KOMISJA
EUROPEJSKA

Bruksela, dnia 20.3.2019 r.
COM(2019) 145 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY EUROPEJSKIEJ I RADY

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

{SWD(2019) 140 final}

I. WPROWADZENIE

Niniejsze sprawozdanie z dalszego postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa jest osiemnastym 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.

W związku z wyborami do Parlamentu Europejskiego, które odbędą się w maju 2019 r., w sprawozdaniu zwrócono szczególną uwagę na ważne działania, jakie podejmowane są na różnych szczeblach w celu zapobiegania cyberzagrożeniom i dezinformacji w kontekście wyborczym. W związku z wezwaniem przez Radę Europejską do podjęcia działań na rzecz ochrony systemów demokratycznych Unii oraz zwalczania dezinformacji w okresie poprzedzającym nadchodzące wybory Unia znacznie usprawniła koordynację działań związanych z zapewnieniem odporności na zagrożenia w zakresie wyborów. Ze względu na to, jak mało jest czasu, by zapewnić gotowość Unii, zanim w maju 2019 r. europejscy wyborcy pójdą do urn, Komisja wzywa wszystkie zaangażowane podmioty – organy rządowe, partie polityczne i w szczególności platformy internetowe – do maksymalizacji wysiłków na rzecz zwiększenia odporności wyborczej i przeciwdziałania dezinformacji. W związku z nadchodzącym posiedzeniem Rady Europejskiej w dniach 21 i 22 marca 2019 r., na którym omawiane będą postępy w tej dziedzinie, Komisja wzywa również państwa członkowskie do wzmocnienia koordynacji działań mających na celu walkę z dezinformacją i zapewnienie ochrony wyborów do Parlamentu Europejskiego.

UE osiągnęła znaczne postępy w pracach nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa dzięki uzgodnieniu szeregu priorytetowych inicjatyw ustawodawczych, które poprawią bezpieczeństwo wszystkich obywateli. W ciągu ostatnich miesięcy[1] Parlament Europejski i Rada osiągnęły porozumienie co do interoperacyjności unijnych systemów informatycznych służących zarządzaniu bezpieczeństwem, granicami i migracjami, jak również co do nowych unijnych zasad mających zamknąć przestrzeń, w jakiej działają terroryści i przestępcy, aby utrudnić im dostęp do prekursorów materiałów wybuchowych, finansowanie działalności i podróżowanie bez bycia zauważonym. Osiągnięcie porozumienia w odniesieniu do 15 z 22 inicjatyw ustawodawczych przedstawionych przez Komisję w obszarze unii bezpieczeństwa (zob. wykaz wszystkich inicjatyw dotyczących unii bezpieczeństwa w *załączniku I*) oznacza, że UE realizuje zamierzenia w tej dziedzinie, która ma priorytetowe znaczenie dla Parlamentu Europejskiego, Rady, i Komisji[2].

Konieczne są jednak dalsze wysiłki. W szczególności współprawodawcy muszą zająć się – jeszcze w trakcie bieżącej kadencji ustawodawczej – pilnym zagrożeniem, jakim są treści o charakterze terrorystycznym w internecie, i osiągnąć porozumienie co do wniosku Komisji. Parlament Europejski i Rada powinny też osiągnąć porozumienie w sprawie wniosku Komisji dotyczącego wzmocnienia Europejskiej Straży Granicznej i Przybrzeżnej, mającego na celu poprawę bezpieczeństwa dzięki lepszej ochronie granic zewnętrznych Unii.

---

[1] Było to możliwe dzięki wcześniejszym postępom w pracach nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa. Pełne informacje na ten temat można znaleźć w poprzednich sprawozdaniach z postępu prac nad stworzeniem unii bezpieczeństwa: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

[2] Zob. wspólna deklaracja w sprawie priorytetów legislacyjnych UE na lata 2018–2019: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32017C1229(01)&from=pl.

Tragiczne wydarzenia, jakie miały miejsce w dniu 15 marca 2019 r. w Christchurch w Nowej Zelandii, pokazują, że terroryzm napędzany przez ekstremistyczne ideologie, czy to prawicowe, czy inne, nadal stanowi ewidentne zagrożenie. Trudności napotykane przy próbach usuwania z platform internetowych treści transmitowanych na żywo i zapobiegania ich ponownej publikacji to kolejny dowód na to, że wniosek Komisji dotyczący treści o charakterze terrorystycznym w internecie ma zasadnicze znaczenie. Bardzo ważne jest pilne osiągnięcie przez współprawodawców porozumienia w sprawie zaproponowanych przepisów dotyczących usuwania z internetu treści o charakterze terrorystycznym. Równie ważne dla zwalczania wszelkich form terroryzmu jest, aby państwa członkowskie w pełni wdrożyły przepisy prawa przyjęte przez UE, szczególnie w związku z atakami terrorystycznymi w Europie, aby zamknąć przestrzeń, w której działają terroryści. Chodzi tu w szczególności o dyrektywę w sprawie zwalczania terroryzmu oraz dyrektywę w sprawie kontroli nabywania i posiadania broni. W ramach walki z ekstremizmem Komisja podejmuje aktywne działania i odpowiednie środki wymierzone przeciwko nielegalnej mowie nienawiści w internecie, antysemityzmowi i nienawiści wobec Muzułmanów.

W niniejszym sprawozdaniu przedstawiono również postępy w realizacji innych priorytetowych inicjatyw dotyczących bezpieczeństwa, a konkretnie środków wspierających ochronę przestrzeni publicznej. Aby możliwe było czerpanie pełnych korzyści z rzeczywistej i skutecznej unii bezpieczeństwa, najważniejszym priorytetem jest pełne i prawidłowe wdrożenie uzgodnionych środków. Komisja aktywnie wspiera w tym zakresie państwa członkowskie, m.in. udostępniając środki finansowe i ułatwiając wymianę najlepszych praktyk. W stosownych przypadkach Komisja wykorzystuje jednak w pełni uprawnienia przysługujące jej na mocy Traktatów w zakresie egzekwowania prawa Unii, m.in. wszczyna w stosownych przypadkach postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego.

Tłem dla publikacji niniejszego sprawozdania są obchody 15. Europejskiego Dnia Pamięci o Ofiarach Terroryzmu w dniu 11 marca 2019 r., piętnaście lat po atakach bombowych w Madrycie, które miały miejsce 11 marca 2004 r., i trzy lata po śmiertelnych atakach w Brukseli i Zaventem, które miały miejsce 22 marca 2016 r. Zapewnienie wsparcia ofiarom ataków terrorystycznych stanowi ważną część prac na rzecz rzeczywistej i skutecznej unii bezpieczeństwa. Aby zwiększyć to wsparcie, w dniu 31 stycznia 2019 r. Komisja przyjęła decyzję w sprawie finansowania projektu pilotażowego, polegającego na ustanowieniu unijnego centrum wiedzy specjalistycznej dla ofiar terroryzmu[3]. Centrum to będzie pełnić rolę ośrodka wiedzy fachowej i platformy dla osób, które z racji swojego zawodu zajmują się ofiarami terroryzmu.

Komisja z zadowoleniem przyjmuje sprawozdanie w sprawie ustaleń i zaleceń Komisji Specjalnej ds. Terroryzmu[4], które stanowi cenny wkład Parlamentu Europejskiego we wspólne prace na rzecz rzeczywistej i skutecznej unii bezpieczeństwa.

II. REALIZACJA PRIORYTETÓW USTAWODAWCZYCH

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

[3] C (2019)636 z 31.1.2019.

[4] Rezolucja Parlamentu Europejskiego z dnia 12 grudnia 2018 r. w sprawie ustaleń i zaleceń Komisji Specjalnej ds. Terroryzmu (2018/2044(INI)).

Wymiana informacji stanowi główny element wsparcia, jakie UE udziela organom krajowym w walce z terroryzmem i poważną przestępczością. Pod tym względem osiągnięcie interoperacyjności ogólnounijnych systemów informacyjnych oznacza radykalną zmianę sposobu, w jaki przekazuje się dane organom krajowym oraz zapewnia ich rzetelność i kompletność. Współprawodawcy osiągnęli porozumienie polityczne w sprawie odnośnych priorytetowych wniosków ustawodawczych, które umożliwiają osiągnięcie **interoperacyjności unijnych systemów informacyjnych** w zakresie zarządzania bezpieczeństwem, granicami i migracjami[5]. Dzięki zaproponowanym środkom unijne systemy informacyjne będą współdziałać w bardziej inteligentny i ukierunkowany sposób, przy pełnym poszanowaniu praw podstawowych. Interoperacyjność systemów umożliwi optymalne wykorzystanie istniejących danych oraz likwidację luk informacyjnych i białych plam, ułatwiając wykrywanie multiplikacji tożsamości oraz przeciwdziałanie oszustwom dotyczącym tożsamości. Komisja jest gotowa wspierać państwa członkowskie we wdrażaniu tych nowych przepisów po ich formalnym przyjęciu przez współprawodawców. Aby do 2020 r. osiągnąć pełną interoperacyjność unijnych systemów informacyjnych służących zarządzaniu bezpieczeństwem, granicami i migracjami, konieczna jest bliska współpraca z agencjami UE oraz wszystkimi państwami członkowskimi i państwami stowarzyszonymi w ramach Schengen. W związku z tym w dniu 5 marca 2019 r. odbyły się pierwsze warsztaty z udziałem ekspertów z państw członkowskich, które miały na celu uruchomienie procesu skutecznej koordynacji.

Na tym etapie przyszła struktura interoperacyjnych systemów informacyjnych UE będzie obejmować wzmocniony **System Informacyjny Schengen**[6], istniejący **wizowy system informacyjny**[7], niedawno uzgodnione rozszerzenie **europejskiego systemu przekazywania informacji z rejestrów karnych**[8] o obywateli państw trzecich, a także nowo ustanowiony unijny **system wjazdu/wyjazdu**[9] i **europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS)**[10].

W ramach technicznego wdrażania europejskiego systemu informacji o podróży oraz zezwoleń na podróż Komisja przedstawiła w dniu 7 stycznia 2019 r. wniosek wprowadzający zmiany techniczne do odnośnego rozporządzenia[11]. Proponowane zmiany dotyczą aktów prawnych odnoszących się do tych unijnych systemów informacyjnych, które ETIAS będzie przeszukiwał w ramach ocen zagrożeń dla bezpieczeństwa lub ryzyka nieuregulowanej migracji dokonywanych w przypadku obywateli państw trzecich zwolnionych z obowiązku wizowego przed ich podróżą do strefy Schengen. Zmiany te są konieczne w celu pełnego ustanowienia ETIAS. Komisja wzywa współprawodawców do przyspieszenia prac nad

---

5 COM(2017) 793 final (12.12.2017), COM(2017) 794 final (12.12.2017), COM(2018) 478 final (13.6.2018), COM(2018) 480 final (13.6.2018). Porozumienie polityczne osiągnięte w dniu 5 lutego 2019 r. zostało zatwierdzone przez Komitet Stałych Przedstawicieli przy Radzie w dniu 13 lutego 2019 r. oraz przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych przy Parlamencie Europejskim w dniu 19 lutego 2019 r.

6 Rozporządzenie (UE) 2018/1860 (28.11.2018), rozporządzenie (UE) 2018/1861 (28.11.2018), rozporządzenie (UE) 2018/1862 (28.11.2018).

7 Rozporządzenie (WE) 767/2008 (9.7.2008).

8 Współprawodawcy osiągnęli porozumienie polityczne w sprawie tego priorytetowego wniosku w dniu 11 grudnia 2018 r. (COM (2017) 344 final (29.6.2017)). Komitet Stałych Przedstawicieli przy Radzie poparł je w dniu 19 grudnia 2018 r., natomiast zgromadzenie plenarne Parlamentu Europejskiego zatwierdziło je w dniu 11 marca 2019 r.

9 Rozporządzenie (UE) 2017/2226 (30.11.2017).

10 Rozporządzenie (UE) 2018/1240 (12.9.2018) i rozporządzenie (UE) 2018/1241 (12.9.2018).

11 COM(2019) 4 final (7.1.2019).

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**[12], który umożliwi dokładniejsze sprawdzenie przeszłości osób ubiegających się o wizę oraz wyeliminowanie luk informacyjnych dzięki lepszej wymianie informacji między państwami 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 kolejnej kadencji Parlamentu Europejskiego szybko rozpoczęli negocjacje w tej sprawie.

W maju 2016 r. Komisja przedstawiła wniosek w sprawie rozszerzenia zakresu **Eurodac**[13] tak, aby obejmował on nie tylko identyfikację osób ubiegających się o azyl, ale także obywateli państw trzecich nielegalnie przebywających w UE i przekraczających jej granice niezgodnie z prawem. Zgodnie z konkluzjami Rady Europejskiej z grudnia 2018 r.[14] oraz komunikatem Komisji z dnia 6 marca 2019 r. w sprawie postępów w realizacji Europejskiego programu w zakresie migracji[15] Komisja wzywa współprawodawców do bezzwłocznego przyjęcia tego wniosku. Dzięki jego przyjęciu Eurodac stanie się częścią przyszłej struktury interoperacyjnych systemów informacyjnych UE i wzbogaci ją o istotne dane dotyczące obywateli państw trzecich nielegalnie przebywających na terytorium UE i przekraczających jej granice niezgodnie z prawem.

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

- do przyjęcia przed wyborami do Parlamentu Europejskiego wniosku ustawodawczego dotyczącego **Eurodac**, który jest bliski uzgodnienia (*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**.

2. Podniesienie poziomu bezpieczeństwa dzięki lepszej kontroli granic zewnętrznych

Solidna ochrona granic zewnętrznych jest warunkiem wstępnym bezpieczeństwa w przestrzeni swobodnego przepływu bez kontroli na granicach wewnętrznych. Jest to zadanie państw członkowskich, które muszą zapewnić zarządzanie swoimi granicami zewnętrznymi zarówno we własnym interesie, jak i we wspólnym interesie wszystkich, z pomocą **Europejskiej Straży Granicznej i Przybrzeżnej**. W odpowiedzi na konkluzje Rady Europejskiej z czerwca 2018 r.[16] we wrześniu 2018 r. Komisja zaproponowała dalsze zwiększenie zdolności Europejskiej Straży Granicznej i Przybrzeżnej[17]. Dzięki temu agencja ta osiągnęłaby nowy poziom operacyjny za sprawą stałej służby liczącej 10 000

12 COM(2018) 302 final (16.5.2018).
13 COM(2016) 272 final (4.5.2016).
14 https://www.consilium.europa.eu/en/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/.
15 COM(2019) 126 final (6.3.2019).
16 https://www.consilium.europa.eu/media/35952/28-euco-final-conclusions-pl.pdf.
17 COM(2018) 631 final (12.9.2018).

funkcjonariuszy straży granicznej sprawujących uprawnienia wykonawcze i posiadających własny sprzęt, przy pełnym poszanowaniu zarówno praw podstawowych, jak i suwerenności państw członkowskich.

Prace legislacyjne nad wnioskiem przebiegają sprawnie, a rozmowy między współprawodawcami weszły w kluczową fazę. Parlament Europejski przyjął swój mandat negocjacyjny w dniu 11 lutego 2019 r., natomiast Rada otrzymała swój mandat w dniu 20 lutego 2019 r. Trójstronne spotkania odbyły się w dniach 27 lutego 2019 r. oraz 12 marca 2019 r. Komisja z zadowoleniem przyjmuje i popiera postępy w pracach nad tym priorytetowym dossier, które wskazują, że wszystkie instytucje dokładają starań, by odnośny wniosek został przyjęty jeszcze przed wyborami do Parlamentu Europejskiego w 2019 r.

Aby podnieść poziom bezpieczeństwa dzięki lepszej kontroli granic zewnętrznych, Komisja wzywa Parlament Europejski i Radę:

- do przyjęcia wniosku ustawodawczego w sprawie wzmocnienia **Europejskiej Straży Granicznej i Przybrzeżnej** jeszcze podczas obecnej kadencji Parlamentu Europejskiego (*inicjatywa przedstawiona w orędziu o stanie Unii w 2018 r.*).

3. Zapobieganie radykalizacji

Reagowanie na zamieszczane w internecie treści o charakterze terrorystycznym jest kluczowym elementem walki z terroryzmem i zapobiegania radykalizacji postaw. W przypadku większości ataków, jakie miały miejsce w Europie w ciągu ostatnich dwóch lat, obecność takich treści odegrała pewną rolę, czy to przez zachęcanie do ataku, czy to instrukcje na temat sposobu jego przeprowadzenia, czy też przez gloryfikowanie śmiertelnych skutków. W związku z ewidentnym zagrożeniem, jakie stwarzają tego typu treści, orędziu przewodniczącego Junckera o stanie Unii w 2018 r. towarzyszył wniosek[18] dotyczący rozporządzenia w sprawie **treści o charakterze terrorystycznym w internecie**, w którym określono ramy prawne mające zapobiegać wykorzystywaniu dostawców usług hostingowych do rozpowszechniania w internecie takich treści. Z uwagi na to, że ewentualne szkody spowodowane publikacją treści o charakterze terrorystycznym rosną z każdą godziną, gdy pozostają dostępne, istotne jest, aby przyszłe przepisy przewidywały skuteczne środki mające na celu jak najszybsze usuwanie takich treści z internetu. Przepisy te muszą jednocześnie dawać pełne gwarancje co do wolności słowa i innych praw podstawowych.

Rada przyjęła swój mandat negocjacyjny w grudniu 2018 r., ale trwają jeszcze prace w Parlamencie Europejskim. Byłoby pożądane, by Parlament zdołał przyjąć mandat negocjacyjny w marcu 2019 r.[19]. Z uwagi na kluczowe znaczenie, jakie mają dla usuwania z internetu treści terrorystycznych ogólnounijne ramy prawne zawierające jasne zasady i odpowiednie zabezpieczenia, Komisja wzywa obu współprawodawców do osiągnięcia porozumienia w sprawie proponowanych przepisów jeszcze w trakcie obecnej kadencji Parlamentu Europejskiego.

[18] COM(2018) 640 final (12.9.2018).

[19] W dniu 4 marca 2019 r. Komisja Rynku Wewnętrznego i Ochrony Konsumentów Parlamentu Europejskiego głosowała nad swoją opinią. W dniu 11 marca 2019 r. Komisja Kultury i Edukacji Parlamentu Europejskiego głosowała nad swoim sprawozdaniem. Oczekuje się, że Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego będzie głosować nad swoim sprawozdaniem w dniu 21 marca 2019 r.

Jednocześnie Komisja nadal wspiera działania państw członkowskich mające **zapobiegać radykalizacji postaw**. Specjalny unijny mechanizm współpracy skupia przedstawicieli krajowych i pomaga zapewnić, by wsparcie na szczeblu UE odpowiadało potrzebom państw członkowskich[20]. Jednym z przykładów niedawnych działań podjętych w tym zakresie jest konferencja „Europejskie miasta przeciwko radykalizacji postaw", zorganizowana wspólnie z Komitetem Regionów w dniu 26 lutego 2019 r. Z kolei w dniu 13 marca 2019 r. Komisja zorganizowała spotkanie ekspertów z krajowymi decydentami w celu określenia praktycznych działań mających na celu dalsze wsparcie służb więziennych i probacyjnych. Wyniki tych prac zostaną uwzględnione w podręczniku przygotowywanym przez sieć upowszechniania wiedzy o radykalizacji postaw, który będzie poświęcony rehabilitacji i reintegracji sprawców przestępstw o charakterze terrorystycznym, powracających zagranicznych bojowników i osób zradykalizowanych w więzieniach (zob. również sekcja IV.4 na temat działań zewnętrznych).

Aby zapobiec radykalizacji postaw, Komisja wzywa Parlament Europejski:

- do przyjęcia w trybie priorytetowym mandatu negocjacyjnego w sprawie wniosku ustawodawczego służącego zapobieganiu rozpowszechnianiu **w internecie treści o charakterze terrorystycznym** w celu umożliwienia współprawodawcom osiągnięcia porozumienia podczas obecnej kadencji Parlamentu Europejskiego (*inicjatywa przedstawiona w orędziu o stanie Unii w 2018 r.*).

4. Podnoszenie poziomu cyberbezpieczeństwa

W dalszym ciągu rośnie liczba klasycznych zagrożeń dla cyberbezpieczeństwa systemów i danych, a w 2018 r. wzrosła aktywność podmiotów działających w złych intencjach wymierzona przeciwko różnym celom i ofiarom. Przeciwdziałanie cyberprzestępczości i zwiększanie cyberbezpieczeństwa pozostaje zatem jednym z priorytetowych obszarów unijnych działań. UE poczyniła wymierne postępy w zwiększaniu cyberbezpieczeństwa, realizując działania określone we wspólnym komunikacie z września 2017 r.[21] „Odporność, prewencja i obrona: budowanie solidnego bezpieczeństwa cybernetycznego Unii Europejskiej".

W dniu 12 marca 2019 r. na sesji plenarnej Parlamentu Europejskiego potwierdzono porozumienie polityczne, które współprawodawcy osiągnęli w kwestii **aktu w sprawie cyberbezpieczeństwa**. Akt ten, który ma wejść w życie w maju 2019 r., zwiększy zdolności w zakresie cyberbezpieczeństwa oraz stan przygotowania państw członkowskich i przedsiębiorstw. Ustanowi unijne ramy certyfikacji cyberbezpieczeństwa produktów, systemów i usług technologii informacyjno-komunikacyjnych. Poprawi również współpracę i koordynację między państwami członkowskimi a instytucjami, agencjami i organami UE, w szczególności współpracę i koordynację z Agencją UE ds. Cyberbezpieczeństwa.

Konieczne są jednak dalsze postępy w odniesieniu do wniosku Komisji z września 2018 r. w sprawie **Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków**

[20] Po raz pierwszy określono potrzeby państw członkowskich w zakresie zapobiegania radykalizacji w tzw. strategicznych wytycznych w zakresie unijnych działań prewencyjnych; wytyczne te dotyczyły działań na 2019 r. Informacje na ten temat można znaleźć na stronie: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

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

koordynacji[22]. Wniosek ten ma na celu wspieranie technologicznych i przemysłowych zdolności w dziedzinie cyberbezpieczeństwa oraz zwiększenie konkurencyjności unijnej branży cyberbezpieczeństwa. Parlament Europejski i Rada przyjęły swoje mandaty negocjacyjne w dniu 13 marca 2019 r. W dniu 13 marca 2019 r. odbyło się też pierwsze posiedzenie trójstronne. Komisja wzywa obu współprawodawców do osiągnięcia szybkiego porozumienia w sprawie przedstawionych wniosków.

W odpowiedzi na wezwanie Rady Europejskiej[23] do dalszych prac nad zdolnością do reagowania na ataki cybernetyczne i ich powstrzymywania za pomocą ogólnounijnych środków ograniczających UE poczyniła znaczne postępy na drodze do uruchomienia „zestawu narzędzi dla dyplomacji cyfrowej", czyli **ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne**. W dniu 8 marca 2019 r. Wysoka Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa oraz Komisja przedstawiły wspólny wniosek dotyczący rozporządzenia Rady w sprawie środków ograniczających służących przeciwdziałaniu cyberatakom zagrażającym Unii lub jej państwom członkowskim. Komisja i Wysoka Przedstawiciel wzywają do szybkiego przyjęcia wspomnianego wniosku w celu wzmocnienia odporności Unii na cyberataki.

Aby zwiększyć cyberbezpieczeństwo, Komisja i Wysoka Przedstawiciel wzywają Radę:
• do przyjęcia rozporządzenia Rady dotyczącego **środków ograniczających służących przeciwdziałaniu cyberatakom** zagrażającym Unii lub jej państwom członkowskim.

5. Zamknięcie przestrzeni, w której działają terroryści

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

W dniu 14 lutego 2019 r. Parlament Europejski i Rada osiągnęły porozumienie polityczne w sprawie proponowanego rozporządzenia dotyczącego **ograniczeń we wprowadzaniu do obrotu i używaniu prekursorów materiałów wybuchowych**[24]. Wejście w życie rozporządzenia usprawni znacząco istniejące ramy prawne i pozwoli ograniczyć dostęp do niebezpiecznych prekursorów materiałów wybuchowych, które mogłyby być użyte do budowy bomb domowej produkcji. Rozporządzenie to wyeliminuje luki w zakresie bezpieczeństwa przy użyciu środków takich jak zakaz stosowania dodatków chemicznych, obowiązkowe kontrole karalności osób ubiegających się o pozwolenie na zakup substancji objętych ograniczeniami, oraz wyraźne wskazanie, że przepisy stosowane wobec podmiotów gospodarczych dotyczą również przedsiębiorstw prowadzących działalność w internecie.

Na polu walki z finansowaniem terroryzmu współprawodawcy osiągnęli ponadto porozumienie w sprawie proponowanej dyrektywy, której celem jest **ułatwienie wykorzystywania informacji finansowych i innych informacji** do celów zapobiegania poważnym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania[25]. Po formalnym przyjęciu i wdrożeniu dyrektywa ta umożliwi właściwym organom

[22] COM(2018) 630 final (12.9.2018).
[23] Zob. konkluzje Rady Europejskiej z czerwca 2018 r. i października 2018 r.
[24] COM(2018) 209 final (17.4.2018).
[25] Współprawodawcy osiągnęli porozumienie polityczne w sprawie wniosku Komisji w dniu 12 lutego 2019 r. (COM(2018) 213 final (17.4.2018)). Zostało ono zatwierdzone przez Komitet Stałych

ścigania oraz biurom ds. odzyskiwania mienia bezpośredni dostęp do informacji o rachunkach bankowych przechowywanych w scentralizowanych krajowych rejestrach rachunków bankowych. Wzmocni ona również współpracę między krajowymi jednostkami analityki finansowej i organami ścigania oraz ułatwi Europolowi dostęp do informacji finansowych.

W oparciu o dotychczasowe doświadczenia Komisja zbada dalsze możliwości współpracy między jednostkami analityki finansowej poszczególnych państw członkowskich, m.in. w ramach przygotowywanego sprawozdania na temat tej współpracy, przewidzianego w piątej dyrektywie w sprawie przeciwdziałania praniu pieniędzy[26]. Ponadto, zgodnie z wymogiem zawartym w tej dyrektywie, Komisja ocenia również kwestie związane z ewentualnym połączeniem w obrębie UE krajowych scentralizowanych rejestrów rachunków bankowych i systemów wyszukiwania danych. Przeprowadza też analizę środków konfiskaty bez uprzedniego wyroku skazującego w Unii. W odpowiedzi na wezwanie Parlamentu Europejskiego[27] Komisja będzie nadal przeprowadzać ocenę konieczności, technicznej wykonalności i proporcjonalności dodatkowych środków mających na celu śledzenie w UE środków finansowych należących do terrorystów.

W ramach prac nad ograniczeniem przestępstw przeciwko wiarygodności dokumentów w dniu 19 lutego 2019 r. współprawodawcy osiągnęli wstępne porozumienie w odniesieniu do proponowanego rozporządzenia mającego na celu poprawę jakości **zabezpieczeń dokumentów tożsamości obywateli Unii oraz dokumentów pobytowych**[28], tak aby przestępcy i terroryści nie mogli ich używać w oszukańczych celach. Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego potwierdziła to porozumienie w dniu 11 marca 2019 r. Po przyjęciu rozporządzenie to wprowadzi minimalne zabezpieczenia dowodów tożsamości, m.in. identyfikatory biometryczne (wizerunek twarzy i dwa odciski palców) oraz mikroprocesor bezstykowy. Znacznie poprawi to bezpieczeństwo krajowych dowodów tożsamości i dokumentów pobytowych oraz utrudni terrorystom i innym przestępcom niewłaściwe wykorzystanie lub sfałszowanie takich dokumentów w celu wjechania na terytorium UE lub poruszania w jej granicach. Lepiej zabezpieczone dokumenty tożsamości przyczynią się do wzmocnienia zarządzania granicami zewnętrznymi UE. Jednocześnie lepiej zabezpieczone i bardziej wiarygodne dokumenty ułatwią obywatelom UE korzystanie z przysługującego im prawa do swobodnego przemieszczania się.

Potrzebne są jednak dalsze postępy w odniesieniu do wniosków Komisji z kwietnia 2018 r. w sprawie **dostępu do elektronicznego materiału dowodowego**, ponieważ w ponad połowie wszystkich prowadzonych obecnie postępowań karnych wystosowuje się transgraniczne wnioski o dostęp do takiego materiału[29]. Rada przyjęła swój mandat negocjacyjny

---

Przedstawicieli przy Radzie w dniu 20 lutego 2019 r. oraz przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego w dniu 26 lutego 2019 r.

[26] Art. 65 ust. 2 dyrektywy (UE) 2018/843 (19.6.2018) stanowi, że do dnia 1 czerwca 2019 r. Komisja oceni ramy współpracy jednostek analityki finansowej z państwami trzecimi oraz przeszkody i możliwości w zakresie zacieśnienia współpracy między jednostkami analityki finansowej w Unii, w tym ustanowienie mechanizmu koordynacji i wsparcia.

[27] W swoim sprawozdaniu końcowym przyjętym w grudniu 2018 r. Komisja Specjalna ds. Terroryzmu Parlamentu Europejskiego wezwała do ustanowienia unijnego systemu śledzenia środków finansowych wspierających terrorystów w zakresie transakcji dokonywanych przez osoby związane z terroryzmem i jego finansowaniem w ramach jednolitego obszaru płatności w euro.

[28] COM(2018) 212 final (17.4.2018).

[29] Elektroniczne materiały dowodowe są potrzebne w około 85 % dochodzeń w sprawach karnych, a w przypadku dwóch trzecich dochodzeń istnieje potrzeba uzyskania materiałów dowodowych od

w odniesieniu do wniosku dotyczącego rozporządzenia[30] mającego poprawić transgraniczny dostęp do elektronicznego materiału dowodowego w postępowaniach karnych oraz wniosku w sprawie dyrektywy[31] ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych. Od czasu przyjęcia wspomnianych wniosków przez Komisję w kwietniu 2018 r. postępy w pracach nad nimi w Parlamencie Europejskim były jednak bardzo ograniczone. Z uwagi na kluczowe znaczenie, jakie skuteczny dostęp do elektronicznego materiału dowodowego ma dla ścigania przestępstw transgranicznych takich jak terroryzm czy cyberprzestępczość, Komisja wzywa Parlament Europejski do poczynienia postępów w pracach nad odnośnym wnioskiem.

Równolegle Komisja pracuje nad swoimi **międzynarodowymi inicjatywami w zakresie dostępu do elektronicznego materiału dowodowego** w ramach trwających negocjacji dotyczących drugiego protokołu dodatkowego do budapeszteńskiej konwencji Rady Europy o cyberprzestępczości oraz w kontekście rozmów ze Stanami Zjednoczonymi. W dniu 5 lutego 2019 r. Komisja przyjęła zalecenia[32] dotyczące mandatów negocjacyjnych w odniesieniu do obu tych inicjatyw. Rada omawia obecnie projekty mandatów, m.in. na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniach 7–8 marca 2019 r. Komisja wzywa Radę do przyjęcia decyzji upoważniającej do udziału w negocjacjach dotyczących drugiego protokołu dodatkowego do wspomnianej konwencji, jak również decyzji upoważniającej do rozpoczęcia rokowań ze Stanami Zjednoczonymi w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego. Szybkie prowadzenie tych negocjacji jest ważne, aby rozwijać współpracę międzynarodową w zakresie wymiany elektronicznych materiałów dowodowych, zapewniając jednocześnie zgodność z prawem UE i wynikającymi z niego obowiązkami państw członkowskich oraz uwzględniając przyszłe zmiany w tym prawie.

Aby zamknąć przestrzeń, w której działają terroryści, Komisja wzywa:

- **Parlament Europejski** do pilnego przyjęcia mandatu negocjacyjnego w sprawie wniosków ustawodawczych dotyczących **elektronicznego materiału dowodowego** w celu niezwłocznego rozpoczęcia rozmów trójstronnych z Radą (*priorytet wspólnej deklaracji*);
- **Radę** do przyjęcia decyzji upoważniającej do udziału w negocjacjach dotyczących **drugiego protokołu dodatkowego do uchwalonej w ramach Rady Europy Konwencji o cyberprzestępczości**, jak również decyzji upoważniającej do rozpoczęcia **rokowań ze Stanami Zjednoczonymi** w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego.

III. ZAPOBIEGANIE DEZINFORMACJI I OCHRONA WYBORÓW PRZED INNYMI ZAGROŻENIAMI CYBERNETYCZNYMI

dostawców usług internetowych mających siedzibę w innej jurysdykcji. Zob. ocena skutków towarzysząca wnioskowi ustawodawczemu (SWD (2018) 118 final (17.4.2018).

30 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.

31 COM(2018) 226 final (17.4.2018). Rada przyjęła swój mandat negocjacyjny w sprawie proponowanej dyrektywy w dniu 8 marca 2019 r. na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych.

32 COM(2019) 70 final (5.2.2019) i COM(2019) 71 final (5.2.2019).

Ryzyko, że podmioty trzecie i wewnętrzne będą ingerować w debaty publiczne i manipulować wyborami jest bardziej realne niż kiedykolwiek wcześniej i może jeszcze bardziej wzrosnąć, w miarę jak zbliża się termin wyborów do Parlamentu Europejskiego. Potencjalne konsekwencje takich ingerencji – w postaci osłabienia lub delegitymizacji instytucji demokratycznych – stanowią poważne, strategiczne i rosnące zagrożenie. Są jednym z podstawowych wyzwań dla UE w zakresie bezpieczeństwa, które wykraczają poza granice państw i wymagają wspólnej, transgranicznej reakcji.

Kampanie wyborcze przed wyborami do Parlamentu Europejskiego rozpoczną się na dobre w marcu. W przededniu posiedzenia Rady Europejskiej, które odbędzie się w dniach 21–22 marca 2019 r., Komisja wzywa państwa członkowskie do wzmocnienia koordynacji i wymiany informacji, aby zapobiegać dezinformacji i chronić proces wyborczy przed zagrożeniami cybernetycznymi. Państwa członkowskie powinny w pełni wykorzystywać udostępnione przez UE narzędzia i kanały informacyjne, w szczególności nowo utworzony system wczesnego ostrzegania[33]. Ze względu na już istniejące zagrożenia Komisja wzywa ponadto platformy internetowe do przyspieszenia działań we wszystkich państwach członkowskich, aby pomóc zapewnić uczciwe wybory do Parlamentu Europejskiego w maju 2019 r.

Aby wspierać wysiłki w tym zakresie i zachęcać do ich podejmowania, Komisja i Wysoka Przedstawiciel nadal realizują działania w dwóch uzupełniających się obszarach walki z zagrożeniami cybernetycznymi. Są to: zapobieganie dezinformacji i zwiększanie odporności wyborów na zagrożenia.

1. *Przeciwdziałanie dezinformacji*

Narażanie obywateli na wielkoskalową dezinformację, w tym mylące lub całkowicie fałszywe informacje, może stanowić duże zagrożenie wynikające z technologii cyfrowych i jest poważnym problemem w kontekście zbliżających się eurowyborów. Komisja ściśle monitoruje wdrażanie działań zapowiedzianych w **komunikacie z kwietnia 2018 r. w sprawie zwalczania dezinformacji w internecie**[34].

Oprócz tego Komisja śledzi uważnie postępy we wdrażaniu **kodeksu postępowania w zakresie zwalczania dezinformacji**, który podpisali w październiku 2018 r. przedstawiciele platform internetowych, wiodących sieci społecznościowych, reklamodawców i branży reklamowej (zob. poniżej). Komisja przeprowadzi jego kompleksową ocenę po upływie pierwszego 12-miesięcznego okresu stosowania kodeksu. Jeżeli jego wdrożenie i wpływ okażą się niezadowalające, Komisja może zaproponować dalsze środki, w tym środki o charakterze ustawodawczym.

W oparciu o dotychczasowe prace oraz w odpowiedzi na wezwanie do ochrony demokratycznych systemów Unii wystosowane przez Radę Europejską w czerwcu 2018 r. Komisja i Wysoka Przedstawiciel przedstawiły w grudniu 2018 r. **wspólny plan działania na**

[33] Zgodnie z założeniami Planu działania na rzecz zwalczania dezinformacji, przedstawionego przez Komisję i Wysoką Przedstawiciel w grudniu 2018 r. (zob. poniżej), system wczesnego ostrzegania będzie stanowił dla państw członkowskich, instytucji UE i jej partnerów centrum wymiany informacji na temat bieżących kampanii dezinformacyjnych i umożliwi im skoordynowaną reakcję. System ten będzie oparty wyłącznie na informacjach z publicznych źródeł i informacjach jawnych.

[34] COM(2018) 236 final (26.4.2018) oraz odnośne sprawozdanie z wykonania (COM(2018) 794 final (5.12.2018)).

rzecz zwalczania dezinformacji[35]. W planie działania podkreślono, że według **Komórki UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych** największe zagrożenie dla UE stanowi dezinformacja ze strony Federacji Rosyjskiej. Ma ona charakter systematyczny, jest zasilana dużymi zasobami i prowadzona na inną skalę niż dezinformacja prowadzona przez inne państwa. Aby przeciwdziałać zagrożeniom, jakie stwarza dezinformacja, w planie działania przewiduje się zwiększenie środków przeznaczonych na walkę z tym zjawiskiem, w szczególności środków na specjalne **grupy zadaniowe ds. komunikacji strategicznej** Europejskiej Służby Działań Zewnętrznych (ESDZ), w tym na grupę zadaniową ds. komunikacji strategicznej dotyczącej Wschodu[36]. W planie działania przewiduje się również zwiększenie zasobów przeznaczonych na ten cel i postuluje wzmocnienie budżetu w ciągu najbliższych dwóch lat.

W planie działania przewidziano konkretne środki służące zwalczaniu dezinformacji, a jednym z nich było utworzenie **systemu wczesnego ostrzegania**. System ten ustanowiono w marcu 2019 r. z myślą o wyborach do Parlamentu Europejskiego. Ma on ułatwić instytucjom UE i państwom członkowskim wymianę danych i ocen dotyczących kampanii dezinformacyjnych oraz przekazywanie ostrzeżeń na temat zagrożeń związanych z dezinformacją.

W planie działania przewidziano również, że wdrażanie wspomnianego wyżej kodeksu postępowania, który podpisały platformy internetowe, będzie ściśle monitorowane. W dniu 29 stycznia 2019 r. Komisja opublikowała **sprawozdania złożone przez sygnatariuszy kodeksu** – Google, Facebook, Twitter, Mozillę i stowarzyszenia branżowe reprezentujące sektor reklamy. Komisja przyjęła wprawdzie z zadowoleniem poczynione postępy, wezwała jednak sygnatariuszy do zwiększenia podejmowanych wysiłków w związku z wyborami do Parlamentu Europejskiego w 2019 r.[37].

W dniu 28 lutego 2019 r. Komisja opublikowała **sprawozdania platform Facebook, Google i Twitter** na temat postępów poczynionych w styczniu 2019 r. w wypełnianiu ich zobowiązań w zakresie zwalczania dezinformacji. W swoich sprawozdaniach platformy nie dostarczyły wystarczająco szczegółowych informacji świadczących o tym, że nowa polityka i narzędzia są wdrażane we wszystkich państwach członkowskich terminowo i przy użyciu wystarczających zasobów. W przypadku wszystkich sygnatariuszy istnieją duże możliwości poprawy[38]. Komisja wzywa platformy w szczególności do zapewnienia pełnej przejrzystości reklam politycznych, zanim we wszystkich państwach członkowskich UE rozpocznie się kampania przed wyborami do Parlamentu Europejskiego. Na potrzeby badań i weryfikacji faktów należy też umożliwić odpowiedni dostęp do umieszczonych na platformach danych oraz zapewnić należytą współpracę między platformami a poszczególnymi państwami członkowskimi za pośrednictwem punktów kontaktowych w ramach systemu wczesnego ostrzegania.

---

35 JOIN(2018) 36 final (5.12.2018).

36 Od 2015 r., czyli od momentu swojego powstania, grupa zadaniowa ds. komunikacji strategicznej dotyczącej Wschodu skatalogowała, poddała analizie i zwróciła uwagę na ponad 5 000 przykładów dezinformacji ze strony Federacji Rosyjskiej, odkryła liczne narracje dezinformacyjne, szerzyła wiedzę na temat narzędzi, technik i intencji kampanii dezinformacyjnych oraz je ujawniała.

37 Więcej szczegółowych informacji można znaleźć pod adresem: http://europa.eu/rapid/press-release_IP-19-746_pl.htm.

38 Więcej szczegółowych informacji można znaleźć pod adresem: http://europa.eu/rapid/press-release_STATEMENT-19-1379_pl.htm.

Kolejne sprawozdanie dotyczące wdrażania wspomnianego kodeksu Komisja przedstawi w dniu 20 marca 2019 r.

2. Wzmacnianie odporności na zagrożenia w zakresie wyborów

W dniu 12 września 2018 r. Komisja przyjęła pakiet środków mający na celu zwiększenie odporności unijnych systemów wyborczych i skierowany do państw członkowskich oraz europejskich i krajowych partii politycznych i fundacji, w tym zalecenie w sprawie sieci współpracy wyborczej, przejrzystości w internecie, ochrony przed cyberincydentami i przeciwdziałania kampaniom dezinformacyjnym, wytyczne dotyczące stosowania unijnych przepisów o ochronie danych osobowych[39], jak również zmiany legislacyjne zaostrzające zasady finansowania partii politycznych na poziomie europejskim.

W swojej rezolucji z dnia 28 października 2018 r. Parlament Europejski wyraził zadowolenie z przyjęcia tego pakietu. Z zadowoleniem przyjęła go również Rada w swoich konkluzjach z dnia 19 lutego 2019 r. w sprawie zapewnienia wolnych i uczciwych wyborów europejskich, wyrażających wspólne zobowiązanie wszystkich państw członkowski do przyjęcia skoordynowanego europejskiego podejścia do ochrony uczciwości zbliżających się eurowyborów. W dniu 7 marca 2019 r. Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych omówiła aktualną sytuację.

Zmiana rozporządzenia w sprawie **statusu i finansowania europejskich partii politycznych i europejskich fundacji politycznych**[40] umożliwia nakładanie sankcji na niezgodne z prawem wykorzystywanie danych osobowych w przypadku prób wywierania wpływu na wynik wyborów do Parlamentu Europejskiego. W następstwie osiągnięcia w styczniu 2019 r. porozumienia politycznego[41] Parlament Europejski zatwierdził tę zmianę na posiedzeniu plenarnym w dniu 12 marca 2019 r. Ma ona wejść w życie przed wyborami do Parlamentu Europejskiego w 2019 r.

Zalecenie w sprawie **sieci współpracy wyborczej, przejrzystości w internecie, ochrony przed cyberincydentami i przeciwdziałania kampaniom dezinformacyjnym w kontekście wyborów do Parlamentu Europejskiego**[42] jest skierowane do państw członkowskich oraz krajowych i europejskich partii politycznych i fundacji. Przedstawia ono propozycje konkretnych działań, jakie odpowiednie podmioty powinny podejmować w tych obszarach. Z myślą o wdrożeniu tego zalecenia krajowe sieci wyborcze wyznaczyły punkty kontaktowe do udziału w **europejskiej sieci współpracy ds. wyborów**, której celem jest ostrzeganie o zagrożeniach, wymiana najlepszych praktyk między sieciami krajowymi, omawianie wspólnych rozwiązań zidentyfikowanych problemów oraz zachęcanie do realizacji wspólnych projektów i inicjatyw z udziałem sieci krajowych. Na pierwszym posiedzeniu sieci w dniu 21 stycznia 2019 r. uczestnicy potwierdzili, że kompleksowe podejście ma zasadnicze znaczenie dla zapewnienia uczciwości wyborów, pozwalając jednocześnie zachować otwartą, demokratyczną debatę i zapewnić równe warunki działania partii politycznych. W dniu 27 lutego 2019 r. odbyło się drugie posiedzenie europejskiej sieci współpracy ds. wyborów, podczas którego skupiono się na kwestiach związanych z monitorowaniem i egzekwowaniem

[39] COM(2018) 638 final (12.9.2018).

[40] COM(2018) 636 final (12.9.2018).

[41] W dniu 16 stycznia 2018 r. współprawodawcy osiągnęli w tej sprawie porozumienie polityczne, które zostało zatwierdzone przez Komitet Stałych Przedstawicieli przy Radzie w dniu 25 stycznia 2019 r. oraz przez Komisję Spraw Konstytucyjnych Parlamentu Europejskiego w dniu 29 stycznia 2019 r.

[42] C(2018) 5949 final (12.9.2018).

przepisów istotnych z punktu widzenia wyborów, w tym na ochronie danych, regulacjach dotyczących mediów, egzekwowaniu prawa, przejrzystości i mediach społecznościowych, a także na kwestii zaangażowania różnych zainteresowanych stron w działalność monitorującą. Podczas tego posiedzenia stworzono podstawy umożliwiające członkom sieci udział w inicjatywie z zakresu cyberodporności natychmiast po kolejnym posiedzeniu, które zaplanowano na dzień 5 kwietnia 2019 r.

Parlament Europejski i Komisja zorganizowały wspólnie **warsztaty na temat zwiększania odporności wyborów na zagrożenia cybernetyczne**. Warsztaty odbyły się w dniu 19 lutego 2019 r. i miały na celu poprawę bezpieczeństwa i odporności systemów wyborczych i infrastruktury na stale zmieniające się zagrożenia dla cyberbezpieczeństwa. Krajowe organy ds. cyberbezpieczeństwa z poszczególnych państw członkowskich, Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji oraz platformy internetowe omówiły pilne działania istotne dla zapewnienia uczciwości tegorocznych wyborów do Parlamentu Europejskiego.

Instytucje UE i państwa członkowskie ściśle współpracują również w zakresie innych **inicjatyw służących zwiększaniu świadomości**, których celem jest ochrona uczciwości procesu wyborczego oraz zaangażowanie podmiotów z sektora prywatnego i publicznego, w tym mediów, platform internetowych i społeczeństwa obywatelskiego.

Aby zapobiegać dezinformacji i zapewnić odporność wyborów na zagrożenia, Komisja i Wysoka Przedstawiciel wzywają państwa członkowskie do:

- szybkiego i zdecydowanego podjęcia działań przewidzianych we **wspólnym planie działania na rzecz zwalczania dezinformacji** opublikowanym w grudniu 2018 r.

IV. WDROŻENIE INNYCH PRIORYTETOWYCH INICJATYW DOTYCZĄCYCH BEZPIECZEŃSTWA

1. Wdrażanie środków ustawodawczych w ramach unii bezpieczeństwa

Aby możliwe było czerpanie pełnych korzyści z rzeczywistej i skutecznej unii bezpieczeństwa, najważniejszym priorytetem jest pełne i prawidłowe wdrożenie uzgodnionych środków. Komisja aktywnie wspiera w tym zakresie państwa członkowskie, m.in. udostępniając środki finansowe i ułatwiając wymianę najlepszych praktyk. W stosownych przypadkach Komisja wykorzystuje jednak w pełni uprawnienia przysługujące jej na mocy Traktatów w zakresie egzekwowania prawa Unii, m.in. wszczyna w stosownych przypadkach postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego.

Co się tyczy wdrożenia **unijnej dyrektywy w sprawie danych dotyczących przelotu pasażera**[43], w dniu 19 lipca 2018 r. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 14 państwom członkowskim z tytułu braku zawiadomienia o przyjęciu przepisów krajowych w pełni transponujących tę dyrektywę[44], będącą narzędziem o kluczowym znaczeniu w walce z terroryzmem i poważną przestępczością. Dziewięć z tych państw członkowskich zgłosiło już dokonanie pełnej

[43] Dyrektywa (UE) 2016/681 (27.4.2016).

[44] Bułgaria, Czechy, Estonia, Grecja, Hiszpania, Francja, Cypr, Luksemburg, Niderlandy, Austria, Portugalia, Rumunia, Słowenia i Finlandia.

transpozycji jej przepisów[45]. Państwa członkowskie, które nadal jej nie dokonały, otrzymały uzasadnione opinie (Hiszpania w dniu 24 stycznia 2019 r., Niderlandy i Finlandia w dniu 7 marca 2019 r.). 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.

Termin transpozycji **dyrektywy w sprawie zwalczania terroryzmu**[46] upłynął w dniu 8 września 2018 r. W dniu 22 listopada 2018 r. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 16 państwom członkowskim z tytułu braku zawiadomienia o przyjęciu przepisów krajowych w pełni transponujących tę dyrektywę. Dziewięć z tych państw członkowskich zgłosiło już dokonanie jej pełnej transpozycji[47]. Komisja wzywa pozostałe siedem państw członkowskich do jak najszybszego podjęcia niezbędnych działań[48].

Termin transpozycji **dyrektywy w sprawie kontroli nabywania i posiadania broni**[49] upłynął w dniu 14 września 2018 r. Do chwili obecnej sześć państw członkowskich zgłosiło pełną transpozycję[50] a pięć – częściową transpozycję[51]. 22 państwa członkowskie[52], w tym państwa, które zgłosiły częściową transpozycję, otrzymały wezwania do usunięcia uchybienia wystosowane przez Komisję w dniu 22 listopada 2018 r.

Jeżeli chodzi o transpozycję do prawa krajowego **dyrektywy w sprawie egzekwowania przepisów o ochronie danych**[53], w dniu 19 lipca 2018 r. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 19 państwom członkowskim w związku z brakiem informacji o przyjęciu przepisów krajowych zapewniających pełną transpozycję dyrektywy[54]. Na chwilę obecną 17 państw członkowskich zgłosiło pełną transpozycję a pięć – częściową transpozycję[55]. Do tej pory zamknięto

---

45 Bułgaria, Estonia, Grecja, Francja, Cypr, Luksemburg, Austria, Portugalia i Rumunia (stan na dzień 11 marca 2019 r.).

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

47 Bułgaria, Czechy, Niemcy, Estonia, Hiszpania, Francja, Chorwacja, Włochy, Łotwa, Litwa, Węgry, Malta, Niderlandy, Austria, Portugalia, Słowacja, Finlandia i Szwecja zgłosiły transpozycję (stan na dzień 11 marca 2019 r.).

48 Belgia, Polska, Rumunia i Słowenia zgłosiły częściową transpozycję. Grecja, Cypr i Luksemburg nie zgłosiły żadnych środków transpozycji (stan na dzień 11 marca 2019 r.).

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

50 Dania, Francja, Chorwacja, Włochy, Malta i Austria (stan na dzień 11 marca 2019 r.).

51 Czechy, Estonia, Litwa, Portugalia i Zjednoczone Królestwo (stan na dzień 11 marca 2019 r.).

52 Belgia, Bułgaria, Czechy, Niemcy, Estonia, Irlandia, Grecja, Hiszpania, Cypr, Łotwa, Litwa, Luksemburg, Węgry, Niderlandy, Polska, Portugalia, Rumunia, Słowenia, Słowacja, Finlandia, Szwecja i Zjednoczone Królestwo (stan na dzień 11 marca 2019 r.).

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

54 Belgia, Bułgaria, Czechy, Estonia, Grecja, Hiszpania, Francja, Chorwacja, Cypr, Łotwa, Litwa, Luksemburg, Węgry, Niderlandy, Polska, Portugalia, Rumunia, Słowenia i Finlandia. Do Komisji spływają odpowiedzi od państw członkowskich, w tym notyfikacje odpowiednich przepisów. Obecnie trwa ich analiza (stan na dzień 11 marca 2019 r.).

55 Belgia, Niemcy, Estonia, Irlandia, Francja, Chorwacja, Włochy, Litwa, Luksemburg, Węgry, Malta, Austria, Polska, Rumunia, Słowacja, Szwecja i Zjednoczone Królestwo zgłosiły dokonanie pełnej transpozycja do prawa krajowego. Czechy, Portugalia, Finlandia, Słowenia i Niderlandy zgłosiły częściową transpozycję, a Dania dokończyła transpozycję (stan na dzień 11 marca 2019 r.).

postępowania przeciwko sześciu państwom członkowskim[56], a w dniu 25 stycznia 2019 r. dziewięć państw członkowskich otrzymało uzasadnioną opinię[57].

Do dnia 9 maja 2019 r. Komisja powinna przedstawić sprawozdanie na temat tego, czy identyfikacja operatorów usług kluczowych ma spójny charakter. Zgodnie z notyfikacjami przekazanymi przez państwa członkowskie pełnej transpozycji **dyrektywy w sprawie bezpieczeństwa sieci i informacji**[58] dokonało 25 państw członkowskich, a częściowej – jedno państwo członkowskie[59]. W styczniu 2019 r. Komisja zamknęła postępowania w sprawie uchybienia zobowiązaniom wszczęte przeciwko sześciu państwom członkowskim z tytułu braku powiadomienia o środkach transpozycji[60]. Dziewięć państw członkowskich[61] objętych jest postępowaniami w sprawie uchybienia zobowiązaniom państwa członkowskiego z powodu braku powiadomienia o pełnej transpozycji dyrektywy. W ramach transpozycji dyrektywy w sprawie bezpieczeństwa sieci i informacji państwa członkowskie miały przedłożyć Komisji do dnia 9 listopada 2018 r. informacje o operatorach usług kluczowych, których zidentyfikowały na swoim terytorium. Obecnie Komisja przeprowadza ocenę informacji przekazanych przez państwa członkowskie[62].

Komisja przeprowadza też obecnie ocenę transpozycji **czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy**[63], a jednocześnie weryfikuje, czy państwa członkowskie wdrażają odnośne przepisy. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko wszystkim 28 państwom członkowskim, ponieważ uznała, że przekazane przez nie informacje wskazują, że nie dokonały one pełnej transpozycji tej dyrektywy[64]. W odpowiednich przypadkach będzie ona w dalszym ciągu korzystać ze swoich uprawnień w celu zapewnienia pełnego wdrożenia tej dyrektywy.

---

56 Belgia, Francja, Chorwacja, Litwa, Luksemburg i Węgry (stan na dzień 11 marca 2019 r.).
Grecja, Cypr, Hiszpania, Słowenia, Portugalia, Czechy, Bułgaria, Łotwa i Niderlandy (stan na dzień 11 marca 2019 r.).

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

59 Bułgaria, Czechy, Dania, Niemcy, Grecja, Estonia, Irlandia, Hiszpania, Francja, Chorwacja, Włochy, Cypr, Łotwa, Litwa, Malta, Niderlandy, Austria, Polska, Portugalia, Rumunia, Słowenia, Słowacja, Finlandia, Szwecja i Zjednoczone Królestwo zgłosiły dokonanie pełnej transpozycji dyrektywy. Węgry zgłosiły jej częściową transpozycję. Belgia i Luksemburg nie zgłosiły Komisji żadnych krajowych środków transpozycji (stan na dzień 11 marca 2019 r.).

60 Irlandia, Hiszpania, Francja, Chorwacja, Niderlandy i Portugalia (stan na dzień 11 marca 2019 r.).

61 Bułgaria, Belgia, Dania, Łotwa, Litwa, Luksemburg, Węgry, Austria i Rumunia (stan na dzień 11 marca 2019 r.).

62 Bułgaria, Cypr, Czechy, Niemcy, Dania, Estonia, Hiszpania, Finlandia, Francja, Chorwacja, Węgry, Irlandia, Włochy, Litwa, Malta, Niderlandy, Polska, Portugalia, Słowacja, Szwecja i Zjednoczone Królestwo (stan na dzień 11 marca 2019 r.).

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

64 Komisja wszczęła postępowania przeciwko wszystkim państwom członkowskim z tytułu braku powiadomienia o przepisach krajowych stanowiących pełną transpozycję dyrektywy, ponieważ zgodnie z przeprowadzoną oceną uznała, że niektóre przepisy tej dyrektywy nie zostały transponowane.

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 trzy państwa członkowskie nadal mają obowiązek zgłoszenia dokonania jej transpozycji do prawa krajowego, zaś dwa kolejne obowiązane są uzupełnić to zgłoszenie[65];
- **dyrektywy w sprawie bezpieczeństwa sieci i informacji**, w przypadku której dwa państwa członkowskie nadal mają obowiązek zgłoszenia dokonania jej transpozycji do prawa krajowego, a jedno państwo obowiązane jest uzupełnić to zgłoszenie[66];
- **dyrektywy w sprawie zwalczania terroryzmu**, w przypadku której trzy państwa członkowskie nadal mają obowiązek zgłoszenia dokonania jej transpozycji do prawa krajowego, zaś cztery kolejne obowiązane są uzupełnić to zgłoszenie[67];
- **dyrektywy w sprawie kontroli nabywania i posiadania broni**, w odniesieniu do której 17 państw członkowskich nadal ma obowiązek zgłoszenia dokonania transpozycji do prawa krajowego, zaś pięć państw członkowskich obowiązanych jest uzupełnić to zgłoszenie[68];
- **dyrektywy w sprawie egzekwowania przepisów o ochronie danych**, w odniesieniu do której pięć państw członkowskich nadal ma obowiązek zgłoszenia dokonania transpozycji do prawa krajowego, a pięć kolejnych musi uzupełnić to zgłoszenie[69]; oraz
- **czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy**, w odniesieniu do której jedno państwo członkowskie obowiązane jest uzupełnić zgłoszenie dokonania transpozycji[70].

2. Ochrona przestrzeni publicznej: zalecane dobre praktyki

W ramach działań praktycznych mających wzmocnić ochronę przed terroryzmem i odporność na to zagrożenie Komisja w dalszym ciągu wspiera wysiłki państw członkowskich i władz lokalnych w zakresie **ochrony przestrzeni publicznej**. Prace służące realizacji

65 Hiszpania, Niderlandy i Finlandia nie zgłosiły jeszcze dokonania transpozycji. Czechy i Słowenia zgłosiły dokonanie częściowej transpozycji i mają uzupełnić swoje zgłoszenie (stan na dzień 11 marca 2019 r.). Powyższe informacje o zgłoszonej pełnej transpozycji opierają się na deklaracjach państw członkowskich i pozostają bez uszczerbku dla kontroli transpozycji przeprowadzanej przez służby Komisji.

66 Belgia i Luksemburg nie zgłosiły jeszcze dokonania transpozycji. Węgry zgłosiły dokonanie częściowej transpozycji i mają uzupełnić swoje zgłoszenie (stan na dzień 11 marca 2019 r.).

67 Grecja, Cypr i Luksemburg nie zgłosiły jeszcze dokonania transpozycji. Belgia, Polska, Rumunia i Słowenia zgłosiły dokonanie częściowej transpozycji i mają uzupełnić swoje zgłoszenie (stan na dzień 11 marca 2019 r.).

68 Belgia, Bułgaria, Niemcy, Irlandia, Grecja, Hiszpania, Cypr, Łotwa, Luksemburg, Węgry, Niderlandy, Polska, Rumunia, Słowenia, Słowacja, Finlandia i Szwecja nie zgłosiły jeszcze dokonania transpozycji. Czechy, Estonia, Litwa, Portugalia i Zjednoczone Królestwo zgłosiły dokonanie częściowej transpozycji i muszą uzupełnić swoje zgłoszenie (stan na dzień 11 marca 2019 r.). Powyższe informacje o zgłoszonej pełnej transpozycji opierają się na deklaracjach państw członkowskich i pozostają bez uszczerbku dla kontroli transpozycji przeprowadzanej przez służby Komisji.

69 Bułgaria, Grecja, Hiszpania, Cypr i Łotwa nie zgłosiły jeszcze dokonania transpozycji. Czechy, Portugalia, Niderlandy, Finlandia i Słowenia zgłosiły dokonanie częściowej transpozycji i mają uzupełnić swoje zgłoszenie (stan na dzień 11 marca 2019 r.).

70 Rumunia zgłosiła do tej pory dokonanie jedynie częściowej transpozycji i musi uzupełnić swoje zgłoszenie. Wszystkie pozostałe państwa członkowskie zgłosiły dokonanie pełnej transpozycji dyrektywy. Ocena Komisji wskazuje jednak, że niektóre przepisy tej dyrektywy nie zostały jeszcze w pełni transponowane do prawa krajowego (stan na dzień 11 marca 2019 r.).

opublikowanego w październiku 2017 r. planu działania na rzecz wspierania ochrony przestrzeni publicznej[71] skupiają się na przygotowaniu odpowiednich wskazówek oraz gromadzeniu dobrych praktyk. We współpracy z organami publicznymi i podmiotami prywatnymi eksploatującymi przestrzeń publiczną Komisja określiła – w ramach tzw. forum operatorów[72] – dobre praktyki dotyczące szeregu środków, które wszystkie podmioty i organy publiczne zaangażowane w ochronę przestrzeni publicznej mogą wdrożyć w celu zwiększenia bezpieczeństwa[73]. Zapewnią one podstawy, które pozwolą ukierunkować przyszłe prace nad ochroną przestrzeni publicznej we wszystkich odpowiednich sektorach (zob. ramkę poniżej).

Dobre praktyki organów publicznych i podmiotów prywatnych w zakresie zwiększania bezpieczeństwa przestrzeni publicznej

Ocena i planowanie

- opracowanie i przeprowadzenie ocen podatności na zagrożenia w celu zidentyfikowania potencjalnych zagrożeń związanych z atakami z zewnątrz lub wewnątrz;
- opracowanie i wdrożenie planów bezpieczeństwa dla danego obiektu lub wydarzenia, obejmujących działania przygotowawcze, na wypadek sytuacji wyjątkowych i naprawcze, w których to planach wskazuje się odpowiednie środki ochrony otoczenia danego obiektu lub wydarzenia. Środki ochrony muszą być skuteczne, dyskretne, proporcjonalne i dostosowane do danych warunków i otoczenia oraz uwzględniać ich specyficzny charakter;
- wyznaczenie i przeszkolenie osoby, która będzie odpowiadać za koordynację i wdrażanie środków ochrony przewidzianych w planie bezpieczeństwa; oraz
- opracowanie i wdrożenie planu zarządzania kryzysowego.

Działania informacyjne i szkolenia

- inicjowanie publicznych kampanii informacyjnych na temat zgłaszania podejrzanych zachowań i sposobów reagowania w przypadku ataku zagrażającego bezpieczeństwu obiektu lub wydarzenia;
- opracowanie i wdrożenie w odniesieniu do wszystkich pracowników programu pogłębiania wiedzy w zakresie bezpieczeństwa wewnętrznego;
- opracowanie i wdrożenie programu pogłębiania wiedzy na temat zagrożeń wewnętrznych, który pomoże chronić obiekt lub wydarzenie przed zagrożeniami wewnętrznymi takimi jak sabotaż, kradzież tajemnic handlowych lub atak terrorystyczny;
- opracowanie podstawowych programów szkolenia w zakresie bezpieczeństwa dla wszystkich pracowników i organizacja ukierunkowanych szkoleń w tym zakresie przyczyniających się do rozwoju kultury bezpieczeństwa organizacji. Opracowanie działań motywujących pracowników do wprowadzania rzetelnych praktyk w zakresie bezpieczeństwa i zachowania wysokiego poziomu czujności; oraz
- organizowanie regularnych ćwiczeń w zakresie bezpieczeństwa, które pomogą określić poziom przygotowania do zapobiegania atakom i reagowania na nie.

Ochrona fizyczna

[71] COM(2017) 612 final (18.10.2017).

[72] Forum operatorów publiczno-prywatnych utworzono w ramach opublikowanego w październiku 2017 r. planu działania na rzecz wspierania ochrony przestrzeni publicznej. Skupia ono decydentów z państw członkowskich i podmioty działające w różnych branżach, takich jak wydarzenia masowe i rozrywka, hotelarstwo, galerie handlowe, ośrodki sportowe i kulturalne, węzły transportowe i inne.

[73] Więcej informacji na temat dobrych praktyk można znaleźć w dokumencie roboczym służb Komisji „Dobre praktyki na rzecz skuteczniejszej ochrony przestrzeni publicznych” (SWD (2019) 140 (20.3.2019)).

- przeprowadzanie oceny kwestii związanych z bezpieczeństwem i ochroną fizyczną od początku procesu projektowania nowego obiektu lub wydarzenia;
- ocena koniecznych kontroli dostępu i barier, przy jednoczesnym unikaniu tworzenia nowych słabych punktów. Kontrola dostępu i bariery utrudniające dostęp nie powinny narażać na ryzyko innych elementów systemu ani tworzyć nowych słabych punktów, które mogłyby być celem ataku;
- ocena najbardziej odpowiedniej technologii wykrywania materiałów wybuchowych, broni palnej, broni białej, jak również czynników chemicznych, biologicznych, radiologicznych i jądrowych.

Współpraca

- wyznaczenie punktów kontaktowych i określenie roli i zakresu odpowiedzialności poszczególnych podmiotów w ramach współpracy publiczno-prywatnej w kwestiach bezpieczeństwa (np. współpracy między operatorami, podmiotami świadczącymi usługi ochroniarskie i organami ścigania) w celu zapewnienia lepszej regularnej komunikacji i współpracy;
- ustanowienie terminowej komunikacji opartej na zaufaniu oraz współpracy umożliwiającej wymianę informacji o określonym ryzyku i zagrożeniach między właściwymi organami publicznymi, lokalnymi organami ścigania i sektorem prywatnym;
- koordynowanie prac nad ochroną przestrzeni publicznej na poziomie lokalnym, regionalnym i krajowym oraz angażowanie się w działania informacyjne i wymianę dobrych praktyk na wszystkich szczeblach, w tym na poziomie UE; oraz
- opracowanie i udostępnienie przez organy publiczne i operatorów praktycznych zaleceń i materiałów zawierających wytyczne w sprawie wykrywania zagrożeń dla bezpieczeństwa, ograniczania takich zagrożeń i reagowania na nie.

3. Słabe punkty infrastruktury cyfrowej

Odporność cyfrowa ma kluczowe znaczenie dla ochrony szeroko rozumianej działalności rządów, badań przemysłowych, własności intelektualnej, planów biznesowych, wyborów, instytucji demokratycznych oraz danych osobowych. Jedną z kluczowych kwestii związanych z cyberbezpieczeństwem, której poświęca się dużo uwagi w debacie publicznej w całej UE, są sieci nowej generacji (5G). Na niedawnym nieformalnym posiedzeniu Rady dotyczącym telekomunikacji, które odbyło się w dniu 1 marca 2019 r. w Bukareszcie, ministrowie wyrazili poparcie dla skoordynowanego europejskiego podejścia mającego na celu wzmocnienie odporności cyfrowej UE w odniesieniu do sieci 5G. Infrastruktura 5G jest ważnym elementem gospodarki cyfrowej. Oprócz usług konsumenckich technologia 5G ma umożliwić również usługi o kluczowym znaczeniu dla sektorów pionowych, takich jak transport, energia i opieka zdrowotna. Normy dotyczące sieci 5G mają charakter globalny a sprzęt i urządzenia oferowane będą przez szereg dostawców działających na skalę światową.

Wprowadzenie sieci 5G w najbliższych latach oznacza radykalną zmianę w stosunku do wcześniejszych technologii. Przechowywanie danych w chmurze umożliwi połączenie miliardów urządzeń tworzących internet rzeczy i będzie sprzyjać kolejnym innowacjom w dziedzinie sztucznej inteligencji, stwarzając nowe możliwości dla obywateli i przedsiębiorców. Cyberbezpieczeństwo jest zatem sprawą szczególnej wagi, jako że wykorzystanie ewentualnych słabych punktów infrastruktury cyfrowej może powodować poważne szkody. Ponieważ internet nie ma granic, naruszenie bezpieczeństwa w jednym państwie członkowskim może mieć wpływ na bezpieczeństwo w wielu innych.

UE musi przyjąć wspólne podejście dotyczące bezpieczeństwa sieci 5G w celu ochrony krytycznej infrastruktury cyfrowej przed potencjalnymi poważnymi zagrożeniami. W tym celu po szczycie Rady Europejskiej w dniach 21–22 marca 2019 r. Komisja wyda zalecenie w sprawie wspólnego unijnego podejścia do zagrożeń dla bezpieczeństwa sieci 5G, które będzie się opierać na skoordynowanych unijnych środkach w zakresie oceny ryzyka i zarządzania ryzykiem, na ramach skutecznej współpracy i wymiany informacji oraz na wspólnej orientacji sytuacyjnej obejmującej sieci łączności o krytycznym znaczeniu. Dyskusja na temat ewentualnych środków powinna uwzględniać wykorzystanie technologii kwantowych na potrzeby bezpieczeństwa sieci oraz ochrony przechowywanych danych[74].

W dniu 12 marca 2019 r. Parlament Europejski przyjął rezolucję w sprawie w zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia.

4. Działania zewnętrzne

Pomyślnie postępują negocjacje między UE a Kanadą co do **zmienionej umowy w sprawie danych dotyczących przelotu pasażera**. Na ich przebieg może pozytywnie wpłynąć zbliżający się szczyt UE-Kanada, który odbędzie się w Montrealu w dniach 11–12 kwietnia 2019 r.

Komisja współpracuje z władzami Stanów Zjednoczonych w celu przygotowania nadchodzącej wspólnej oceny **umowy UE-USA w sprawie danych dotyczących przelotu pasażera**[75], zgodnie z jej postanowieniami. Trwają też prace w ramach piątego wspólnego przeglądu **umowy UE-USA w sprawie programu śledzenia środków finansowych należących do terrorystów**[76]. Przegląd ten posłuży nie tylko weryfikacji postanowień dotyczących zabezpieczeń, kontroli i wzajemności, lecz pozwoli również ocenić wartość tego programu jako narzędzia zwalczania terroryzmu zarówno dla UE, jak i Stanów Zjednoczonych.

Bieżące wydarzenia w Syrii doprowadziły do zwrócenia większej uwagi na dyskusję dotyczącą **zagranicznych bojowników terrorystycznych** przebywających lub zatrzymanych w strefach konfliktu. UE gotowa jest wspierać państwa członkowskie, jeśli zwrócą się o taką pomoc, w zakresie wymiany informacji i dochodzeń, a w szczególności współpracy z partnerami międzynarodowymi i za pośrednictwem Europolu, jak również udzielać pomocy w oparciu o wiedzę fachową i najlepsze praktyki dotyczące resocjalizacji i reintegracji zgromadzone w ramach sieci upowszechniania wiedzy o radykalizacji postaw. UE może również udzielać wsparcia w zakresie budowania zdolności państwom trzecim szczególnie dotkniętym problemem powracających zagranicznych bojowników. Decyzja o repatriacji zagranicznych bojowników terrorystycznych i ich rodzin z obszarów objętych konfliktami pozostaje w gestii poszczególnych państw członkowskich.

UE i Egipt współprzewodniczyły posiedzeniu plenarnemu grupy roboczej ds. Afryki Wschodniej w ramach **Globalnego Forum Przeciwdziałania Terroryzmowi**, które odbyło się w dniu 20 lutego 2019 r. w Nairobi i w którym wzięło udział wielu przedstawicieli służb

[74] Zob. też komunikat pt. „Europejska inicjatywa dotycząca przetwarzania w chmurze – budowanie w Europie konkurencyjnej gospodarki opartej na danych i wiedzy” (COM(2016) 178 final (19.4.2016)).

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

[76] Dz.U. L 195 z 27.7.2010, s. 5.

sądowniczych i policyjnych z Somalii, Kenii, Sudanu, Ugandy, Dżibuti, Etiopii, Jemenu i Tanzanii.

V. WNIOSKI

UE poczyniła znaczne postępy we wspólnych pracach nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa: w ostatnich tygodniach i miesiącach Parlament Europejski i Rada przyjęły szereg priorytetowych inicjatyw ustawodawczych. W związku ze zbliżającymi się wyborami do Parlamentu Europejskiego w maju 2019 r. konieczne są jednak dalsze działania, które pozwolą rozwiązać pilne kwestie związane z bezpieczeństwem. Przede wszystkim Komisja wzywa współprawodawców, by po przyjęciu przez Parlament Europejski mandatu negocjacyjnego rozpoczęli bezzwłocznie negocjacje w sprawie proponowanych przepisów dotyczących usuwania z internetu treści o charakterze terrorystycznym tak, aby umożliwić osiągnięcie porozumienia w tej kwestii jeszcze w trakcie jego obecnej kadencji. Jeśli chodzi o propozycję wzmocnienia Europejskiej Straży Granicznej i Przybrzeżnej, negocjacje osiągnęły już etap rozmów trójstronnych, co pokazuje, że wszystkie instytucje dokładają starań, by przyjąć ten wniosek jeszcze przed wyborami do Parlamentu Europejskiego. Komisja wzywa również państwa członkowskie do wdrożenia wszystkich uzgodnionych środków dotyczących unii bezpieczeństwa, aby zapewnić ich pełną skuteczność z pożytkiem dla bezpieczeństwa wszystkich obywateli.

Biorąc pod uwagę, jak mało jest czasu na to, by zapewnić gotowość Unii, nim w maju 2019 r. europejscy wyborcy pójdą do urn, Komisja wzywa wszystkie zaangażowane podmioty do maksymalizacji wysiłków na rzecz zwiększenia odporności na zagrożenia w zakresie wyborów i przeciwdziałania dezinformacji. W związku z posiedzeniem Rady Europejskiej, które odbędzie się w dniach 21–22 marca 2019 r., państwa członkowskie powinny usprawnić koordynację i wymianę informacji, aby zapobiegać dezinformacji i zapewnić ochronę wyborów przed zagrożeniami cybernetycznymi. Jednocześnie platformy internetowe powinny nasilić we wszystkich państwach członkowskich działania mające pomóc w zapewnieniu, by wybory do Parlamentu Europejskiego w maju 2019 r. były uczciwe. Aby chronić rzetelność tych wyborów, Komisja będzie w nadchodzących miesiącach i tygodniach nadal wspierać takie wysiłki oraz zachęcać do ich podejmowania.