług telekomunikacyjnych obowiązku przechowywania danych dotyczących łączności przez określony okres w celu ewentualnego udostępnienia ich organom ścigania, w następstwie uchylenia przez Trybunał Sprawiedliwości dyrektywy w sprawie zatrzymywania danych w 2014 r.[14]. Od tego czasu nie istnieje unijny instrument regulujący zatrzymywanie danych, a niektóre państwa członkowskie przyjęły własne krajowe przepisy dotyczące zatrzymywania danych. Szwedzkie i brytyjskie przepisy o zatrzymywaniu danych zostały zakwestionowane przed Trybunałem Sprawiedliwości, który wydał swój wyrok *Tele2* w dniu 21 grudnia[15]. Trybunał Sprawiedliwości stwierdził, że przepisy krajowe, które - w celu zwalczania przestępczości - przewidują ogólne i masowe zachowywanie wszystkich danych o połączeniach i lokalizacji abonentów i użytkowników dotyczące wszystkich środków komunikacji elektronicznej, są niezgodne z prawem UE. Konsekwencje tego wyroku są obecnie analizowane, a Komisja opracuje wytyczne, w jaki sposób krajowe przepisy o zatrzymywaniu danych mogą być konstruowane zgodnie z wyrokiem.

Przestępstwa pozostawiają ślady cyfrowe, które mogą stanowić dowód w postępowaniach sądowych; łączność elektroniczna między podejrzanymi często jest jedynym tropem, który mogą wykorzystać organy ścigania i prokuratorzy. Jednak uzyskanie dostępu do **dowodów elektronicznych** – zwłaszcza jeśli są przechowywane za granicą lub w chmurze – może być skomplikowane technicznie i prawnie, a ponadto często jest uciążliwe proceduralnie, co uniemożliwia śledczym niezbędne szybkie działanie. Aby zniwelować te problemy, Komisja analizuje obecnie rozwiązania, które pozwolą śledczym na otrzymywanie transgranicznych dowodów elektronicznych, w tym na skuteczniejszą wzajemną pomoc prawną, na znalezienie sposobów bezpośredniej współpracy z dostawcami usług internetowych oraz na zaproponowanie kryteriów służących ustalaniu właściwości sądów oraz jej wykonywania w cyberprzestrzeni, w pełnej zgodności z obowiązującymi przepisami o ochronie danych.[16]W dniu 9 grudnia 2016 r. Komisja zdała raport z osiągniętych postępów Radzie ds. Sprawiedliwości i Spraw Wewnętrznych[17].

Kompleksowy (i nadal się toczący) proces konsultacji eksperckich pozwolił Komisji na określenie różnych, często złożonych problemów wynikających z dostępu do dowodów elektronicznych, na lepsze zrozumienie obowiązujących przepisów i praktyk w państwach członkowskich, oraz na określenie możliwych wariantów politycznych. Sprawozdanie z postępu prac zawiera przegląd propozycji, które pojawiły się dotychczas w trakcie zbierania informacji oraz w procesie konsultacji eksperckich. Komisja przeanalizuje je dokładniej w nadchodzących miesiącach, we współpracy z

---

[14] Wyrok Trybunału Sprawiedliwości w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland* z dnia 8 kwietnia 2014 r.

[15] Wyrok Trybunału Sprawiedliwości w sprawach połączonych C-203/15 i C-698/15 *Tele2* z dnia 21 grudnia 2016 r.

[16] Zgodnie ze zobowiązaniem podjętym w Europejskiej agendzie bezpieczeństwa, COM(2015)185 final, oraz komunikacie Komisji pt. Realizacja Europejskiej agendy bezpieczeństwa w celu zwalczania terroryzmu i utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa, COM(2016)230 final.

[17] W swoich konkluzjach dotyczących usprawnienia wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni z dnia 9 czerwca 2016 r., Rada wezwała Komisję do podjęcia konkretnych działań, opracowania wspólnego unijnego podejścia oraz przedstawienia rezultatów do czerwca 2017 r.

zainteresowanymi podmiotami. Jak ogłoszono w programie prac Komisji, Komisja przedstawi inicjatywę w tej dziedzinie w 2017 r.

VI. WNIOSEK

Kolejne sprawozdanie, którego termin wyznaczono na 1 marca, będzie okazją do przeglądu postępów we wdrażaniu tych i innych kluczowych założeń.