KOMISJA
EUROPEJSKA

Bruksela, dnia 18.10.2017r.
COM(2017) 608 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY EUROPEJSKIEJ I RADY

Jedenaste 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 jedenastym comiesięcznym sprawozdaniem i obejmuje działania w dwóch głównych dziedzinach: zwalczanie terroryzmu i przestępczości zorganizowanej oraz środków, które wspierają występowanie tych zjawisk, oraz wzmocnienie naszej obrony i budowanie odporności wobec wymienionych zagrożeń.

Przewodniczący Jean-Claude Juncker w orędziu o stanie Unii[1] podkreślił, że Unia Europejska musi być silniejsza w walce z terroryzmem, wykorzystując faktyczne postępy dokonane w ciągu ostatnich trzech lat. Jak zapowiedziano w liście intencyjnym[2] skierowanym do Parlamentu Europejskiego i prezydencji Rady oraz w towarzyszącym mu planie działania na rzecz bardziej zjednoczonej, silniejszej i demokratyczniejszej Unii, w niniejszym sprawozdaniu Komisja przedstawia **pakiet środków antyterrorystycznych**, które mają zostać podjęte w ciągu najbliższych szesnastu miesięcy. Wspomniane środki operacyjne pomogą państwom członkowskim wyeliminować istotne słabe punkty obnażone podczas ostatnich ataków terrorystycznych i rzeczywiście sprawią, że zwiększy się poziom bezpieczeństwa. Przyczyni się to do stworzenia kompletnej unii bezpieczeństwa, w której terroryści nie będą już mogli wykorzystywać luk w celu popełniania okrutnych zbrodni. Oprócz tych praktycznych krótkoterminowych środków Komisja pracuje nad utworzeniem w przyszłości europejskiej jednostki wywiadu zgodnie z zapowiedzią przewodniczącego Junckera w ramach jego wizji Unii Europejskiej do 2025 r.

Pakiet środków antyterrorystycznych obejmuje:

- środki mające wspierać państwa członkowskie w **ochronie przestrzeni publicznej** (rozdział II), w tym plan działania dotyczący wspierania ochrony przestrzeni publicznej oraz plan działania dotyczący zwiększenia gotowości na wypadek zagrożenia w zakresie bezpieczeństwa chemicznego, biologicznego, radiologicznego i jądrowego;
- środki dotyczące **odcięcia dostępu do środków wykorzystywanych przez terrorystów** w celu przygotowywania i przeprowadzania ataków, takich jak **substancje niebezpieczne** lub **finansowanie terroryzmu** (rozdział III), w tym zalecenie w sprawie podjęcia niezwłocznych kroków, by zapobiec czynieniu niewłaściwego użytku z prekursorów materiałów wybuchowych, a także środków wspierających organy ścigania i organy sądowe, gdy w trakcie dochodzenia stwierdzą one **stosowanie szyfrowania**;
- kolejne kroki w zakresie **przeciwdziałania radykalizacji postaw** (rozdział IV);
- kolejne kroki w zakresie wzmocnienia **zewnętrznego wymiaru** walki z terroryzmem (rozdział V), w tym wnioski dotyczące decyzji Rady w sprawie zawarcia, w imieniu Unii Europejskiej, Konwencji Rady Europy o zapobieganiu terroryzmowi i protokołu do tej konwencji, a także zalecenia Rady dotyczącego upoważnienia do rozpoczęcia negocjacji na temat zmiany umowy z Kanadą w sprawie danych dotyczących przelotu pasażera.

[1] http://europa.eu/rapid/press-release_SPEECH-17-3165_pl.htm.
[2] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_pl.pdf.

II. ŚRODKI NA RZECZ POPRAWY OCHRONY I ODPORNOŚCI WOBEC TERRORYZMU

1. Zwiększona ochrona przestrzeni publicznej

W swoich przekazach propagandowych i przy wyborze celów terroryści koncentrują się raczej na przestrzeni publicznej, takiej jak strefy ruchu pieszego, miejsca turystyczne, węzły transportowe, centra handlowe, sale koncertowe i place miejskie, o czym świadczą ataki dokonane np. w Barcelonie, Berlinie, Brukseli, Londynie, Manchesterze, Nicei, Paryżu i Sztokholmie. Wspólną cechą tych wszystkich tzw. miękkich celów jest ich otwarty i publiczny charakter, a także duże skupiska ludzi, co sprawia, że są oni naturalnie narażeni na zagrożenia.

Możemy uczynić więcej, by zmniejszyć podatność tych miejsc na zagrożenia, wykrywać zagrożenia na wcześniejszym etapie i zwiększyć odporność. Dlatego w **planie działania dotyczącym ochrony przestrzeni publicznej**[3], przedstawionym wraz z niniejszym sprawozdaniem, Komisja określiła środki na rzecz wsparcia państw członkowskich na poziomie krajowym, regionalnym i lokalnym w ich dążeniach do zwiększenia ochrony fizycznej przed zagrożeniami terrorystycznymi. Choć „zerowe ryzyko" jest niemożliwe, plan działania ma na celu wspieranie państw członkowskich w wykrywaniu zagrożeń, zmniejszaniu podatności przestrzeni publicznej na zagrożenia, łagodzeniu konsekwencji ataku terrorystycznego i poprawie współpracy.

UE może udzielać wsparcia na rzecz ochrony przestrzeni publicznej w dwojaki sposób. Po pierwsze, może wspierać **wymianę najlepszych praktyk w wymiarze transgranicznym, m.in. poprzez finansowanie**. Obejmuje to na przykład środki promujące i wspierające rozwój innowacyjnych i dyskretnych barier mających chronić miasta, ale nie wpływających na otwarty charakter miast (ochrona już na etapie projektowania). W celu finansowego wsparcia środków przedstawionych w planie działania Komisja ogłosiła zaproszenie do składania wniosków w ramach Funduszu Bezpieczeństwa Wewnętrznego – części dotyczącej współpracy policyjnej – na łączną kwotę wynoszącą 18,5 mln EUR. To finansowanie krótkoterminowe zostanie uzupełnione w 2018 r. w postaci finansowania w ramach innowacyjnych działań miejskich finansowanych z Europejskiego Funduszu Rozwoju Regionalnego, gdzie głównym tematem będzie bezpieczeństwo, a łączne finansowanie wyniesie maks. 100 mln EUR. Konsultacje publiczne rozpoczęły się dnia 15 września 2017 r. Ich celem jest wymiana przez miasta pomysłów dotyczących innowacyjnych rozwiązań w zakresie bezpieczeństwa. Pomoże to Komisji w opracowaniu planowanych zaproszeń do składania wniosków w tym obszarze.

Po drugie, UE może wzmocnić **współpracę z szeroką grupą zainteresowanych podmiotów**, co ma zasadnicze znaczenie dla poprawy ochrony przestrzeni publicznej. Należy lepiej zorganizować wymianę doświadczeń i łączenie zasobów. Komisja powoła forum, by nawiązać kontakty z podmiotami prywatnymi, takimi jak centra handlowe, organizatorzy koncertów, areny sportowe, hotele i wypożyczalnie samochodów. Ułatwi to szerzenie wiedzy na temat bieżących wyzwań w zakresie bezpieczeństwa i zachęci partnerstwa publiczno-prywatne zajmujące się kwestiami bezpieczeństwa do zadbania o wyższy poziom ochrony. Również organy lokalne i regionalne mają do odegrania fundamentalną rolę w kwestii

[3] COM(2017) 612 final z 18.10.2017.

ochrony przestrzeni publicznej i konieczne jest powiązanie ich z odnośnymi działaniami na poziomie unijnym. Komisja zwiększy zaangażowanie tych zainteresowanych podmiotów i zainicjuje dialog z przedstawicielami organów lokalnych i regionalnych, m.in. z burmistrzami większych miast, w celu wymiany informacji i najlepszych praktyk w dziedzinie ochrony przestrzeni publicznej. W następstwie deklaracji z Nicei[4] z dnia 29 września 2017 r. na początku przyszłego roku Komisja planuje zorganizować wspólnie z Komitetem Regionów spotkanie wysokiego szczebla z udziałem burmistrzów, którzy podpisali wspomnianą deklarację, i z innymi zainteresowanymi przedstawicielami władz lokalnych i regionalnych, by kontynuować wymianę najlepszych praktyk w dziedzinie ochrony przestrzeni publicznej.

Komisja będzie także dalej działała na rzecz ochrony i odporności **infrastruktury krytycznej**. W kompleksowej ocenie polityki bezpieczeństwa UE[5] zwrócono ponadto uwagę na konieczność przystosowania europejskiego programu ochrony infrastruktury krytycznej[6] do pojawiających się zagrożeń. Komisja rozpoczęła ocenę dyrektywy[7] w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej. W ocenie uwzględnione zostaną wyciągnięte wnioski i zmiany, jakie zaszły w ostatnich latach, np. przyjęcie dyrektywy w sprawie bezpieczeństwa sieci i informacji[8]. W międzyczasie udoskonalano europejski program ochrony infrastruktury krytycznej poprzez uwzględnienie w nim pojawiających się wyzwań takich jak zagrożenia wewnętrzne i zagrożenia hybrydowe oraz poszerzenie zewnętrznego zasięgu programu za sprawą współpracy z państwami sąsiadującymi we wschodnim sąsiedztwie i na Bałkanach Zachodnich.

Przez wiele lat celem ataków terrorystycznych, jak i narzędziem do przeprowadzania takich ataków był sektor transportowy (np. porwane samoloty lub taranowanie przechodniów za pomocą ciężarówek). W obliczu tych ataków konieczna jest ocena, w jakim stopniu przepisy **bezpieczeństwa transportu** zapewniają bezpieczeństwo, a jednocześnie gwarantuja istnienie sieci transportowych o płynnym ruchu. Sektor powietrzny jest znacznie lepiej chroniony, więc w atakach terrorystycznych obiera się coraz bardziej oportunistyczne podejście i coraz częściej ich celem jest przestrzeń publiczna. I tak celem wysokiego ryzyka jest m.in. **transport kolejowy**, gdyż związana z nim infrastruktura jest ze swojej natury otwarta. Obecnie nie ma unijnych ram prawnych regulujących kwestię ochrony kolejowego transportu pasażerskiego przed terroryzmem i poważnymi przestępstwami. Dnia 15 czerwca 2017 r. Komisja przystąpiła wraz z państwami członkowskimi do wspólnej oceny ryzyka transportu

---

4 Deklaracja z Nicei została przyjęta na konferencji burmistrzów regionu eurośródziemnomorskiego, która odbyła się w Nicei dnia 29 sierpnia 2017 r. z inicjatywy mera Nicei, z udziałem przedstawicieli Komisji. Konferencja miała na celu wymianę najlepszych praktyk na poziomie miast, a także poziomie lokalnym i regionalnym, na temat zapobiegania radykalizacji postaw i ochrony przestrzeni publicznej. http://www.nice.fr/uploads/media/default/0001/15/TERRORISME%20EUROPE%20Déclaration%20-%20der%20version.pdf.

5 Zob. Dziewiąte sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2017) 407 final z 26.7.2017) oraz załączony dokument roboczy służb Komisji (SWD(2017) 278 final).

6 W europejskim programie ochrony infrastruktury krytycznej (EPCIP) przedstawiono ramy działań UE mających na celu poprawę ochrony infrastruktury krytycznej w Europie: we wszystkich państwach członkowskich i wszystkich odnośnych sektorach działalności gospodarczej. Kluczową podstawą tych prac jest dyrektywa w sprawie europejskiej infrastruktury krytycznej z 2008 r. (dyrektywa 2008/114/WE z 8.12.2008).

7 Dyrektywa 2008/114/WE z 8.12.2008.

8 Dyrektywa (UE) 2016/1148 z 6.7.2016.

kolejowego i pracuje nad dalszymi środkami, by poprawić bezpieczeństwo pasażerskiego transportu kolejowego. Komisja opracowuje ponadto wytyczne dotyczące najlepszych praktyk w dziedzinie bezpieczeństwa dla sektora komercyjnego **transportu drogowego**. Główny nacisk położony będzie na poprawę bezpieczeństwa ciężarówek przez ograniczenie zagrożenia polegającego na nieuprawnionym dostępie do ciężarówek, np. porwaniu lub kradzieży przez terrorystów w celu dokonania ataku w postaci staranowania przechodniów. Wytyczne będą dostępne przed końcem 2017 r. i będą skierowane do przedstawicieli krajowych sektorów transportu drogowego. Komisja będzie ponadto kontynuowała prace nad poprawą **bezpieczeństwa transportu morskiego**, zwłaszcza nad wzmocnieniem ochrony infrastruktury związanej z transportem morskim, w tym portów i obiektów portowych, kontenerowców i statków pasażerskich, np. statków do rejsów wycieczkowych i promów.

2. Zwiększenie gotowości na wypadek zagrożenia w zakresie bezpieczeństwa chemicznego, biologicznego, radiologicznego i jądrowego

Choć prawdopodobieństwo ataków z użyciem substancji chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ) jest w UE nadal niskie, tego rodzaju zagrożenie generalnie się rozwija. Istnieją przesłanki, by sądzić, że niektórzy przestępcy lub grupy terrorystyczne mogą mieć zamiar nabycia materiałów CBRJ, a także zdobycia wiedzy i zdolności, by wykorzystywać je do celów terrorystycznych. W propagandzie terrorystycznej wiele się mówi o możliwości ataków przy użyciu materiałów CBRJ. Także w kompleksowej ocenie polityki bezpieczeństwa UE[9] wskazano na konieczność zwiększenia gotowości na wypadek wystąpienia tych zagrożeń.

By lepiej przygotować się do stawiania czoła zagrożeniom CBRJ w nadchodzących latach, Komisja przedstawia wraz z niniejszym sprawozdaniem **plan działania mający poprawić gotowość na wypadek zagrożenia w zakresie bezpieczeństwa chemicznego, biologicznego, radiologicznego i jądrowego**[10]. Plan ten przewiduje szereg środków mających zwiększyć gotowość, poprawić odporność i koordynację na poziomie UE, np. stworzenie unijnej sieci bezpieczeństwa CBRJ, która zrzeszałaby wszystkie podmioty zajmujące się tematyką ataków CBRJ. Wsparcie dla sieci będzie oferowało m.in. centrum wiedzy na temat ataków CBRJ utworzone przy Europejskim Centrum ds. Zwalczania Terroryzmu (ECTC), które działa w ramach Europolu. Ważne jest także, by optymalniej korzystać z dostępnych zasobów, w związku z czym w planie działania proponuje się poprawę gotowości na wypadek ataków CBRJ i zdolności reagowania na takie ataki przez organizowanie szkoleń i ćwiczeń z udziałem wszystkich różnych służb pierwszego reagowania (zajmujących się egzekwowaniem prawa, ochroną ludności, zdrowiem) i w stosownych przypadkach partnerów wojskowych i prywatnych. Wsparciem dla sieci będą również istniejące narzędzia na poziomie UE, zwłaszcza Unijny Mechanizm Ochrony Ludności[11] i Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL). By zapewnić lepsze wsparcie na wypadek ataku CBRJ, państwa członkowskie powinny w dalszym ciągu wzmacniać istniejącą europejską zdolność reagowania kryzysowego w ramach wspomnianego mechanizmu ochrony ludności. W tym kontekście zachęca się państwa członkowskie do deklarowania nowych zdolności.

---

9 Zob. Dziewiąte sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2017) 407 final z 26.7.2017) oraz załączony dokument roboczy służb Komisji (SWD(2017) 278 final).

10 COM(2017) 610 final z 18.10.2017.

11 Decyzja 1313/2013 z 17.12.2013.

Przepisy Unii dotyczące **poważnych transgranicznych zagrożeń zdrowia**[12] zapewniają gotowość, nadzór i koordynację w sytuacjach kryzysowych związanych ze zdrowiem w całej UE. W tym kontekście unijny system wczesnego ostrzegania i reagowania będzie lepiej powiązany z innymi systemami ostrzegania, jakie UE stosuje na wypadek zagrożeń biologicznych, chemicznych, środowiskowych i innych niezidentyfikowanych zagrożeń. W ramach programu w dziedzinie zdrowia finansuje się także przeprowadzane na obszarze całej UE ćwiczenia z zakresu gotowości na wypadek sytuacji wyjątkowej i reagowania na takie sytuacje oraz wspólne działania wspierające państwa członkowskie w ich staraniach na rzecz wzmocnienia zdolności z zakresu laboratoriów, szczepień oraz podstawowych zdolności zgodnie z międzynarodowymi przepisami w dziedzinie zdrowia.

Wszystkie inicjatywy otrzymają wsparcie w postaci dedykowanych prac badawczych, finansowania i współpracy ze stosownymi partnerami międzynarodowymi.

III. ZWALCZANIE ŚRODKÓW WSPIERAJĄCYCH TERRORYZM

1. Finansowanie terroryzmu: transgraniczny dostęp do informacji finansowych

Informacje o finansowych działaniach osób podejrzanych o terroryzm mogą dostarczyć ważnych wskazówek w trakcie dochodzenia antyterrorystycznego. Z uwagi na wiarygodność i dokładność danych finansowych (w tym danych na temat transakcji finansowych) dane te mogą one być pomocne przy identyfikowaniu terrorystów, znajdowaniu powiązań ze wspólnikami, ustalaniu, jak podejrzani działają, jak wygląda ich logistyka i przemieszczanie się, a także przy rozpracowywaniu sieci terrorystycznych. Szybki ogląd finansowych działań podejrzanych i ich wspólników może zapewnić organom ścigania kluczowe informacje dla przeciwdziałania atakom lub reagowania w następstwie dokonanego ataku. Nowe problemy stwarza coraz bardziej powszechne zjawisko polegające na dokonywaniu prowizorycznych ataków na małą skalę; elementy wskazujące na próby i plany ataków mogą być mniej oczywiste, gdy takie ataki planuje się z krótkim wyprzedzeniem. Transakcje finansowe związane z planowanymi atakami na małą skalę mogą nie wydawać się podejrzane, co w rezultacie powoduje, że takie informacje są przekazywane właściwym organom dopiero po ataku.

Zgodnie z zapowiedzią w planie działania w sprawie finansowania terroryzmu z 2016 r.[13] **Komisja analizuje obecnie konieczność zastosowania dodatkowych środków**, by ułatwić dostęp do informacji finansowych będących w posiadaniu innych jurysdykcji na terenie UE do celów dochodzeń antyterrorystycznych. W trzecim sprawozdaniu z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa z grudnia 2016 r.[14] Komisja przedstawiła swoją wstępną analizę i stwierdziła, że będzie kontynuowała ocenę, biorąc szczególnie pod uwagę ewentualny wpływ na prawa podstawowe, a zwłaszcza prawo do ochrony danych osobowych. Od tamtej pory Komisja prowadzi konsultacje z zainteresowanymi podmiotami i analizuje mechanizmy, za pomocą których właściwe organy mogą obecnie uzyskać dostęp do istotnych informacji, zwłaszcza danych finansowych, jakimi dysponują państwa członkowskie, przeszkody uniemożliwiające szybkie i skuteczne działanie w tym celu oraz ewentualne środki, by wyeliminować takie przeszkody.

---

12 Decyzja 1082/2013/UE z 22.10.2013.
13 COM(2016) 50 final z 2.2.2016.
14 COM(2016) 831 final z 21.12.2016.

Poza bieżącą oceną Komisja w dalszym ciągu promuje **wymianę najlepszych praktyk** dotyczących technik dochodzeniowych i analiz metod, jakich terroryści używają do gromadzenia i przenoszenia środków finansowych, m.in. udziela wsparcia finansowego w wysokości 2,5 mln EUR na podstawie ogłoszonego dzisiaj zaproszenia do składania wniosków.

W tym kontekście Komisja bada także, jak **usprawnić współpracę między jednostkami analityki finansowej**[15], które zostały powołane w celu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, ich wykrywania i skutecznego zwalczania. W sprawozdaniu z grudnia 2016 r. sporządzonym przez jednostki analityki finansowej i powiązanym dokumencie roboczym służb Komisji na temat usprawnienia współpracy między jednostkami analityki finansowej[16] podkreślono liczne ograniczenia w uprawnieniach krajowych nadanych tym jednostkom, a także przedstawiono następujące rozwiązania tych problemów: i) wdrożenie czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy[17] wraz ze zmianami[18], które są obecnie przedmiotem negocjacji; ii) inne inicjatywy podjęte przez unijną platformę skupiającą jednostki analityki finansowej w celu usprawnienia współpracy operacyjnej, szczególnie za pomocą wytycznych, standaryzacji prac i rozwiązań operacyjnych, które mają zostać wdrożone w ramach sieci jednostek analityki finansowej FIU.Net; oraz iii) środki regulacyjne w celu rozwiązania innych kwestii wynikających z różnego statusu i rozbieżnych kompetencji jednostek analityki finansowej, zwłaszcza w celu ułatwienia koordynacji i wymiany informacji między samymi jednostkami, a także między jednostkami analityki finansowej i organami ścigania.

Trwają również prace nad ułatwieniem **dostępu do danych finansowych w poszczególnych państwach członkowskich**. Wnioskowane zmiany do **czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy**[19], będące obecnie przedmiotem negocjacji ze współustawodawcami, doprowadziłyby do ustanowienia scentralizowanych rejestrów rachunków bankowych lub systemów odzyskiwania danych we wszystkich państwach członkowskich, do których dostęp miałyby jednostki analityki finansowej i inne właściwe organy odpowiadające za przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu. Takie rejestry, jak tylko powstaną we wszystkich państwach członkowskich, ułatwią wykrywanie danych o rachunkach. W oparciu o te działania Komisja pracuje obecnie nad inicjatywą dotyczącą **poszerzenia dostępu organów ścigania do takich rejestrów rachunków bankowych**[20], by wzmocnić zdolność tych organów w zakresie szybszego wykrywania rachunków bankowych.

W trakcie konsultacji z zainteresowanymi podmiotami podniesiono także kwestię **przeszkód w uzyskiwaniu danych na temat transakcji finansowych, będących w posiadaniu innych**

---

15 Jednostki analityki finansowej zostały powołane na mocy decyzji Rady 2000/642/WSiSW z dnia 17 października 2000 r. Ich funkcjonowanie reguluje także dyrektywa 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu Pod względem operacyjnym są one niezależne i autonomiczne. Odpowiadają za gromadzenie i analizowanie sprawozdań o podejrzanych transakcjach i innych informacji dotyczących prania pieniędzy, powiązanych z nimi przestępstw źródłowych lub finansowania terroryzmu przez odnośne podmioty, a także za przekazywanie właściwym organom wyników swoich analiz i wszelkich stosownych informacji.

16 SWD(2017)275 final z 26.6.2017.

17 Dyrektywa (UE) 2015/849 z 20.5.2015.

18 COM(2016) 450 final z 5.7.2016.

19 COM(2016) 450 final z 5.7.2016.

20 http://ec.europa.eu/info/law/better-regulation/initiatives/Ares-2017-3971182.

państw członkowskich. W stosownych przypadkach państwa członkowskie mogą wymieniać między sobą informacje o rachunkach bankowych za pomocą kanałów współpracy policyjnej w ciągu ośmiu godzin[21]. Dostęp do danych na temat transakcji finansowych, będących w posiadaniu innych państw członkowskich, można również ułatwić za pośrednictwem jednostek analityki finansowej. Jeśli tego rodzaju informacje są niezbędne jako dowód w procesie karnym, może zaistnieć konieczność wnioskowania o nie w ramach wzajemnej pomocy prawnej. Europejski nakaz dochodzeniowy[22] daje nowe możliwości uzyskiwania danych o transakcjach finansowych w znacznie szybszy sposób niż w ramach wzajemnej pomocy prawnej. Do tej pory, kilka miesięcy po terminie transpozycji do prawa krajowego, tylko 16 państw członkowskich dokonało transpozycji europejskiego nakazu dochodzeniowego. Pozostałe państwa członkowskie wzywa się do dokonania tego bez dalszej zwłoki. Zapowiadane na początek 2018 r. wnioski ustawodawcze w sprawie dowodów elektronicznych również przyczynią się do ułatwienia dostępu transgranicznego do takich danych.

W konsultacjach z zainteresowanymi podmiotami zwrócono także uwagę na **przeszkody utrudniające wykrywanie danych o transakcjach finansowych, będących w posiadaniu innych państw członkowskich**. W ramach działań mających zniwelować te przeszkody oraz w ramach bieżącej oceny Komisja oceni konieczność, wykonalność pod względem technicznym oraz proporcjonalność połączenia scentralizowanych rejestrów rachunków bankowych, biorąc pod uwagę wszystkie istniejące i planowane instrumenty, które ułatwiają dostęp do danych o transakcjach finansowych, będących w posiadaniu innych państw członkowskich.

W tym celu Komisja będzie **kontynuowała konsultacje ze wszystkimi zainteresowanymi podmiotami** na temat konieczności, technicznej wykonalności oraz proporcjonalności ewentualnych nowych środków na poziomie Unii w celu ułatwienia i przyspieszenia dostępu transgranicznego do danych o transakcjach finansowych, w tym na temat procedur zapewniających poufność. Komisja podsumuje wyniki trwających ocen dotyczących wykorzystywania informacji finansowych do celów dochodzeń antyterrorystycznych i w listopadzie 2017 r. zorganizuje spotkanie na wysokim szczeblu z udziałem zainteresowanych podmiotów. Kluczowe kwestie do omówienia to:

- główne przeszkody utrudniające skuteczny i terminowy dostęp do danych o transakcjach finansowych, będących w posiadaniu innych państw członkowskich, do celów dochodzeń antyterrorystycznych;
- konieczność, techniczna wykonalność i proporcjonalność ewentualnych dodatkowych środków ułatwiających dostęp transgraniczny do danych o transakcjach finansowych do celów dochodzeń antyterrorystycznych w szybki, skuteczny i bezpieczny sposób.

Komisja sporządzi sprawozdanie z wyników tych rozmów.

---

[21] Decyzja ramowa Rady 2006/960/WSiSW (tzw. inicjatywa szwedzka) przewiduje następujące terminy, w jakich organy ścigania muszą odpowiedzieć na zagraniczne wnioski o udostępnienie informacji: osiem godzin w nagłych sytuacjach, gdy informacje lub dane wywiadowcze, których dotyczy wniosek, są przechowywane w bazie danych, do której organ ścigania ma bezpośredni dostęp; oraz dłuższe terminy, w przypadku gdy informacje lub dane wywiadowcze, których dotyczy wniosek, nie są przechowywane w bezpośrednio dostępnej bazie danych.

[22] Dyrektywa 2014/41 z 3.4.2014.

2. Materiały wybuchowe: dalsze ograniczenie dostępu do prekursorów materiałów wybuchowych

Rozporządzenie w sprawie prekursorów materiałów wybuchowych[23] ogranicza dostęp do siedmiu substancji chemicznych i korzystanie z nich przez przeciętnych użytkowników (są to tzw. prekursory materiałów wybuchowych podlegające ograniczeniom, wymienione w wykazie w załączniku I do tego rozporządzenia). W lutym 2017 r. Komisja przyjęła sprawozdanie w sprawie stosowania tego rozporządzenia przez państwa członkowskie[24]. W sprawozdaniu stwierdzono, że wykonanie rozporządzenia przyczyniło się do ograniczenia dostępu do niebezpiecznych prekursorów materiałów wybuchowych, które mogą zostać użyte niezgodnie z ich przeznaczeniem do wytwarzania materiałów wybuchowych domowymi sposobami. Państwa członkowskie donosiły także o przypadkach, gdzie dzięki stosowaniu rozporządzenia wykryto planowane ataki terrorystyczne na wczesnym etapie[25]. By zapewnić pełne wykonanie rozporządzenia, w maju i wrześniu 2016 r. Komisja wszczęła postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko kilku państwom członkowskim w związku z niepełnym wdrożeniem przez nie rozporządzenia. Według stanu na październik 2017 r. w toku znajdują się jeszcze tylko dwa postępowania przeciwko Hiszpanii i Rumunii.

Mimo tych wspólnych wysiłków niedawne ataki i akty terrorystyczne pokazują, że **zagrożenie w postaci materiałów wybuchowych wytwarzanych domowym sposobem** jest w Europie w dalszym ciągu poważne. Substancje te w dalszym ciągu są dostępne i używane do celów wytwarzania materiałów wybuchowych domowym sposobem. Materiałem wybuchowym użytym w większości ataków terrorystycznych był trinadtlenek triacetonu (TATP), wytworzony domowym sposobem. Z doniesień wynika, że ten materiał wybuchowy terroryści wybierają najczęściej[26].

Zważywszy na obecne zagrożenie w postaci prekursorów materiałów wybuchowych konieczne jest podjęcie natychmiastowych kroków, by zapewnić jak najlepsze wykonanie obecnego rozporządzenia przez wszystkie państwa członkowskie. Z tego powodu Komisja opublikowała wraz z niniejszym sprawozdaniem **zalecenie**[27], w którym podała wytyczne na temat bezzwłocznych kroków, które należy podjąć, by zapobiec czynieniu niewłaściwego użytku z prekursorów materiałów wybuchowych. Komisja zachęca państwa członkowskie do pełnego wykonania tego zalecenia, by w miarę możliwości jak najbardziej ograniczyć dostęp do prekursorów materiałów wybuchowych i ich stosowanie przez terrorystów, a także by lepiej kontrolować, czy takie materiały są stosowane zgodnie z prawem, i sprawniej działać w przypadku stwierdzenia podejrzanych transakcji. W tym celu Komisja jest gotowa pomagać państwom członkowskim.

Ponadto Komisja poszerza zakres **przeglądu rozporządzenia w sprawie prekursorów materiałów wybuchowych** o ewaluację, po której nastąpi ocena skutków w pierwszym

[23] Rozporządzenie 98/2013 z 15.1.2017.

[24] COM(2017) 103 final z 28.2.2017.

[25] Dnia 23 czerwca 2017 r. Ministerstwo Spraw Wewnętrznych Belgii poinformowało, że w ciągu roku otrzymało 30 doniesień na temat podejrzanej sprzedaży. W okresie od lutego do czerwca 2017 r. Francja otrzymała 11 doniesień dotyczących w dużej mierze nadtlenku wodoru.

[26] Sprawozdanie z 2017 r. dotyczące sytuacji w zakresie terroryzmu oraz tendencji terrorystycznych w UE (TE-SAT): https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

[27] C(2017) 6950 final z 18.10.2017.

półroczu 2018 r. Przedmiotem ewaluacji będzie analiza przydatności, skuteczności, efektywności, spójności i wartości dodanej rozporządzenia oraz zidentyfikowanie problemów oraz przeszkód, które mogą wymagać podjęcia dalszych działań. W trakcie oceny skutków analizie poddane zostaną różne warianty strategiczne dla rozwiązania stwierdzonych problemów i wyeliminowania zidentyfikowanych przeszkód.

3. Szyfrowanie: wspieranie organów ścigania w dochodzeniach

Stosowanie technik szyfrowania ma zasadnicze znaczenie dla zapewnienia cyberbezpieczeństwa i ochrony danych osobowych. W swoim ustawodawstwie UE konkretnie wskazuje rolę, jaką szyfrowanie odgrywa w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych[28]. Równocześnie w kontekście dochodzeń organy ścigania i organy wymiaru sprawiedliwości coraz częściej stoją przed wyzwaniami związanymi z faktem, że przestępcy stosują techniki szyfrowania. Rzutuje to na zdolność tych organów do uzyskiwania informacji niezbędnych jako dowody w dochodzeniach oraz do ścigania przestępstw i karania przestępców. Zakłada się, że w nadchodzących latach techniki szyfrowania będą stosowane przez przestepców coraz powszechniej, a ich wpływ na dochodzenia będzie coraz większy.

W związku z apelem skierowanym w grudniu 2016 r. przez Radę ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych Komisja **omówiła rolę szyfrowania w dochodzeniach z odpowiednimi zainteresowanymi podmiotami**, poruszając zarówno aspekty techniczne, jak i prawne. W gronie tych podmiotów znaleźli się przedstawiciele Europolu, europejskiej sieci sądowej ds. cyberprzestępczości, Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Agencji Praw Podstawowych Unii Europejskiej (FRA) oraz organów ścigania, organizacji przemysłowych i organizacji społeczeństwa obywatelskiego z państw członkowskich. Na forum grupy roboczej Rady regularnie zdawano raport z postępów, a dnia 18 września 2017 r. przeprowadzono warsztaty z udziałem przedstawicieli państw członkowskich. W trakcie tego procesu zorganizowano szereg obrad okrągłego stołu z organizacjami przemysłowymi i organizacjami społeczeństwa obywatelskiego.

W następstwie tych dyskusji z państwami członkowskimi i zainteresowanymi podmiotami, a także w oparciu o ich wkład, Komisja stwierdza, że należy wdrożyć następujący zestaw **środków wspierających organy ścigania i organy wymiaru sprawiedliwości**, gdy w trakcie dochodzeń mają one do czynienia z przypadkami stosowania szyfrowania przez przestępców. Środki te obejmują a) środki prawne mające ułatwić dostęp do zaszyfrowanych dowodów, b) środki techniczne mające poprawić zdolności w dziedzinie rozszyfrowywania. Komisja będzie w dalszym ciągu monitorowała rozwój sytuacji.

a) ramy prawne dotyczące dostępu transgranicznego do dowodów elektronicznych

Organy ścigania niejednokrotnie stoją przed problemem, jakim jest uzyskanie dostępu do dowodów zgromadzonych w innym państwie. Zachodzące obecnie zmiany ustawodawcze na szczeblu unijnym mogą pomóc organom ścigania i organom wymiaru sprawiedliwości w sprawnym uzyskiwaniu dostępu do niezbędnych, lecz ewentualnie zaszyfrowanych informacji, jakimi dysponują inne państwa członkowskie. Skuteczne dochodzenie i ściganie przestępstw wymaga odpowiednich ram prawnych. W tym celu na początku 2018 r. Komisja

[28] Art. 32 rozporządzenia 2016/679 z dnia 27 kwietnia 2017 r.

przedstawi wnioski dotyczące ułatwienia **dostępu transgranicznego do dowodów elektronicznych**. Równocześnie Komisja wdraża zestaw praktycznych środków[29] mających poprawić dostęp transgraniczny do dowodów elektronicznych w przypadku dochodzeń, w tym finansowanie szkoleń na temat współpracy transgranicznej, rozwój platformy elektronicznej służącej do wymiany informacji w obrębie UE oraz standaryzacja form współpracy sądowej między państwami członkowskimi.

b) środki techniczne

W zależności od tego, w jaki sposób przestępcy korzystają z szyfrowania, organy ścigania i organy wymiaru sprawiedliwości mogą być w stanie odzyskać część informacji. Wiele państw członkowskich powołało krajowe służby dysponujące wiedzą fachową na temat problemu szyfrowania w kontekście dochodzeń. Większość państw członkowskich nie ma jednak dostępu do wiedzy fachowej i zasobów na odpowiednim poziomie. To poważnie osłabia zdolność tych organów do uzyskania dostępu do zaszyfrowanych informacji w trakcie dochodzeń. Z tego powodu Komisja wnioskuje o **szereg środków wspierających organy w państwach członkowskich**, bez zakazywania stosowania systemów szyfrowania, ich ograniczania ani osłabiania.

Po pierwsze, Komisja będzie wspierać **Europol** w dalszym rozwoju jego zdolności w zakresie rozszyfrowywania. W tym celu Komisja wnioskowała, w kontekście przygotowywania budżetu UE na rok 2018, o utworzenie w Europolu łącznie 86 dodatkowych stanowisk związanych z kwestiami bezpieczeństwa (o 19 więcej niż przewidziano w budżecie na 2017 r.), zwłaszcza w Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu. Ocenione zostanie zapotrzebowanie na dodatkowe zasoby i w kolejnym sprawozdaniu z postępu prac nad stworzeniem unii bezpieczeństwa Komisja przedstawi, jakie środki finansowe zostaną przeznaczone na ten cel. Pod uwagę należy wziąć przyszły rozwój technologiczny na podstawie badań i rozwoju w ramach programu „Horyzont 2020" i innych programów finansowanych ze środków unijnych. Nie będą uwzględniane środki, które mogłyby osłabić systemy szyfrowania lub mieć wpływ na większą lub nieograniczoną liczbę osób.

Po drugie, w celu wsparcia organów ścigania i organów wymiaru sprawiedliwości na poziomie krajowym należy ustanowić **sieć punktów kontaktowych dysponujących specjalistyczną wiedzą**. Bez zastępowania krajowych inicjatyw można lepiej dzielić się zdolnościami i wiedzą fachową na poziomie krajowym. Zachęca się państwa członkowskie do korzystania z finansowania z programów krajowych w ramach Funduszu Bezpieczeństwa Wewnętrznego – części dotyczącej współpracy policyjnej – w celu stworzenia, rozbudowy lub rozwoju krajowych punktów kontaktowych dysponujących wiedzą fachową. Na poziomie europejskim Komisja będzie wspierać Europol w zakresie zapewniania funkcji sieci, by ułatwiać współpracę między takimi krajowymi punktami.

Po trzecie, organy w państwach członkowskich powinny dysponować **zestawem alternatywnych narzędzi i technik dochodzeniowych**, by ułatwić rozwój środków i korzystanie z nich w celu uzyskiwania niezbędnych informacji zaszyfrowanych przez przestępców. Taka sieć krajowych punktów powinna przyczyniać się do rozwoju zestawu technik, a Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu jest

[29] Zob. także Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2017) 354 final z 29.6.2017).

najlepszym miejscem do stworzenia i prowadzenia repozytorium takich technik i narzędzi. Nie będą uwzględniane środki, które mogłyby osłabić systemy szyfrowania lub mieć wpływ na większą lub nieograniczoną liczbę osób.

Po czwarte, należy zwrócić uwagę na **ważną rolę, jaką pełnią dostawcy usług i inni partnerzy przemysłowi** w zapewnianiu rozwiązań charakteryzujących się zaawansowanym szyfrowaniem. Zważywszy na zaangażowanie Komisji w takie zaawansowane szyfrowanie lepsza i bardziej zorganizowana współpraca między organami, dostawcami usług i innymi partnerami przemysłowymi pomogłaby w promowaniu lepszego zrozumienia istniejących i pojawiających się wyzwań po różnych stronach. Komisja będzie wspierać usystematyzowany dialog z dostawcami usług i innymi przedsiębiorstwami w ramach Forum UE ds. Internetu i sieci punktów kontaktowych dysponujących wiedzą fachową, a w stosownych przypadkach z przedstawicielami społeczeństwa obywatelskiego.

Po piąte, **programy szkoleniowe** kierowane do pracowników organów ścigania i organów wymiaru sprawiedliwości powinny gwarantować, że odpowiedzialni funkcjonariusze będą lepiej przygotowani do uzyskiwania niezbędnych informacji zaszyfrowanych przez przestępców. By wspierać rozwój programów szkoleniowych, Komisja zamierza zapewnić finansowanie w wysokości 500 000 EUR w ramach rocznego programu prac na 2018 r. Funduszu Bezpieczeństwa Wewnętrznego – z części dotyczącej współpracy policyjnej. W stosownych przypadkach będzie brana pod uwagę wiedza fachowa europejskiej grupy ds. szkolenia i edukacji w zakresie cyberprzestępczości (ECTEG). Komisja będzie także wspierać szkolenia realizowane przez Agencję Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL), a państwa członkowskie zachęca się do korzystania na cele szkoleniowe z finansowania przeznaczonego na ich programy krajowe realizowane w ramach Funduszu Bezpieczeństwa Wewnętrznego – części dotyczącej współpracy policyjnej

Po szóste, istnieje konieczność **stałej oceny technicznych i prawnych aspektów** szyfrowania w kontekście dochodzeń, zważywszy na stały rozwój technik szyfrowania, coraz bardziej powszechne korzystanie z nich przez przestępców oraz ich wpływ na dochodzenia. Komisja będzie kontynuować te ważne prace. Będzie także wspierać rozwój funkcji obserwacyjnej we współpracy z Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu, europejską siecią sądową ds. cyberprzestępczości i Eurojustem.

IV. Przeciwdziałanie radykalizacji postaw

1. Grupa ekspertów wysokiego szczebla ds. radykalizacji postaw

Niedawne ataki, szczególnie te dokonane przez pojedyncze osoby, tzw. „samotne wilki", a także tempo radykalizacji, jaką niektórzy z tych sprawców przeszli, dotkliwie przypominają o tym, jak ważne jest zapobieganie i przeciwdziałanie radykalizacji postaw. Komisja powołała **grupę ekspertów wysokiego szczebla ds. radykalizacji postaw**, by przyspieszyć działania zapobiegające i przeciwdziałające radykalizacji postaw oraz by usprawnić koordynację i współpracę między wszystkimi odnośnymi zainteresowanymi podmiotami, korzystając z dotychczasowych osiągnięć[30]. Zadaniem grupy jest formułowanie zaleceń dotyczących dalszych prac w tym obszarze, a pierwsze wstępne sprawozdanie zostanie sporządzone w tym roku. W grudniu 2017 r. Komisja przekaże Radzie ds. Wymiaru

[30] Zob. także Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2017) 354 final z 29.6.2017).

Sprawiedliwości i Spraw Wewnętrznych sprawozdanie z postępów prac. Grupa zajmie się także ramowymi warunkami niezbędnymi do wzmacniania zdolności i wiedzy fachowej na temat przeciwdziałania radykalizacji postaw, w tym ewentualną potrzebą dalszych struktur współpracy na szczeblu UE. W tym kontekście niektóre państwa członkowskie postulują o utworzenie unijnego centrum ds. zapobiegania radykalizacji postaw. Grupa rozważy zasadność tego postulatu i wartość dodaną takiego centrum.

Jedną z priorytetowych kwestii, która będzie omawiana przez grupę, jest **radykalizacja postaw w zakładach karnych.** Obecnie kładzie się nacisk na wykonanie przez państwa członkowskie działań określonych w konkluzjach Rady ds. WSiSW w sprawie wzmacniania reakcji wymiaru sprawiedliwości w sprawach karnych na radykalizację postaw z dnia 20 listopada 2015 r.[31]. Dnia 27 lutego 2018 r. Komisja zorganizuje konferencję dla zainteresowanych podmiotów na temat reakcji wymiaru sprawiedliwości w sprawach karnych na radykalizację postaw i przedstawi wyniki realizowanych obecnie projektów.

Komisja uwzględni konkluzje i zalecenia grupy w planie prac nad obecnymi inicjatywami (w szczególności w Centrum Doskonałości w ramach Sieci Upowszechniania Wiedzy o Radykalizacji Postaw), a także przy korzystaniu ze swoich instrumentów finansowania (w tym z Funduszu Bezpieczeństwa Wewnętrznego, ale także z innych powiązanych funduszy, takich jak Erasmus+, program „Sprawiedliwość" czy Europejski Fundusz Społeczny).

2. Przeciwdziałanie radykalizacji w sieci

Terroryści w dalszym ciągu wykorzystują internet, by szerzyć radykalizację postaw, rekrutować przyszłych terrorystów, przygotowywać ataki i prowokować do nich, a także chwalić się popełnionymi przez siebie okrucieństwami. Rada Europejska[32], uczestnicy szczytu G7[33] i G20[34], wezwali niedawno do podjęcia dalszych działań, by stawić czoła temu globalnemu wyzwaniu, i przypomnieli o odpowiedzialności przemysłu w tym względzie.

W lipcu 2017 r. Forum UE ds. Internetu przygotowało **plan działania dotyczący zwalczania treści terrorystycznych w internecie**, wzywając przemysł internetowy do podjęcia zdecydowanych działań, przeznaczenia zasobów i opracowania niezbędnych narzędzi technologicznych w celu zapewnienia szybkiego wykrywania i usuwania szkodliwych materiałów. W planie działania wzywa się do poczynienia szybkich postępów w wielu obszarach[35] i ustanowienia mechanizmu regularnej sprawozdawczości, by mierzyć i oceniać wyniki.

Dnia 29 września 2017 r. Komisja zorganizowała posiedzenie urzędników wysokiego szczebla w ramach Forum UE ds. Internetu, by podsumować **wdrożenie planu działania dotyczącego zwalczania treści terrorystycznych w internecie**. Wiele przedsiębiorstw zaczyna stosować automatyczne wykrywanie, co pozwala im na korzystanie z technicznej wiedzy w celu identyfikowania treści terrorystycznych w momencie, gdy są one umieszczane w internecie. Niektóre przedsiębiorstwa donoszą, że obecnie automatycznie wykrywanych

[31] Konkluzje Rady Unii Europejskiej i państw członkowskich zebranych w Radzie w sprawie wzmacniania reakcji wymiaru sprawiedliwości w sprawach karnych na radykalizację skutkującą terroryzmem i brutalnym ekstremizmem (14382/15).

[32] http://www.consilium.europa.eu/en/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.

[33] http://www.consilium.europa.eu/en/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

[34] http://www.consilium.europa.eu/en/press/press-releases/2017/07/07-g20-counter-terrorism/.

[35] COM(2017) 407 final z 26.7.2017.

jest 75 % treści i że zwracają się one do osób analizujących takie treści o ostateczną decyzję w sprawie ich usunięcia, natomiast w przypadku pozostałych przedsiębiorstw 95 % treści wykrywanych jest przy pomocy firmowych narzędzi do wykrywania. Stanowi to konkretny postęp, jednak Komisja wezwała wszystkie przedsiębiorstwa do przyspieszenia procesu wdrażania tych narzędzi, by zapewnić szybsze wykrywanie, ograniczyć czas dostępności takich terrorystycznych treści w internecie oraz zagwarantować szybsze i skuteczniejsze usuwanie terrorystycznych materiałów propagandowych. Komisja wezwała także przedsiębiorstwa do rozbudowania używanego przez nie narzędzia, jakim jest „baza hashów", by zagwarantować, że usuwane treści terrorystyczne nie będą ponownie umieszczane na innych platformach, co pomoże ograniczyć rozprzestrzenianie takich treści na wielu platformach. Narzędzie to należałoby rozbudować zarówno pod względem treści, tak by analizowało ono nie tylko nagrania wideo i zdjęcia/obrazki, jak i pod względem używających je przedsiębiorstw.

Komisja nadal pomaga organizacjom społeczeństwa obywatelskiego w szerzeniu w internecie pozytywnych **przekazów alternatywnych**. W dniu 6 października 2017 r. Komisja ogłosiła zaproszenie do składania wniosków w sprawie zapewnienia finansowania w wysokości 6 mln EUR na rzecz konsorcjum podmiotów społeczeństwa obywatelskiego, które przygotowują i prowadzą takie kampanie.

Dnia 6 grudnia 2017 r. Komisja Europejska zwoła **Forum UE ds. Internetu na poziomie ministerialnym** z udziałem przedstawicieli wysokiego szczebla przemysłu internetowego w celu oceny postępów i przygotowania gruntu pod przyszłe działania.

Działania podejmowane w celu wyeliminowania treści terrorystycznych w internecie w ramach Forum UE ds. Internetu należy postrzegać w szerszym kontekście zwalczania nielegalnych treści w internecie. Komisja wsparła te działania, przyjmując dnia 28 września 2017 r. komunikat zawierający zestawienie **wytycznych i zasad, w ramach których wzywa się platformy internetowe** do intensyfikacji zwalczania nielegalnych treści w internecie[36] we współpracy z organami krajowymi, państwami członkowskimi i innymi odpowiednimi zainteresowanymi stronami. Celem komunikatu jest ułatwienie i przyspieszenie wdrażania dobrych praktyk w zakresie zapobiegania występowaniu nielegalnych treści, ich wykrywania, usuwania i uniemożliwiania dostępu do nich, by zapewnić skuteczne usuwanie takich treści, zwiększyć przejrzystość i chronić prawa podstawowe. Ma on również na celu wyjaśnienie, jaką odpowiedzialność ponoszą platformy, gdy podejmują proaktywne działania w celu wykrywania lub usuwania nielegalnych treści oraz uniemożliwiania dostępu do nich. Komisja oczekuje, że w najbliższych miesiącach platformy internetowe podejmą zdecydowane działania, m.in. w kontekście stosownych dialogów, np. na Forum UE ds. Internetu na temat terroryzmu i niezgodnego z prawem nawoływania do nienawiści.

Równocześnie Komisja będzie monitorowała postępy i oceni, czy konieczne są dodatkowe środki w celu zapewnienia szybkiego i proaktywnego wykrywania i usuwania nielegalnych treści w internecie, w tym ewentualne środki prawne uzupełniające istniejące ramy regulacyjne. Prace te potrwają do maja 2018 r.

[36] Komunikat w sprawie zwalczania nielegalnych treści w internecie „W kierunku większej odpowiedzialności platform internetowych" (COM(2017) 555 final z 28.9.2017.

Jeśli chodzi o ustawodawstwo, wniosek Komisji[37] w sprawie **przeglądu dyrektywy o audiowizualnych usługach medialnych**, złożony w maju 2016 r., wspiera zwalczanie nawoływania do nienawiści. Ma on na celu dostosowanie tej dyrektywy do decyzji ramowej w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii[38] i Karty praw podstawowych. Przewiduje ponadto nałożenie na państwa członkowskie obowiązku zapewnienia, by platformy służące do wymiany nagrań wideo stosowały właściwe środki w celu ochrony wszystkich obywateli przed podburzaniem do przemocy lub nienawiści. Takie środki obejmują m.in. mechanizmy polegające na oznaczaniu i zgłaszaniu legalnych treści.

V. ZEWNĘTRZNY WYMIAR WALKI Z TERRORYZMEM

1. Działania zewnętrzne UE w zakresie walki z terroryzmem

Działania zewnętrzne UE w zakresie zwalczania terroryzmu przyczyniają się do osiągania głównego celu, jakim jest wzmocnienie bezpieczeństwa wewnętrznego UE. Dlatego należy nadal wzmacniać strategiczne i polityczne kontinuum między bezpieczeństwem wewnętrznym i zewnętrznym UE, by poprawić skuteczność działań antyterrorystycznych we wszystkich dziedzinach.

Komisja wspiera finansowo szerokie spektrum działań zewnętrznych, by podnieść poziom bezpieczeństwa. Od dnia 1 stycznia 2017 r. na ponad 600 bieżących projektów przeznaczy się finansowanie w wysokości ponad 2,3 mld EUR. Szereg działań jest albo skoncentrowanych na kwestiach bezpieczeństwa (tj. konkretne działania dotyczące takich zagadnień jak walka z finansowaniem terroryzmu, przeciwdziałanie radykalizacji postaw, granice, zakłady karne) lub dotyczy kwestii bezpieczeństwa (tj. programy, które mają na celu wyeliminowanie podstawowych przyczyn braku bezpieczeństwa i skarg przez zapewnienie pomocy w poprawie edukacji, dostępu do zasobów naturalnych i energii, dobrych rządów i sektora bezpieczeństwa, wsparcia na rzecz społeczeństwa obywatelskiego).

W dniu 19 czerwca 2017 r. Rada do Spraw Zagranicznych odnowiła kierownictwo strategiczne w tych obszarach, przyjmując kompleksowe **wnioski w sprawie działań zewnętrznych UE w dziedzinie zwalczania terroryzmu**[39]. Wysoki przedstawiciel i Komisja Europejska wspólnie będą dążyć, w razie konieczności, do udanej realizacji tych wniosków. By zapewnić czasową i pełną realizację wniosków oraz przekazać Radzie sprawozdanie do czerwca 2018 r., rozpoczęto wspólny proces koordynacji między Europejską Służbą Działań Zewnętrznych i Komisją Europejską. Priorytetowo potraktowane zostaną:

- **Wzmocnienie sieci zrzeszającej ekspertów ds. zwalczania terroryzmu pracujących w delegaturach UE:** Eksperci ds. zwalczania terroryzmu powinni coraz bardziej angażować się w programowanie wsparcia UE i w koordynację na poziomie lokalnym współpracy poszczególnych państw członkowskich z naszymi partnerami w zakresie zwalczania terroryzmu. W tym celu zintensyfikowany zostanie program szkoleń dla ekspertów, którzy będą przechodzić ten program przed oddelegowaniem i w jego trakcie. Ich zadania będą skupiały się raczej na pismach w sprawie konkretnych misji, a ich kontakty z agencjami UE w dziedzinie wymiaru

[37] COM(2016) 287 final z 25.5.2016.
[38] Decyzja ramowa Rady 2008/913/WSiSW z 28.11.2008.
[39] http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/.

sprawiedliwości i spraw wewnętrznych będą bardziej stabilne. By sieć ekspertów ds. zwalczania terroryzmu[40] obejmowała wszystkie obszary o wysokim priorytecie, jej zasięg zostanie poszerzony o Róg Afryki, Azję Środkową i Azję Południowo-Wschodnią.

- **Usprawnienie współpracy między misjami i operacjami prowadzonymi w ramach wspólnej polityki bezpieczeństwa i obrony a agencjami UE w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych** w zakresie gromadzenia, analizy i wymiany informacji oraz dalsze badanie, jak usprawnić powiązania między podmiotami wojskowymi i organami ścigania do celów zwalczania terroryzmu. By poprawić wymianę danych i informacji między wspólną polityką bezpieczeństwa i obrony a polityką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, istotne znaczenie będzie miało wspieranie przeglądu elementów bieżących ram regulacyjnych i pilotowanie procesu tworzenia komórek ds. informacji o przestępczości na potrzeby wybranych misji i operacji prowadzonych w ramach wspólnej polityki bezpieczeństwa i obrony. Ważne będzie dalsze ułatwianie i usprawnianie powiązań między działaniami agencji UE w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych w piorytetowych państwach trzecich, w tym udoskonalenie, w miarę możliwości, wymiany informacji między podmiotami w UE i poza UE.
- **Wzmocnienie współpracy międzynarodowej w dziedzinie zwalczania terroryzmu oraz przeciwdziałanie brutalnemu ekstremizmowi i jego zwalczanie** z krajami partnerskimi na Bałkanach Zachodnich, Bliskim Wschodzie, w Turcji, Zatoce Perskiej, Sahelu i Rogu Afryki; z kluczowymi partnerami strategicznymi, m.in. USA, Kanadą i Australią; oraz z kluczowymi partnerami regionalnymi i wielostronnymi, m.in. USA, NATO, Światowym Forum na rzecz Zwalczania Terroryzmu, Grupą Specjalną ds. Przeciwdziałania Praniu Pieniędzy, Unią Afrykańską, Stowarzyszeniem Narodów Azji Południowo-Wschodniej, Radą Współpracy Państw Zatoki i Ligą Państw Arabskich.

2. Konwencja Rady Europy o zapobieganiu terroryzmowi

By zacieśnić współpracę międzynarodową w zakresie zwalczania terroryzmu, Komisja przedkłada wraz z niniejszym sprawozdaniem **wnioski**[41] **w sprawie decyzji Rady dotyczących zawarcia konwencji Rady Europy o zapobieganiu terroryzmowi i jej protokołu dodatkowego.** Konwencja[42], przyjęta przez Radę Europy w dniu 16 maja 2005 r., dotyczy kryminalizacji działalności terrorystycznej i związanej z terroryzmem, współpracy międzynarodowej w zakresie takich przestępstw, a także ochrony, odszkodowań oraz wsparcia dla ofiar terroryzmu. Konwencja weszła w życie dnia 1 czerwca 2007 r. Wszystkie państwa członkowskie UE podpisały tę konwencję, natomiast 23 państwa członkowskie UE ją ratyfikowały. Celem protokołu dodatkowego[43], przyjętego przez Radę Europy dnia 18 maja 2015 r., jest uzupełnienie konwencji o zestaw przepisów mających na celu wdrożenie aspektów prawa karnego rezolucji Rady Bezpieczeństwa ONZ nr 2178 (2014)[44] w sprawie

---

[40] Do tej pory UE oddelegowuje swoich ekspertów ds. zwalczania terroryzmu do delegatur UE w: Algierii, Bośni i Hercegowinie (z mandatem regionalnym na Bałkanach Zachodnich), Czadzie (Sahel), Iraku, Jordanii, Libanie, Libii (w Tunisie), Maroku, Nigerii, Pakistanie, Arabii Saudyjskiej, Tunezji i Turcji.

[41] COM(2017) 606 final z18.10.2017 i COM(2017) 607 final z 18.10.2017.

[42] https://rm.coe.int/168008371c.

[43] https://rm.coe.int/168047c5ea.

[44] http://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf.

zagrożeń dla pokoju i bezpieczeństwa międzynarodowego spowodowanych przez akty terrorystyczne. Protokół dodatkowy stanowi odpowiedź na tę rezolucję, ponieważ promuje wspólne zrozumienie przestępstw związanych z zagranicznymi bojownikami terrorystycznymi i reagowanie na te przestępstwa. Protokół dodatkowy wszedł w życie dnia 1 lipca 2017 r.

W dniu 22 października 2015 r. UE podpisała wspomnianą konwencję i załączony do niej protokół dodatkowy. Zważywszy na to, że UE przyjęła kompleksowy zestaw instrumentów prawnych w celu zwalczania terroryzmu, przede wszystkim dyrektywę w sprawie zwalczania terroryzmu[45], jest ona teraz gotowa do wypełnienia swojego zobowiązania, by stać się stroną tej konwencji i protokołu dodatkowego.

3. Zmieniona umowa z Kanadą w sprawie danych dotyczących przelotu pasażera

W swojej opinii z dnia 26 lipca 2017 r.[46] Trybunał Sprawiedliwości UE stwierdził, że umowa między Kanadą i UE w sprawie przekazywania i korzystania z danych dotyczących przelotu pasażera podpisana dnia 25 czerwca 2014 r. nie może zostać zawarta w swym obecnym brzmieniu z powodu kilku przepisów, które nie są zgodne z prawami podstawowymi respektowanymi przez UE, w szczególności z prawem ochrony danych i zasadą poszanowania życia prywatnego. Komisja jest obecnie w kontakcie z Kanadą, m.in. na marginesie zbliżającego się posiedzenia ministrów spraw wewnętrznych w ramach szczytu G7 (Ischia, 19-20 października 2017 r.), by przygotować się do nadchodzących negocjacji w sprawie zmian do umowy. W tym celu Komisja przedstawiła, wraz z niniejszym sprawozdaniem, **zalecenie[47] dla Rady w sprawie wydania zgody na rozpoczęcie negocjacji na temat zmienionej umowy** zgodnie ze wszystkimi wymogami określonymi przez Trybunał Sprawiedliwości w swojej opinii. Wzywa się Radę do szybkiego wydania zgody na podjęcie negocjacji. Mając na uwadze, że dane PNR są ważnym narzędziem w walce z terroryzmem i poważną przestępczością międzynarodową, Komisja podejmie niezbędne kroki w celu zapewnienia kontynuacji przekazywania danych PNR do Kanady przy pełnym poszanowaniu praw podstawowych w myśl opinii Trybunału.

W tym kontekście Komisja podkreśla swoje stałe wsparcie dla państw członkowskich przy wdrażaniu dyrektywy UE w sprawie danych dotyczących przelotu pasażera[48]; opinia Trybunału Sprawiedliwości nie ma wpływu na zobowiązania państw członkowskich wynikające z tej dyrektywy.

4. Wzmocnienie współpracy Europolu z państwami trzecimi

Współpraca z państwami trzecimi odgrywa ważną rolę w zwalczaniu terroryzmu i przestępczości zorganizowanej, co podkreślono w konkluzjach Rady do Spraw Zagranicznych z czerwca 2017 r. w sprawie działań zewnętrznych UE w dziedzinie zwalczania terroryzmu UE[49] i w odnośnych strategiach regionalnych UE[50]. Zanim

[45] Dyrektywa 2017/541 z 15.3.2017.
[46] Opinia nr 1/15 Trybunału Sprawiedliwości (26.7.2017).
[47] COM(2017) 605 final z 18.10.2017.
[48] Dyrektywa 2016/681 z 27.4.2016.
[49] http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/.
[50] Obejmuje to zmienioną europejską politykę sąsiedztwa (JOIN(2015) 50 final z 18.11.2015).

rozporządzenie w sprawie Europolu[51] weszło w życie dnia 1 maja 2017 r., Europol zawarł, zgodnie z poprzednią podstawą prawną[52], umowy z wieloma państwami trzecimi, by zapewnić ramy współpracy w zakresie wymiany informacji technicznych i strategicznych. Niektóre z tych umów przewidują również możliwość wymiany danych osobowych[53]. Umowy te pozostają w mocy.

Od dnia 1 maja 2017 r. nowe **rozporządzenie w sprawie Europolu** określa zasady stosunków zewnętrznych Europolu z państwa trzecimi, zwłaszcza warunki wymiany danych osobowych z organami Unii, państwami trzecimi i organizacjami międzynarodowymi. Zgodnie z Traktatem i wspomnianym rozporządzeniem Komisja odpowiada, w imieniu Unii, za negocjowanie umów międzynarodowych z państwami trzecimi w sprawie wymiany danych osobowych z Europolem[54]. O ile jest to konieczne dla wykonania jego zadań, Europol może nawiązywać i utrzymywać współpracę z partnerami zewnętrznymi zgodnie z ustaleniami roboczymi i administracyjnymi, które nie zezwalają na wymianę dane osobowych.

W świetle potrzeb operacyjnych Unii pod względem współpracy w zakresie bezpieczeństwa z państwami trzecimi i zgodnie z rozporządzeniem w sprawie Europolu **Komisja przedstawi przed upływem tego roku Radzie zalecenia** dotyczące zgody na rozpoczęcie negocjacji między UE a Algierią, Egiptem, Izraelem, Jordanią, Libanem, Marokiem, Tunezją i Turcją, by zapewnić podstawę prawną przekazywania danych osobowych między Europolem a wymienionymi państwami trzecimi[55]. Takie porozumienia dodatkowo wzmocnią zdolności Europolu w zakresie współpracy z tymi państwami trzecimi w zakresie zapobiegania i zwalczania rodzajów przestępstw wchodzących w zakres celów Europolu.

VI. WNIOSEK

W niniejszym sprawozdaniu omówiono pakiet środków antyterrorystycznych, które będą służyć dalszemu wspieraniu państw członkowskich w ich działaniach na rzecz wyeliminowania bieżących zagrożeń dla bezpieczeństwa. Komisja zachęca państwa członkowskie i Radę do wdrożenia tych środków w trybie priorytetowym. Komisja będzie na bieżąco informować Parlament Europejski i Radę o postępach.

---

51 Rozporządzenie 2016/794 z 11.5.2016.

52 Decyzja Rady 2009/371/WSiSW z 6.4.2009.

53 Europol zawarł umowy pozwalające na wymianę danych osobowych z następującymi państwami trzecimi: Albania, Australia, Bośnia i Hercegowina, Kanada, Kolumbia, była jugosłowiańska republika Macedonii, Gruzja, Islandia, Liechtenstein, Mołdawia, Monako, Czarnogóra, Norwegia, Serbia, Szwajcaria, Ukraina i Stany Zjednoczone. Zarząd Europolu wydał zgodę na rozpoczęcie negocjacji w sprawie umowy między Europolem i Izraelem, lecz negocjacje te nie zostały zakończone, w momencie gdy nowe rozporządzenie w sprawie Europolu wchodziło w życie.

54 Rozporządzenie w sprawie Europolu przewiduje także przekazywanie danych osobowych między Europolem i państwem trzecim na podstawie decyzji Komisji, w której stwierdza ona, że dane państwo zapewnia odpowiedni stopień ochrony danych („decyzja stwierdzająca odpowiedni stopień ochrony").

55 Oprócz podanych państw trzecich Komisja przywołuje ramy strategiczne decyzji stwierdzających odpowiedni stopień ochrony, a także inne narzędzia do przekazywania danych i międzynarodowe instrumenty ochrony danych, jak podano w komunikacie Komisji w sprawie wymiany i ochrony danych osobowych w zglobalizowanym świecie (COM(2017) 7 final z 10.1.2017), w którym Komisja zachęca państwa trzecie do przystąpienia do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz do jej protokołu dodatkowego.

Kolejne sprawozdanie z postępu prac nad bezpieczeństwem Unii zostanie przedstawione w grudniu 2017 r., a jego głównym tematem będzie interoperacyjność systemów informacyjnych UE w dziedzinie bezpieczeństwa, zarządzanie migracjami i granicami. W tym kontekście Komisja przypomina o znaczeniu, jakie mają postępy pracach nad priorytetami ustawodawczymi dotyczącymi systemów informacyjnych.