KOMISJA
EUROPEJSKA

Strasburg, dnia 16.5.2017 r.
COM(2017) 261 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY EUROPEJSKIEJ I RADY

Siódme 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 siódmym comiesięcznym sprawozdaniem i obejmuje działania w dwóch głównych dziedzinach: zwalczania terroryzmu i przestępczości zorganizowanej oraz środków, które je wspierają, oraz wzmocnienia naszej obrony i rozwijania odporności wobec wymienionych zagrożeń. W niniejszym sprawozdaniu skoncentrowano się na pracach na rzecz interoperacyjności systemów informacyjnych co celów zapewnienia bezpieczeństwa oraz zarządzania granicami i przepływami migracyjnymi, która pozwoli na skuteczniejsze i wydajniejsze zarządzanie danymi w UE, przy pełnym poszanowaniu wymogów związanych z ochroną danych, tak aby lepiej chronić granice zewnętrzne i wzmocnić bezpieczeństwo wewnętrzne z korzyścią dla wszystkich obywateli. Niniejsze sprawozdanie zawiera również zaktualizowane informacje na temat postępów w zakresie kluczowych inicjatyw ustawodawczych i nieustawodawczych.

Niedawny globalny cyberatak, w ramach którego zablokowano tysiące systemów komputerowych przy użyciu oprogramowania typu ransomware, ponownie pokazał, jak pilną potrzebą jest udoskonalenie unijnej odporności cybernetycznej i działań zabezpieczających, biorąc pod uwagę rosnącą przestępczość zorganizowaną wykorzystującą cyberprzestrzeń, jak określono w ostatnim sprawozdaniu z postępu prac nad stworzeniem unii bezpieczeństwa[1] oraz jak podkreślono w przeprowadzonej przez Europol ocenie zagrożenia poważną i zorganizowaną przestępczością w Unii Europejskiej[2]. Komisja przyspiesza prace w dziedzinie bezpieczeństwa cybernetycznego, w szczególności poprzez przegląd strategii Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego z 2013 r.[3], ogłoszony przy okazji przeglądu śródokresowego jednolitego rynku cyfrowego[4], aby zapewnić aktualną i skuteczną reakcję na te zagrożenia.

W orędziu o stanie Unii wygłoszonym przez przewodniczącego Jeana-Claude'a Junckera we wrześniu 2016 r.[5] oraz w konkluzjach Rady Europejskiej z grudnia 2016 r.[6] podkreślono, jak istotne znaczenie ma likwidacja niedociągnięć w zarządzaniu danymi oraz poprawa interoperacyjności istniejących systemów informacyjnych. Niedawne ataki terrorystyczne spowodowały jeszcze większe skupienie się na tym celu, ponieważ wykazały pilną potrzebę zapewnienia interoperacyjności systemów informacyjnych, a także wyeliminowania obecnych niedociągnięć, które powodują, że osoby podejrzane o terroryzm mogą rejestrować się pod różnymi pseudonimami w różnych, niepowiązanych ze sobą bazach danych. Niniejsze sprawozdanie określa, w jaki sposób Komisja zamierza podejść do zadania, jakim jest **osiągnięcie interoperacyjności systemów informacyjnych dotyczących bezpieczeństwa oraz zarządzania granicami i przepływami migracyjnymi do 2020 r.,** aby zapewnić funkcjonariuszom straży granicznej, funkcjonariuszom organów ścigania, w tym służbom celnym, urzędnikom imigracyjnym oraz organom wymiaru sprawiedliwości dostęp do niezbędnych informacji. Stanowi to kontynuację działań zapoczątkowanych w

---

1 COM(2016) 213 final (12.4.2017).

2 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

3 JOIN(2013) 1 final (7.2.2013).

4 COM(2017) 228 final (10.5.2017). Zob. również czwarte sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa, COM(2017) 41 final (25.1.2017).

5 Orędzie o stanie Unii w 2016 r. (14.9.2016), https://ec.europa.eu/commission/state-union-2016_pl

6 Konkluzje Rady Europejskiej (15.12.2016), http://www.consilium.europa.eu/en/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/

kwietniu 2016 r. dzięki komunikatowi Komisji pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa”[7] oraz przez prace grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, którą Komisja powołała w następstwie tego komunikatu.

II. SPRAWNIEJSZE I BARDZIEJ INTELIGENTNE SYSTEMY INFORMACYJNE

1. Komunikat Komisji z kwietnia 2016 r. i podjęte dotąd kroki

W komunikacie Komisji z kwietnia 2016 r. pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” wskazano kilka strukturalnych niedociągnięć związanych z systemami informacyjnymi:

- niektóre z istniejących systemów mają nieoptymalne mechanizmy działania;
- w unijnej strukturze zarządzania danymi istnieją pewne luki informacyjne;
- systemy informatyczne są zarządzane w różny sposób i tworzą skomplikowany układ;
- zarządzanie danymi dotyczącymi granic i bezpieczeństwa odbywa się w ramach fragmentarycznych struktur, a informacje przechowywane są oddzielnie w niepowiązanych systemach, co sprawia, że pewne dane pozostają nieuwzględnione.

Aby wyeliminować te niedociągnięcia, **Komisja zaproponowała działania w trzech obszarach**, podkreślając, że prace Komisji będą opierać się na wymaganiach Karty praw podstawowych, a w szczególności na kompleksowych ramach w zakresie ochrony danych osobowych UE.

Po pierwsze, Komisja określiła możliwe warianty służące **maksymalizacji korzyści wynikających z istniejących systemów, podkreślając, że państwa członkowskie muszą w pełni wykorzystywać te systemy.** Następnie Komisja przedstawiła w grudniu 2016 r. wniosek ustawodawczy dotyczący wzmocnienia systemu informacyjnego Schengen (SIS)[8], który jest najskuteczniejszym istniejącym narzędziem pozwalającym na współpracę straży granicznej, organów celnych, funkcjonariuszy policji oraz organów wymiaru sprawiedliwości. Komisja przedstawiła również w maju 2016 r. wniosek ustawodawczy dotyczący wzmocnienia bazy danych Eurodac[9] obejmującej dane w zakresie azylu i nieuregulowanej migracji, co ułatwi powroty i pomoże zwalczać nieuregulowaną migrację. W styczniu 2016 r. Komisja przedstawiła wniosek ustawodawczy dotyczący ułatwienia wymiany danych z rejestrów karnych na temat obywateli państw trzecich w UE poprzez usprawnienie Europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS)[10]. Zgodnie z zapowiedziami[11], w następstwie dyskusji z współprawodawcami na temat wniosku ze stycznia 2016 r., Komisja przedstawi w czerwcu 2017 r. dodatkowy wniosek dotyczący utworzenia scentralizowanego systemu[12] pozwalającego identyfikować

---

7 COM(2016) 205 final (6.4.2016).

8 COM(2016) 881 final (21.12.2016), COM(2016) 882 final (21.12.2016), COM(2016) 883 final (21.12.2016).

9 COM(2016) 272 final (4.5.2016).

10 COM(2016) 7 final (19.1.2016).

11 Zob. piąte sprawozdanie z postępów na rzecz rzeczywistej i skutecznej unii bezpieczeństwa, COM(2017) 203 final (2.3.2017).

12 Kiedy państwa członkowskie będą poszukiwać informacji o wyrokach skazujących wobec obywatela państwa trzeciego, scentralizowany system przekieruje je do tych państw członkowskich, w których można znaleźć szczegółowe dane w rejestrze skazanych.

skazanych obywateli państw trzecich oraz wskazać, które państwa członkowskie posiadają informacje na ich temat.

W czerwcu 2017 r. Komisja przedstawi również wniosek ustawodawczy mający na celu zmianę mandatu prawnego agencji eu-LISA[13], w tym uwzględnienie zadania, jakim jest osiągnięcie interoperacyjności scentralizowanych systemów informacyjnych UE dotyczących bezpieczeństwa, zarządzania granicami i przepływami migracyjnymi.

Po drugie, w komunikacie określono możliwe warianty **opracowania nowych i uzupełniających działań, które pozwolą usunąć luki w unijnej strukturze zarządzania danymi**. W szczególności Komisja stwierdziła, że istnieją znaczne luki informacyjne w odniesieniu do obywateli państw trzecich odwiedzających obszar Schengen oraz, w obrębie tej samej grupy, w odniesieniu do obywateli państw trzecich zwolnionych z obowiązku wizowego wjeżdżających na teren UE przez granice lądowe. Obecnie nie rejestruje się przekroczeń granic zewnętrznych przez obywateli państw trzecich, nie ma również dostępnych informacji o obywatelach państw trzecich zwolnionych z obowiązku wizowego przed ich przybyciem na zewnętrzną granicę lądową. W związku z tym Komisja przedstawiła wnioski ustawodawcze dotyczące ustanowienia dwóch nowych systemów informacyjnych, które pozwoliłyby zlikwidować te luki. W kwietniu 2016 r. Komisja przedstawiła wniosek dotyczący unijnego systemu wjazdu/wyjazdu w celu modernizacji zarządzania granicami zewnętrznymi, aby poprawić jakość i skuteczność kontroli[14]. W listopadzie 2016 r. Komisja przedstawiła wniosek dotyczący europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS), gromadzącego informacje o wszystkich osobach podróżujących do UE bez wizy, tak aby przeprowadzać z wyprzedzeniem kontrole pod kątem nieuregulowanej migracji oraz kontrole bezpieczeństwa[15].

Trzecim obszarem wspomnianym w komunikacie była **konieczność poprawy interoperacyjności systemów informacyjnych**. W komunikacie określono, że biorąc pod uwagę złożone ramy ochrony danych osobowych w UE oraz znaczny postęp w zakresie technologii i bezpieczeństwa informatycznego, istnieje możliwość osiągnięcia interoperacyjności systemów informacyjnych przy równoczesnych niezbędnych surowych przepisach dotyczących dostępu i wykorzystania danych, bez uszczerbku dla celowości. W komunikacie przedstawiono **cztery różne rozwiązania** służące osiągnięciu interoperacyjności:

- **pojedynczy interfejs wyszukiwania** do przeszukiwania kilku systemów informacyjnych jednocześnie oraz do uzyskiwania łącznych wyników wyszukiwania na jednym ekranie;
- **wzajemne połączenia między systemami informacyjnym**, dzięki którym dane zarejestrowane w jednym systemie będą automatycznie dostępne do wglądu w innym systemie;
- stworzenie **wspólnego serwisu do porównywania danych biometrycznych**, który obsługiwałaby różne systemy informacyjne;
- **wspólne repozytorium tożsamości** oparte na danych alfanumerycznych na potrzeby różnych systemów informacyjnych (w tym na wspólnych cechach biograficznych, takich jak imię i nazwisko oraz data urodzenia).

[13] Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości.
[14] COM(2016) 194 final (6.4.2016).
[15] COM(2016) 731 final (16.11.2016).

Komisja podjęła dyskusję na temat tego, w jaki sposób systemy informacyjne w Unii Europejskiej mogłyby lepiej wspierać zarządzanie granicami i zapewnianie bezpieczeństwa wewnętrznego, a także powołała grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, aby przyspieszyć prace w tej dziedzinie (zob. sekcja II.3 poniżej).

2. Postępy w priorytetowych dossier dotyczących systemów informacyjnych

Do wykonywania swoich obowiązków funkcjonariusze straży granicznej, funkcjonariusze organów ścigania oraz organy wymiaru sprawiedliwości potrzebują dostępu do poprawnych i pełnych danych. **Dlatego Parlament Europejski i Rada powinny przyspieszyć prace nad priorytetowymi wnioskami związanymi z systemami informacyjnymi**, które wymieniono w pierwszej części komunikatu z kwietnia 2016 r. Jak określono powyżej, ma to kluczowe znaczenie dla zapewnienia większej skuteczności systemów informacyjnych w zakresie ochrony granic i bezpieczeństwa, a także pozwoli usunąć poważne luki informacyjne poprzez ustanowienie nowych systemów niezbędnych do zabezpieczenia granic zewnętrznych.

Najbardziej zaawansowane są prace nad wnioskiem w sprawie **unijnego systemu wjazdu/wyjazdu**. Obecnie prowadzone są rozmowy trójstronne, a zakładany termin ich zakończenia w czerwcu 2017 r., wyznaczony przez Radę Europejską, jest realny do osiągnięcia. Postępują dyskusje techniczne nad europejskim **systemem informacji o podróży i zezwoleń na podróż** (ETIAS), jednak obie instytucje muszą dopiero określić swoje stanowiska negocjacyjne. Przyjęcie mandatu przez Radę jest planowane na czerwiec 2017 r., podczas gdy Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego zamierza przyjąć swój mandat negocjacyjny we wrześniu 2017 r. We wspólnej deklaracji w sprawie priorytetów legislacyjnych na rok 2017[16] uznano, że wniosek ten należy potraktować priorytetowo, aby zapewnić jego przyjęcie przed końcem 2017 r. Komisja będzie w dalszym ciągu wspierać współprawodawców w osiągnięciu tego celu. Obie instytucje prowadzą również prace nad wnioskiem Komisji w sprawie wzmocnienia **systemu informacyjnego Schengen (SIS)**. Pierwszy etap dyskusji nad tymi trzema wnioskami na poziomie grup roboczych Rady zostanie zakończony podczas maltańskiego przewodnictwa w Radzie. Sprawozdawca Parlamentu Europejskiego przewiduje przedstawienie projektu sprawozdania w Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) do końca czerwca 2017 r. Jeśli chodzi o wniosek ustawodawczy dotyczący wzmocnienia systemu **Eurodac**, Rada zgodziła się na częściowe podejście ogólne w grudniu 2016 r., podczas gdy Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego planuje głosowanie nad sprawozdaniem w maju 2017 r. Etap rozmów trójstronnych powinien rozpocząć się zaraz po tym.

3. Prace grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności

W czerwcu 2016 r. Komisja powołała grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności. Zadaniem grupy ekspertów było zajęcie się **prawnymi, technicznymi i operacyjnymi aspektami czterech różnych rozwiązań** służących zapewnieniu interoperacyjności systemów informacyjnych, w tym rozważenie konieczności,

[16] Wspólna deklaracja w sprawie priorytetów legislacyjnych na rok 2017 (13.12.2016), https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf

wykonalności technicznej i proporcjonalności dostępnych rozwiązań oraz ich wpływu na ochronę danych[17]. Grupa ekspertów została również poproszona o zidentyfikowanie niedociągnięć i ewentualnych luk informacyjnych spowodowanych złożonością i rozdrobnieniem systemów informacyjnych[18] oraz zaproponowanie sposobów ich wyeliminowania. W skład grupy weszli eksperci z państw członkowskich i państw stowarzyszonych Schengen, oraz eksperci z agencji eu-LISA, Europolu, Europejskiego Urzędu Wsparcia w dziedzinie Azylu, Europejskiej Agencji Straży Granicznej i Przybrzeżnej i Agencji Praw Podstawowych. W pracach grupy jako pełnoprawni członkowie uczestniczyli Koordynator UE ds. Zwalczania Terroryzmu oraz Europejski Inspektor Ochrony Danych. Przedstawiciele Sekretariatu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego oraz Sekretariatu Generalnego uczestniczyli w posiedzeniach grupy w charakterze obserwatorów.

Komisja z zadowoleniem przyjęła sprawozdanie końcowe[19] grupy ekspertów wysokiego szczebla z dnia 11 maja 2017 r. Grupa ekspertów stwierdziła, że **konieczne i wykonalne pod względem technicznym są prace w kierunku trzech rozwiązań służących zapewnieniu interoperacyjności systemów informacyjnych**, które to rozwiązania mogą zasadniczo zarówno **przynieść korzyści operacyjne**, jak i zostać ustanowione **zgodnie z wymogami ochrony danych**:

- europejski portal wyszukiwania[20];
- wspólny serwis porównywania danych biometrycznych oraz
- wspólne repozytorium tożsamości.

Zdaniem grupy ekspertów rozwiązanie polegające na wzajemnym połączeniu systemów powinno być rozpatrywane indywidualnie w każdym przypadku. Jednym z takich przypadków jest wzajemne połączenie planowanego unijnego systemu wjazdu/wyjazdu i wizowego systemu informacyjnego[21]. We wniosku Komisji dotyczącym unijnego systemu wjazdu/wyjazdu postanowiono, że dane zawarte w wizowym systemie informacyjnym będą regularnie i automatycznie przeglądane przez unijny system wjazdu/wyjazdu w celu zachowania niewielkiego zestawu danych (naklejka wizowa, liczba wjazdów, okres pobytu), co umożliwi unijnemu systemowi wjazdu/wyjazdu prawidłowe przetwarzanie danych dotyczących posiadaczy wizy zgodnie z wymogami dotyczącymi minimalizacji danych i spójności danych. Grupa ekspertów stwierdziła, że zakładając wystarczający postęp w zakresie pozostałych trzech rozwiązań służących zapewnieniu interoperacyjności systemów, wzajemne połączenia między systemami nie są konieczne wyłącznie w celu poprawy wymiany informacji.

---

17 Decyzja Komisji 2016/C 257/03 (17.6.2016).

18 Zob. dokument programowy grupy ekspertów (czerwiec 2016 r.): http://ec.europa.eu/transparency/regexpert/ index.cfm?do=groupDetail.groupDetailDoc&id=24081&no=2.

19 Sprawozdanie końcowe grupy ekspertów można znaleźć na stronie: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1. W załącznikach do sprawozdania znajdują się streszczenie sprawozdania Agencji Praw Podstawowych oraz oświadczenie Europejskiego Inspektora Ochrony Danych i oświadczenie Koordynatora UE ds. Zwalczania Terroryzmu.

20 Termin „pojedynczy interfejs wyszukiwania" zastąpiono terminem „europejski portal wyszukiwania", aby uniknąć ewentualnego pomylenia z krajowymi pojedynczymi interfejsami wyszukiwania, które istnieją w państwach członkowskich w odniesieniu do krajowych systemów informacyjnych.

21 Rozporządzenie (WE) nr 767/2008 (9.7.2008).

W sprawozdaniu końcowym grupy ekspertów podkreślono również **znaczenie pełnego wdrożenia i stosowania istniejących systemów informacyjnych**. Grupa przyjrzała się również zdecentralizowanym **ramom z Prüm** dotyczącym wymiany danych o DNA, odciskach palców i rejestracji pojazdów,[22] zalecając przeprowadzenie studium wykonalności dotyczącego scentralizowanego mechanizmu trasowania oraz ewentualnie uzupełnienia ich o nowe funkcje. Jeśli chodzi o zdecentralizowany system ustanowiony przez **dyrektywę w sprawie danych o przelocie pasażera (PNR)**[23], grupa ekspertów zaleciła studium wykonalności w sprawie scentralizowanego mechanizmu dotyczącego danych pasażera przekazywanych przed podróżą (API) oraz danych o przelocie pasażera (PNR) jako narzędzia wsparcia technicznego umożliwiającego połączalność z przewoźnikami lotniczymi. Grupa uznała, że wzmocniłoby to skuteczność jednostek do spraw informacji o pasażerach po wdrożeniu przez państwa członkowskie dyrektywy UE w sprawie danych o przelocie pasażera.

Komisja będzie dalej skupiać się na **pełnym wdrożeniu istniejących systemów informacyjnych**. Istotne jest, aby państwa członkowskie w pełni zastosowały istniejące systemy, wykorzystując w pełni ich potencjał. Komisja będzie w dalszym ciągu udzielać kompleksowego wsparcia, zgodnie ze swoim planem wdrożenia[24], aby pomóc zapewnić wdrożenie dyrektywy w sprawie danych o przelocie pasażera (PNR) przez wszystkie państwa członkowskie do maja 2018 r. Komisja będzie ściśle współpracować ze wszystkimi państwami członkowskimi nad zakończeniem pełnego wdrożenia ram z Prüm, w szczególności z pięcioma państwami członkowskimi, które nadal muszą wdrożyć decyzje z Prüm. W duchu zaleceń grupy ekspertów Komisja zbada sposoby wzmocnienia funkcjonowania i skuteczności tych systemów podczas ich stosowania przez państwa członkowskie.

Grupa ekspertów zidentyfikowała **lukę informacyjną związaną z przekraczaniem granic zewnętrznych przez obywateli UE**. W swoim sprawozdaniu końcowym nawiązuje ona do niedawnego wprowadzenia systematycznych kontroli w odpowiednich bazach danych w odniesieniu do wszystkich osób, które korzystają z prawa do swobodnego przemieszczania się na mocy prawa Unii, w momencie wjazdu do strefy Schengen lub wyjazdu z niej[25]. Grupa podkreśla, że czas i miejsce tych kontroli nie są rejestrowane, oraz zauważa, że mogłoby to dostarczyć przydatnych informacji do celów egzekwowania prawa. Grupa ekspertów zaleca w związku z tym dalszą analizę proporcjonalności i wykonalności systematycznego rejestrowania wszystkich przekroczeń granic zewnętrznych przez obywateli UE[26].

Komisja zauważa, że w sprawozdaniu grupy ekspertów nie wykazano konieczności i proporcjonalności rejestrowania przekroczeń granic zewnętrznych przez wszystkich obywateli UE. Jeżeli pojawią się dalsze elementy wskazujące na konieczność i proporcjonalność takiej rejestracji, Komisja jest gotowa ocenić potrzebę dalszych działań. W międzyczasie Komisja przeanalizuje powiązane zalecenie grupy ekspertów, aby podjąć prace w kierunku ewentualnego rejestrowania „trafień” w systemie informacji Schengen

[22] Decyzja Rady 2008/615/WSiSW (23.6.2008).
[23] Dyrektywa (UE) 2016/681 (27.4.2016).
[24] SWD(2016) 426 final (28.11.2016).
[25] Rozporządzenie (UE) 2017/458 z 15.3.2017.
[26] Grupa ekspertów omówiła również możliwość rozszerzenia proponowanego unijnego systemu wjazdu/wyjazdu na obywateli UE lub rozszerzonego wykorzystania dzienników zdarzeń z systemu informacyjnego Schengen. Oba te rozwiązania zostały odrzucone.

dotyczących osób, wobec których istnieje w systemie ostrzeżenie, jako możliwy sposób rejestrowania podróży tych obywateli UE, którzy zostali uznani za potencjalnie zaangażowanych w terroryzm lub inne formy poważnych przestępstw.

Grupa ekspertów zidentyfikowała również **lukę informacyjną związaną z wizami długoterminowymi, dokumentami pobytowymi oraz kartami pobytowymi**. Zauważyła, że państwa członkowskie dysponują ograniczonymi środkami do kontroli ważności tych dokumentów, jeżeli zostały one wydane przez inne państwo członkowskie. Grupa zasugerowała, że mogłoby to skłaniać do rozważenia utworzenia centralnego unijnego repozytorium zawierającego informacje o wizach długoterminowych, dokumentach pobytowych oraz kartach pobytu. Komisja oceni potrzebę stworzenia takiego repozytorium, w tym jego konieczność, techniczną wykonalność oraz proporcjonalność.

Grupa ekspertów stwierdziła również, że **organy celne** pełnią bardzo ważną rolę we współpracy międzyagencyjnej na granicach zewnętrznych. Dlatego Komisja w dalszym ciągu analizuje techniczne, operacyjne i prawne aspekty interoperacyjności systemów celnych.

III. W STRONĘ INTEROPERACYJNOŚCI SYSTEMÓW INFORMACYJNYCH

1. Celem Komisji jest interoperacyjność systemów informacyjnych do 2020 r.

Głównym celem jest zagwarantowanie funkcjonariuszom straży granicznej, funkcjonariuszom organów ścigania, urzędnikom imigracyjnym oraz organom wymiaru sprawiedliwości dostępu do niezbędnych informacji, które pozwolą lepiej chronić granice zewnętrzne oraz wzmocnić bezpieczeństwo wewnętrzne z korzyścią dla wszystkich obywateli. Dlatego pierwszym krokiem jest właściwe funkcjonowanie różnych systemów informacyjnych w tej dziedzinie oraz szybkie przyjęcie wniosków ustawodawczych będących obecnie przedmiotem prac.

Zgodnie z komunikatem z kwietnia 2016 r. oraz z wnioskami i zaleceniami grupy ekspertów Komisja określa **nowe podejście do zarządzania danymi dotyczącymi ochrony granic i bezpieczeństwa**, zakładające pełną interoperacyjność wszystkich scentralizowanych systemów informacyjnych UE w dziedzinie bezpieczeństwa, zarządzania granicami i zarządzania przepływami migracyjnymi[27], przy pełnym poszanowaniu praw podstawowych, tak aby:

- różne systemy mogły być przeszukiwane jednocześnie przy użyciu **europejskiego portalu wyszukiwania**, w pełnym poszanowaniu zasady celowości oraz praw dostępu, aby lepiej wykorzystywać istniejące systemy informacyjne, ewentualnie dzięki uproszczonym przepisom regulującym dostęp dla organów ścigania[28];

[27] System informacyjny Schengen, wizowy system informacyjny, system Eurodac, planowany unijny system wjazdu/wyjazdu, planowany unijny system informacji o podróży oraz zezwoleń na podróż (ETIAS) oraz planowany europejski system przekazywania informacji z rejestrów karnych (ECRIS) dotyczący obywateli państw trzecich.

[28] Komitet Stałych Przedstawicieli (Coreper) Rady po udzieleniu prezydencji Rady w dniu 2 marca 2017 r. mandatu do rozpoczęcia międzyinstytucjonalnych negocjacji w sprawie unijnego systemu wjazdu/wyjazdu wezwał Komisję do przedstawienia wniosku dotyczącego kompleksowych ram regulujących dostęp organów ścigania do różnych baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych w celu większego uproszczenia, spójności, skuteczności i reakcji na potrzeby operacyjne. Grupa ekspertów zaleca, aby ramy regulujące dostęp dla organów ścigania były oparte na podejściu dwustopniowym, polegającym na tym, że faktyczne wyświetlenie danych byłoby przewidziane dopiero po upewnieniu się, że dane istnieją. Pozwoliłoby to poprawić skuteczność, a jednocześnie zmniejszyć liczbę przypadków dostępu organów ścigania i ich zakres.

- różne systemy wykorzystywały jeden **wspólny serwis do porównywania danych biometrycznych**, umożliwiający równoczesne przeszukiwanie różnych systemów informacyjnych zawierających dane biometryczne, w miarę możliwości pozwalający na oznaczenie „wynik/brak wyniku", które wskazywałoby związek z powiązanymi danymi biometrycznymi znalezionymi w innym systemie[29];
- systemy wykorzystywały **wspólne repozytorium tożsamości** oparte na alfanumerycznych danych dotyczących tożsamości[30], aby wykryć, czy dana osoba jest zarejestrowana pod różnymi tożsamościami w różnych bazach danych.

To nowe podejście musi zapewniać zgodność systemów ze **szczegółowymi postanowieniami dotyczącymi ochrony danych**, z konkretnymi przepisami regulującymi dostęp dla właściwych organów, oddzielnymi przepisami dotyczącymi zasady celowości dla każdej kategorii danych oraz przepisami odnoszącymi się do zatrzymywania danych. Takie podejście do interoperacyjności doprowadziłoby do wzajemnego połączenia wszystkich systemów.

Nowe podejście przyczyniłoby się do przezwyciężenia obecnych niedociągnięć w unijnej strukturze zarządzania danymi, w tym do uwzględnienia kwestii, których dotychczasowe podejście nie obejmowało. Agencja **eu-LISA** będzie odgrywać kluczową rolę w pracach nad osiągnięciem interoperacyjności systemów informacyjnych, w tym podczas bieżących i przyszłych analiz technicznych (zob. sekcja III.2 poniżej). Wniosek ustawodawczy, który Komisja przedstawi w czerwcu 2017 r., wzmocni mandat eu-LISA i umożliwi zagwarantowanie wdrożenia tego nowego podejścia. Komisja będzie również nadal angażować Europejskiego Inspektora Ochrony Danych oraz Agencję Praw Podstawowych w prace nad interoperacyjnością.

Zapewnienie wysokiego poziomu **jakości danych ma zasadnicze znaczenie dla skuteczności systemów informacyjnych**. Interoperacyjność będzie funkcjonować wyłącznie wtedy, gdy systemy informacyjne będą zasilane poprawnymi i pełnymi danymi. Komisja wskazała już, że jakość danych to kwestia wymagająca dalszych działań na poziomie UE[31]. W trybie pilnym, wspólnie z agencją eu-LISA, będzie wdrażać zalecenia wydane przez grupę ekspertów, służące poprawie jakości danych w unijnych systemach informacyjnych.

Komisja będzie prowadzić prace nad zaleceniami grupy ekspertów dotyczącymi automatycznej kontroli jakości, „hurtowni danych" zdolnej do analizowania zanonimizowanych danych pobranych z odpowiednich systemów informacyjnych do celów statystycznych i sprawozdawczych, oraz modułów szkoleniowych poświęconych jakości danych dla pracowników odpowiedzialnych za wprowadzanie danych do systemów na poziomie krajowym. W przyszłym wniosku ustawodawczym uwzględniona zostanie ważna rola agencji eu-LISA w zapewnianiu wysokiej jakości danych w scentralizowanych systemach informacyjnych.

Interoperacyjność wymaga technicznej interakcji pomiędzy istniejącymi systemami informacyjnymi. Celem **uniwersalnego formatu wiadomości (UMF)** na szczeblu UE jest

---

[29] Konieczne są dalsze analizy techniczne dotyczące ewentualnego uwzględnienia funkcji oznaczania we wspólnym serwisie do porównywania danych biometrycznych oraz wpływu tego serwisu na ochronę danych – zob. sekcja III.2 poniżej.

[30] Repozytorium obejmowałoby również wspólne cechy biograficzne, takie jak imię i nazwisko, data urodzenia oraz płeć.

[31] Czwarte sprawozdanie z postępów na rzecz rzeczywistej i skutecznej unii bezpieczeństwa, COM(2017) 41 final (25.1.2017).

ułatwienie tej interakcji. Wspólnie z agencją eu-LISA Komisja podejmie prace nad zaleceniami grupy ekspertów dotyczącymi wzmocnienia uniwersalnego formatu wiadomości zgodnie z bieżącymi pracami, w celu uwzględnienia opracowanego formatu w scentralizowanych unijnych systemach informacyjnych.

2. Dalsze kroki w celu osiągnięcia interoperacyjności systemów informacyjnych do 2020 r.

Równocześnie z pracami nad priorytetowymi dossier dotyczącymi systemów informacyjnych Komisja zachęca Parlament Europejski i Radę do podjęcia **wspólnych dyskusji nad kierunkiem dalszych działań** służących osiągnięciu interoperacyjności, jak określono w komunikacie. W tym celu Komisja przedstawi i omówi te kwestie z Komisją Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego w dniu 29 maja 2017 r. oraz z państwami członkowskimi na szczycie Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniu 8 czerwca 2017 r. W oparciu o te dyskusje trzy instytucje powinny odbyć trójstronne spotkania na szczeblu technicznym[32] jesienią 2017 r., aby omówić dalsze działania służące osiągnięciu interoperacyjności, jak określono w niniejszym komunikacie, w tym potrzeby operacyjne w zakresie ochrony granic i bezpieczeństwa oraz sposoby zapewnienia proporcjonalności i pełnej zgodności z prawami podstawowymi. Celem jest jak najszybsze osiągnięcie **konsensusu co do dalszego kierunku działań** (najpóźniej do końca 2017 r.) oraz co do dalszych kroków niezbędnych do osiągnięcia interoperacyjności systemów informacyjnych do 2020 r.

Równocześnie ze wspólnymi dyskusjami między trzema instytucjami i bez przesądzania o wyniku Komisja oraz eu-LISA będą w ciągu roku 2017 prowadzić **dalszą analizę techniczną w sprawie zidentyfikowanych rozwiązań w zakresie interoperacyjności**, poprzez serię badań technicznych i dowodów słuszności koncepcji. Komisja będzie regularnie informować Parlament Europejski i Radę o postępach w tej analizie technicznej.

Korzystając z kontaktów z Parlamentem Europejskim i Radą, jak również z wyników trwających prac legislacyjnych nad systemami informacyjnymi oraz dalszych analiz technicznych, **Komisja pracuje intensywnie nad przedstawieniem, jak najszybciej[33], wniosku ustawodawczego o interoperacyjności**. Zgodnie z zasadami lepszego stanowienia prawa przygotowanie wniosku ustawodawczego będzie obejmowało konsultacje społeczne oraz ocenę skutków, w tym w zakresie praw podstawowych oraz w szczególności prawa do ochrony danych osobowych. Wraz z wnioskiem ustawodawczym dotyczącym interoperacyjności Komisja przedstawi również wniosek ustawodawczy dotyczący przeglądu podstawy prawnej dla wizowego systemu informacyjnego[34], w ramach działań następczych dotyczących sprawozdania z oceny przedstawionego w październiku 2016 r.[35]. Wizowy system informacyjny to jeden ze scentralizowanych systemów informacyjnych, który powinien być częścią nowego podejścia do zarządzania danymi w zakresie granic i bezpieczeństwa.

Wspólne dyskusje pomiędzy trzema instytucjami na temat dalszych kierunków działań służących osiągnięciu interoperacyjności do 2020 r. nie powinny opóźniać prac nad

[32] Spotkania techniczne mogłyby być wzorowane na spotkaniu na temat inteligentnych granic, które odbyło się w lutym 2015 r.

[33] Będzie to wymagało porozumienia ze współprawodawcami na temat powiązanych inicjatyw ustawodawczych będących obecnie przedmiotem dyskusji – zob. sekcja II.2 powyżej.

[34] Rozporządzenie (WE) nr 767/2008 (9.7.2008).

[35] COM(2016) 655 final (14.10.2016).

wnioskami ustawodawczymi dotyczącymi systemów informacyjnych, które są obecnie przedmiotem dyskusji współprawodawców. Większość z tych wniosków została już wymieniona we wspólnej deklaracji jako pilne i kluczowe priorytety. Wszystkie wnioski służą wyeliminowaniu znaczących luk informacyjnych wymagających podjęcia pilnych działań, również zgodnie z zaleceniami grupy ekspertów. Dodatkowy wniosek ustawodawczy dotyczący europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS) dla obywateli państw trzecich, który Komisja przedstawi w czerwcu 2017 r., będzie również w pełni zgodny z zaleceniami grupy ekspertów w zakresie interoperacyjności oraz z podejściem określonym w niniejszym komunikacie. W celu wdrożenia tego nowego podejścia w sposób, który jest wykonalny, niezbędne są stabilne podstawy prawne dla wszystkich odnośnych systemów informacyjnych. Dlatego należy najpierw osiągnąć porozumienie w sprawie wniosków ustawodawczych będących obecnie przedmiotem dyskusji.

IV. WDROŻENIE INNYCH PRIORYTETOWYCH INICJATYW DOTYCZĄCYCH BEZPIECZEŃSTWA

1. Inicjatywy ustawodawcze

W dniu 1 maja 2017 r. weszło w życie nowe **rozporządzenie w sprawie Europolu**[36]. Stanowi ono punkt zwrotny dla Europolu oraz wprowadza szereg nowych elementów, które sprawiają, że unijny organ ścigania może stać się prawdziwym centrum wymiany informacji na temat poważnej przestępczości transgranicznej oraz terroryzmu. Europol będzie dysponować narzędziami, dzięki którym stanie się skuteczniejszy, wydajniejszy i w większym stopniu rozliczalny. W szczególności zmienione ramy przetwarzania danych wzmocnią zdolność Europolu do opracowywania analiz dotyczących przestępczości służących państwom członkowskim, a solidny system ochrony danych zapewni niezależny i skuteczny nadzór nad ochroną danych.

Tak jak wymaga tego Traktat, działania Europolu będą w dalszym ciągu nadzorowane przez Parlament Europejski wraz z parlamentami narodowymi, co zwiększy przejrzystość działań agencji oraz jej legitymację w oczach obywateli.

Aby zminimalizować negatywne skutki wycofania się Danii z Europolu w następstwie wyników referendum w Danii w dniu 3 grudnia 2016 r., w dniu 30 kwietnia 2017 r. **podpisano umowę o współpracy operacyjnej między Europolem a Danią**. Jak uzgodniono we wspólnym oświadczeniu przewodniczącego Komisji Jeana-Claude'a Junckera, przewodniczącego Rady Donalda Tuska oraz premiera Danii Larsa Løkke Rassmussena z dnia 15 grudnia 2016 r.[37], porozumienie określa specjalne uzgodnienia operacyjne zapewniające wystarczający poziom współpracy operacyjnej między Danią a Europolem, w tym wymianę danych operacyjnych oraz oficerów łącznikowych, z zastrzeżeniem zastosowania odpowiednich zabezpieczeń. Chociaż porozumienie nie zastępuje pełnego członkostwa Danii w Europolu, tj. dostępu do repozytoriów danych Europolu oraz pełnego członkostwa w gremiach zarządzających Europolu, Dania zgodziła się na stosowanie orzecznictwa Europejskiego Trybunału Sprawiedliwości i uznanie kompetencji Europejskiego Inspektora Ochrony Danych oraz wdrożyła do prawa duńskiego odpowiednie

[36] Rozporządzenie (UE) 2016/794 (11.5.2016).

[37] Oświadczenie przewodniczącego Komisji Europejskiej Jeana-Claude'a Junckera, przewodniczącego Rady Europejskiej Donalda Tuska oraz premiera Danii Larsa Løkke Rasmussena (15.12.2016), http://europa.eu/rapid/press-release_IP-16-4398_en.htm

unijne przepisy ochrony danych[38]. Jak określono we wspólnym oświadczeniu, uzgodnienia te obowiązują pod warunkiem dalszego członkostwa Danii w UE i w strefie Schengen.

W dniu 28 kwietnia 2017 r. Komisja przyjęła decyzję wykonawczą w sprawie wspólnych protokołów i formatów danych wykorzystywanych przez przewoźników lotniczych podczas przekazywania **danych dotyczących przelotu pasażera (PNR)** jednostkom do spraw informacji o pasażerach zgodnie z dyrektywą UE w sprawie danych dotyczących przelotu pasażera[39]. Wspomniana decyzja wykonawcza harmonizuje aspekty techniczne przekazywania danych dotyczących przelotu pasażera przez przewoźników lotniczych. Uzgodnione formaty danych oraz protokoły transmisji będą obowiązkowe dla wszystkich operacji przekazywania danych dotyczących przelotu pasażera przez przewoźników lotniczych jednostkom do spraw informacji o pasażerach od dnia 28 kwietnia 2018 r.

W dniu 25 kwietnia 2017 r. Rada formalnie przyjęła nową **dyrektywę w sprawie broni palnej**[40]. Państwa członkowskie mają teraz 15 miesięcy na wprowadzenie wymaganych kontroli dotyczących nabywania i posiadania broni palnej w celu zapewnienia, aby grupy przestępcze lub terroryści nie wykorzystywali niejednolitych przepisów istniejących w całej Unii. W dniu 28 kwietnia 2017 r. grupa ekspertów ds. standardów pozbawiania broni palnej cech użytkowych osiągnęła porozumienie dotyczące nowych standardów pozbawiania broni palnej cech użytkowych, w perspektywie przyjęcia zmienionego rozporządzenia Komisji (UE) nr 2015/2403 przed lipcem 2017 r. Obecna zmieniona wersja ma na celu wyjaśnienie pewnych standardów technicznych w celu zapewnienia właściwego stosowania wszystkich technicznych procedur pozbawiania broni palnej cech użytkowych.

2. Wdrażanie działań o charakterze nieustawodawczym

Niedawny cyberatak na szeroką skalę z użyciem oprogramowania ransomware w dniu 12 maja 2017 r. podkreślił pilną potrzebę przyspieszenia działań przez UE i jej agencje oraz państwa członkowskie w celu zwalczania rosnącego zagrożenia **cyberprzestępczością**, z naciskiem na wykrywanie i prewencję. Europejskie Centrum ds. Walki z Cyberprzestępczością przy Europolu (EC3) odegrało ważną rolę w reakcji organów ścigania na niedawny atak, opierając się na działaniach przeprowadzonych poprzednio w tej dziedzinie, zwłaszcza w ramach kampanii „No more ransom". Unijny zespół reagowania na incydenty komputerowe (CERT)-EU pozostawał w ścisłym kontakcie z Europejskim Centrum ds. Walki z Cyberprzestępczością, Zespołami Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym w odnośnych państwach, jednostkami ścigania cyberprzestępczości oraz kluczowymi partnerami przemysłowymi w celu zmniejszenia zagrożeń i pomocy ofiarom. W śródokresowym przeglądzie jednolitego rynku cyfrowego w dniu 10 maja 2017 r. Komisja ogłosiła zamiar dokonania do września 2017 r. przeglądu strategii Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego z 2013 r. Prace te zostały przyspieszone w celu zapewnienia, by obecny nacisk na prewencję został rozszerzony, aby skupić się w większym stopniu na wykrywaniu i zapobieganiu. Celem powinno być zarówno zmniejszenie prawdopodobieństwa cyberataków, jak i ich skutków, poprzez wzmocnienie odporności i dalsze rozwijanie działań państw członkowskich w zakresie budowania krajowych zdolności i pełnego wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji[41]. Potencjalne akty cyberprzestępczości (lub przestępczości

[38] Dyrektywa (UE) 2016/680 (27.4.2016).
[39] Dyrektywa (UE) 2016/681 (27.4.2016).
[40] http://www.consilium.europa.eu/pl/press/press-releases/2017/04/25-control-acquisition-possession-weapons/
[41] Dyrektywa (UE) 2016/1148 (6.7.2016).

wykorzystującej cyberprzestrzeń) nie wynikają tylko z niedociągnięć w systemach lub oprogramowaniu, ale również z zachowań, które prowadzą do niskiego poziomu higieny cyfrowej. Komisja nie tylko wzmocni mandat Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), ale również przedstawi wnioski dotyczące opracowania norm bezpieczeństwa cybernetycznego, certyfikacji oraz oznakowania, aby zapewnić większe bezpieczeństwo cybernetyczne systemów i urządzeń. Komisja skupi się również na rozwijaniu umiejętności cyfrowych i zdolności technicznych w całej Unii Europejskiej.

W obecnych warunkach, gdy istnieją różne zagrożenia związane z polityką publiczną lub bezpieczeństwem wewnętrznym, **wzmocnione kontrole policyjne** na terytorium państw członkowskich, w tym w obszarach przygranicznych, mogą być zarówno konieczne, jak i uzasadnione, aby zwiększyć bezpieczeństwo w ramach strefy Schengen. Dlatego też w dniu 2 maja 2017 r. Komisja przedstawiła zalecenie w sprawie proporcjonalnych kontroli policyjnych oraz współpracy policyjnej w strefie Schengen[42]. W zaleceniu określono środki, jakie państwa Schengen powinny podjąć, aby zapewnić skuteczniejsze wykorzystywanie istniejących uprawnień policyjnych do reagowania na zagrożenia porządku publicznego lub bezpieczeństwa wewnętrznego. Jeżeli jest to konieczne i uzasadnione, państwa członkowskie powinny zintensyfikować kontrole policyjne na obszarach przygranicznych oraz na głównych szlakach transportowych. Decyzje w sprawie takich kontroli, ich umiejscowienia oraz intensywności, leżą całkowicie w gestii państw członkowskich; decyzje te powinny zawsze być proporcjonalne do zidentyfikowanych zagrożeń. Ponadto Komisja zaleca, aby wszystkie państwa członkowskie wzmocniły transgraniczną współpracę policyjną w celu przeciwdziałania zagrożeniom dla porządku publicznego lub bezpieczeństwa wewnętrznego.

W dziedzinie **bezpieczeństwa lotnictwa** nastąpiły w ostatnich tygodniach zmiany, mianowicie USA oraz Zjednoczone Królestwo nałożyły nowe środki bezpieczeństwa na loty przychodzące z wielu krajów Bliskiego Wschodu, Afryki Północnej oraz Turcji, wymagające przewożenia dużych urządzeń elektronicznych w bagażu rejestrowanym. Po stronie UE postępowały prace dotyczące oceny ryzyka i podatności na zagrożenia w związku z lotami przychodzącymi z krajów trzecich. W następstwie informacji, że Stany Zjednoczone mogą planować wprowadzenie podobnych środków w odniesieniu do lotów z unijnych portów lotniczych, Komisja ułatwiła kontakty na szczeblu politycznym w celu zapewnienia koordynacji działań między USA a UE. Na spotkaniu, które odbędzie się w Brukseli w dniu 17 maja 2017 r., USA i UE dokonają wspólnej oceny potencjalnych zagrożeń i wypracują wspólne podejście do przeciwdziałania ewentualnym powstającym zagrożeniom.

W Stałym Komitecie Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego (COSI) Rady trwają prace nad nowym **cyklem polityki unijnej dotyczącej poważnej i zorganizowanej przestępczości międzynarodowej** na lata 2018-2021, uwzględniającym osiem priorytetowych zagrożeń przestępczością określonych przez Komisję w ostatnim sprawozdaniu z postępu prac nad stworzeniem unii bezpieczeństwa[43]. Przyjęcie przez Radę konkluzji w sprawie nowego cyklu polityki unijnej planowane jest na 18 maja 2017 r.

---

[42] W dniu 2 maja 2017 r. Komisja zatwierdziła zasadniczo zalecenie w sprawie proporcjonalności kontroli policyjnych oraz współpracy policyjnej w strefie Schengen (C(2017) 2923). Formalne przyjęcie nastąpiło w dniu 12 maja 2017 r.

[43] COM(2017) 213 final (12.4.2017). Osiem priorytetowych zagrożeń przestępczością zidentyfikowanych przez Komisję to: cyberprzestępczość, przestępstwa związane z narkotykami, przemyt migrantów, zorganizowana przestępczość przeciwko mieniu, handel ludźmi, nielegalny handel bronią palną, oszustwa związane z VAT oraz przestępstwa przeciwko środowisku.

W następstwie sprawozdania z postępów przedstawionego przez Komisję Radzie ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w grudniu 2016 r. i dotyczącego trwających prac na rzecz poprawy transgranicznego dostępu do **dowodów elektronicznych**[44] dla osób prowadzących dochodzenia w sprawach karnych Komisja obecnie kończy przeprowadzanie oceny i przedstawi propozycje dalszych działań, które zostaną omówione na szczycie Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w dniu 8 czerwca 2017 r.

Komisja wspierała prace, które na tym etapie podejmuje grupa państw członkowskich w celu utrzymania systemu e-CODEX, służącego transgranicznej współpracy sądowej oraz cyfrowemu dostępowi do procedur prawnych. Komisja przyjęła do wiadomości, że te państwa członkowskie uważają, że nie jest to trwałe rozwiązanie. Na poziomie grupy roboczej Rady państwa członkowskie przeanalizowały różne warianty i stwierdziły, że najlepszym podmiotem, który zapewniłby utrzymanie i operacyjność systemu e-CODEX, byłaby eu-LISA. Aby zbadać, które rozwiązanie jest najlepsze, Komisja rozpoczęła ocenę wpływu różnych wariantów utrzymania systemu e-CODEX. Wyniki tej analizy wpływu będą dostępne jesienią 2017 r.

Wyżej wspomniane przyjęcie dyrektywy w sprawie broni palnej jest ważnym krokiem naprzód w kierunku wdrożenia przepisów o legalnym nabywaniu i posiadaniu broni palnej. Komisja zajmuje się również kwestią **nielegalnego handlu bronią palną,** zarówno w UE, jak i poza jej granicami. W dniu 16 marca 2017 r. w Kijowie odbyły się obrady techniczne okrągłego stołu UE-Ukraina w sprawie nielegalnego handlu bronią palną. Było to pierwsze posiedzenie tego rodzaju pomiędzy UE a Ukrainą, służące poprawie wymiany informacji związanych z nielegalnym handlem bronią palną. Drugie techniczne obrady okrągłego stołu UE-Tunezja w sprawie nielegalnego handlu bronią palną odbyły się w Tunezji dnia 28 marca 2017 r. Zarówno w odniesieniu do Ukrainy, jak i Tunezji, ustalono plan działań, który obejmuje misje eksperckie UE mające na celu ocenę ram administracyjnych tych państw, zorganizowanie konferencji wysokiego szczebla w sprawie powiązanego prawodawstwa oraz zaproponowanie szkoleń, wizyt studyjnych i warsztatów na temat praktycznych aspektów zarządzania danymi oraz na temat współpracy operacyjnej.

Komisja i Europejska Służba Działań Zewnętrznych przekazały Radzie w dniu 12 maja 2017 r. **wspólny nieoficjalny dokument w sprawie unijnych działań zewnętrznych służących przeciwdziałaniu terroryzmowi**, określający priorytetowe państwa, dziedziny i instrumenty, które powinny zostać objęte działaniami UE w tej dziedzinie. Ten wspólny dokument jest przyczynkiem do dyskusji na temat przeglądu konkluzji Rady z lutego 2015 r. w sprawie zewnętrznych działań w zakresie zwalczania terroryzmu[45], w celu przyjęcia nowych konkluzji Rady podczas szczytu Rady do Spraw Zagranicznych w czerwcu 2017 r.

Pierwsze warsztaty UE i krajów sąsiadujących na temat **ochrony infrastruktury krytycznej** miały miejsce w Bukareszcie w dniach 16–17 marca 2017 r., jako część szerszego

---

[44] Zob. nieoficjalny dokument Służb Komisji: Sprawozdanie z postępów stanowiące działanie następcze do konkluzji Rady Unii Europejskiej dotyczących usprawnienia działania wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni (2.12.2016): http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf. W swoich konkluzjach w sprawie usprawnienia działania wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni z dnia 9 czerwca 2016 r. Rada wezwała Komisję do podjęcia konkretnych działań, opracowania wspólnego unijnego podejścia oraz zaprezentowania wyników do czerwca 2017 r.

[45] Konkluzje Rady w sprawie zwalczania terroryzmu (9.2.2015): http://www.consilium.europa.eu/en/press/press-releases/ 2015/02/150209-council-conclusions-counter-terrorism/.

zewnętrznego wymiaru europejskiego programu ochrony infrastruktury krytycznej. Oprócz państw członkowskich wśród uczestników byli przedstawiciele ośmiu państw Europy Wschodniej i Bałkanów Zachodnich. Celem pierwszych warsztatów było nawiązanie kontaktów oraz wymiana informacji o środkach i narzędziach służących do ochrony infrastruktury krytycznej. Określono możliwe obszary dalszej współpracy, w tym wspólne szkolenia oraz ćwiczenia skupione wokół praktycznych aspektów (operacyjnych), studia dotyczące zależności regionalnych oraz wzajemne oceny strategii krajowych w zakresie ochrony infrastruktury krytycznej.

V. PODSUMOWANIE

Komisja wzywa Parlament Europejski i Radę do poczynienia postępów w zakresie priorytetów ustawodawczych dotyczących systemów informacyjnych w dziedzinie bezpieczeństwa oraz zarządzania granicami i przepływami migracyjnymi. Pozwoli to wzmocnić istniejące systemy oraz usunąć wykryte luki informacyjne w odpowiedzi na potrzeby funkcjonariuszy straży granicznej, funkcjonariuszy organów ścigania, w tym służb celnych, urzędników imigracyjnych oraz organów wymiaru sprawiedliwości, a także stworzy podstawy dla osiągnięcia większej interoperacyjności tych systemów.

Jako działania następcze w odniesieniu do komunikatu z kwietnia 2016 r. pt. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa” oraz w świetle zaleceń grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności Komisja określiła nowe podejście do zarządzania danymi do celów zarządzania granicami i zapewnienia bezpieczeństwa, zgodnie z którym wszystkie scentralizowane unijne systemy informacyjne w dziedzinie bezpieczeństwa oraz zarządzania granicami i przepływami migracyjnymi powinny być interoperacyjne, w pełnym poszanowaniu praw podstawowych. W tym celu, opierając się na trwających pracach ustawodawczych i technicznych dotyczących systemów informacyjnych, Komisja przedstawi w czerwcu 2017 r. wniosek ustawodawczy w celu wzmocnienia mandatu agencji eu-LISA, umożliwiający jej wdrożenie tego nowego podejścia, a następnie jak najszybciej przedstawi wniosek ustawodawczy w sprawie interoperacyjności. Komisja wzywa Parlament Europejski i Radę do przeprowadzenia dyskusji w sprawie proponowanego kierunku dalszych działań. Pozwoli to tym trzem instytucjom na osiągnięcie konsensusu co do dalszych kierunków działań służących osiągnięciu interoperacyjności oraz co do niezbędnych kroków służących jej wdrożeniu do 2020 r., w pełnej zgodności z prawami podstawowymi. Wdrożenie podejścia w zakresie interoperacyjności sprawiłoby, że zarządzanie danymi w Unii Europejskiej byłoby skuteczniejsze i wydajniejsze, co pozwoliłoby lepiej chronić granice zewnętrzne oraz wzmocnić bezpieczeństwo wewnętrzne z korzyścią dla wszystkich obywateli.