KOMISJA
EUROPEJSKA

Bruksela, dnia 24.7.2019 r.
COM(2019) 353 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY EUROPEJSKIEJ I RADY

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

Europejczycy słusznie oczekują, że Unia zapewni im bezpieczeństwo. Komisja pod przewodnictwem Jeana-Claude'a Junckera od samego początku traktuje bezpieczeństwo jako najważniejszy priorytet. W nowym programie strategicznym Rady Europejskiej na lata 2019–2024 cel „ochrona obywateli i swobód" zajmuje najważniejsze miejsce wśród czterech priorytetów Unii[1]. Ponadto Rada Europejska ogłosiła, że wzmocni działania Unii na rzecz walki z terroryzmem i przestępczością transgraniczną, w tym poprzez poprawę współpracy i wymiany informacji oraz dalsze opracowywanie wspólnych instrumentów.

Dzięki ścisłej współpracy między Parlamentem Europejskim, Radą i Komisją UE poczyniła znaczne postępy we wspólnych działaniach na rzecz skutecznej i rzeczywistej unii bezpieczeństwa, wprowadzając szereg priorytetowych inicjatyw ustawodawczych i wdrażając szeroki wachlarz środków pozalegislacyjnych w celu wsparcia państw członkowskich i zwiększenia bezpieczeństwa wszystkich obywateli[2]. Unia podjęła zdecydowane działania w celu zawężenia terrorystom i przestępcom pola działania, utrudniając terrorystom pozyskiwanie środków do przeprowadzenia ataków poprzez zakazy nabywania i wykorzystywania określonych rodzajów broni palnej i materiałów wybuchowych oraz ograniczanie dostępu do finansowania. Ponadto UE wzmocniła wymianę informacji między państwami członkowskimi oraz zamknęła luki informacyjne i martwe pola, walcząc jednocześnie z radykalizacją, chroniąc Europejczyków w internecie, zwalczając zagrożenia cybernetyczne i przestępczość wykorzystującą cyberprzestrzeń, umacniając zarządzanie zewnętrznymi granicami Unii oraz współpracę międzynarodową w dziedzinie bezpieczeństwa.

Jednocześnie nadal szereg priorytetowych inicjatyw w ramach unii bezpieczeństwa oczekuje na przyjęcie przez współprawodawców. Niniejsze sprawozdanie, przedstawiane w następstwie ukonstytuowania się w dniu 2 lipca 2019 r. Parlamentu Europejskiego 9. kadencji:

- określa, w jakich przypadkach od współprawodawców oczekuje się podjęcia działań w odpowiedzi na bezpośrednie zagrożenia. Szczególnie pilna jest potrzeba podjęcia działań w celu **zwalczania propagandy terrorystycznej i radykalizacji w internecie**;
- określa czekające na przyjęcie priorytetowe inicjatywy w ramach unii bezpieczeństwa, które wymagają dalszych działań ze strony współprawodawców, aby zwiększyć **cyberbezpieczeństwo** i ułatwić dostęp do elektronicznego **materiału dowodowego** oraz zakończyć prace nad sprawniejszymi i inteligentniejszymi systemami informacyjnymi na potrzeby zarządzania bezpieczeństwem, granicami i migracją;
- aktualizuje informacje na temat wspólnych, niecierpiących zwłoki prac rozpoczętych w marcu 2019 r. w celu oceny i wzmocnienia **bezpieczeństwa sieci 5G** w oparciu o krajowe oceny ryzyka przedłożone przez państwa członkowskie do dnia 15 lipca 2019 r.;
- podejmuje kwestię pakietu czterech sprawozdań dotyczących **przeciwdziałania praniu pieniędzy**, przyjętych przez Komisję w dniu 24 lipca 2019 r., w których analizuje się obecne zagrożenia i słabe punkty w zakresie prania pieniędzy, oraz ocenia, w jaki sposób odpowiednie ramy regulacyjne UE stosowane są w sektorze prywatnym i publicznym;

---

1 https://www.consilium.europa.eu/media/39919/a-new-strategic-agenda-2019-2024-pl.pdf

2 Więcej informacji na ten temat można znaleźć w zestawieniu informacji na temat: „Unia bezpieczeństwa: Europa, która chroni" (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_pl.pdf) oraz osiemnastym sprawozdaniu z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM (2019) 145 final z 20.3.2019).

- przedstawia aktualne informacje na temat postępów poczynionych od marca 2019 r.[3] we wdrażaniu środków ustawodawczych w ramach unii bezpieczeństwa, przewidujących interoperacyjność systemów informacyjnych jako jeden z głównych priorytetów do szybkiego i pełnego wdrożenia przez państwa członkowskie;
- dokonuje bilansu bieżących prac mających na celu przeciwdziałanie dezinformacji i ochronę wyborów przed zagrożeniami cybernetycznymi, działań na rzecz zwiększenia gotowości i ochrony przed zagrożeniami dla bezpieczeństwa, a także współpracy z partnerami międzynarodowymi w kwestiach bezpieczeństwa.

II. REALIZACJA PRIORYTETÓW USTAWODAWCZYCH

1. Zapobieganie radykalizacji postaw w internecie i w społecznościach

Zapobieganie radykalizacji jest centralnym elementem reakcji UE na terroryzm, zarówno w internecie, jak i w naszych społecznościach.

Atak w Christchurch w Nowej Zelandii w dniu 15 marca 2019 r. przypomniał w zatrważający sposób, jak internet może być wykorzystany do celów terrorystycznych, niezależnie od tego, czy pożywką terroryzmu jest dżihadyzm, prawicowy ekstremizm czy inna skrajna ideologia. Bezpośrednia relacja wideo z ataku w Christchurch obiegła internet tak szeroko i tak szybko, że nie ulega już wątpliwości, jak ważne jest zapewnienie platformom internetowym odpowiednich środków do powstrzymywania szybkiego rozpowszechniania takich treści.

W odpowiedzi szefowie państw lub rządów niektórych państw członkowskich i państw trzecich, przewodniczący Jean-Claude Juncker oraz platformy internetowe poparli w dniu 15 maja 2019 r. **„apel o podjęcie działań w obliczu ataku w Christchurch”**[4], określający wspólne działania, które mają służyć wyeliminowaniu w internecie treści terrorystycznych i brutalnych treści ekstremistycznych. Dalsze zobowiązania związane z tą kwestią podjęte zostały przez G7[5] i G20[6].

Komisja zajęła się już realnym i wyraźnym zagrożeniem stwarzanym przez treści o charakterze terrorystycznym w internecie, przyjmując **wniosek ustawodawczy** zapowiedziany przez przewodniczącego Junckera w orędziu o stanie Unii z 2018 r. We wniosku proponuje się jasne i zharmonizowane ramy prawne zapobiegające wykorzystywaniu usług hostingowych do rozpowszechniania w internecie treści o charakterze terrorystycznym[7]. Proponowane środki zobowiązywałyby platformy internetowe do usuwania treści o charakterze terrorystycznym w ciągu jednej godziny po otrzymaniu nakazu ich usunięcia ze strony właściwych organów w dowolnym państwie członkowskim. Ponadto na platformy nadużywane do rozpowszechniania treści o charakterze terrorystycznym nakładano by obowiązek zastosowania proaktywnych środków w celu wykrywania tych treści i zapobiegania ich ponownemu pojawianiu się – z jasnymi zasadami i gwarancjami. Organy państw członkowskich musiałyby powołać specjalne służby dysponujące uprawnieniami i zasobami umożliwiającymi skuteczne wykrywanie treści o charakterze terrorystycznym i wydawania nakazów ich usunięcia.

---

[3] Zob. osiemnaste sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2019) 145 final z 20.3.2019).

[4] https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. Prezydent Francji Emmanuel Macron i premier Nowej Zelandii Jacinda Ardern zaprosili przywódców politycznych i przedstawicieli platform internetowych do Paryża na 15 maja 2019 r., aby zainaugurować tę inicjatywę.

[5] https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

[6] Na szczycie G20 w Osace, który odbył się w dniach 28–29 czerwca 2019 r., przywódcy potwierdzili swoje zobowiązanie do działania na rzecz ochrony ludzi przed wykorzystywaniem internetu do celów terroryzmu i sprzyjającego mu brutalnego ekstremizmu (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

[7] COM(2018) 640 final z 12.9.2018.

Pozwoli to na stworzenie szybkiego i skutecznego ogólnounijnego systemu oraz wprowadzi solidne zabezpieczenia, w tym skuteczne mechanizmy składania skarg i dochodzenia roszczeń na drodze sądowej.
Zaproponowane środki pomogą zapewnić sprawne funkcjonowanie jednolitego rynku cyfrowego, a jednocześnie podniosą poziom bezpieczeństwa i zaufania w internecie oraz wzmocnią ochronę wolności słowa i informacji.

W grudniu 2018 r. Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych uzgodniła podejście ogólne do wniosku. Parlament Europejski przyjął swoje stanowisko w pierwszym czytaniu w kwietniu 2019 r. **Komisja wzywa obu współprawodawców do jak najszybszego podjęcia międzyinstytucjonalnych negocjacji w sprawie tej priorytetowej inicjatywy mającej na celu usuwanie treści o charakterze terrorystycznym w internecie**, z myślą o osiągnięciu szybkiego porozumienia w sprawie unijnych ram regulacyjnych zawierających jasne zasady i gwarancje.

Równolegle Komisja kontynuuje współpracę z platformami internetowymi w ramach **Forum UE ds. Internetu**[8]. Zgodnie z zapowiedzią przewodniczącego Junckera na spotkaniu w Paryżu w dniu 15 maja 2019 r. w sprawie apelu o podjęcie działań w obliczu ataku z Christchurch Komisja rozpoczęła wraz z Europolem prace nad opracowaniem **unijnego protokołu kryzysowego**, aby umożliwić rządom i platformom internetowym szybkie i skoordynowane reagowanie na rozpowszechnianie treści o charakterze terrorystycznym w internecie, na przykład bezpośrednio po ataku terrorystycznym. Prace te rozpoczęto na szczeblu międzynarodowym w odpowiedzi na „apel o podjęcie działań w obliczu ataku z Christchurch". Oprócz dalszych dyskusji z państwami członkowskimi i przedstawicielami branży oraz zaplanowanej na wrzesień 2019 r. symulacji sytuacji kryzysowej Komisja zwoła na dzień 7 października 2019 r. posiedzenie ministerialne w ramach Forum UE ds. Internetu w celu zatwierdzenia protokołu kryzysowego UE.

Ponadto Komisja kontynuuje wysiłki na rzecz **wspierania państw członkowskich i podmiotów lokalnych w zapobieganiu i zwalczaniu radykalizacji postaw** w społecznościach lokalnych w całej Europie. Wymaga to długofalowych, trwałych wysiłków z udziałem wszystkich właściwych podmiotów na szczeblu lokalnym, krajowym i unijnym. **Rada Sterująca ds. działań Unii w zakresie zapobiegania i przeciwdziałania radykalizacji postaw**, utworzona w sierpniu 2018 r. w celu doradzania Komisji w sprawie sposobu wzmocnienia reakcji politycznej UE w tej dziedzinie, odbyła swoje drugie posiedzenie w dniu 17 czerwca 2019 r. w celu zbadania możliwości dalszych działań w obszarach priorytetowych, takich jak radykalizacja postaw w więzieniach i przeciwdziałanie ideologiom ekstremistycznym. Jako że największe kompetencje w zakresie identyfikacji wczesnych sygnałów ostrzegawczych o radykalizacji postaw i sposobów radzenia sobie z nimi mają często specjaliści zajmujący się tym w sposób praktyczny na poziomie lokalnym, finansowana przez UE **sieć upowszechniania wiedzy o radykalizacji postaw**[9] nadal wspiera działania służb pierwszej linii, łącząc około 5 000 specjalistów ze społeczeństwa obywatelskiego, szkół i policji, a także krajowych koordynatorów i decydentów.

Niedawna współpraca działających w terenie specjalistów w ramach sieci doprowadziła do głębszego zrozumienia wyzwań związanych z prawicowym ekstremizmem. W tym roku sieć upowszechniania

[8] Zainicjowane w 2015 r. **Forum UE ds. Internetu** służy współpracy ministrów spraw wewnętrznych UE, branży internetowej i innych zainteresowanych stron w ramach dobrowolnego partnerstwa w celu rozwiązania problemu przestępczego wykorzystywania internetu przez grupy terrorystyczne oraz w celu ochrony obywateli.

[9] W 2011 r. Komisja utworzyła **sieć upowszechniania wiedzy o radykalizacji postaw**, aby zbliżyć do siebie specjalistów zajmujących się tym w praktyce, w pierwszej linii i na szczeblu lokalnym. W 2015 r. Komisja wzmocniła tę sieć dzięki utworzeniu Centrum Doskonałości w ramach Sieci Upowszechniania Wiedzy o Radykalizacji Postaw w celu opracowania bardziej ukierunkowanych wytycznych, wsparcia i doradztwa dla zainteresowanych stron w państwach członkowskich oraz zwiększenia wiedzy fachowej i umiejętności różnych podmiotów. Więcej informacji na temat działalności sieci upowszechniania wiedzy o radykalizacji postaw: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

wiedzy o radykalizacji postaw będzie publikowała arkusze informacyjne, aby pomóc osobom odpowiedzialnym za wyznaczanie kierunków polityki i praktykom identyfikować główne formy i przejawy prawicowego i islamskiego ekstremizmu, takie jak typowa narracja, język, formy, symbole, typologie i strategie. Wreszcie, jako że wiodącą rolę w zapobieganiu i zwalczaniu radykalizacji postaw odgrywają lokalne podmioty i **miasta**, Komisja wspiera ich inicjatywy w tym zakresie. W następstwie konferencji pt. „Miasta UE przeciwko radykalizacji postaw", która odbyła się 26 lutego 2019 r., w dniu 8 lipca 2019 r. odbyło się pierwsze posiedzenie grupy pilotażowej obejmującej około 20 miast, zorganizowane przez mera Strasburga, w celu intensywniejszej wymiany najlepszych praktyk i zwiększenia wysiłków miast w tej dziedzinie.

Jednocześnie trwają prace nad wspieraniem krajów partnerskich w walce z radykalizacją, która może prowadzić do terroryzmu, w tym w więzieniach.

W celu przeciwdziałania zagrożeniu stwarzanemu przez treści o charakterze terrorystycznym w internecie Komisja wzywa Parlament Europejski i Radę do:

- rozpoczęcia negocjacji w sprawie wniosku ustawodawczego mającego na celu zapobieganie **rozpowszechnianiu w internecie treści o charakterze terrorystycznym**, z myślą o osiągnięciu szybkiego porozumienia w sprawie unijnych ram regulacyjnych zawierających jasne zasady i gwarancje.

2. Podnoszenie poziomu cyberbezpieczeństwa

Cyberbezpieczeństwo pozostaje jednym z głównych wyzwań w zakresie bezpieczeństwa. UE poczyniła wymierne postępy[10] w zwalczaniu „klasycznych" zagrożeń sieciowych dotyczących systemów i danych, realizując działania określone we wspólnym komunikacie z września 2017 r.[11] „Odporność, prewencja i obrona: budowanie solidnego bezpieczeństwa cybernetycznego Unii Europejskiej". Obejmują one również akt UE w sprawie cyberbezpieczeństwa[12], który daje Agencji Unii Europejskiej ds. Cyberbezpieczeństwa stały mandat, wzmacnia jej rolę i ustanawia unijne ramy certyfikacji cyberbezpieczeństwa. Komisja poruszyła również kwestię wymogów sektorowych, na przykład poprzez swoje zalecenie w sprawie cyberbezpieczeństwa w sektorze energetycznym przyjęte w dniu 3 kwietnia 2019 r.[13]. Jednak stały wzrost aktywności podmiotów działających w złych intencjach, atakujących różne cele i ofiary, oznacza, że wysiłki na rzecz zwalczania cyberprzestępczości i zwiększenia cyberbezpieczeństwa pozostają priorytetem działań UE.

Parlament Europejski i Rada nadal muszą osiągnąć porozumienie w sprawie priorytetowej inicjatywy Komisji dotyczącej **Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji**[14]. Wniosek ten ma na celu wspieranie technologicznych i przemysłowych zdolności w dziedzinie cyberbezpieczeństwa oraz zwiększenie konkurencyjności unijnej branży cyberbezpieczeństwa. Obaj współprawodawcy przyjęli mandaty negocjacyjne w marcu 2019 r. Ponieważ zakończenie negocjacji międzyinstytucjonalnych nie było możliwe przed końcem

[10] Więcej informacji można znaleźć w broszurze pt. „Jak zapewnić cyberbezpieczeństwo w Unii Europejskiej: odporność, odstraszanie, obrona": https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

[11] JOIN(2017) 450 final (13.9.2017).

[12] Akt UE w sprawie cyberbezpieczeństwa (rozporządzenie (UE) 2019/881 z dnia 17 kwietnia 2019 r.) po raz pierwszy wprowadza ogólnounijne przepisy dotyczące certyfikacji cyberbezpieczeństwa produktów, procesów i usług. Przewiduje on ponadto nowy stały mandat Agencji UE ds. Cyberbezpieczeństwa oraz zwiększenie zasobów potrzebnych do realizacji jej celów. Więcej informacji na temat zaproszenia do składania wniosków można znaleźć na stronie internetowej: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

[13] C(2019) 2400 final (3.4.2019) i SWD(2019) 1240 final (3.4.2019).

[14] COM(2018) 630 final z 12.9.2018.

poprzedniej kadencji Parlamentu Europejskiego, przyjął on formalnie stanowisko w pierwszym czytaniu. W międzyczasie trwają dyskusje między państwami członkowskimi w Radzie, ze szczególnym naciskiem na interakcję między proponowanym rozporządzeniem ustanawiającym europejskie centrum i sieć kompetencji w dziedzinie cyberbezpieczeństwa z jednej strony a programami „Horyzont Europa" i „Cyfrowa Europa" z drugiej strony. **Komisja wzywa obu współprawodawców do wznowienia i szybkiego zakończenia międzyinstytucjonalnych negocjacji w sprawie tej priorytetowej inicjatywy na rzecz zwiększenia cyberbezpieczeństwa.**

Komisja nadal **wspiera badania naukowe i innowacje** związane z cyberbezpieczeństwem, udostępniając 135 mln EUR w obecnych wieloletnich ramach finansowych na projekty w obszarach takich jak cyberbezpieczeństwo w infrastrukturze krytycznej, inteligentne systemy zarządzania bezpieczeństwem i prywatnością oraz narzędzia przeznaczone specjalnie dla obywateli oraz małych i średnich przedsiębiorstw[15]. W lipcu 2019 r. Komisja opublikowała nowe zaproszenie do składania wniosków w ramach instrumentu „Łącząc Europę", udostępniając 10 mln EUR ze środków UE na finansowanie kluczowych podmiotów określonych w dyrektywie w sprawie bezpieczeństwa sieci i systemów informatycznych[16], takich jak europejskie zespoły reagowania na incydenty bezpieczeństwa komputerowego, operatorzy usług kluczowych (np. banki, szpitale, dostawcy usług użyteczności publicznej, linie lotnicze, dostawcy nazw domen) oraz różne organy publiczne. Po raz pierwszy europejskie organy ds. certyfikacji cyberbezpieczeństwa również kwalifikują się do ubiegania się o udział w tym programie, aby móc wdrożyć akt bezpieczeństwa cybernetycznego UE.

W dniu 17 maja 2019 r. Rada przyjęła **system sankcji**, który umożliwia UE stosowanie ukierunkowanych środków ograniczających w celu zapobiegania cyberatakom stanowiącym zagrożenie zewnętrzne dla UE lub jej państw członkowskich i reagowania na nie. Nowy system sankcji jest częścią **unijnego zestawu narzędzi dyplomacji cyfrowej**[17], czyli ram umożliwiających wspólne reagowanie w skali UE na szkodliwe działania w sieci.[18] Dzięki nim UE może zapobiegać szkodliwym działaniom w cyberprzestrzeni i reagować na nie z wykorzystaniem wszystkich środków dostępnych w ramach wspólnej polityki zagranicznej i bezpieczeństwa.

Oprócz działań w obliczu zagrożeń cybernetycznych dla systemów i danych UE podejmuje również działania w celu sprostania złożonym i wieloaspektowym wyzwaniom związanym z **zagrożeniami hybrydowymi**[19]. W swoich konkluzjach z 21 czerwca 2019 r. Rada Europejska [20]podkreśliła, że „UE musi zapewnić skoordynowane reagowanie na zagrożenia hybrydowe i cybernetyczne i zwiększyć współpracę z właściwymi podmiotami na szczeblu międzynarodowym". Komisja z zadowoleniem przyjmuje fakt, że przeciwdziałanie zagrożeniom hybrydowym stanowi również priorytet fińskiej prezydencji w Radzie oraz że na nieformalnym posiedzeniu ministrów sprawiedliwości i spraw wewnętrznych w Helsinkach w dniach 18–19 lipca 2019 r. przeprowadzono dyskusję na temat kierunków polityki w sprawie zagrożeń hybrydowych. Podobne dyskusje na temat zagrożeń hybrydowych toczyły się między dyrektorami ds. polityki obrony UE w dniach 7–8 lipca 2019 r. oraz między dyrektorami politycznymi UE w dniach 9–10 lipca 2019 r., a ich wyniki zostaną przekazane ministrom spraw zagranicznych i ministrów obrony podczas wspólnej nieformalnej sesji w dniach 29–

---

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Dyrektywa (UE) 2016/1148 (6.7.2016).

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pl/pdf

18 Obejmują one ataki cybernetyczne oraz ich próby o potencjalnie znaczących skutkach, w tym np. dostęp do systemów informacyjnych lub przechwytywanie danych przez infrastrukturę cyfrową, taką jak sieci 5G (zob. również sekcja III dotycząca zwiększenia bezpieczeństwa infrastruktury cyfrowej).

19 Zob. sprawozdanie w sprawie wdrażania wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym z 2016 r. oraz wspólny komunikat z 2018 r. w sprawie zwiększania odporności na zagrożenia hybrydowe i wzmacniania zdolności do reagowania na nie (SWD(2019) 200 final z 28.5.2019). Zob. również wniosek ustawodawczy z września 2016 r. dotyczący rozporządzenia ustanawiającego unijny system kontroli wywozu, transferu, pośrednictwa, pomocy technicznej i tranzytu w odniesieniu do produktów podwójnego zastosowania (wersja przekształcona) (COM(2016) 616 final z 28.9.2016).

20 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf

Aby podnieść poziom cyberbezpieczeństwa, Komisja wzywa Parlament Europejski i Radę do:
• szybkiego osiągnięcia porozumienia w sprawie wniosku ustawodawczego w sprawie **Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji** .

3. Poprawa dostępu organów ścigania do elektronicznego materiału dowodowego

UE podjęła dalsze działania, aby pozbawić terrorystów i przestępców środków do działania, utrudniając im dostęp do prekursorów materiałów wybuchowych[21], finansowanie działalności[22] i podróżowanie bez bycia zauważonym[23].

Negocjacje w sprawie wniosków Komisji z kwietnia 2018 r. mających na celu poprawę **dostępu organów ścigania do elektronicznego materiału dowodowego** powinny zostać zakończone w możliwie najkrótszym terminie – ponad połowa wszystkich dochodzeń w sprawie przestępstw wiąże się obecnie z transgranicznym wnioskiem o dostęp do dowodów elektronicznych[24]. Rada przyjęła swoje stanowisko negocjacyjne w sprawie wniosku dotyczącego rozporządzenia[25] mającego poprawić transgraniczny dostęp do elektronicznego materiału dowodowego w dochodzeniach oraz wniosku w sprawie dyrektywy[26] ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych. Z uwagi na kluczowe znaczenie, jakie skuteczny dostęp do elektronicznego materiału dowodowego ma dla prowadzenia dochodzeń i ścigania przestępstw transgranicznych takich jak terroryzm czy cyberprzestępczość, Komisja wzywa Parlament Europejski do poczynienia postępów w pracach nad odnośnym wnioskiem, aby umożliwić współprawodawcom jego szybkie przyjęcie.

Równolegle Komisja pracuje nad poprawą i zapewnieniem niezbędnych zabezpieczeń w **międzynarodowej wymianie dowodów elektronicznych** w kontekście toczących się negocjacji nad drugim dodatkowym protokołem do budapeszteńskiej konwencji Rady Europy o cyberprzestępczości, a także ze Stanami Zjednoczonymi, zgodnie z mandatami negocjacyjnymi udzielonymi przez Radę na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniach 6–7 czerwca 2019 r.[27]. W dniach 9–11 lipca 2019 r. Komisja uczestniczyła w ostatniej rundzie negocjacji w sprawie drugiego dodatkowego protokołu do budapeszteńskiej konwencji Rady Europy w sprawie cyberprzestępczości. Komisja i władze Stanów Zjednoczonych przygotowują

---

21 Rozporządzenie (UE) 2019/1148 (20.6.2019) w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych.

22 Dyrektywa (UE) 2019/1153 (11.7.2019) ustanawiająca zasady ułatwiające korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania.

23 Rozporządzenie (UE) 2019/1157 (20.6.2019) w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się.

24 Elektroniczne materiały dowodowe są potrzebne w około 85 % dochodzeń w sprawach karnych, a w przypadku dwóch trzecich dochodzeń istnieje potrzeba uzyskania materiałów dowodowych od dostawców usług internetowych mających siedzibę w innej jurysdykcji. Zob. ocena skutków towarzysząca wnioskowi ustawodawczemu (SWD (2018) 118 final (17.4.2018).

25 COM(2018) 225 final (17.4.2018). Rada przyjęła swój mandat negocjacyjny w sprawie proponowanego rozporządzenia w dniu 7 grudnia 2018 r. na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych.

26 COM(2018) 226 final (17.4.2018). Rada przyjęła swoje stanowisko negocjacyjne w sprawie proponowanej dyrektywy w dniu 8 marca 2019 r. na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych.

27 https://www.consilium.europa.eu/pl/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

obecnie na szczeblu technicznym formalne rozpoczęcie negocjacji w sprawie umowy między Unią Europejską a Stanami Zjednoczonymi w sprawie transgranicznego dostępu do dowodów elektronicznych.

Aby poprawić dostęp organów ścigania do dowodów elektronicznych, Komisja wzywa Parlament Europejski do:

- przyjęcia mandatu negocjacyjnego w sprawie wniosków ustawodawczych dotyczących **elektronicznego materiału dowodowego** w celu szybkiego rozpoczęcia rozmów trójstronnych z Radą. *(priorytet wspólnej deklaracji)*

4. Sprawniejsze i bardziej inteligentne systemy informacyjne służące zarządzaniu bezpieczeństwem, granicami i migracjami

Po przyjęciu przepisów dotyczących **interoperacyjności systemów informacyjnych**[28], które pozwolą wyeliminować luki informacyjne i martwe pola, pomagając w wykrywaniu multiplikacji tożsamości i zwalczaniu oszustw dotyczących tożsamości, Komisja szybko uruchomiła szereg inicjatyw mających na celu wsparcie państw członkowskich w procesie ich wdrażania, w tym w razie potrzeby finansowanie, a także warsztaty służące wymianie wiedzy fachowej i najlepszych praktyk. Ścisła współpraca między agencjami UE, wszystkimi państwami członkowskimi i państwami stowarzyszonymi w ramach Schengen będzie miała zasadnicze znaczenie dla osiągnięcia do 2020 r. ambitnego celu pełnej interoperacyjności systemów informacyjnych UE służących do zarządzania bezpieczeństwem, granicami i migracją.

Warunkiem osiągnięcia tego celu jest również szybkie i pełne wdrożenie uzgodnionych ostatnio przepisów, aby stworzyć nowe systemy informacyjne – unijny system wjazdu/wyjazdu[29] i europejski system informacji o podróży oraz zezwoleń na podróż[30] – a także wzmocnić System Informacyjny Schengen[31] i rozszerzyć europejski system przekazywania informacji z rejestrów karnych[32] na obywateli państw trzecich. Nowa struktura silniejszych i inteligentniejszych systemów informacyjnych służących do zarządzania bezpieczeństwem, granicami i migracją poprawi sytuację w terenie jedynie wówczas, gdy wszystkie elementy zostaną w pełni i zgodnie z ustalonym harmonogramem wdrożone na szczeblu unijnym i przez każde państwo członkowskie.

Jednocześnie współprawodawcy muszą podjąć dalsze działania w celu ukończenia prac nad silniejszymi i inteligentniejszymi systemami informacji na potrzeby zarządzania bezpieczeństwem, granicami i migracją.
W ramach technicznego wdrażania **europejskiego systemu informacji o podróży oraz zezwoleń na podróż** Komisja przedstawiła w dniu 7 stycznia 2019 r. dwa wnioski wprowadzające zmiany techniczne do odnośnego rozporządzenia[33], które są konieczne do pełnego wdrożenia systemu. Komisja wzywa współprawodawców do przyspieszenia prac nad wspomnianymi zmianami technicznymi w celu jak najszybszego osiągnięcia porozumienia, dzięki czemu możliwe będzie sprawne i terminowe wdrożenie systemu ETIAS oraz jego uruchomienie na początku 2021 r.

W maju 2018 r. Komisja przedstawiła wniosek mający **wzmocnić istniejący wizowy system informacyjny**[34], który umożliwi dokładniejsze sprawdzanie przeszłości osób ubiegających się o wizę oraz wyeliminowanie luk informacyjnych dzięki lepszej wymianie informacji między państwami

[28] Rozporządzenie (UE) 2019/817 (20.5.2019) i rozporządzenie (UE) 2019/818 (20.5.2019).
[29] Rozporządzenie (UE) 2017/2226 (30.11.2017).
[30] Rozporządzenie (UE) 2018/1240 (12.9.2018) i rozporządzenie (UE) 2018/1241 (12.9.2018).
[31] Rozporządzenie (UE) 2018/1860 (28.11.2018), rozporządzenie (UE) 2018/1861 (28.11.2018), rozporządzenie (UE) 2018/1862 (28.11.2018).
[32] Rozporządzenie (UE) 2019/816 (17.4.2019).
[33] COM(2019) 3 final oraz COM(2019) 4 final (7.1.2019).
[34] COM(2018) 302 final (16.5.2018).

członkowskimi
Rada przyjęła swój mandat negocjacyjny w dniu 19 grudnia 2018 r., a w dniu 13 marca 2019 r. na posiedzeniu plenarnym Parlamentu Europejskiego odbyło się głosowanie nad sprawozdaniem dotyczącym tego wniosku, kończące pierwsze czytanie. Komisja wzywa obu współprawodawców, by w ramach nowej kadencji Parlamentu Europejskiego szybko rozpoczęli negocjacje w tej sprawie.

W maju 2016 r. Komisja przedstawiła wniosek w sprawie rozszerzenia zakresu systemu **Eurodac**[35] tak, aby obejmował on nie tylko identyfikację osób ubiegających się o azyl, ale także obywateli państw trzecich nielegalnie przebywających w UE i przybywających do UE niezgodnie z prawem. Zgodnie z konkluzjami Rady Europejskiej z grudnia 2018 r.[36] oraz komunikatem Komisji z dnia 6 marca 2019 r. w sprawie postępów w realizacji Europejskiego programu w zakresie migracji[37] Komisja wzywa współprawodawców do przyjęcia tego wniosku. Przyjęcie tych wniosków ustawodawczych jest konieczne, aby Eurodac mógł się stać częścią przyszłej struktury interoperacyjnych systemów informacyjnych UE i wzbogacić ją o istotne dane dotyczące obywateli państw trzecich nielegalnie przebywających na terytorium UE i przybywających do UE niezgodnie z prawem.

Aby wzmocnić systemy informacyjne służące zarządzaniu bezpieczeństwem, granicami i migracjami, Komisja wzywa Parlament Europejski i Radę:

- do przyjęcia wniosku ustawodawczego w sprawie **Eurodac** *(priorytet wspólnej deklaracji)*;
- do poczynienia postępów w pracach z myślą o osiągnięciu szybkiego porozumienia w sprawie proponowanych zmian technicznych koniecznych do ustanowienia **europejskiego systemu informacji o podróży oraz zezwoleń na podróż**.

III. ZWIĘKSZENIE BEZPIECZEŃSTWA INFRASTRUKTURY CYFROWEJ

Odporność naszej cyfrowej infrastruktury ma kluczowe znaczenie dla rządów i przedsiębiorstw, dla bezpieczeństwa naszych danych osobowych i funkcjonowania naszych instytucji demokratycznych. **Sieci piątej generacji (5G)**, które zostaną uruchomione w najbliższych latach, będą stanowić cyfrowy szkielet naszych społeczeństw i gospodarek, łącząc miliardy obywateli, obiekty i systemy, m.in. w krytycznych sektorach, takich jak energetyka, transport, bankowość i ochrona zdrowia, a także systemy kontroli przemysłowej zawierające informacje szczególnie chronione i wspierające systemy bezpieczeństwa.

Technologia 5G, która w 2025 r. będzie według szacunków generować w skali globalnej przychody rzędu 225 mld euro, stanowi kluczowy atut Europy, który pozwoli jej konkurować na światowych rynkach, a **bezpieczeństwo sieci 5G ma zatem decydujące znaczenie dla zapewnienia strategicznej autonomii Unii**. Zapewnienie wysokiego poziomu cyberbezpieczeństwa wymaga skoordynowanych działań zarówno na szczeblu krajowym, jak i europejskim, ponieważ wszelkie słabe punkty sieci 5G w jednym państwie członkowskim miałyby wpływ na całą Unię.

Po wyrażeniu w marcu 2019 r. w Radzie Europejskiej poparcia przez szefów państw lub rządów[38] Komisja przedstawiła w dniu 26 marca 2019 r. **zalecenie w sprawie cyberbezpieczeństwa sieci 5G**[39], określające działania w zakresie analizy zagrożeń cyberbezpieczeństwa związanych z sieciami 5G oraz wzmocnienie środków zapobiegawczych. Zalecenia opierają się na skoordynowanej unijnej ocenie ryzyka i środkach zarządzania ryzykiem, skutecznych ramach współpracy i wymiany informacji oraz wspólnej orientacji sytuacyjnej UE obejmującej krytyczne sieci łączności.

---

35 COM(2016) 272 final (4.5.2016).
36 https://www.consilium.europa.eu/pl/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
37 COM(2019) 126 final (6.3.2019).
38 https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/pl/pdf
39 C(2019) 2335 final (26.3.2019).

Jako **pierwszy etap** procesu zapoczątkowanego zaleceniem, do dnia 15 lipca 2019 r. wszystkie państwa członkowskie zakończyły swoją **krajową ocenę ryzyka** i przedstawiły swoje ustalenia Komisji i Agencji UE ds. Cyberbezpieczeństwa lub ogłosiły, że wkrótce to uczynią. Krajowe oceny ryzyka przeprowadzono według zbioru wytycznych i wspólnego wzoru sprawozdań z ustaleń, uzgodnionych przez państwa członkowskie i Komisję w celu promowania spójności i ułatwienia wymiany informacji na temat wyników krajowych na szczeblu UE. Parametry oceniane we wszystkich państwach członkowskich obejmowały:

- główne zagrożenia i podmioty stanowiące zagrożenie mające wpływ na sieci 5G;
- stopień wrażliwości elementów i funkcji sieci 5G oraz innych aktywów oraz
- różne typy podatności na zagrożenia, w tym zagrożenia techniczne i inne, np. potencjalnie związane z łańcuchem dostaw 5G.

Ponadto w prace nad krajowymi ocenami ryzyka zaangażowanych było szereg podmiotów odpowiedzialnych w państwach członkowskich, w tym, w zależności od kompetencji w danym kraju, organy ds. cyberbezpieczeństwa, telekomunikacji oraz służby bezpieczeństwa i wywiadu, które zacieśniły współpracę i koordynację swoich działań. Równolegle, zgodnie ze swoimi krajowymi harmonogramami uruchamiania sieci 5G, szereg państw członkowskich podjęło już kroki w celu zaostrzenia wymogów w zakresie bezpieczeństwa w tym obszarze, a kilka innych zasygnalizowało, że zamierza rozważyć wprowadzenie w najbliższej przyszłości nowych środków.

W oparciu o wyniki krajowej oceny ryzyka organy ds. cyberbezpieczeństwa z poszczególnych państw członkowskich w grupie współpracy ds. bezpieczeństwa sieci i systemów informatycznych[40] przygotują do dnia 1 października 2019 r. **wspólny przegląd zagrożeń na szczeblu UE**, który będzie stanowić drugi etap procesu zapoczątkowanego zaleceniem. Na tej podstawie w trzecim etapie grupa współpracy przygotuje do dnia 31 grudnia 2019 r. **wspólny zestaw unijnych środków zaradczych** w celu wyeliminowania zidentyfikowanych zagrożeń. Komisja oraz Agencja UE ds. Cyberbezpieczeństwa będą nadal wspierać wdrażanie zalecenia.

Prace grupy współpracy ds. bezpieczeństwa sieci i systemów informatycznych wspierane są przez kilka innych forów. Organ Europejskich Regulatorów Łączności Elektronicznej przygotowuje analizę wszystkich istniejących środków bezpieczeństwa, które mogą mieć znaczenie dla sieci 5G. Nowa specjalna grupa ekspertów w Agencji UE ds. Cyberbezpieczeństwa rozpoczęła prace nad sprawozdaniem przekrojowym zagrożeń 5G. Ponadto, w następstwie wejścia w życie w dniu 27 czerwca 2019 r. aktu o cyberbezpieczeństwie, Komisja i Agencja UE ds. Cyberbezpieczeństwa podejmą wszelkie niezbędne kroki w celu ustanowienia ogólnounijnych ram certyfikacji. Państwa członkowskie spotkały się również w czerwcu 2019 r. w ramach komitetu ds. norm, aby omówić cyberbezpieczeństwo i normalizację w odpowiedzi na zalecenie, aby zbadać przyszłe wyzwania związane z normalizacją cyberbezpieczeństwa, w tym sieci 5G, i rozpatrzyć odpowiednie inicjatywy polityczne na szczeblu UE.

Bezpieczeństwo sieci 5G ma również dla Unii strategiczne znaczenie. Inwestycje zagraniczne w sektorach strategicznych, nabywanie aktywów, technologii i infrastruktury o krytycznym znaczeniu w Unii oraz dostawy urządzeń mających krytyczne znaczenie mogą również stanowić zagrożenie dla bezpieczeństwa Unii.

[40] Grupa współpracy ds. bezpieczeństwa sieci i systemów informatycznych została powołana na mocy dyrektywy (UE) 2016/1148 (6.7.2016 r.) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Jak przewidziano w zaleceniu, w ramach grupy współpracy ds. bezpieczeństwa sieci i systemów informatycznych utworzono specjalny obszar prac pod kierownictwem kilku państw członkowskich. Grupa ta spotkała się już trzykrotnie – w kwietniu, maju i lipcu 2019 r. – w celu wymiany informacji na temat podejść krajowych i omówienia sposobów sprawniejszego przygotowania skoordynowanej oceny ryzyka UE.

Nowe **unijne ramy dotyczące monitorowania bezpośrednich inwestycji zagranicznych**[41] weszły w życie z dniem 10 kwietnia 2019 r. W ciągu najbliższych 18 miesięcy Komisja i państwa członkowskie UE podejmą niezbędne kroki, aby zagwarantować, że UE będzie mogła od dnia 11 października 2020 r. w pełni stosować rozporządzenie w sprawie monitorowania inwestycji.

IV. PRZECIWDZIAŁANIE PRANIU PIENIĘDZY

Zdolność przestępców i terrorystów do przelewania środków między rachunkami bankowymi w kilka godzin umożliwia im łatwiejsze przygotowanie aktów terroru lub pranie w różnych państwach członkowskich dochodów pochodzących z działalności przestępczej. Aby sprostać temu wyzwaniu, Unia opracowała solidne **ramy regulacyjne dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu**, zgodnie z międzynarodowymi standardami przyjętymi przez Grupę Specjalną ds. Przeciwdziałania Praniu Pieniędzy.

Biorąc pod uwagę konieczność dotrzymywania kroku zmieniającym się tendencjom, rozwojowi technologicznemu i zdolnościom przestępców do wykorzystywania wszelkich luk lub niedoskonałości w systemie, w dniu 24 lipca 2019 r. Komisja przyjęła **pakiet czterech sprawozdań**, w których przeanalizowano obecne zagrożenia i podatność na zagrożenia związane z praniem pieniędzy oraz oceniono sposób stosowania ram regulacyjnych przez odpowiednie podmioty zarówno w sektorze prywatnym, jak i publicznym[42].

Pakiet zawiera **ocenę potencjalnych połączeń między krajowymi scentralizowanymi rejestrami rachunków bankowych** i **systemów wyszukiwania danych** w UE. Takie scentralizowane krajowe systemy umożliwiają identyfikację każdej osoby fizycznej lub prawnej posiadającej lub kontrolującej rachunki płatnicze, rachunki bankowe i skrytki depozytowe – taka informacja ma często kluczowe znaczenie dla właściwych organów w walce z praniem pieniędzy i finansowaniem terroryzmu. Piąta dyrektywa w sprawie przeciwdziałania praniu pieniędzy[43] nakłada na państwa członkowskie obowiązek ustanowienia takich scentralizowanych systemów i zapewnienia bezpośredniego dostępu do nich swoim krajowym jednostkom analityki finansowej. Niedawno przyjęte przepisy mające na celu ułatwienie wykorzystywania informacji finansowych do zwalczania poważnych przestępstw[44] zapewniają wyznaczonym organom ścigania i biurom ds. odzyskiwania mienia bezpośredni dostęp do ich odpowiednich krajowych scentralizowanych rejestrów rachunków bankowych. W oparciu o to, zgodnie z wymogami dyrektywy w sprawie przeciwdziałania praniu pieniędzy, sprawozdanie zawiera ocenę różnych rozwiązań informatycznych na szczeblu UE, które już funkcjonują lub są opracowywane, które mogą posłużyć jako model możliwego połączenia krajowych scentralizowanych systemów. Biorąc pod uwagę, że przyszła ogólnoeuropejska sieć połączeń między scentralizowanymi mechanizmami przyspieszyłaby dostęp do informacji finansowych i ułatwiłaby współpracę

---

41 Rozporządzenie (UE) 2019/452 z 19.3.2019 r. ustanawiające ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii. Te nowe ramy tworzą mechanizm współpracy, w ramach którego państwa członkowskie i Komisja będą mogły wymieniać informacje i sygnalizować obawy związane z konkretnymi inwestycjami. Umożliwi to Komisji wydawanie opinii, gdy dana inwestycja zagraża bezpieczeństwu lub porządkowi publicznemu w więcej niż jednym państwie członkowskim, lub gdy może zaszkodzić realizacji projektu lub programu mającego znaczenie dla całej UE. Państwo członkowskie, w którym dokonano inwestycji, ma ostatnie słowo w odniesieniu do sposobu traktowania inwestycji.

42 Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM (2019) 370 final z 24.7.2019) (w jęz. angielskim), Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts (COM(2019) 372 final z 24.7.2019) (w jęz. angielskim), Report on the assessment of recent alleged money laundering cases involving EU credit institutions (COM(2019) 373 final z 24.7.2019) (w jęz. angielskim), Report assessing the framework for cooperation between Financial Intelligence Units (COM(2019) 371 final z 24.7.2019) (w jęz. angielskim).

43 Dyrektywa (UE) 2015/849 (20.5.2015).

44 Dyrektywa (UE) 2019/1153 (20.6.2019).

transgraniczną między właściwymi organami, Komisja zamierza przeprowadzić dalsze konsultacje z odpowiednimi zainteresowanymi stronami, rządami oraz jednostkami analityki finansowej, organami ścigania i biurami ds. odzyskiwania mienia jako potencjalnymi „użytkownikami końcowymi" ewentualnego systemu wzajemnych połączeń.

W ramach rozważań Komisji na temat działalności jednostek analityki finansowej sprawozdanie oceniające **współpracę między jednostkami analityki finansowej** dotyczy zarówno współpracy w obrębie Unii, jak i z państwami trzecim[45]. Wskazano w nim pewne niedociągnięcia, które prawdopodobnie będą nadal istnieć, dopóki zadania i obowiązki w zakresie transgranicznej współpracy jednostek analityki finansowej nie zostaną wyraźniej określone w unijnych ramach prawnych dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Ocena wskazuje również na potrzebę wzmocnienia mechanizmu koordynacji i wspierania transgranicznej współpracy i analiz.

Wychodząc poza dotychczasowe działania dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, a także w odpowiedzi na wezwanie ze strony Parlamentu Europejskiego[46] Komisja będzie nadal przeprowadzać ocenę konieczności, technicznej wykonalności i proporcjonalności dodatkowych środków śledzenia finansowania terroryzmu w UE[47].

V. WDRAŻANIE INNYCH PRIORYTETOWYCH INICJATYW DOTYCZĄCYCH BEZPIECZEŃSTWA

1. Wdrażanie środków ustawodawczych w ramach unii bezpieczeństwa

Osiągnięcie porozumienia w sprawie środków w ramach unii bezpieczeństwa nie jest końcem tego procesu – niezbędne jest następnie zapewnienie ich szybkiego i pełnego wdrożenia przez państwa członkowskie, tak aby można było z tych środków w pełni korzystać. W tym celu Komisja aktywnie wspiera państwa członkowskie, m.in. udostępniając środki finansowe i ułatwiając wymianę najlepszych praktyk.
W stosownych przypadkach Komisja gotowa jest jednak w pełni wykorzystać przysługujące jej na mocy Traktatów uprawnienia w zakresie egzekwowania prawa Unii, m.in. wszcząć w stosownych przypadkach postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego.

Termin wdrożenia **unijnej dyrektywy w sprawie danych dotyczących przelotu pasażera**[48] upłynął w dniu 25 maja 2018 r. Do tej pory 25 państw członkowskich zgłosiło Komisji pełną transpozycję[49]. Pomimo wszczętych w dniu 19 lipca 2018 r. postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego w dwóch państwach członkowskich pełna transpozycja nadal nie została przeprowadzona[50]. Równocześnie Komisja w dalszym ciągu wspiera wszystkie państwa członkowskie w działaniach zmierzających do ukończenia tworzenia ich systemów zarządzania danymi dotyczącymi przelotu pasażera, między innymi poprzez ułatwianie wymiany informacji i najlepszych praktyk.

---

45 Ocena ta jest wymagana na mocy art. 65 ust. 2 piątej dyrektywy (UE) 2018/843 w sprawie przeciwdziałania praniu pieniędzy (30.5.2018).

46 W swoim sprawozdaniu końcowym przyjętym w grudniu 2018 r. Komisja Specjalna ds. Terroryzmu Parlamentu Europejskiego wezwała do ustanowienia unijnego systemu śledzenia finansowania terroryzmu, skupiającego się na transakcjach dokonywanych przez osoby powiązane z terroryzmem i jego finansowaniem w ramach jednolitego obszaru płatności w euro.

47 Zob. osiemnaste sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2019) 145 final z 20.3.2019).

48 Dyrektywa (UE) 2016/681 (27.4.2016).

49 Powyższe informacje o zgłoszonej pełnej transpozycji opierają się na deklaracjach państw członkowskich i pozostają bez uszczerbku dla kontroli transpozycji przeprowadzanej przez służby Komisji.

50 Słowenia zgłosiła jej częściową transpozycję. Hiszpania nie zgłosiła transpozycji (stan na dzień 24 lipca 2019 r.).

Termin transpozycji **dyrektywy w sprawie zwalczania terroryzmu**[51] upłynął w dniu 8 września 2018 r. Do tej pory 22 państw członkowskich zgłosiło Komisji pełną transpozycję. Trzy państwa członkowskie nadal nie zgłosiły przyjęcia przepisów krajowych w pełni transponujących dyrektywę, pomimo wszczętych w dniu 22 listopada 2018 r. postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego.[52]

Termin transpozycji **dyrektywy w sprawie kontroli nabywania i posiadania broni**[53] upłynął w dniu 14 września 2018 r. Do tej pory 8 państw członkowskich zgłosiło Komisji pełną transpozycję. 20 państw członkowskich nadal nie zgłosiło przyjęcia krajowych środków w pełni transponujących dyrektywę, pomimo wszczętych w dniu 22 listopada 2018 r. postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego[54].

Termin transpozycji do prawa krajowego **dyrektywy o ochronie danych w sprawach karnych**[55] upłynął w dniu 6 maja 2018 r. Do tej pory 20 państw członkowskich zgłosiło Komisji pełną transpozycję[56]. Siedem państw członkowskich nadal nie zgłosiło przyjęcia krajowych środków w pełni transponujących dyrektywę, pomimo wszczętych w dniu 19 lipca 2018 r. przez Komisję postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego[57].

Państwa członkowskie miały dokonać transpozycji do prawa krajowego **dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych**[58] do dnia 9 maja 2018 r. Do chwili obecnej 26 państw członkowskich zgłosiło Komisji pełną transpozycję dyrektywy, a 2 państwa członkowskie dokonały częściowej transpozycji[59]. Ponadto do dnia 9 listopada 2018 r., zgodnie z dyrektywą, państwa członkowskie były zobowiązane do identyfikacji operatorów usług kluczowych. Do dnia 9 maja 2019 r. Komisja miała przedłożyć Parlamentowi Europejskiemu i Radzie sprawozdanie oceniające spójność podejścia w zakresie identyfikacji operatorów usług kluczowych w państwach członkowskich. Ponieważ jednak kilka państw członkowskich nie przedłożyło jeszcze pełnych informacji na temat procesu identyfikacji, Komisja musiała przesunąć swoje sprawozdanie w czasie.

Komisja przeprowadza obecnie ocenę transpozycji **czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy**[60], a jednocześnie weryfikuje, czy państwa członkowskie wdrożyły odnośne przepisy. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 24 państwom członkowskim, ponieważ uznała, że przekazane przez nie informacje nie wskazują, że dokonały one pełnej transpozycji tej dyrektywy[61].

---

51 Dyrektywa (UE) 2017/541 (15.3.2017).

52 Polska zgłosiła jej częściową transpozycję. Grecja i Luksemburg nie zgłosiły transpozycji (stan na dzień 24 lipca 2019 r.).

53 Dyrektywa (UE) 2017/853 (17.5.2017).

54 Belgia, Czechy, Estonia, Litwa, Polska, Portugalia, Szwecja i Zjednoczone Królestwo zgłosiły dokonanie częściowej transpozycji. Niemcy, Irlandia, Grecja, Hiszpania, Cypr, Luksemburg, Węgry, Niderlandy, Rumunia, Słowenia, Słowacja i Finlandia nie zgłosiły transpozycji (stan na dzień 24 lipca 2019 r.).

55 Dyrektywa (UE) 2016/680 (27.4.2016).

56 20 państw członkowskich zakończyło transpozycję (stan na dzień 24 lipca 2019 r.).

57 Łotwa, Portugalia, Słowenia i Finlandia zgłosiły dokonanie częściowej transpozycji. Grecja i Hiszpania nie zgłosiły transpozycji. Niemcy zgłosiły pełną transpozycję, jednak zdaniem Komisji nie jest ona kompletna (stan na dzień 24 lipca 2019 r.).

58 Dyrektywa (UE) 2016/1148 (27.4.2016).

59 Belgia i Węgry dokonały częściowej transpozycji dyrektywy (stan na dzień 24 lipca 2019 r.).

60 Dyrektywa (UE) 2015/849 (20.5.2015).

61 Belgia, Bułgaria, Czechy, Dania Niemcy, Estonia, Irlandia, Hiszpania, Francja, Włochy, Cypr, Łotwa, Litwa, Węgry, Niderlandy, Austria, Polska, Portugalia, Rumunia, Słowenia, Słowacja, Finlandia, Szwecja i Zjednoczone Królestwo (stan na dzień 24 lipca 2019 r.).

Komisja wzywa państwa członkowskie do pilnego zastosowania niezbędnych środków służących pełnej transpozycji następujących dyrektyw do prawa krajowego oraz zawiadomienia o tym Komisji:

- **dyrektywy UE w sprawie danych dotyczących przelotu pasażera**, w przypadku której 1 państwo członkowskie nadal musi zgłosić dokonanie jej transpozycji do prawa krajowego, a 1 państwo członkowskie musi uzupełnić to zgłoszenie[62];
- **dyrektywy w sprawie zwalczania terroryzmu**, w przypadku której 2 państwa członkowskie nadal muszą zgłosić dokonanie jej transpozycji do prawa krajowego, zaś 1 państwo członkowskie musi uzupełnić to zgłoszenie[63];
- **dyrektywy w sprawie kontroli nabywania i posiadania broni**, w odniesieniu do której 12 państw członkowskich nadal musi zgłosić dokonanie transpozycji do prawa krajowego, zaś 8 państw członkowskich musi uzupełnić to zgłoszenie[64];
- **dyrektywy o ochronie danych w sprawach karnych**, w odniesieniu do której 2 państwa członkowskie nadal muszą zgłosić dokonanie transpozycji do prawa krajowego, a 5 państw członkowskich musi uzupełnić to zgłoszenie[65];
- **dyrektywy w sprawie bezpieczeństwa systemów informatycznych**, w odniesieniu do której 2 państwa członkowskie nadal muszą uzupełnić zgłoszenie transpozycji[66]; oraz
- **czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy**, w odniesieniu do której 24 państwa członkowskie nadal muszą uzupełnić zgłoszenie transpozycji[67].

2. Przeciwdziałanie dezinformacji i ochrona wyborów przed innymi zagrożeniami cybernetycznymi

Ochrona procesów demokratycznych i instytucji przed dezinformacją i związanymi z nią zakłóceniami jest poważnym wyzwaniem dla społeczeństw na całym świecie. Aby rozwiązać ten problem, UE wprowadziła **solidne ramy skoordynowanych działań przeciwko dezinformacji**, z pełnym poszanowaniem wartości europejskich i praw podstawowych[68]. Jak stwierdzono we wspólnym komunikacie z dnia 14 czerwca 2019 r. w sprawie realizacji planu działania przeciwko dezinformacji[69], prace nad kilkoma uzupełniającymi się elementami pomogły zawęzić pole działania dla dezinformacji i zachować integralność wyborów do Parlamentu Europejskiego

Rada Europejska, w swoich konkluzjach z 21 czerwca 2019 r.[70], z zadowoleniem przyjęła zamiar Komisji przeprowadzenia dogłębnej oceny realizacji zobowiązań podjętych przez platformy

62 Słowenia zgłosiła jej częściową transpozycję. Hiszpania nie zgłosiła transpozycji (stan na dzień 24 lipca 2019 r.).

63 Polska zgłosiła jej częściową transpozycję. Grecja i Luksemburg nie zgłosiły transpozycji (stan na dzień 24 lipca 2019 r.).

64 Belgia, Czechy, Estonia, Litwa, Polska, Portugalia, Szwecja i Zjednoczone Królestwo zgłosiły dokonanie częściowej transpozycji. Niemcy, Irlandia, Grecja, Hiszpania, Cypr, Luksemburg, Węgry, Niderlandy, Rumunia, Słowenia, Słowacja i Finlandia nie zgłosiły transpozycji (stan na dzień 24 lipca 2019 r.).

65 Łotwa, Portugalia, Słowenia i Finlandia zgłosiły dokonanie częściowej transpozycji. Grecja i Hiszpania nie zgłosiły transpozycji. Niemcy zgłosiły pełną transpozycję, jednak zdaniem Komisji nie jest ona kompletna (stan na dzień 24 lipca 2019 r.).

66 Belgia i Węgry dokonały częściowej transpozycji dyrektywy (stan na dzień 24 lipca 2019 r.).

67 Belgia, Bułgaria, Czechy, Dania, Niemcy, Estonia, Irlandia, Hiszpania, Francja, Włochy, Cypr, Łotwa, Litwa, Węgry, Niderlandy, Austria, Polska, Portugalia, Rumunia, Słowenia, Słowacja, Finlandia, Szwecja i Zjednoczone Królestwo (stan na dzień 24 lipca 2019 r.).

68 Zob. Plan działania na rzecz zwalczania dezinformacji (JOIN (2018) 36 final z 5.12.2018).

69 JOIN (2019) 12 final (14.6.2019).

70 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf Apel Rady Europejskiej opiera się na wkładzie prezydencji rumuńskiej, a także Komisji i Wysokiej Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa w sprawie wniosków wyciągniętych w związku z dezinformacją i zapewnienia wolnych i uczciwych wyborów, w tym na wspólnym komunikacie w sprawie realizacji planu działania na rzecz zwalczania dezinformacji.

internetowe i innych sygnatariuszy na mocy **kodeksu postępowania w zakresie zwalczania dezinformacji**[71] i wezwała Komisję oraz Wysoką Przedstawiciel Unii Europejskiej do Spraw Zagranicznych i Polityki Bezpieczeństwa, aby w sposób ciągły oceniały i odpowiednio reagowały na „zmieniający się charakter zagrożeń, a także rosnące ryzyko złośliwych ingerencji i manipulacji w internecie, związane z rozwojem sztucznej inteligencji i technik gromadzenia informacji".

Komisja i Wysoka Przedstawiciel będą kontynuować prace w tej dziedzinie zgodnie z konkluzjami Rady Europejskiej. W marcu 2019 r. Komisja i Wysoka Przedstawiciel utworzyły **system wczesnego ostrzegania** między instytucjami UE a państwami członkowskimi w celu ułatwienia wymiany informacji na temat kampanii dezinformacyjnych oraz koordynacji działań. Pierwsze spotkanie pomiędzy punktami kontaktowymi państw członkowskich po wyborach do Parlamentu Europejskiego odbyło się w Tallinie w dniach 3–4 czerwca 2019 r. W celu dalszego wzmocnienia systemu wczesnego ostrzegania Wysoka Przedstawiciel i Komisja, w ścisłej współpracy z państwami członkowskimi, dokonają jesienią 2019 r. przeglądu funkcjonowania systemu wczesnego ostrzegania. Opracują one również wspólne metody analizy i reagowania na kampanie dezinformacyjne, a także wzmocnią partnerstwa z partnerami międzynarodowymi, takimi jak G7 i NATO.

Trwają również prace w ramach **Europejskiej Sieci Współpracy w zakresie Wyborów**[72], która w dniu 7 czerwca 2019 r. odbyła pierwsze posiedzenie w celu podsumowania wyborów do Parlamentu Europejskiego. Przemyślenia te, wraz z dalszymi informacjami od właściwych organów krajowych, partii politycznych i platform internetowych, przyczynią się do sporządzenia kompleksowego sprawozdania Komisji na temat wyborów do Parlamentu Europejskiego, które ma zostać przyjęte w październiku 2019 r. Państwa członkowskie wykorzystywały tę sieć w odniesieniu do innych wyborów niż do Parlamentu Europejskiego, co podkreśla jej szerszą przydatność do zapewnienia integralności demokracji w UE.

Komisja będzie również nadal monitorować i wspierać realizację zobowiązań podjętych przez platformy w **kodeksie postępowania w zakresie zwalczania dezinformacji**. Sprawozdania przedstawione przez Google, Twitter i Facebook w ramach kodeksu postępowania pokazują, że wszystkie platformy podjęły przed wyborami do Parlamentu Europejskiego działania, dokonując oznakowania reklam politycznych i udostępniając je publicznie za pośrednictwem przeszukiwalnych bibliotek reklamowych. Jednocześnie istnieją możliwości poprawy wskazane przez Europejską Grupę Regulatorów Audiowizualnych Usług Medialnych[73]. W szczególności nadal brakuje dostępu do szczegółowych surowych danych niezbędnych do kompleksowego monitorowania. Ponadto platformy powinny zapewnić środowiskom badawczym rzeczywisty dostęp do danych

[71] Kodeks praktyk został podpisany przez platformy internetowe Facebook, Google, Twitter i Mozilla, a także przez reklamodawców i branżę reklamową w październiku 2018 r. i określa on normy w zakresie samoregulacji mające na celu zwalczanie dezinformacji. Kodeks ma umożliwić osiągnięcie celów określonych w komunikacie Komisji z kwietnia 2018 r. w sprawie zwalczania dezinformacji w internecie (COM(2018)236 final z 26.4.2018 r.) poprzez ustanowienie szerokiego zakresu zobowiązań, od przejrzystości reklam politycznych po zamykanie fałszywych kont i pozbawianie podmiotów będących źródłem dezinformacji możliwości spieniężania treści.

[72] Europejska sieć współpracy ds. wyborów skupia punkty kontaktowe krajowych sieci współpracy wyborczej organów właściwych do spraw wyborów i organów odpowiedzialnych za monitorowanie i egzekwowanie istotnych w kontekście wyborczym przepisów dotyczących działalności w internecie. Europejska sieć współpracy ds. wyborów ma na celu ostrzeganie o zagrożeniach, wymianę najlepszych praktyk między sieciami krajowymi, omawianie wspólnych rozwiązań dla zidentyfikowanych wyzwań oraz zachęcanie do wspólnych projektów i ćwiczeń w ramach sieci krajowych.

[73] Europejska grupa regulatorów audiowizualnych usług medialnych zrzesza szefów lub przedstawicieli wysokiego szczebla krajowych niezależnych organów regulacyjnych w dziedzinie usług audiowizualnych, aby doradzać Komisji w kwestii wdrażania unijnej dyrektywy o audiowizualnych usługach medialnych (dyrektywa 2010/13/UE z 10.3.2010). Na swoim ostatnim posiedzeniu w dniach 20–21 czerwca 2019 r. w Bratysławie grupa przedstawiła wyniki prac przeprowadzonych do tej pory w zakresie dezinformacji, ze szczególnym uwzględnieniem wyborów do Parlamentu Europejskiego w 2019 r. oraz powiązanych obszarów reklamy politycznej i tematycznej.

zgodnie z przepisami dotyczącymi ochrony danych osobowych. Jeszcze w tym roku Komisja przeprowadzi kompleksową ocenę realizacji wszystkich zobowiązań wynikających z kodeksu postępowania w jego początkowym okresie trwającym 12 miesięcy. Na tej podstawie Komisja może rozważyć podjęcie dalszych działań, w tym o charakterze regulacyjnym, w celu poprawy długoterminowego reagowania UE na dezinformację.

3. Gotowość i ochrona

Wzmocnienie obrony i budowanie odporności na zagrożenia bezpieczeństwa to ważny aspekt działań na rzecz rzeczywistej i skutecznej unii bezpieczeństwa. Obejmuje to wsparcie udzielane przez Komisję państwom członkowskim i władzom lokalnym w celu **ochrony przestrzeni publicznej**[74], jak również udzielane państwom członkowskim wsparcie w zakresie wzmocnienia gotowości na **chemiczne, biologiczne, radiologiczne i jądrowe zagrożenia dla bezpieczeństwa**[75], m.in. wdrożenia dwóch planów działań w tej dziedzinie i analizy potrzeb w zakresie potencjału reagowania, który ma zostać stworzony w ramach rescEU[76]. Jeśli chodzi o zmieniające się zagrożenia chemiczne[77], Komisja we współpracy z państwami członkowskimi i w porozumieniu z partnerami międzynarodowymi opracowała wykaz substancji chemicznych stanowiących największe zagrożenie w przypadku wykorzystania do celów terrorystycznych. Wykaz UE stanowi podstawę dalszych prac mających na celu ograniczenie dostępności tych chemikaliów oraz współpracę z producentami w zakresie poprawy zdolności wykrywania.

Technologie w zakresie bezzałogowych statków powietrznych umożliwiają prowadzenie szerokiego zakresu możliwych operacji. W związku z szybkim rozwojem w ostatnich latach rynku systemów bezzałogowych statków powietrznych do celów wojskowych, cywilnych, handlowych i hobbystycznych, **drony** stanowią szansę, ale także coraz większe zagrożenie bezpieczeństwa dla infrastruktury krytycznej (w tym lotnictwa), przestrzeni publicznej i organizowanych imprez, podatnych na zagrożenia miejsc i osób fizycznych. W Europie wykorzystywano już drony do zakłócania operacji lotniczych i operacji egzekwowania prawa, do kontroli krytycznej infrastruktury oraz do przemytu do więzień oraz przez granice.

Komisja wspiera państwa członkowskie w przeciwdziałaniu rosnącemu zagrożeniu stwarzanemu przez drony dla obywateli i krytycznych funkcji społecznych, bez rezygnowania z ich praktycznego wykorzystywania, np. w operacjach reagowania kryzysowego. Komisja przyjęła niedawno **wspólne ogólnounijne przepisy w sprawie bezpiecznego stosowania dronów**[78] w celu zmniejszenia ryzyka

---

74 Zob. „Dobre praktyki organów publicznych i podmiotów prywatnych w zakresie zwiększania bezpieczeństwa przestrzeni publicznej", jak określono w osiemnastym sprawozdaniu z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM (2019) 145 final z 20.3.2019). Podstawą jest plan działania z października 2017 r. w zakresie wspierania ochrony przestrzeni publicznej (COM (2017) 612 final z 18.10.2017). W dniu 5 czerwca 2019 r. odbyło się trzecie posiedzenie forum operatorów w ramach Forum UE w sprawie ochrony przestrzeni publicznych. Zgromadziło ono przedstawicieli państw członkowskich UE i prywatnych operatorów przestrzeni publicznej, reprezentowanych przez 14 europejskich stowarzyszeń, obejmujących sektory: hotelarsko-gastronomiczny, występów na żywo, muzyki i rozrywki, parków rozrywki i atrakcji turystycznych, lotnictwa, transportu kolejowego, centrów handlowych, telekomunikacji, a także prywatnych usług ochroniarskich i producentów wyposażenia do ochrony bezpieczeństwa.

75 Zwłaszcza poprzez wdrożenie planu działania z października 2017 r. na rzecz zwiększania gotowości na wypadek chemicznych, biologicznych, radiologicznych i jądrowych zagrożeń dla bezpieczeństwa (COM (2017) 610 final z 18.10.2017).

76 Zob. art. 12 ust. 2 decyzji 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności (17.12.2013), zmienionej decyzją (UE) 2019/420 (13.3.2019).

77 Zob. wzmocnione działania przeciwko zagrożeniom chemicznym określone w piętnastym sprawozdaniu z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM (2018) 470 final z 13.6.2018).

78 Dz.U. L 152 z 11.6.2019 – rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.

związanego z ich użyciem w złych zamiarach. Zasady te obejmują przepisy wymagające rejestracji operatorów i umożliwiające identyfikację na odległość. Ponadto Komisja wspiera państwa członkowskie, monitorując tendencje w zakresie zagrożenia stwarzanego przez drony, finansując odpowiednie projekty badawcze i środki budowania zdolności, oraz ułatwiając wymianę między państwami członkowskimi i innymi zainteresowanymi stronami. W celu zwiększenia tego wsparcia Komisja zorganizuje w dniu 17 października 2019 r. międzynarodową konferencję wysokiego szczebla poświęconą przeciwdziałaniu zagrożeniom stwarzanym przez drony.

Odpowiadając na potrzebę zajęcia szerszego stanowiska w sprawie polityki UE dotyczącej **ochrony infrastruktury krytycznej**[79], w dniu 23 lipca 2019 r. Komisja przedstawiła ocenę europejskiej dyrektywy w sprawie ochrony infrastruktury krytycznej[80], jako ram prawnych dla rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony. W ocenie stwierdzono, że kontekst, w którym funkcjonują infrastruktury krytyczne w Europie, znacznie się zmienił od czasu wejścia w życie dyrektywy, w tym nastąpiły zmiany legislacyjne w sektorach szczególnie objętych dyrektywą, takich jak energetyka[81], oraz że przepisy dyrektywy są tylko częściowo adekwatne ze względu na zmiany sytuacji ogólnej. Jednocześnie państwa członkowskie nadal wspierają politykę UE w zakresie ochrony infrastruktury krytycznej, pod warunkiem że jest zgodna z zasadą pomocniczości i stanowi wartość dodaną.

4. Wymiar zewnętrzny

Ze względu na transgraniczny i globalny charakter większości zagrożeń dla bezpieczeństwa, przed którymi stoi Unia, współpraca z organizacjami międzynarodowymi i krajami partnerskimi spoza UE stanowi integralną część działań na rzecz rzeczywistej i skutecznej unii bezpieczeństwa.

Wykorzystanie korzyści wynikających ze współpracy wielostronnej stanowi integralną część tych działań i obejmuje współpracę między UE a ONZ, co zostało niedawno wzmocnione podpisaniem w Nowym Jorku w dniu 24 kwietnia 2019 r. **ram w sprawie zwalczania terroryzmu między ONZ a UE**, przy okazji drugiego dialogu politycznego na wysokim szczeblu w sprawie zwalczania terroryzmu[82]. Ramy te propagują współpracę w zakresie budowania zdolności w celu zwalczania terroryzmu oraz zapobiegania i przeciwdziałania brutalnemu ekstremizmowi w Afryce, na Bliskim Wschodzie i w Azji. Wyznaczają one priorytety i obszary współpracy ONZ-UE do roku 2020.

Współpraca w zakresie bezpieczeństwa z Bałkanami Zachodnimi jest szczególnym priorytetem regionalnym i realizuje szereg priorytetowych działań związanych z bezpieczeństwem określonych w strategii dla Bałkanów Zachodnich z 2018 r.[83]. W tym celu w dniu 4 kwietnia 2019 r. Komisja zorganizowała pierwsze posiedzenie międzyagencyjnej grupy zadaniowej ds. Bałkanów Zachodnich, na którym przedstawiciele siedmiu agencji UE dzielili się swoimi doświadczeniami i zacieśnili współpracę operacyjną z partnerami w regionie, w tym w zwalczaniu przestępczości zorganizowanej, terroryzmu, broni palnej, narkotyków, przemytu migrantów i handlu ludźmi. Rozpoczęto badania hybrydowe zagrożeń z udziałem wszystkich sześciu krajów Bałkanów Zachodnich. Kolejnym konkretnym przykładem współpracy z tym regionem jest umowa o statusie Europejskiej Straży Granicznej i Przybrzeżnej zawarta między UE a Albanią, która weszła w życie w dniu 1 maja 2019 r.,

---

79 W kompleksowej ocenie polityki bezpieczeństwa UE z 2017 r. (SWD(2017) 278 final z 26.7.2017) zwrócono uwagę na potrzebę zajęcia ogólnego stanowiska w sprawie unijnej polityki ochrony infrastruktury krytycznej.

80 Celem dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony jest poprawa ochrony infrastruktury krytycznej w Unii Europejskiej.

81 W szczególności rozporządzenie (UE) 2017/1938 (25.10.2017) dotyczące środków zapewniających bezpieczeństwo dostaw gazu ziemnego i rozporządzenie (UE) 2019/941 (5.6.2019) w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

83 COM(2018) 65 final (6.2.2018).

po czym szybko wysłano zespoły Europejskiej Agencji Straży Granicznej i Przybrzeżnej na granicę z Grecją. Jest to pierwsze takie porozumienie z państwem trzecim i rozmieszczenie europejskich zespołów w państwie trzecim. Podobne umowy powinny zostać wkrótce podpisane z innymi krajami regionu.

Ponadto w lipcu 2019 r. oddelegowano do Albanii oficera łącznikowego Europolu w celu dalszego wspierania władz albańskich w ich wysiłkach na rzecz zapobiegania przestępczości zorganizowanej i jej zwalczania. Aby zintensyfikować walkę z nielegalnym handlem bronią palną, w dniu 27 czerwca 2019 r. Komisja przedstawiła ocenę planu działania na lata 2015–2019 **w zakresie zwalczania handlu bronią** między UE a południowo-wschodnim regionem Europy[84]. Ocena pokazuje wartość dodaną współpracy, ale podkreśla się w niej, że nadal konieczne są dalsze wysiłki, np. poprzez wprowadzenie skutecznych krajowych ośrodków koordynacji w dziedzinie broni palnej lub poprzez harmonizację zbierania informacji i zgłaszania przypadków konfiskaty broni palnej.

UE przyznaje równie wysoki priorytet rozwijaniu **współpracy z państwami Bliskiego Wschodu i Afryki Północnej** w dziedzinie bezpieczeństwa. UE zainicjowała dialog dotyczący bezpieczeństwa z Tunezją i Algierią. UE i Tunezja odbyły w dniu 12 czerwca w Tunisie 3. dialog na temat bezpieczeństwa i walki z terroryzmem, natomiast w dniu 12 listopada 2018 r. w Algierze odbył się 2. dialog w sprawie bezpieczeństwa i walki z terroryzmem UE–Algieria. W następstwie niedawnego posiedzenia Rady Stowarzyszenia z dnia 27 czerwca, w którym UE i Maroko uznały znaczenie pogłębienia współpracy w dziedzinie bezpieczeństwa, prowadzone są rozmowy mające na celu zainicjowanie zorganizowanego dialogu w sprawie bezpieczeństwa z Marokiem. Równolegle prowadzone są rozmowy mające na celu rozwinięcie zorganizowanego dialogu w sprawie bezpieczeństwa z Egiptem, co zostało również potwierdzone na ostatnim spotkaniu urzędników wyższego szczebla między UE a Egiptem, które odbyło się w dniu 10 lipca w Kairze.

Na mocy mandatu Rady Komisja rozpoczęła nieformalne rozmowy z większością krajów **Bliskiego Wschodu i Afryki Północnej** w celu rozpoczęcia formalnych negocjacji w sprawie międzynarodowej umowy o wymianie danych osobowych między Agencją Unii Europejskiej ds. Współpracy Organów Ścigania (**Europol**) i odpowiednimi właściwymi organami w krajach **Bliskiego Wschodu i Afryki Północnej** w celu zwalczania poważnej przestępczości i terroryzmu. W tym kontekście Komisja promuje również zawieranie porozumień roboczych bezpośrednio między Europolem a organami partnerskimi w krajach **Bliskiego Wschodu i Afryki Północnej**, aby zapewnić formalne ramy regularnej współpracy na szczeblu strategicznym.

UE i **Stany Zjednoczone** są bliskimi i strategicznymi partnerami w stawianiu czoła wspólnym zagrożeniom i w zwiększaniu bezpieczeństwa. Na posiedzeniu ministrów sprawiedliwości i spraw wewnętrznych w dniu 19 czerwca 2019 r. UE i Stany Zjednoczone potwierdziły, że zwalczanie terroryzmu jest jednym z ich głównych priorytetów. Jeżeli chodzi o umowę w sprawie danych dotyczących przelotu pasażera między UE a USA [85], obie strony ponownie podkreśliły znaczenie tej umowy i zobowiązały się do rozpoczęcia we wrześniu 2019 r. wspólnej oceny jej wdrożenia, zgodnie z postanowieniami umowy. Obie strony zobowiązały się również do wzmożenia wspólnych wysiłków w walce z terroryzmem, w tym poprzez rozszerzenie do celów dochodzenia i ścigania wymiany informacji zgromadzonych w strefach operacyjnych.

W celu pogłębienia tej współpracy Komisja, wraz z Koordynatorem UE ds. Zwalczania Terroryzmu, zorganizowała w dniu 10 lipca 2019 r. w Brukseli warsztaty wysokiego szczebla poświęcone informacji z terenów operacyjnych. W warsztatach wzięli udział urzędnicy wyższego szczebla z ministerstw obrony, spraw wewnętrznych i sprawiedliwości, Stanów Zjednoczonych, z Europolu i Eurojustu oraz przedstawiciele organizacji międzynarodowych, w celu wymiany poglądów na temat

[84] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_pl.pdf

[85] Dz.U. L 215 z 11.8.2012, s. 5.

wykorzystywania informacji z terenów operacyjnych i aby wspólnie zastanowić się nad wyzwaniami proceduralnymi, prawnymi i operacyjnymi, przed którymi stoją oni obecnie w dążeniu do zidentyfikowania terrorystów i postawienia ich przed sądem. UE i Stany Zjednoczone przeprowadziły również w Brukseli w dniach 14–15 maja 2019 r. dialog poświęcony budowaniu zdolności w zakresie ograniczania ryzyka ataku chemicznego, biologicznego, radiologicznego i jądrowego (CBRJ), aby skoordynować swoje starania na rzecz redukcji zagrożeń związanych z bronią masowego rażenia i wzmocnić globalne bezpieczeństwo w zakresie CBRJ.

Umowa między UE a Stanami Zjednoczonymi w sprawie programu śledzenia środków finansowych należących do terrorystów[86] obowiązuje od 2010 r. i reguluje przekazywanie i przetwarzanie danych do celów identyfikacji, śledzenia i ścigania terrorystów i ich sieci. Zawiera ona gwarancje zapewniające ochronę danych obywateli UE i przewiduje regularny przegląd postanowień dotyczących zabezpieczeń, kontroli i wzajemności. W regularnym sprawozdaniu z oceny[87] opublikowanym w dniu 22 lipca 2019 r. Komisja wyraziła przekonanie, że umowa ta, w tym jej podstawowe zabezpieczenia i instrumenty kontroli, jest odpowiednio wdrażana. Komisja z zadowoleniem przyjmuje stałą przejrzystość wymiany informacji przez organy Stanów Zjednoczonych, co świadczy o wartości programu śledzenia środków finansowych należących do terrorystów we wspólnych staraniach na rzecz walki z terroryzmem. Przekazane na mocy umowy informacje odegrały zasadniczą rolę w prowadzeniu konkretnych dochodzeń dotyczących ataków terrorystycznych na terytorium Europy, w tym ataków w Sztokholmie, Barcelonie i Turku w 2017 r. Państwa członkowskie i Europol zwiększyły stopień wykorzystywania mechanizmu, a dane pochodzące z programu śledzenia środków finansowych należących do terrorystów pozwoliły wygenerować siedem razy więcej wskazówek dochodzeniowych niż w poprzednim okresie sprawozdawczym. Kolejny wspólny przegląd umowy ma zostać przeprowadzony w 2021 r.

Jeśli chodzi o międzynarodową współpracę w zakresie wymiany **danych dotyczących przelotu pasażera w celu zwalczania terroryzmu i poważnej przestępczości**, podczas 17. szczytu UE–Kanada w Montrealu w dniach 17–18 lipca 2019 r. UE i Kanada z zadowoleniem przyjęły zakończenie negocjacji co do nowej umowy w sprawie danych dotyczących przelotu pasażera. Podczas gdy Kanada zwróciła uwagę na obowiązujący ją wymóg kontroli prawnej, strony zobowiązały się, z zastrzeżeniem tej kontroli, do jak najszybszego sfinalizowania umowy, uznając jej istotną rolę w zwiększaniu bezpieczeństwa przy jednoczesnym zapewnieniu prywatności i ochrony danych osobowych. Jeżeli chodzi o obowiązującą umowę między UE a Australią w sprawie danych dotyczących przelotu pasażera[88], w kontekście wspólnego przeglądu i wspólnej oceny umowy w sierpniu 2019 r. odbędzie się w Canberze wizyta zespołu UE.

Komisja współpracuje również z państwami członkowskimi w Radzie na temat stanowiska UE na zbliżającej się 40. sesji **Organizacji Międzynarodowego Lotnictwa Cywilnego**, która odbędzie się w dniach 24 września – 4 października 2019 r. Na sesji wyznaczony zostanie kierunek polityczny i wydane zostaną instrukcje dla Rady Międzynarodowej Organizacji Lotnictwa Cywilnego dotyczące prac technicznych w zakresie norm Organizacji Międzynarodowego Lotnictwa Cywilnego w odniesieniu do przetwarzania danych dotyczących przelotu pasażera. Rada zatwierdziła dokument informacyjny przygotowany przez Komisję w celu przedstawienia stanowiska Unii w sprawie podstawowych zasad, które powinny stanowić podstawę wszelkich przyszłych standardów w zakresie danych dotyczących przelotu pasażera. Dokument informacyjny zostanie przedłożony innym członkom organu niż państwa członkowskie UE.

VI. WNIOSKI

Dzięki ścisłej współpracy między Parlamentem Europejskim, Radą, państwami członkowskimi

[86] Dz.U. L 195 z 27.7. 2010, s. 5.
[87] COM(2019) 342 final (22.7.2019).
[88] Dz.U. L 186 z 14.7.2012, s. 4.

i Komisją UE poczyniła w ostatnich latach znaczne postępy we wspólnych działaniach na rzecz rzeczywistej i skutecznej unii bezpieczeństwa, uzgadniając szereg priorytetowych inicjatyw ustawodawczych. Państwa członkowskie, przy wsparciu Komisji, wdrażają również szereg nielegislacyjnych środków operacyjnych w celu zwiększenia bezpieczeństwa dla wszystkich obywateli. Jednocześnie istnieje nadal szereg priorytetowych inicjatyw w ramach unii bezpieczeństwa, które oczekują na przyjęcie przez współprawodawców, aby można było stawić czoła bezpośrednim zagrożeniom. Komisja wzywa Parlament Europejski i Radę do podjęcia niezbędnych kroków w celu szybkiego osiągnięcia porozumienia w sprawie wniosków ustawodawczych dotyczących przeciwdziałania propagandzie terrorystycznej i radykalizacji w internecie, zwiększenia cyberbezpieczeństwa, ułatwienia dostępu do elektronicznego materiału dowodowego oraz ukończenia prac nad skuteczniejszymi i inteligentniejszymi systemami informacji na potrzeby zarządzania bezpieczeństwem, granicami i migracją.

Komisja wzywa państwa członkowskie do szybkiego i całkowitego wdrożenia wszystkich przepisów przyjętych w ramach unii bezpieczeństwa w celu zapewnienia pełnych płynących z niej korzyści. Ponadto Komisja wzywa państwa członkowskie do kontynuowania i zintensyfikowania kluczowych prac nad praktycznymi środkami mającymi na celu zwiększenie bezpieczeństwa infrastruktury cyfrowej, przeciwdziałanie dezinformacji i innym zagrożeniom w cyberprzestrzeni, zwiększenie gotowości i ochrony oraz wzmocnienie współpracy z partnerami spoza Unii w obliczu wspólnych zagrożeń. Łącznie środki te wzmacniają wspólnie bezpieczeństwo wszystkich obywateli.