



KOMISJA  
EUROPEJSKA

Bruksela, dnia 30.10.2019 r.  
COM(2019) 552 final

**KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY  
EUROPEJSKIEJ I RADY**

**Dwudzieste 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 dwudziestym 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.

Komisja pod przewodnictwem Jeana-Claude'a Junckera od samego początku traktuje bezpieczeństwo jako najważniejszy priorytet. Opierając się na Europejskiej agendzie bezpieczeństwa z kwietnia 2015 r.<sup>1</sup> oraz na komunikacie dotyczącym torowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa z kwietnia 2016 r.<sup>2</sup>, UE zareagowała na serię ataków terrorystycznych i na coraz poważniejsze zagrożenia bezpieczeństwa w sposób skoordynowany oraz poczyniła znaczne postępy w dążeniu do zwiększenia naszego wspólnego bezpieczeństwa<sup>3</sup>. Coraz wyraźniej widać, że stojące obecnie przed nami wyzwania – niezależnie od tego, czy mają postać terroryzmu, przestępczości zorganizowanej, cyberataków, dezinformacji czy innych pojawiających się zagrożeń cybernetycznych – stanowią wspólne zagrożenia. Tylko działając wspólnie możemy osiągnąć taki poziom bezpieczeństwa zbiorowego, jakiego słusznie domagają się i oczekują obywatele. Porozumienie w tej kwestii stanowi podstawę postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa. Wsparcie udzielane na szczeblu UE stosownie do potrzeb zgłaszanych przez organy krajowe działające na rzecz zapewnienia bezpieczeństwa obywateli koncentruje się na środkach ustawodawczych i operacyjnych, w przypadku których wspólne działania mogą wywrzeć wpływ na bezpieczeństwo państw członkowskich. Prace te są podejmowane w ścisłej współpracy z Parlamentem Europejskim i Radą, przy zapewnieniu pełnej przejrzystości wobec szerzej rozumianej opinii publicznej. Pełne poszanowanie praw podstawowych stanowi centralny element tych prac, gdyż bezpieczeństwo Unii można zapewnić wyłącznie wówczas, gdy obywatele będą mieli pewność, że ich prawa podstawowe są w pełni przestrzegane.

UE podjęła działania na rzecz **zwalczania terroryzmu**, zamykając przestrzeń, w której działają terroryści; nowe przepisy utrudniają im uzyskanie dostępu do materiałów wybuchowych, broni palnej i finansowania, a także ograniczają ich swobodę przemieszczania się. UE zintensyfikowała **wymianę informacji**, aby zapewnić funkcjonariuszom działającym na pierwszej linii, takim jak funkcjonariusze policji i straży granicznej, skuteczny dostęp do dokładnych i kompletnych danych przy maksymalnym wykorzystaniu dostępnych informacji oraz wyeliminowaniu luk informacyjnych i martwych pól. Solidna ochrona granic zewnętrznych jest warunkiem wstępnym bezpieczeństwa w przestrzeni swobodnego przepływu bez kontroli na granicach wewnętrznych. W marcu 2019 r. Parlament Europejski i Rada osiągnęły porozumienie w sprawie wzmocnionej i w pełni wyposażonej **Europejskiej Straży Granicznej i Przybrzeżnej**, a nowe rozporządzenie ma wejść w życie na początku grudnia 2019 r. UE utworzyła platformę oraz zapewniła finansowanie na rzecz osób działających w społecznościach lokalnych, aby sprzyjać wymianie najlepszych praktyk w zakresie **zwalczania radykalizacji postaw i przeciwdziałania brutalnemu ekstremizmowi**, a także przedstawianiu propozycji nowych przepisów umożliwiających

<sup>1</sup> COM(2015) 185 final (28.4.2015).

<sup>2</sup> COM(2016) 230 final (20.4.2016).

<sup>3</sup> Wcześniejsze sprawozdania z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa są dostępne pod adresem: [https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en).

skuteczne usuwanie treści o charakterze terrorystycznym w internecie. Wsparcie UE przyczyniło się do **zwiększenia odporności miast** na ataki; opracowano również plany działania w zakresie wspierania ochrony przestrzeni publicznej i wzmocnienia gotowości na chemiczne, biologiczne, radiologiczne i jądrowe zagrożenia bezpieczeństwa. UE zajęła się również **zagrożeniami dla cyberbezpieczeństwa i zagrożeniami cybernetycznymi**, wdrażając nową unijną strategię w dziedzinie cyberbezpieczeństwa oraz przyjmując odpowiednie przepisy, a także przeciwdziałając **dezinformacji**, aby wzmocnić ochronę naszych wyborów. Trwają prace nad poprawą bezpieczeństwa naszej **cyfrowej infrastruktury krytycznej**, które obejmują zacieśnianie współpracy w zakresie **cyberbezpieczeństwa sieci 5G** w całej Europie.

Pozostaje jednak jeszcze wiele do zrobienia. Atak na synagogę i zabójstwo dwóch obywateli w Halle w Niemczech w dniu 9 października 2019 r., relacjonowane na żywo za pomocą transmisji strumieniowej, w szokujący sposób przypomniały o zagrożeniu ze strony brutalnego prawicowego ekstremizmu i antysemityzmu. Wydarzenie to ponownie zwróciło uwagę na problem przestępczego wykorzystywania internetu do szerzenia propagandy terrorystycznej, a tym samym na **konieczność przyjęcia ogólnounijnych przepisów dotyczących usuwania treści o charakterze terrorystycznym w internecie**. Na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych, które odbyło się w dniach 7–8 października 2019 r., omówiono kwestię brutalnego prawicowego ekstremizmu i terroryzmu oraz zwrócono uwagę na konieczność podejmowania dalszych starań m.in. na rzecz przeciwdziałania rozpowszechnianiu bezprawnych, prawicowych treści ekstremistycznych w internecie i poza nim. Jednocześnie zabójstwo trzech policjantów i jednego członka personelu na komendzie głównej policji w Paryżu w dniu 3 października 2019 r. dowodzi, że zagrożenie związane z terroryzmem inspirowanym działalnością dżihadystów pozostaje realne oraz że należy kontynuować wysiłki na rzecz wspierania państw członkowskich w walce z tym zagrożeniem. Biorąc pod uwagę ostatnie wydarzenia w Syrii Północnej, ucieczka uwięzionych członków ISIS/Daisz może wywrzeć poważny wpływ na bezpieczeństwo w Europie. Należy zagwarantować, aby państwa członkowskie w pełni wykorzystywały istniejące systemy informacyjne do wykrywania i identyfikowania zagranicznych bojowników terrorystycznych przekraczających granice zewnętrzne. Prowadzone są również prace nad wykorzystywaniem informacji z terenów operacyjnych do ścigania zagranicznych bojowników terrorystycznych.

W niniejszym sprawozdaniu przedstawiono postępy osiągnięte w ostatnim czasie w pracach nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa oraz zaznaczono obszary wymagające podjęcia dalszych działań. Sprawozdanie zawiera aktualne informacje na temat wdrażania uzgodnionych środków dotyczących **cyberbezpieczeństwa sieci 5G**, w szczególności na temat **unijnego sprawozdania z oceny ryzyka** opublikowanego w dniu 9 października 2019 r. oraz **przeciwdziałania dezinformacji**.

W niniejszym sprawozdaniu skupiono się w szczególności na **zewnętrznym wymiarze współpracy** w ramach unii bezpieczeństwa w świetle podpisania dwóch dwustronnych **porozumień w sprawie zwalczania terroryzmu** z Albanią i Republiką Macedonii Północnej oraz na postępach poczynionych w rozwijaniu współpracy z partnerskimi państwami trzecimi na rzecz wymiany **danych dotyczących przelotu pasażera**. Ponadto przy okazji publikacji niniejszego sprawozdania Komisja przyjęła wniosek o upoważnienie do podjęcia rokowań w sprawie umowy między UE a **Nową Zelandią** w sprawie wymiany danych osobowych do celów zwalczania poważnej przestępczości i terroryzmu.

## II. REALIZACJA PRIORYTETÓW USTAWODAWCZYCH

### 1. Zapobieganie radykalizacji postaw w internecie i w społecznościach

**Zapobieganie radykalizacji postaw** stanowi fundament działań podejmowanych przez Unię w odpowiedzi na zagrożenia stwarzane przez terroryzm. W tym zakresie należy podkreślić, że internet jest najważniejszym polem działalności terrorystów w XXI w. Miejsca, w których zradykalizowane jednostki mogą się komunikować i wymieniać treściami, umożliwiając powstawanie globalnych, rozrastających się sieci zrzeszających zarówno dżihadystów, jak i brutalnych prawicowych ekstremistów. Dlatego też Komisja kontynuuje swoje dwutorowe podejście do walki z radykalizacją w internecie; proponowane przepisy dotyczące usuwania niezgodnych z prawem treści o charakterze terrorystycznym w internecie powinny wzmocnić dobrowolne partnerstwo z platformami internetowymi.

W tym kontekście zasadnicze znaczenie ma **wniosek ustawodawczy w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym** zawierający przejrzyste przepisy i gwarancje zobowiązujące platformy internetowe do usuwania treści o charakterze terrorystycznym w ciągu godziny od otrzymania uzasadnionego wniosku od właściwych organów, a także do zastosowania proaktywnych środków proporcjonalnych do poziomu narażenia na treści o charakterze terrorystycznym<sup>4</sup>. Parlament Europejski i Rada prowadzą obecnie negocjacje międzyinstytucjonalne; pierwsze posiedzenie trójstronne odbyło się w dniu 17 października 2019 r. Biorąc pod uwagę zagrożenia związane z obecnością treści o charakterze terrorystycznym w internecie, Komisja wzywa współprawodawców do osiągnięcia porozumienia w sprawie proponowanych przepisów do końca 2019 r.

Proponowane przepisy stanowią uzupełnienie dobrowolnego partnerstwa z branżą internetową oraz innymi zainteresowanymi stronami utworzonego w ramach **Forum UE ds. Internetu**. Od momentu jego utworzenia w 2015 r. Forum pełni funkcję katalizatora zapewniającego przedsiębiorstwom internetowym możliwość aktywnego podejmowania działań w celu identyfikowania i usuwania treści o charakterze terrorystycznym w internecie, przygotowując grunt pod wdrożenie branżowej inicjatywy polegającej na ustanowieniu wspólnej bazy danych (ang. „shared database of hashes”)<sup>5</sup> oraz pod utworzenie Globalnego Internetowego Forum Przeciwdziałania Terroryzmowi. Unijna jednostka ds. zgłaszania podejrzanych treści w internecie wchodząca w skład Europolu, tj. unijnego organu ścigania, odgrywa zasadniczą rolę w procesie zacieśniania współpracy z przedsiębiorstwami internetowymi oraz przyczynia się do osiągnięcia ogólnych celów Forum UE ds. Internetu. Na ostatnim posiedzeniu ministrów w ramach Forum UE ds. Internetu, które odbyło się w dniu 7 października 2019 r., państwa członkowskie UE i wysokiej rangi przedstawiciele przedsiębiorstw internetowych zobowiązali się do współpracy w ramach tzw. **unijnego protokołu kryzysowego**. W unijnym protokole kryzysowym wyznaczono progi zacieśnionej współpracy oraz ustanowiono nowe metody skuteczniejszego reagowania w sytuacjach kryzysowych. Prace te rozpoczęto na szczepku międzynarodowym w odpowiedzi na „apel o podjęcie działań w obliczu ataku w Christchurch”<sup>6</sup>, dążąc do zapewnienia skoordynowanej

<sup>4</sup> COM(2018) 640 final (12.9.2018).

<sup>5</sup> Narzędzie ustanowione przez konsorcjum przedsiębiorstw, aby usprawnić współpracę na rzecz zapobiegania rozpowszechnianiu treści o charakterze terrorystycznym na różnych platformach.

<sup>6</sup> W odpowiedzi na ataki w Christchurch w Nowej Zelandii, które miały miejsce w dniu 15 marca 2019 r., 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 ogłosić „apel

i szybkiej reakcji w celu zahamowania rozpowszechniania wirusowych treści o charakterze terrorystycznym lub wirusowych, brutalnych treści ekstremistycznych.

Niezależnie od wdrażania wspomnianych środków służących przeciwdziałaniu radykalizacji w internecie Komisja w dalszym ciągu wspiera podejmowane na szczeblu krajowym i lokalnym wysiłki na rzecz **przeciwdziałania i zapobiegania radykalizacji w terenie**. Korzystając z bogactwa doświadczeń i wiedzy fachowej zdobytych w ramach sieci upowszechniania wiedzy o radykalizacji postaw, UE oferuje podmiotom na szczeblu lokalnym, w tym władzom miejskim<sup>7</sup>, ukierunkowane wsparcie oraz zapewnia praktykom, badaczom i decydentom możliwość wymiany informacji. W ramach sieci opracowano m.in. konkretne wytyczne i zorganizowano warsztaty, aby wesprzeć właściwe organy w rozwiązywaniu problemu dzieci przybywających ze stref konfliktu<sup>8</sup>. Aby zapewnić ciągłość działań podejmowanych w ramach sieci upowszechniania wiedzy o radykalizacji postaw, Komisja uruchomiła procedurę dotyczącą nowej umowy ramowej, której wartość szacuje się na 61 mln EUR na przestrzeni czterech lat, począwszy od 2020 r.<sup>9</sup>

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

- zakończenia negocjacji w sprawie wniosku ustawodawczego mającego na celu zapobieganie rozpowszechnianiu w internecie treści o charakterze terrorystycznym do końca roku.

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

UE zintensyfikowała wymianę informacji, co ułatwiło przeciwdziałanie oszustwom dotyczącym tożsamości<sup>10</sup>, usprawniło kontrole graniczne<sup>11</sup>, przyczyniło się do modernizacji

o podjęcie działań w obliczu ataku w Christchurch”. Przewodniczący Jean-Claude Juncker poparł tę inicjatywę i zapowiedział rozpoczęcie prac nad unijnym protokołem kryzysowym.

<sup>7</sup> Informacje na temat współpracy z władzami miejskimi w kwestiach związanych z bezpieczeństwem można również znaleźć w sekcji V.2 poświęconej gotowości i ochronie, w szczególności w części dotyczącej ochrony przestrzeni publicznej.

<sup>8</sup> [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation\\_awareness\\_network/ran-papers/docs/issue\\_paper\\_child\\_returnees\\_from\\_conflict\\_zones\\_112016\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf)

<sup>9</sup> Umowa ramowa została podzielona na dwie części: 29 000 000 EUR przewidziano na wspieranie działań podejmowanych w ramach sieci upowszechniania wiedzy o radykalizacji postaw przez kolejne cztery lata, a 32 000 000 EUR na zwiększanie zdolności państw członkowskich, organów na szczeblu krajowym, regionalnym i lokalnym oraz priorytetowych państw trzecich w zakresie skutecznego radzenia sobie z radykalizacją postaw, w szczególności dzięki zapewnieniu możliwości tworzenia sieci kontaktów, świadczeniu ukierunkowanych i zorientowanych na potrzeby usług oraz prowadzeniu badań naukowych i analiz.

<sup>10</sup> 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.

<sup>11</sup> Wprowadzenie systematycznych kontroli wszystkich obywateli na granicach zewnętrznych przeprowadzanych z wykorzystaniem Systemu Informacyjnego Schengen. Wszystkie państwa Schengen, a także Rumunia, Bułgaria, Chorwacja i Cypr, stosują wprowadzone w kwietniu 2017 r. przepisy dotyczące systematycznych weryfikacji danych w odpowiednich bazach danych na granicach zewnętrznych. Zgodnie z tymi przepisami dopuszcza się możliwość stosowania tymczasowych odstępstw na granicach lądowych lub morskich, ale wyłącznie w odniesieniu do obywateli Unii, z uwagi na nieproporcjonalny wpływ tych

ogólnounijnych baz danych organów ścigania<sup>12</sup>, wyeliminowało luki informacyjne<sup>13</sup> oraz wzmocniło unijny organ ścigania – Europol<sup>14</sup>. W tym kontekście kluczowa jest **interoperacyjność systemów informacyjnych UE**<sup>15</sup>, która oznacza jak najlepsze wykorzystywanie dostępnych informacji oraz eliminowanie martwych pól. W odpowiedzi na potrzeby osób działających na pierwszej linii interoperacyjność zapewni funkcjonariuszom organów ścigania, funkcjonariuszom straży granicznej i urzędnikom imigracyjnym szybszy, bardziej systematyczny dostęp do informacji, dzięki czemu przyczyni się do poprawy bezpieczeństwa wewnętrznego i zarządzania granicami.

Interoperacyjność i wszelkie związane z nią innowacje będą jednak mogły wywrzeć pozytywny wpływ na kwestie związane z bezpieczeństwem, granicami i zarządzaniem migracją w terenie wyłącznie wówczas, gdy każde państwo członkowskie w pełni wdroży powiązane przepisy. Dlatego też **wdrażanie** interoperacyjności stanowi najważniejszy priorytet unii bezpieczeństwa, zarówno na szczeblu politycznym, jak i na szczeblu technicznym. Komisja i Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) wspierają państwa członkowskie wiedzą fachową oraz wymieniają z nimi najlepsze praktyki za pośrednictwem sieci koordynatorów krajowych, a także opracowują bilans wyników, aby umożliwić przyjęcie skutecznych rozwiązań w obszarze monitorowania i koordynacji. 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.

Parlament Europejski i Rada **nie zakończyły jeszcze prac legislacyjnych** w tym zakresie. Szybkie wypracowanie porozumienia w sprawie wszystkich oczekujących na przyjęcie wniosków ustawodawczych ma zasadnicze znaczenie dla zagwarantowania kompleksowego i terminowego wdrożenia interoperacyjności. Po pierwsze, w ramach technicznego wdrażania **europejskiego systemu informacji o podróży oraz zezwoleń na podróż** należy wprowadzić zmiany techniczne do odnośnych rozporządzeń<sup>16</sup>, które są konieczne do pełnego wdrożenia

---

przepisów na przepływ ruchu. Obecnie takie odstępstwa zgłosiło sześć państw członkowskich / państw stowarzyszonych w ramach Schengen (Chorwacja, Finlandia, Łotwa, Norwegia, Słowenia i Węgry). Jeżeli chodzi o granice powietrzne, możliwość odstąpienia od stosowania przepisów dotyczących systematycznych kontroli wygasła w kwietniu 2019 r.

<sup>12</sup> Wzmocniony System Informacyjny Schengen (rozporządzenie (UE) 2018/1860 (28.11.2018), rozporządzenie (UE) 2018/1861 (28.11.2018), rozporządzenie (UE) 2018/1862 (28.11.2018)) i rozszerzenie europejskiego systemu przekazywania informacji z rejestrów karnych na obywateli państw trzecich (rozporządzenie (UE) 2019/816 (17.4.2019)). Ze wzmocnieniem Systemu Informacyjnego Schengen wiąże się ogólny obowiązek wprowadzania do systemu powiadomień dotyczących terroryzmu.

<sup>13</sup> Unijny system wjazdu/wyjazdu (rozporządzenie (UE) 2017/2226 (30.11.2017)) oraz europejski system informacji o podróży oraz zezwoleń na podróż (rozporządzenie (UE) 2018/1240 (12.9.2018) i rozporządzenie (UE) 2018/1241 (12.9.2018)).

<sup>14</sup> Na przestrzeni ostatnich lat rola Europolu zdecydowanie się zwiększyła, zarówno jeżeli chodzi o zakres, jak i istotność jego uprawnień. Znaczenie Agencji wzrosło wraz z przyjęciem rozporządzenia w sprawie Europolu w 2016 r. (rozporządzenie (UE) 2016/794 (11.5.2016)). Państwa członkowskie wyraźnie zwiększyły ilość informacji wymienianych z Europolem i za pośrednictwem Europolu. Utworzenie przy Europolu Centrum ds. Zwalczania Terroryzmu (ECTC) zwiększyło zdolności analityczne Agencji w sprawach dotyczących terroryzmu. W ciągu ostatnich lat budżet Europolu stale się zwiększał – z 82 mln EUR w 2014 r. do 138 mln EUR w roku 2019. Negocjacje dotyczące budżetu na rok 2020 są nadal w toku.

<sup>15</sup> Rozporządzenie (UE) 2019/817 (20.5.2019) i rozporządzenie (UE) 2019/818 (20.5.2019).

<sup>16</sup> Rozporządzenie (UE) 2018/1240 (12.9.2018) i rozporządzenie (UE) 2018/1241 (12.9.2018).

systemu. Komisja zwraca się do Parlamentu Europejskiego o przyspieszenie prac nad tymi zmianami technicznymi, aby umożliwić jak najszybsze rozpoczęcie negocjacji międzyinstytucjonalnych. Po drugie, nadal trwają negocjacje międzyinstytucjonalne w sprawie wniosku z maja 2018 r. dotyczącego wzmocnienia i modernizacji istniejącego **wizowego systemu informacyjnego**<sup>17</sup>. Bazując na ustaleniach z pierwszego posiedzenia trójstronnego, które odbyło się w dniu 22 października 2019 r., Komisja wzywa obu współprawodawców do szybkiego zakończenia negocjacji. Po trzecie, nie osiągnięto jeszcze porozumienia w sprawie wniosku Komisji z maja 2016 r. dotyczącego rozszerzenia zakresu systemu **Eurodac**<sup>18</sup>, tak aby były w nim przechowywane nie tylko odciski palców i odpowiednie dane osób ubiegających się o azyl i osób zatrzymanych w związku z próbą niedozwolonego przekroczenia granicy zewnętrznej, ale również nielegalnie przebywających obywateli krajów trzecich. Proponowane zmiany doprowadziłyby również do wydłużenia okresu przechowywania odcisków palców i odpowiednich danych osób przekraczających granice UE niezgodnie z prawem. Komisja wzywa współprawodawców do przejścia do etapu przyjmowania wniosku.

**Aby wzmocnić systemy informacyjne służące zarządzaniu bezpieczeństwem, granicami i migracjami, Komisja wzywa Parlament Europejski i Radę 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**;
- szybkiego przeprowadzenia i zakończenia negocjacji w sprawie wniosku dotyczącego wzmocnienia istniejącego **wizowego systemu informacyjnego**;
- przyjęcia wniosku ustawodawczego w sprawie **Eurodac (priorytet wspólnej deklaracji)**.

### 3. *Zamknięcie przestrzeni, w której działają terroryści*

UE podjęła zdecydowane działania, aby zamknąć przestrzeń, w której działają terroryści; nowe przepisy utrudniają terrorystom i innym przestępcom dostęp do materiałów wybuchowych<sup>19</sup>, broni palnej i finansowania<sup>20</sup>, a także ograniczają ich swobodę przemieszczania się<sup>21</sup>.

Aby wzmocnić reakcję organów sądowych na akty terroryzmu, w dniu 1 września 2019 r. Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) ustanowiła **europejski sądowniczy rejestr zwalczania terroryzmu**. W rejestrze tym będą gromadzone informacje sądowe, aby ustanawiać powiązania w toku postępowań prowadzonych przeciwko podejrzanym o popełnienie przestępstw terrorystycznych, co zwiększy koordynację działań prokuratorów w ramach postępowań przygotowawczych w sprawach dotyczących terroryzmu o potencjalnych skutkach transgranicznych.

<sup>17</sup> COM(2018) 302 final (16.5.2018).

<sup>18</sup> COM(2016) 272 final (4.5.2016).

<sup>19</sup> Rozporządzenie (UE) 2019/1148 (20.6.2019) w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych. Rozporządzenie weszło w życie w dniu 31 lipca 2019 r. i będzie obowiązywało przez okres 18 miesięcy od tej daty.

<sup>20</sup> 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.

<sup>21</sup> Wprowadzenie systematycznych kontroli wszystkich obywateli na granicach zewnętrznych przeprowadzanych z wykorzystaniem Systemu Informacyjnego Schengen.

Należy jednak dołożyć starań, aby wesprzeć i usprawnić prowadzenie postępowań przygotowawczych w sprawach transgranicznych, w szczególności w zakresie **dostępu organów ścigania do elektronicznego materiału dowodowego**. Jeżeli chodzi o wnioski ustawodawcze z kwietnia 2018 r. dotyczące usprawnienia transgranicznego dostępu do elektronicznego materiału dowodowego w postępowaniach przygotowawczych<sup>22</sup>, Parlament Europejski nie przyjął jeszcze swojego stanowiska negocjacyjnego, co uniemożliwia współprawodawcom rozpoczęcie negocjacji. Komisja wzywa Parlament Europejski do poczynienia postępów w pracach nad odnośnym wnioskiem ustawodawczym, aby umożliwić współprawodawcom jego szybkie przyjęcie. Na podstawie swojego wniosku dotyczącego wewnętrznych przepisów unijnych Komisja bierze również udział w **negocjacjach międzynarodowych** na rzecz poprawy transgranicznego dostępu do elektronicznego materiału dowodowego. W dniu 25 września 2019 r. przedstawiciele Komisji i władz Stanów Zjednoczonych odbyli pierwszą formalną rundę negocjacji dotyczących **umowy między Unią Europejską a Stanami Zjednoczonymi w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego**. Kolejną rundę negocjacji zaplanowano na dzień 6 listopada 2019 r. W kontekście trwających negocjacji dotyczących **drugiego protokołu dodatkowego do budapeszteńskiej konwencji Rady Europy o cyberprzestępczości** Komisja uczestniczyła w imieniu Unii w trzech sesjach negocjacyjnych w lipcu, wrześniu i październiku 2019 r. Chociaż w ramach tych negocjacji osiągnięto zadowalające postępy, pozostało do omówienia szereg ważnych kwestii o dużym znaczeniu dla Unii, takich jak gwarancje w zakresie ochrony danych. Negocjacje dotyczące drugiego protokołu dodatkowego będą kontynuowane w listopadzie 2019 r. i przez cały rok 2020. Szybkie prowadzenie obu negocjacji jest ważne, aby rozwijać współpracę międzynarodową w zakresie wymiany elektronicznego materiału dowodowego, zapewniając jednocześnie zgodność z prawem UE i wynikającymi z niego obowiązkami państw członkowskich oraz uwzględniając przyszłe zmiany w tym prawie.

W reakcji na bieżące obawy związane z praniem pieniędzy Parlament Europejski przyjął w dniu 19 września 2019 r. **rezolucję w sprawie stanu wdrażania przepisów Unii dotyczących przeciwdziałania praniu pieniędzy**<sup>23</sup>, stanowiącą odpowiedź na pakiet czterech sprawozdań w sprawie przeciwdziałania praniu pieniędzy przyjętych przez Komisję w dniu 24 lipca 2019 r.<sup>24</sup> Parlament Europejski wezwał państwa członkowskie do zapewnienia właściwego i szybkiego wdrożenia dyrektyw w sprawie przeciwdziałania praniu pieniędzy. Ponadto Parlament Europejski wezwał Komisję do oceny, czy rozporządzenie w sprawie przeciwdziałania praniu pieniędzy byłoby bardziej odpowiednie niż dyrektywa, oraz do zbadania konieczności ustanowienia mechanizmu koordynacji i wsparcia dla jednostek analityki finansowej.

---

<sup>22</sup> COM(2018) 225 final (17.4.2018) oraz COM(2018) 226 final (17.4.2018).

<sup>23</sup> [https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022\\_PL.html](https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_PL.html)

<sup>24</sup> Sprawozdanie w sprawie oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, które ma wpływ na rynek wewnętrzny i dotyczy działalności transgranicznej (COM (2019) 370 (24.7.2019)), sprawozdanie w sprawie integracji krajowych scentralizowanych automatycznych mechanizmów (centralnych rejestrów lub centralnych systemów wyszukiwania danych elektronicznych) państw członkowskich dotyczących rachunków bankowych (COM(2019) 372 final (24.7.2019)), sprawozdanie w sprawie oceny niedawnych domniemyanych przypadków prania pieniędzy z udziałem instytucji kredytowych z UE (COM(2019) 373 final (24.7.2019)), sprawozdanie w sprawie oceny ram współpracy między jednostkami analityki finansowej (COM(2019) 371 final (24.7.2019)).

**Aby poprawić dostęp organów ścigania do elektronicznego materiału dowodowego, Komisja wzywa Parlament Europejski i Radę do:**

- osiągnięcia szybkiego porozumienia w sprawie wniosków ustawodawczych dotyczących **elektronicznego materiału dowodowego (priorytet wspólnej deklaracji).**

#### 4. *Podnoszenie poziomu cyberbezpieczeństwa*

Podnoszenie poziomu cyberbezpieczeństwa pozostaje zasadniczym aspektem działań na rzecz rzeczywistej i skutecznej unii bezpieczeństwa. Dzięki wdrożeniu strategii UE w zakresie bezpieczeństwa cybernetycznego z 2017 r.<sup>25</sup> Unia wzmocniła swoją odporność, co utrudniło przeprowadzanie ataków i przyspieszyło przywracanie stanu sprzed ataku, a także wzmocniła prewencję, zwiększając szanse na złapanie i ukaranie sprawców ataków, m.in. za pomocą ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne. Unia wspiera również państwa członkowskie w dziedzinie cyberobrony, wdrażając ramy polityki UE w zakresie cyberobrony.<sup>26</sup>

Wraz z wejściem w życie aktu o cyberbezpieczeństwie<sup>27</sup> w czerwcu 2019 r. **kształtują się unijne ramy certyfikacji cyberbezpieczeństwa**. Certyfikacja ma zasadnicze znaczenie dla zwiększenia poziomu zaufania na jednolitym rynku cyfrowym i zagwarantowania, że dostępne na nim produkty i usługi są bezpieczne. Ramy certyfikacji zapewnią ogólnounijne systemy certyfikacji jako kompleksowy zbiór zasad, wymogów technicznych, norm i procedur. Pracują nad nimi dwie grupy ekspertów, mianowicie Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa reprezentująca organy państw członkowskich i Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa reprezentująca branżę. Ta druga grupa skupia zarówno popytowa, jak i podażową stronę produktów i usług w zakresie technologii informacyjno-komunikacyjnych, w tym małe i średnie przedsiębiorstwa, dostawców usług cyfrowych, europejskie i międzynarodowe organy normalizacyjne, krajowe jednostki akredytujące, organy nadzorujące ochronę danych oraz jednostki oceniające zgodność.

Parlament Europejski i Rada nadal muszą osiągnąć porozumienie w sprawie inicjatywy ustawodawczej dotyczącej <sup>28</sup>**Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji**. Celem wniosku jest wzmocnienie zdolności Unii w zakresie cyberbezpieczeństwa przez stymulowanie europejskiego technologicznego i przemysłowego ekosystemu cyberbezpieczeństwa oraz koordynację i łączenie odpowiednich zasobów. Komisja wzywa obu współprawodawców do wznowienia i szybkiego zakończenia międzyinstytucjonalnych negocjacji w sprawie tej priorytetowej inicjatywy na rzecz zwiększenia cyberbezpieczeństwa.

Prace nad zwiększeniem cyberbezpieczeństwa obejmują wsparcie zarówno na szczeblu krajowym, jak i regionalnym<sup>29</sup>.

<sup>25</sup> JOIN(2017) 450 final (13.9.2017).

<sup>26</sup> Ramy polityki UE w zakresie cyberobrony (aktualizacja z 2018 r.) przyjęte przez Radę w dniu 19 listopada 2018 r. (14413/18).

<sup>27</sup> Rozporządzenie (UE) 2019/881 (17.4.2019).

<sup>28</sup> COM(2018) 630 final (12.9.2018).

<sup>29</sup> Przykładowo Komisja wspiera międzyregionalne partnerstwo innowacyjne w dziedzinie cyberbezpieczeństwa obejmujące Bretanię, Kastylię-León, Nadrenię Północną-Westfalię, Finlandię Środkową i Estonię w celu stworzenia europejskiego łańcucha wartości w dziedzinie cyberbezpieczeństwa, koncentrującego się na komercjalizacji i zwiększaniu możliwości.

Oprócz działań w obliczu zagrożeń cybernetycznych dla systemów i danych UE kontynuuje działania w celu sprostania złożonym i wieloaspektowym wyzwaniom związanym z **zagrożeniami hybrydowymi**. W Radzie powołano horyzontalną grupę roboczą ds. przeciwdziałania zagrożeniom hybrydowym, aby zwiększyć odporność UE i jej państw członkowskich na zagrożenia hybrydowe oraz wesprzeć działania na rzecz wzmocnienia odporności społeczeństw na sytuacje kryzysowe. Komisja i Europejska Służba Działań Zewnętrznych wspierają te wysiłki zgodnie ze wspólnymi ramami z 2016 r. dotyczącymi przeciwdziałania zagrożeniom hybrydowym<sup>30</sup> oraz ze wspólnym komunikatem z 2018 r.<sup>31</sup> w sprawie zwiększania odporności na zagrożenia hybrydowe i wzmocniania zdolności do reagowania na nie. Ponadto Wspólne Centrum Badawcze opracowuje „modelowe koncepcyjne” ramy na potrzeby opisanie zagrożeń hybrydowych, aby pomóc państwom członkowskim i ich właściwym organom w określeniu rodzajów ataków hybrydowych, na jakie mogą być narażone. Model analizuje sposób, w jaki podmioty (państwowe lub niepaństwowe) wykorzystują szereg narzędzi (od dezinformacji po szpiegostwo lub operacje fizyczne) w różnych dziedzinach (gospodarczej, wojskowej, społecznej i politycznej), aby wpłynąć na obrany cel i w rezultacie osiągnąć szereg założeń.

**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.**

### **III. ZWIĘKSZENIE BEZPIECZEŃSTWA INFRASTRUKTURY CYFROWEJ**

Sieci piątej generacji (5G) będą w przyszłości stanowić podstawę coraz bardziej cyfrowych gospodarek i społeczeństw. Dotyczy to miliardów połączonych przedmiotów i systemów, w tym w kluczowych sektorach, takich jak energetyka, transport, bankowość i opieka zdrowotna, a także w systemach kontroli przemysłowej zawierających wrażliwe informacje oraz w pomocniczych systemach bezpieczeństwa. Zapewnienie cyberbezpieczeństwa i odporności sieci 5G ma zatem podstawowe znaczenie.

W ramach skoordynowanego podejścia państwa członkowskie opublikowały w dniu 9 października 2019 r. sprawozdanie w sprawie **koordynowanej przez UE oceny ryzyka w zakresie cyberbezpieczeństwa w sieciach 5G** przy wsparciu ze strony Komisji i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa<sup>32</sup>. Ten ważny krok stanowi część wdrożenia zalecenia Komisji przyjętego w marcu 2019 r. w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa sieci 5G w całej UE<sup>33</sup>. Sprawozdanie opiera się na wynikach krajowych ocen ryzyka w cyberprzestrzeni przeprowadzonych przez wszystkie państwa członkowskie. Określono w nim główne rodzaje i źródła zagrożenia, najbardziej wrażliwe aktywa, główne słabości (w tym zagrożenia techniczne i inne słabe punkty) oraz szereg strategicznych

<sup>30</sup> JOIN(2016) 18 final (6.4.2016).

<sup>31</sup> JOIN(2018) 16 final (13.6.2018).

<sup>32</sup> Koordynowana przez UE ocena ryzyka w zakresie cyberbezpieczeństwa w sieciach 5G została przeprowadzona przez grupę współpracy złożoną z właściwych organów, utworzoną na mocy dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa (UE) 2016/1148 (6.7.2016), z pomocą Komisji i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa: <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.

<sup>33</sup> C(2019) 2355 final (26.3.2019).

czynników ryzyka. Ocena ta stanowi podstawę do określenia środków ograniczających ryzyko, które mogą być stosowane na szczeblu krajowym i europejskim.

W sprawozdaniu wskazano szereg istotnych **wyzwań w zakresie cyberbezpieczeństwa**, które prawdopodobnie pojawią się lub nabiorą większego znaczenia w sieciach 5G. Te wyzwania w zakresie cyberbezpieczeństwa są związane głównie z najważniejszymi *innowacjami* w technologii 5G, w szczególności ze znaczeniem oprogramowania oraz szerokiego zakresu usług i aplikacji obsługiwanych przez 5G, jak również z rolą *dostawców* w tworzeniu i obsłudze sieci 5G oraz stopniem zależności od poszczególnych dostawców. Oznacza to, że produkty, usługi i działania dostawców w coraz większym stopniu stają się częścią obszaru sieci 5G podatnego na ataki. Ponadto szczególnie ważny stanie się profil ryzyka poszczególnych dostawców, w tym prawdopodobieństwo, że dostawca będzie narażony na ingerencję ze strony państwa niebędącego członkiem UE.

Zgodnie z procesem opisanym w zaleceniu Komisji z marca 2019 r. państwa członkowskie powinny zatwierdzić do dnia 31 grudnia 2019 r. **zestaw środków zaradczych**, aby wyeliminować zidentyfikowane ryzyko w cyberprzestrzeni na szczeblu krajowym i unijnym. Komisja i Europejska Służba Działań Zewnętrznych nadal będą prowadzić z podmiotami partnerskimi wymianę informacji na temat cyberbezpieczeństwa i odporności sieci 5G. W tym względzie Komisja jest w kontakcie z NATO w sprawie koordynowanej przez UE oceny ryzyka w zakresie cyberbezpieczeństwa w sieciach 5G.

#### IV. PRZECIWDZIAŁANIE DEZINFORMACJI I OCHRONA WYBORÓW PRZED INNYMI ZAGROŻENIAMI CYBERNETYCZNYMI

UE ustanowiła **ramy skoordynowanych działań przeciwko dezinformacji**, z pełnym poszanowaniem wartości europejskich i praw podstawowych<sup>34</sup>. W ramach Planu działania na rzecz zwalczania dezinformacji<sup>35</sup> kontynuowane są prace nad zawężeniem pola działania dla dezinformacji, m.in. w celu ochrony uczciwości wyborów.

W tym kontekście kluczowa jest współpraca z podmiotami z branży poprzez samoregulacyjny **kodeks postępowania w zakresie zwalczania dezinformacji** dla platform internetowych i sektora reklamy, który zaczął obowiązywać w październiku 2018 r.<sup>36</sup> Komisja oceniła skuteczność kodeksu po pierwszym roku jego obowiązywania, w oparciu o roczne sprawozdania z samooceny przedłożone przez platformy internetowe i pozostałych sygnatariuszy kodeksu i opublikowane w dniu 29 października 2019 r. wraz z oświadczeniem Komisji.<sup>37</sup> W ujęciu ogólnym sprawozdania te pokazują znaczne wysiłki podejmowane przez sygnatariuszy na rzecz wypełnienia podjętych zobowiązań.

Działania podejmowane przez platformy będące sygnatariuszami różnią się pod względem szybkości i zakresu w odniesieniu do pięciu filarów zobowiązań określonych w kodeksie. Ogólnie rzecz biorąc, postępy są bardziej zaawansowane w odniesieniu do zobowiązań związanych z wyborami do Parlamentu Europejskiego w 2019 r., mianowicie w zakresie zlikwidowania zachęt reklamowych i finansowych do dezinformacji (filar 1), zapewnienia przejrzystości reklamy politycznej i tematycznej (filar 2) oraz zapewnienia uczciwości usług w obliczu fikcyjnych kont i zachowań (filar 3). Mniejsze postępy lub brak postępów odnotowano natomiast w odniesieniu do zobowiązań do wzmocnienia pozycji konsumentów (filar 4) oraz zobowiązań do wzmocnienia pozycji środowiska naukowego, między innymi dzięki zapewnieniu przez platformy odpowiedniego i zapewniającego ochronę prywatności dostępu do zbiorów danych do celów badań (filar 5). Istnieją również różnice w zakresie działań podejmowanych przez poszczególne platformy w celu zapewnienia wypełnienia podjętych zobowiązań oraz różnice między państwami członkowskimi dotyczące wdrażania poszczególnych strategii politycznych. Komisja kontynuuje współpracę z sygnatariuszami kodeksu i innymi zainteresowanymi stronami nad zintensyfikowaniem działań podejmowanych przeciwko dezinformacji.

W ramach Planu działania na rzecz zwalczania dezinformacji Komisja i Wysoki Przedstawiciel, we współpracy z państwami członkowskimi, ustanowiły **system wczesnego ostrzegania** w odpowiedzi na kampanie dezinformacyjne. System wczesnego ostrzegania umożliwił instytucjom UE i państwom członkowskim wymianę informacji i analiz przed

<sup>34</sup> Zob. Plan działania na rzecz zwalczania dezinformacji (JOIN(2018) 36 final (5.12.2018)).

<sup>35</sup> JOIN (2019) 12 final (14.6.2019).

<sup>36</sup> Zgodnie z kodeksem platformy internetowe Google, Facebook, Twitter i Microsoft, zobowiązały się do zapobiegania manipulacyjnemu korzystaniu z ich usług przez podmioty działające w złej wierze, zapewnienia przejrzystości i publicznego ujawniania reklam politycznych oraz podejmowania innych działań na rzecz zwiększenia przejrzystości, rozliczalności i wiarygodności ekosystemu internetowego. Stowarzyszenia branżowe z sektora reklamy również zobowiązały się do współpracy z tymi platformami na rzecz poprawy kontroli umieszczania reklam i opracowania narzędzi bezpieczeństwa marki, mających na celu ograniczenie umieszczania na stronach internetowych reklam szerzących dezinformację.

<sup>37</sup> [https://ec.europa.eu/commission/presscorner/detail/en/statement\\_19\\_6166](https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166). Oprócz platform Google, Facebook, Twitter i Microsoft do pozostałych sygnatariuszy kodeksu należą: Mozilla, siedem stowarzyszeń europejskich lub krajowych reprezentujących sektor reklamy oraz EDiMA (europejskie stowarzyszenie reprezentujące platformy i inne spółki technologiczne działające w sektorze internetowym).

wyborami do Parlamentu Europejskiego w 2019 r. oraz koordynowanie reakcji. Prace te zintensyfikowano po wyborach – na bieżąco odbywa się wymiana informacji na poziomie grup roboczych, a różne państwa członkowskie zorganizowały trzy spotkania punktów kontaktowych ds. systemów wczesnego ostrzegania.

Kolejnym praktycznym krokiem w kierunku identyfikacji dezinformacji są prace **zespołu ds. strategicznej komunikacji** (StratCom), w szczególności jego grupy zadaniowej ds. wschodnich (East StratCom Taskforce), która realizuje projekt „EUvsDisinfo” służący monitorowaniu i analizowaniu dezinformacji prokremlowskiej oraz reagowaniu na nią<sup>38</sup>. Od początku 2019 r. pierwszy budżet przeznaczony na ten cel w wysokości 3 mln EUR umożliwił intensyfikację i rozszerzenie zakresu tych działań, tak aby obejmowały one monitorowanie i analizę dezinformacji prokremlowskiej w sieci, radiu i telewizji oraz mediach społecznościowych w 19 językach, od angielskiego po serbski i arabski. Liczba ujawnionych działań dezinformacyjnych zwiększyła się ponad dwukrotnie ze względu na lepszą zdolność monitorowania; dotychczas w 2019 r. odnotowano około 2 000 przypadków dezinformacji w porównaniu z 765 przypadkami w tym samym okresie w 2018 r. Grupa zadaniowa ds. wschodnich odegrała istotną rolę w monitorowaniu i ujawnianiu przypadków dezinformacji prokremlowskiej ukierunkowanej na wybory do Parlamentu Europejskiego w 2019 r. Badaniom towarzyszyła kampania mająca na celu podnoszenie świadomości na temat prób ingerencji w procesy wyborcze na całym świecie. W wyniku działań informacyjnych prowadzonych przez tę grupę w ścisłej współpracy z Parlamentem Europejskim i Komisją wyemitowano ponad 20 wywiadów w mediach, a w kampanii uczestniczyło ponad 300 dziennikarzy.

Komisja podjęła również działania mające na celu **ograniczenie rozprzestrzeniania się dezinformacji i mitów na temat instytucji i polityki UE**. Komisja utworzyła sieć ekspertów ds. komunikacji wraz z portalem internetowym dostarczającym interaktywnych materiałów informacyjnych na temat polityki UE oraz wyzwań związanych z dezinformacją i jej wpływem na społeczeństwo. Ponadto Komisja, we współpracy z Parlamentem Europejskim i Europejską Służbą Działań Zewnętrznych, rozpoczęła cykl kampanii w mediach społecznościowych poświęconych zwalczaniu dezinformacji<sup>39</sup>.

## **V. WDRAŻANIE INNYCH PRIORYTETOWYCH INICJATYW DOTYCZĄCYCH BEZPIECZEŃSTWA**

### *1. Wdrażanie środków ustawodawczych w ramach unii bezpieczeństwa*

Uzgodnione środki w ramach unii bezpieczeństwa przyniosą pełne korzyści dotyczące bezpieczeństwa tylko wtedy, gdy wszystkie państwa członkowskie zapewnią ich szybkie i pełne wdrożenie. W tym celu Komisja aktywnie wspiera państwa członkowskie we wdrażaniu przepisów UE, m.in. udostępniając środki finansowe i ułatwiając wymianę najlepszych praktyk. Komisja wykorzystuje 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.

**Termin transpozycji unijnej dyrektywy w sprawie danych dotyczących przelotu**

---

<sup>38</sup> [www.euvsdisinfo.eu](http://www.euvsdisinfo.eu)

<sup>39</sup> <https://europa.eu/euprotects/>

**pasażera**<sup>40</sup> upłynął w dniu 25 maja 2018 r. Do tej pory 25 państw członkowskich zgłosiło Komisji pełną transpozycję<sup>41</sup>, co stanowi znaczący postęp od lipca 2018 r., kiedy to Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 14 państwom członkowskim<sup>42</sup>. Dwa państwa członkowskie nie zgłosiły jeszcze pełnej transpozycji pomimo trwających postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego wszczętych w dniu 19 lipca 2018 r.<sup>43</sup> 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**<sup>44</sup> upłynął w dniu 8 września 2018 r. Do tej pory 22 państwa członkowskie zgłosiły Komisji pełną transpozycję, co stanowi znaczący postęp od listopada 2018 r., kiedy to Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 16 państwom członkowskim<sup>45</sup>. Trzy państwa członkowskie nie zgłosiły jeszcze pełnej transpozycji pomimo trwających postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego<sup>46</sup>. Dnia 25 lipca 2019 r. Komisja wystosowała do dwóch państw członkowskich uzasadnione opinie dotyczące niezgłoszenia pełnej transpozycji dyrektywy<sup>47</sup>. W odpowiedzi oba państwa członkowskie zapowiedziały, że prace ustawodawcze zostaną zakończone do końca bieżącego roku.

Termin transpozycji **dyrektywy w sprawie kontroli nabywania i posiadania broni**<sup>48</sup> upłynął w dniu 14 września 2018 r. Do tej pory 13 państw członkowskich zgłosiło pełną transpozycję. 15 państw członkowskich nie zgłosiło jeszcze pełnej transpozycji pomimo trwających postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego wszczętych w dniu 22 listopada 2018 r.<sup>49</sup> Dnia 25 lipca 2019 r. Komisja wystosowała do 20 państw członkowskich uzasadnione opinie dotyczące niezgłoszenia pełnej transpozycji dyrektywy. W odpowiedzi pięć państw członkowskich zgłosiło pełną transpozycję dyrektywy<sup>50</sup>.

---

<sup>40</sup> Dyrektywa (UE) 2016/681 (27.4.2016). Dania nie uczestniczyła w przyjęciu tej dyrektywy, nie jest nią związana ani jej nie stosuje.

<sup>41</sup> Powyższe informacje o zgłoszonej pełnej transpozycji opierają się na deklaracjach państw członkowskich i pozostają bez uszczerbku dla kontroli transpozycji przeprowadzanej przez służby Komisji (stan na dzień 17 października 2019 r.).

<sup>42</sup> Zob. szesnaste sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2018) 690 final (10.10.2018)).

<sup>43</sup> Słowenia zgłosiła częściową transpozycję. Hiszpania nie zgłosiła transpozycji (stan na dzień 17 października 2019 r.).

<sup>44</sup> Dyrektywa (UE) 2017/541 (15.3.2017). Dyrektywa ta nie ma zastosowania w Zjednoczonym Królestwie, Irlandii i Danii.

<sup>45</sup> Zob. siedemnaste sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2018) 845 final (11.12.2018)).

<sup>46</sup> Grecja i Luksemburg nie zgłosiły krajowych środków wykonawczych. Polska zgłosiła środki krajowe, co stanowi częściową transpozycję (stan na dzień 17 października 2019 r.).

<sup>47</sup> Grecja i Luksemburg.

<sup>48</sup> Dyrektywa (UE) 2017/853 (17.10.2019).

<sup>49</sup> Belgia, Czechy, Estonia, Polska, Szwecja Słowacja i Zjednoczone Królestwo zgłosiły środki transpozycji w odniesieniu do części nowych przepisów. Cypr, Niemcy, Grecja, Hiszpania, Luksemburg, Węgry, Rumunia i Słowenia nie zgłosiły żadnych środków transpozycji (stan na dzień 17 października 2019 r.).

<sup>50</sup> Finlandia, Irlandia, Litwa, Niderlandy, Portugalia (stan na dzień 17 października 2019 r.).

Termin na dokonanie transpozycji **dyrektywy o ochronie danych w sprawach karnych**<sup>51</sup> upłynął w dniu 6 maja 2018 r. Do tej pory 25 państw członkowskich zgłosiło Komisji pełną transpozycję, co stanowi znaczący postęp od lipca 2018 r., kiedy to Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 19 państwom członkowskim<sup>52</sup>. Trzy państwa członkowskie nie zgłosiły jeszcze pełnej transpozycji pomimo trwających postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego<sup>53</sup>. Dnia 25 lipca 2019 r. Komisja podjęła decyzję o skierowaniu spraw dwóch państw członkowskich<sup>54</sup> do Trybunału Sprawiedliwości Unii Europejskiej w związku z brakiem transpozycji dyrektywy i wystosowała wezwanie do usunięcia uchybienia do jednego państwa członkowskiego<sup>55</sup> w związku z brakiem pełnej transpozycji dyrektywy<sup>56</sup>.

Komisja przeprowadza obecnie ocenę transpozycji **czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy**<sup>57</sup>, a jednocześnie weryfikuje, czy państwa członkowskie wdrażają odnośne przepisy. Państwa członkowskie miały dokonać transpozycji tej dyrektywy do prawa krajowego do dnia 26 czerwca 2018 r. Komisja nadal prowadzi postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 21 państwom członkowskim, ponieważ uznała, że informacje przekazane przez te państwa nie wskazują, że dokonały one pełnej transpozycji tej dyrektywy<sup>58</sup>.

Komisja przeprowadziła ocenę zgodności transpozycji **dyrektyw dotyczących cyberprzestępczości**. W lipcu i październiku 2019 r. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 23 państwom członkowskim<sup>59</sup>, ponieważ uznała, że informacje dotyczące krajowych przepisów wykonawczych przekazane przez te państwa członkowskie nie wskazują, że dokonały one prawidłowej transpozycji **dyrektywy w sprawie zwalczania niegodziwego traktowania dzieci w celach seksualnych**<sup>60</sup>. W lipcu i październiku 2019 r. Komisja wszczęła również postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko czterem państwom członkowskim<sup>61</sup>, ponieważ uznała, że informacje dotyczące krajowych przepisów wykonawczych przekazane przez te państwa członkowskie nie wskazują, że dokonały one prawidłowej transpozycji **dyrektywy dotyczącej ataków na systemy informatyczne**<sup>62</sup>.

---

<sup>51</sup> Dyrektywa (UE) 2016/680 (27.4.2016).

<sup>52</sup> Zob. szesnaste sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2018) 690 final (10.10.2018)).

<sup>53</sup> Słowenia zgłosiła częściową transpozycję. Hiszpania nie zgłosiła transpozycji. Niemcy zgłosiły pełną transpozycję, jednak zdaniem Komisji nie jest ona kompletna (stan na dzień 17 października 2019 r.).

<sup>54</sup> Grecja i Hiszpania.

<sup>55</sup> Niemcy.

<sup>56</sup> Grecja zgłosiła pełną transpozycję, która jest obecnie przedmiotem oceny przez Komisję.

<sup>57</sup> Dyrektywa (UE) 2015/849 (20.5.2015).

<sup>58</sup> Belgia, Bułgaria, Czechy, Dania, Niemcy, Estonia, Irlandia, Francja, Włochy, Cypr, Łotwa, Litwa, Węgry, Niderlandy, Austria, Polska, Rumunia, Słowacja, Finlandia, Szwecja i Zjednoczone Królestwo (stan na dzień 17 października 2019 r.). Zamknięto już 7 postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego dotyczących tej dyrektywy.

<sup>59</sup> Belgia, Bułgaria, Czechy, Niemcy, Estonia, Grecja, Hiszpania, Francja, Chorwacja, Włochy, Łotwa, Litwa, Luksemburg, Węgry, Malta, Austria, Polska, Portugalia, Rumunia, Słowenia, Słowacja, Finlandia i Szwecja.

<sup>60</sup> Dyrektywa 2011/93/UE (13.12.2011).

<sup>61</sup> Bułgaria, Włochy, Portugalia i Słowenia.

<sup>62</sup> Dyrektywa 2013/40/UE (12.8.2013).

**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 wykorzystywania danych dotyczących przelotu pasażera**, w przypadku której jedno państwo członkowskie nadal musi zgłosić dokonanie jej transpozycji do prawa krajowego, zaś jedno państwo członkowskie musi uzupełnić to zgłoszenie<sup>63</sup>;
- **dyrektywy w sprawie zwalczania terroryzmu**, w przypadku której 2 państwa członkowskie nadal muszą zgłosić dokonanie jej transpozycji do prawa krajowego, zaś jedno państwo członkowskie musi uzupełnić to zgłoszenie<sup>64</sup>;
- **dyrektywy w sprawie kontroli nabywania i posiadania broni**, w odniesieniu do której 8 państw członkowskich nadal musi zgłosić dokonanie transpozycji do prawa krajowego, zaś 7 państw członkowskich musi uzupełnić to zgłoszenie<sup>65</sup>;
- **dyrektywy o ochronie danych w sprawach karnych**, w odniesieniu do której jedno państwo członkowskie nadal musi zgłosić dokonanie transpozycji do prawa krajowego, zaś 2 państwa członkowskie muszą uzupełnić to zgłoszenie<sup>66</sup>;
- **czwartej dyrektywy w sprawie przeciwdziałania praniu pieniędzy**, w odniesieniu do której 21 państw członkowskich nadal musi uzupełnić zgłoszenie<sup>67</sup>;
- **dyrektywy w sprawie zwalczania niegodziwego traktowania dzieci w celach seksualnych**, w odniesieniu do której przeciwko 23 państwom członkowskim wszczęto postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego w związku z nieprawidłową transpozycją<sup>68</sup>;
- **dyrektywy dotyczącej ataków na systemy informatyczne**, w odniesieniu do której przeciwko 4 państwom członkowskim wszczęto postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego w związku z nieprawidłową transpozycją<sup>69</sup>.

## 2. Gotowość i ochrona

Budowanie odporności na zagrożenia bezpieczeństwa stanowi podstawowy element działań na rzecz rzeczywistej i skutecznej unii bezpieczeństwa. Komisja wspiera państwa członkowskie i władze lokalne we wzmacnianiu ochrony przestrzeni publicznej, wdrażając plan działania z października 2017 r. oraz partnerstwo na rzecz bezpieczeństwa w przestrzeni publicznej ze stycznia 2019 r. w ramach agendy miejskiej dla UE. W działaniach tych

<sup>63</sup> Słowenia zgłosiła częściową transpozycję. Hiszpania nie zgłosiła transpozycji (stan na dzień 17 października 2019 r.).

<sup>64</sup> Grecja i Luksemburg nie zgłosiły transpozycji. Polska zgłosiła częściową transpozycję (stan na dzień 17 października 2019 r.).

<sup>65</sup> Belgia, Czechy, Estonia, Polska, Szwecja Słowacja i Zjednoczone Królestwo zgłosiły środki transpozycji w odniesieniu do części nowych przepisów. Cypr, Niemcy, Grecja, Hiszpania, Luksemburg, Węgry, Rumunia i Słowenia nie zgłosiły żadnych środków transpozycji (stan na dzień 17 października 2019 r.).

<sup>66</sup> Słowenia zgłosiła częściową transpozycję. Hiszpania nie zgłosiła transpozycji. Niemcy zgłosiły pełną transpozycję, jednak zdaniem Komisji nie jest ona kompletna (stan na dzień 17 października 2019 r.).

<sup>67</sup> Belgia, Bułgaria, Czechy, Dania, Niemcy, Estonia, Irlandia, Francja, Włochy, Cypr, Łotwa, Litwa, Węgry, Niemcy, Austria, Polska, Rumunia, Słowacja, Finlandia, Szwecja i Zjednoczone Królestwo (stan na dzień 17 października 2019 r.).

<sup>68</sup> Belgia, Bułgaria, Czechy, Niemcy, Estonia, Grecja, Hiszpania, Francja, Chorwacja, Włochy, Łotwa, Litwa, Luksemburg, Węgry, Malta, Austria, Polska, Portugalia, Rumunia, Słowenia, Słowacja, Finlandia i Szwecja.

<sup>69</sup> Bułgaria, Włochy, Portugalia i Słowenia.

uczestniczą miasta, które skontaktowały się z Komisją i poprosiły o wsparcie w sprostaniu wyzwaniom, jakie napotkały w związku z ochroną przestrzeni publicznej.

Wymiana najlepszych praktyk między władzami lokalnymi oraz z podmiotami prywatnymi ma kluczowe znaczenie dla zwiększania bezpieczeństwa przestrzeni publicznej. Było to główne zagadnienie omawiane w trakcie **Europejskiego Tygodnia Bezpieczeństwa**, który odbył się w Nicei we Francji, w dniach od 14 do 18 października 2019 r., zorganizowanego w ramach projektu „Ochrona miast stowarzyszonych przed terroryzmem poprzez zapewnienie bezpieczeństwa obszarów miejskich” finansowanego ze środków UE. Podczas tego wydarzenia, w którym wzięło udział 500 uczestników z miast z całej Europy, organów krajowych i instytucji badawczych, zaznaczono, jak ważna jest ścisła współpraca między wszystkimi zainteresowanymi stronami, zarówno publicznymi, jak i prywatnymi, oraz podkreślono rolę nowych technologii w poprawie ochrony miast. Zagadnienie ochrony przestrzeni publicznej znalazło się także w programie **Europejskiego Tygodnia Regionów i Miast** w Brukseli, który odbył się w dniach 7–10 października 2019 r. Podczas tego wydarzenia zorganizowano warsztaty poświęcone partnerstwu na rzecz bezpieczeństwa w przestrzeni publicznej w ramach agendy miejskiej dla UE. Tematem przewodnim była rola władz lokalnych w dziedzinie polityki bezpieczeństwa, unijne regulacje i finansowanie na rzecz sprostania najpoważniejszym zagrożeniom bezpieczeństwa w miejskiej przestrzeni publicznej, jak również takie kluczowe zagadnienia jak innowacje poprzez inteligentne rozwiązania i technologie, w tym koncepcja uwzględniania bezpieczeństwa na etapie projektowania, zapobiegania i włączenia społecznego. Komisja przyczynia się również do wspierania innowacji w miastach w tych obszarach za pomocą niedawnego zaproszenia do składania wniosków w ramach innowacyjnych działań miejskich, którego wyniki ogłoszono w sierpniu 2019 r. Spośród wybranych projektów trzy miasta (Pireus w Grecji, Tampere w Finlandii i Turyn we Włoszech) będą testowały nowe rozwiązania w zakresie kwestii związanych z bezpieczeństwem w miastach<sup>70</sup>.

Aby **lepiej chronić miejsca kultu** oraz poznać potrzeby różnych grup religijnych, dnia 7 października 2019 r. Komisja zorganizowała spotkanie z przedstawicielami społeczności żydowskich, muzułmańskich, chrześcijańskich i buddyjskich. Podczas spotkania stanowiącego element wdrożenia planu działania UE z 2017 r. w zakresie wspierania ochrony przestrzeni publicznej wskazano, że poziom świadomości i gotowości w zakresie bezpieczeństwa znacząco się różni między poszczególnymi społecznościami religijnymi, podkreślając znaczenie dalszej wymiany dobrych praktyk. W trakcie spotkania wykazano również, że wprowadzenie podstawowych środków bezpieczeństwa i lepsza świadomość w zakresie bezpieczeństwa nie stoją w sprzeczności z utrzymaniem otwartego i dostępnego charakteru miejsc kultu. Komisja będzie gromadziła dobre praktyki i materiały mające na celu podnoszenie świadomości na swojej elektronicznej platformie przeznaczony dla ekspertów oraz zwróci na tę kwestię uwagę organów bezpieczeństwa państw członkowskich w ramach publiczno-prywatnego forum na rzecz ochrony przestrzeni publicznej.

Jednym z obszarów wymagających dalszej uwagi jest rosnące zagrożenie bezpieczeństwa infrastruktury krytycznej i przestrzeni publicznej, jakie stwarzają **bezzałogowe statki**

---

<sup>70</sup> Innowacyjne działania miejskie są instrumentem współfinansowanym przez Europejski Fundusz Rozwoju Regionalnego. Więcej informacji można znaleźć na stronie: <https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals>.

**powietrzne.** Uzupełniając niedawno przyjęte przepisy UE<sup>71</sup> dotyczące bezpiecznej eksploatacji bezzałogowych statków powietrznych w przestrzeni powietrznej, w której latają załogowe statki powietrzne, oraz nie osłabiając możliwości użytecznego wykorzystania bezzałogowych statków powietrznych, Komisja wspiera państwa członkowskie w analizowaniu tendencji w szkodliwym używaniu takich statków, finansując odpowiednie badania i ułatwiając testowanie środków przeciwdziałających. Jak pokazano w trakcie międzynarodowej konferencji na wysokim szczeblu dotyczącej zwalczania zagrożeń, jakie stwarzają bezzałogowe systemy powietrzne, która odbyła się w Brukseli w dniu 17 października 2019 r., podstawową rolę pełni wymiana doświadczeń i najlepszych praktyk. W wydarzeniu tym zorganizowanym przez Komisję wzięło udział 250 uczestników będących przedstawicielami państw członkowskich, organizacji międzynarodowych, partnerskich państw trzecich, branży, środowisk akademickich i społeczeństwa obywatelskiego, aby omówić zagrożenia bezpieczeństwa stwarzane przez bezzałogowe statki powietrzne oraz sposoby reagowania na nie. Spotkanie pokazało, że potrzebna jest regularna ocena ryzyka związanego z bezzałogowymi statkami powietrznymi oraz ścisła współpraca między władzami lotniczymi a organami ścigania w celu dalszego opracowywania europejskich przepisów w zakresie bezpiecznej eksploatacji bezzałogowych statków powietrznych. Konieczne jest również kontynuowanie testowania środków zaradczych przeciwko bezzałogowym statkom powietrznym w ramach skoordynowanego europejskiego podejścia. Ponadto uczestnicy spotkania byli zgodni co do tego, że aby bezzałogowe statki powietrzne były bezpieczne i niezawodne w eksploatacji oraz aby było trudno je wykorzystać w sposób niewłaściwy i szkodliwy, konieczna jest ścisła współpraca między organami i branżą.

### 3. *Wymiar zewnętrzny*

Ponieważ większość zagrożeń bezpieczeństwa, przed jakim stoi Unia, wykracza poza granice UE i stanowi zagrożenia globalne, współpraca z krajami partnerskimi, organizacjami i odpowiednimi zainteresowanymi stronami odgrywa zasadniczą rolę w budowaniu rzeczywistej i skutecznej unii bezpieczeństwa.

Podstawowym elementem tej współpracy jest wymiana informacji. Wraz z niniejszym sprawozdaniem Komisja przyjęła zalecenie w sprawie decyzji Rady upoważniającej do pojęcia rokowań w sprawie **umowy między UE a Nową Zelandią w sprawie wymiany danych osobowych między Europolem a właściwymi organami Nowej Zelandii do celów zwalczania poważnej przestępczości i terroryzmu**. Umowa taka dodatkowo wzmocni zdolności Europolu w zakresie współdziałania z Nową Zelandią na rzecz zapobiegania przestępstwom wchodzących w zakres mandatu Europolu oraz zwalczania takich przestępstw. Podpisane w kwietniu 2019 r. porozumienie robocze między Europolem a policją Nowej Zelandii określa ramy dla zorganizowanej współpracy na szczeblu strategicznym, nie zapewnia ono jednak podstawy prawnej wymiany danych osobowych. Wymiana danych osobowych w pełnym poszanowaniu prawa Unii i praw podstawowych jest kluczowa dla skutecznej współpracy operacyjnej policji. Wcześniej Komisja zidentyfikowała osiem państw priorytetowych w regionie Bliskiego Wschodu / Afryki Północnej na podstawie zagrożenia terrorystycznego, wyzwań związanych z migracją i potrzeb operacyjnych Europolu, z którymi

---

<sup>71</sup> Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.

należy rozpocząć negocjacje.<sup>72</sup> Uwzględniając potrzeby operacyjne organów ścigania w całej UE oraz potencjalne korzyści płynące ze ściślejszej współpracy w tym obszarze, jak wykazały również działania następcze podjęte w związku z atakiem w Christchurch w marcu 2019 r., Komisja uważa, że konieczne jest dodanie Nowej Zelandii do grupy państw priorytetowych, z którymi należy rozpocząć negocjacje w najbliższym czasie.

Kolejnym ważnym elementem unijnej współpracy z partnerskimi państwami trzecimi na rzecz bezpieczeństwa jest przekazywanie **danych dotyczących przelotu pasażera**. Dnia 27 września 2019 r. Komisja przyjęła zalecenie w sprawie decyzji Rady upoważniającej do podjęcia rokowań w sprawie **umowy między UE a Japonią** w sprawie przekazywania danych dotyczących przelotu pasażera w celu zapobiegania terroryzmowi i innym poważnym przestępstwom o charakterze transgranicznym oraz walki z nimi przy pełnym poszanowaniu zabezpieczeń ochrony danych i praw podstawowych<sup>73</sup>. Zalecenie to jest analizowane na poziomie grupy roboczej Rady, a Komisja wzywa Radę do szybkiego przyjęcia mandatu negocjacyjnego z Japonią. Podpisanie umowy przed igrzyskami olimpijskimi, które odbędą się w 2020 r., przyniosłoby wymierne korzyści pod względem bezpieczeństwa.

Na szczepku globalnym Komisja wspiera działania podejmowane przez **Organizację Międzynarodowego Lotnictwa Cywilnego** na rzecz ustanowienia normy w zakresie przetwarzania danych dotyczących przelotu pasażera. Jest to odpowiedź na wezwanie Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych zawarte w rezolucji nr 2396, w której wzywa się wszystkie państwa członkowskie ONZ do rozwijania zdolności w zakresie gromadzenia, przetwarzania i analizowania danych dotyczących przelotu pasażera. Dnia 13 września 2019 r. Komisja przedstawiła wniosek<sup>74</sup> dotyczący decyzji Rady w sprawie stanowiska, jakie ma być zajęte w imieniu Unii Europejskiej na forum Rady Organizacji Międzynarodowego Lotnictwa Cywilnego w odniesieniu do norm i zalecanych metod postępowania w zakresie danych dotyczących przelotu pasażera. Wniosek ten jest analizowany na poziomie grupy roboczej Rady, a Komisja wzywa Radę do szybkiego przyjęcia decyzji. Stanowisko Unii i jej państw członkowskich określono również w dokumencie informacyjnym pt. „Normy i zasady dotyczące gromadzenia, wykorzystywania, przetwarzania i ochrony danych dotyczących przelotu pasażera”, który przedłożono podczas 40. sesji Organizacji Międzynarodowego Lotnictwa Cywilnego.

Jeżeli chodzi o prace nad nową umową w sprawie danych dotyczących przelotu pasażera z **Kanadą**, Komisja dąży do szybkiego sfinalizowania prac nad tą umową. Z kolei latem bieżącego roku zainicjowano połączony wspólny przegląd i wspólną ocenę umowy w sprawie danych dotyczących przelotu pasażera z **Australią**, jak również wspólną ocenę umowy w sprawie danych dotyczących przelotu pasażera ze **Stanami Zjednoczonymi**, rozpoczynając od wizyt w Canberze i Waszyngtonie odpowiednio w sierpniu i we wrześniu 2019 r. Podczas sesji zamkniętej dnia 14 października 2019 r. Komisja poinformowała Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego o stanie prac prowadzonych z Japonią, Australią i Kanadą w odniesieniu do danych dotyczących przelotu pasażera.

---

<sup>72</sup> Zob. jedenaste sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2017) 608 final (18.10.2017)). Wspomniane państwa priorytetowe to: Algieria, Egipt, Izrael, Jordania, Liban, Maroko, Tunezja i Turcja.

<sup>73</sup> COM(2019) 420 final (27.9.2019).

<sup>74</sup> COM(2019) 416 final (13.9.2019).

Poczyniono również postępy we współpracy w zakresie bezpieczeństwa z partnerami z **Balkanów Zachodnich** przez wdrażanie wspólnego planu działań przeciwko terroryzmowi dla Bałkanów Zachodnich z października 2018 r. Dnia 9 października Komisja podpisała z Albanią i Republiką Macedonii Północnej dwa niewiążące porozumienia dwustronne w sprawie walki z terroryzmem<sup>75</sup>. W porozumieniach tych przewidziano specjalne działania priorytetowe, które mają być podejmowane przez władze odpowiedniego kraju partnerskiego, obejmujące pięć celów wspólnego planu działania<sup>76</sup> i wskazujące wsparcie, jakie Komisja zamierza zapewnić. Oczekuje się, że w nadchodzących tygodniach podobne porozumienia zostaną podpisane z pozostałymi partnerami z Bałkanów Zachodnich. Ponadto dnia 7 października 2019 r. Komisja podpisała z Czarnogórą umowę o współpracy w zakresie zarządzania granicami między Czarnogórą a Europejską Agencją Straży Granicznej i Przybrzeżnej (Frontex). Umowa ta umożliwia Agencji udzielanie Czarnogórze wsparcia w zarządzaniu granicami w celu rozwiązania problemu migracji nieuregulowanej i przestępczości transgranicznej, co skutkuje zwiększeniem bezpieczeństwa na granicach zewnętrznych UE.

**Aby zacieśnić współpracę z krajami partnerskimi w walce ze wspólnymi zagrożeniami bezpieczeństwa, Komisja wzywa Radę do:**

- przyjęcia decyzji upoważniającej do podjęcia rokowań w sprawie umowy między UE a **Nową Zelandią** w sprawie wymiany danych osobowych do celów zwalczania poważnej przestępczości i terroryzmu;
- przyjęcia decyzji upoważniającej do podjęcia rokowań w sprawie umowy między UE a **Japonią** w sprawie przekazywania danych dotyczących przelotu pasażera;
- przyjęcia proponowanej **decyzji Rady w sprawie stanowiska, jakie ma być zajęte w imieniu UE na forum Rady Organizacji Międzynarodowego Lotnictwa Cywilnego** w odniesieniu do norm i zalecanych metod postępowania w zakresie danych dotyczących przelotu pasażera.

## VI. WNIOSKI

W niniejszym sprawozdaniu przedstawiono szereg środków, które UE podejmuje w walce ze wspólnymi zagrożeniami w Europie oraz w celu zwiększenia naszego wspólnego bezpieczeństwa. Postęp prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa – opartych na założeniu, że najlepszą odpowiedzią na współczesne zagrożenia bezpieczeństwa jest współdziałanie w ramach UE i z państwami trzecimi – jest rezultatem ścisłej współpracy między szeregiem podmiotów, budowania zaufania, dzielenia się zasobami i wspólnego stawiania czoła zagrożeniom: na wszystkich szczeblach sprawowania rządów – od miast i innych podmiotów lokalnych, przez regiony i organy krajowe, aż po szczebel unijny z Parlamentem Europejskim i Radą; angażowania organów publicznych, agencji UE, podmiotów prywatnych i społeczeństwa obywatelskiego; a także wykorzystania wiedzy eksperckiej, narzędzi i zasobów z różnych obszarów polityki, takich jak polityka transportowa, jednolity rynek cyfrowy lub polityka spójności. Tym samym prace

<sup>75</sup> [https://ec.europa.eu/home-affairs/news/news/20191009\\_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia\\_en](https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en)

<sup>76</sup> We wspólnym planie działania przewidziano podjęcie działań skupiających się wokół następujących pięciu celów: solidne ramy na rzecz zwalczania terroryzmu; skuteczne zapobieganie brutalnemu ekstremizmowi i przeciwdziałanie mu; skuteczna wymiana informacji i współpraca operacyjna; budowanie zdolności w zakresie walki z praniem pieniędzy i finansowaniem terroryzmu; wzmocnienie ochrony obywateli i infrastruktury.

podejmowane w ramach unii bezpieczeństwa stanowią nieodłączny element ochrony praw podstawowych oraz ochrony i propagowania naszych wartości.

Prace nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa muszą być kontynuowane. Istnieje potrzeba szybkiego osiągnięcia porozumienia w sprawie istotnych inicjatyw oczekujących na realizację, mianowicie (1) wniosku ustawodawczego w sprawie usuwania treści o charakterze terrorystycznym w internecie, (2) wniosku ustawodawczego w sprawie poprawy dostępu organów ścigania do elektronicznego materiału dowodowego, (3) wniosku ustawodawczego w sprawie ustanowienia Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji, a także (4) rozpatrywanych wniosków legislacyjnych w sprawie sprawniejszych i bardziej inteligentnych systemów informacyjnych służących zarządzaniu bezpieczeństwem, granicami i migracjami. Uzgodnione środki i instrumenty należy przełożyć na rzeczywistość operacyjną w terenie, której musi towarzyszyć terminowe i pełne wdrożenie przepisów UE przez wszystkie państwa członkowskie, aby można było uzyskać wszystkie płynące z tych przepisów korzyści dla bezpieczeństwa. W szczególności wszystkie państwa członkowskie muszą wdrożyć niedawno przyjęte przepisy w zakresie interoperacyjności systemów informacyjnych UE służących do zarządzania bezpieczeństwem, granicami i migracjami, aby można było zrealizować ambitny cel, jakim jest osiągnięcie pełnej interoperacyjności do 2020 r. Europa musi zachować czujność w obliczu pojawiających się i zmieniających zagrożeń oraz musi nadal współdziałać na rzecz zwiększenia bezpieczeństwa wszystkich obywateli.