Rada
Unii Europejskiej

Bruksela, 14 grudnia 2020 r.
(OR. en)

14019/20

JAI 1110	**DROIPEN 124**
COSI 250	**COPEN 384**
ENFOPOL 348	**FREMP 146**
ENFOCUSTOM 142	**JAIEX 119**
IXIM 138	**CFSP/PESC 1121**
CT 118	**COPS 478**
CRIMORG 119	**HYBRID 46**
FRONT 345	**DISINFO 47**
ASIM 95	**TELECOM 264**
VISA 139	**DIGIT 151**
CYBER 278	**COMPET 633**
DATAPROTECT 151	**RECH 522**
CATS 104	

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	10 grudnia 2020 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2020) 797 final
Dotyczy:	KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY Pierwsze sprawozdanie z postępu prac w realizacji strategii UE w zakresie unii bezpieczeństwa

Delegacje otrzymują w załączeniu dokument COM(2020) 797 final.

Zał.: COM(2020) 797 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 9.12.2020 r.
COM(2020) 797 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Pierwsze sprawozdanie z postępu prac w realizacji strategii UE w zakresie unii bezpieczeństwa

I WPROWADZENIE

Bezpieczeństwo to kwestia najwyższej wagi dla obywateli, a ostatnia fala ataków terrorystycznych w Europie jeszcze bardziej uwydatniła konieczność podjęcia działań na szczeblu UE. W dniu 24 lipca 2020 r. Komisja przyjęła **strategię UE w zakresie unii bezpieczeństwa na lata 2020–2025**[1] w celu ukierunkowania działań na obszary priorytetowe, w których UE może wnieść wartość dodaną w stosunku do działań na szczeblu krajowym. Strategia opiera się na postępach poczynionych uprzednio w ramach Europejskiej agendy bezpieczeństwa na lata 2015–2020[2] i zawiera nowe podejście, które ma zapewnić, aby polityka bezpieczeństwa UE odzwierciedlała zmieniający się krajobraz zagrożeń, przyczyniała się do tworzenia długoterminowej, trwałej odporności, uwzględniała zaangażowanie instytucji i agencji Unii, rządów, sektora prywatnego i obywateli w ramach podejścia obejmującego całe społeczeństwo oraz łączyła wiele obszarów polityki, które bezpośrednio wpływają na bezpieczeństwo. Centralny element tych prac stanowi pełne poszanowanie praw podstawowych, jako że bezpieczeństwo Unii można zapewnić wyłącznie wówczas, gdy każdy ma pewność, że jego prawa podstawowe są w pełni przestrzegane.

Zagrożenie ze strony transnarodowych sieci terrorystycznych w wyraźny sposób przypomina, że skoordynowane działania na szczeblu UE są niezbędne do skutecznego działania w celu ochrony Europejczyków i zachowania naszych wspólnych wartości i europejskiego stylu życia. Unaocznia to znamienny fakt, że pojawiają się zagrożenia dla bezpieczeństwa, które są coraz bardziej złożone, transgraniczne i międzysektorowe i, które sprawiają, że ścisła współpraca w zakresie bezpieczeństwa na wszystkich szczeblach staje się w coraz większym stopniu kluczowa. Dotyczy to przestępczości zorganizowanej lub handlu środkami odurzającymi, ale także świata cyfrowego, w którym stale nasilają się cyberprzestępstwa i cyberataki. Zasięg wszystkich tych wyzwań wykracza również poza nasze granice i istnieje wyraźne powiązanie bezpieczeństwa zewnętrznego z wewnętrznym. Kryzys związany z COVID-19 również wyraźnie zwrócił uwagę na kwestię bezpieczeństwa w Europie, ponieważ wystawił na próbę odporność europejskiej infrastruktury krytycznej, gotowość Europy na wypadek sytuacji kryzysowej, europejskie strategiczne łańcuchy wartości i systemy zarządzania kryzysowego, a także odporność naszych społeczeństw na manipulacyjne ingerencje i dezinformację.

Strategia w zakresie unii bezpieczeństwa obejmuje cztery strategiczne priorytety działań na szczeblu UE: środowisko bezpieczeństwa, które wytrzyma próbę czasu, działanie w obliczu zmieniających się zagrożeń, ochrona Europejczyków przed terroryzmem i przestępczością zorganizowaną oraz silny europejski ekosystem bezpieczeństwa. Głównym elementem strategii jest wdrażanie, które stanowi temat przewodni niniejszego sprawozdania: wdrażanie, które wymaga pełnego zaangażowania organów krajowych na pierwszej linii w zakresie bezpieczeństwa w UE. Niniejsze sprawozdanie jest pierwszym sprawozdaniem z postępu prac w ramach przedmiotowej strategii i stanowi spełnienie zobowiązania Komisji dotyczącego przedstawiania regularnych sprawozdań z wdrażania[3]. Dotyczy ono okresu od dnia 31 października 2019 r., kiedy to opublikowano ostatnie

[1] COM(2020) 605.
[2] COM(2016) 230.
[3] W trakcie wysłuchania wiceprzewodniczącego Margaritisa Schinasa przed Parlamentem Europejskim w dniu 3 października 2019 r.

sprawozdanie z postępu prac nad stworzeniem unii bezpieczeństwa w ramach mandatu poprzedniej Komisji[4].

II ŚRODOWISKO BEZPIECZEŃSTWA, KTÓRE WYTRZYMA PRÓBĘ CZASU

1. *Ochrona infrastruktury krytycznej i jej odporność*

W życiu codziennym obywatele są zależni od infrastruktury fizycznej i cyfrowej, która charakteryzuje się coraz większymi wzajemnymi powiązaniami i współzależnościami. Infrastruktura ta ma kluczowe znaczenie dla funkcjonowania gospodarki i społeczeństwa. Bez niezawodnych dostaw energii, przewidywalnego transportu, kompleksowych systemów opieki zdrowotnej lub sieci finansowej opartej na technologiach cyfrowych nie moglibyśmy prowadzić naszego obecnego stylu życia. Pandemia COVID-19 jeszcze wyraźniej unaoczniła nam, jak ważne jest **zapewnienie odporności krytycznych sektorów i operatorów**. UE przyznaje, że we wspólnym interesie leży ochrona infrastruktury krytycznej przed zagrożeniami, jakimi są zarówno klęski żywiołowe, jak i katastrofy spowodowane przez człowieka lub ataki terrorystyczne. Obecnie występuje szerokie spektrum zagrożeń dla infrastruktur krytycznych. Obejmuje ono: terroryzm, działania hybrydowe, cyberataki, incydenty związane z zagrożeniem wewnętrznym; zagrożenia związane z nowymi i powstającymi technologiami (takimi jak bezzałogowe statki powietrzne, sieć 5G, sztuczna inteligencja); wyzwania związane ze zmianą klimatu; zakłócenia łańcuchów dostaw; oraz ingerencje w wybory. Należy uaktualnić i rozszerzyć obecnie obowiązujące przepisy[5]. Zamiast na ochronę nacisk należy położyć na odporność, tak aby zapewnić większą spójność i zgodność zakresu sektorowego oraz skoncentrować się na krytycznych podmiotach świadczących usługi kluczowe.

Będzie to cel przyszłych wniosków dotyczących promowania odporności **infrastruktury fizycznej i cyfrowej**. Ogólny cel polega na zwiększeniu gotowości na szczeblu krajowym i unijnym poprzez budowanie solidnych zdolności na potrzeby zapobiegania zagrożeniom, ich wykrywania, reagowania na nie i ich ograniczania, a także na potrzeby gotowości do działania w sytuacji kryzysowej. Na podstawie obecnie obowiązujących przepisów udało się zwiększyć i udoskonalić zarządzanie ryzykiem w sektorach krytycznych. Należy zintensyfikować wysiłki w tym zakresie. Kluczowym celem zmienionej dyrektywy w sprawie infrastruktury krytycznej będzie promowanie wysokiego wspólnego poziomu odporności w wystarczającej liczbie kluczowych sektorów. Podobnie aktualizacja dyrektywy w sprawie bezpieczeństwa sieci i informacji będzie ukierunkowana na bardziej spójne identyfikowanie „operatorów usług kluczowych" przez państwa członkowskie[6]. W bardziej ogólnym ujęciu pomimo znacznych postępów nadal utrzymuje się nierówny poziom zdolności w zakresie cyberbezpieczeństwa w poszczególnych państwach członkowskich, w związku z czym zmiana będzie miała na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa[7]. W rezultacie poprawi się podejście do odporności infrastruktury fizycznej i cyfrowej i wzrośnie się jego spójność.

---

4 COM(2019) 552.

5 Dyrektywa 2008/114/WE i dyrektywa (UE) 2016/1148.

6 COM(2019) 546. Komisja przeprowadziła ponadto konsultacje publiczne (w dniach 7 lipca – 2 października 2020 r.) oraz wizyty kontrolne we wszystkich państwach członkowskich w celu weryfikacji zgodności pod względem wdrażania dyrektywy w ramach spotkań z operatorami i organami krajowymi.

7 COM(2019) 546.

Prace nad spójniejszymi ram są w toku i są uzupełniane **inicjatywami sektorowymi**, których celem jest wyeliminowanie konkretnych podatności na zagrożenia. Obecnie problematykę szczególnych wyzwań w zakresie cyberbezpieczeństwa dotyczących sektora energetycznego podejmuje się na podstawie zalecenia Komisji z 2019 r.[8], uwzględniając właściwości tego sektora, takie jak wymogi czasu rzeczywistego, ryzyko efektów kaskadowych, połączenie dotychczasowych systemów z nowymi technologiami. Trwają prace nad specjalnym kodeksem sieci dotyczącym cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej, a także nad ochroną odporności i cyberbezpieczeństwem krytycznej infrastruktury energetycznej. Ponadto wznowiono sieć tematyczną dotyczącą ochrony krytycznej infrastruktury energetycznej, która koncentruje się teraz na nowych celach. W czerwcu 2020 r. odbyło się pierwsze posiedzenie sieci; wzięło w nim udział online ponad 100 uczestników. Sieć ta stanowi platformę sprzyjającą transgranicznej współpracy między operatorami i właścicielami krytycznej infrastruktury energetycznej w sektorze energetycznym.

Aby zapewnić wspólny punkt wyjścia na potrzeby współpracy między państwami członkowskimi w zakresie **gotowości na wypadek zagrożeń w sektorze energii elektrycznej**, we wrześniu 2020 r. europejska sieć operatorów systemów przesyłowych energii elektrycznej ustaliła najbardziej istotny regionalny scenariusz kryzysów elektroenergetycznych, jak określono w rozporządzeniu w sprawie gotowości na wypadek zagrożeń[9]. Należą do nich (cyber)ataki, a także pandemie i ekstremalne warunki pogodowe. Państwa członkowskie sporządzą krajowe scenariusze kryzysowe i plany gotowości na wypadek zagrożeń, aby zapobiegać kryzysom elektroenergetycznym i je łagodzić (pierwsze projekty zaplanowano na kwiecień 2021 r.). W ramach wkładu w ten proces w czerwcu 2020 r. wydano zestawienie dobrych praktyk[10] opracowane na podstawie szczegółowego monitorowania wpływu pandemii COVID-19 na sektor energetyczny za pośrednictwem grup koordynacyjnych ds. energii elektrycznej, gazu i ropy naftowej, a także Europejskiej Grupy Organów Regulacyjnych ds. Bezpieczeństwa Jądrowego i unijnej grupy organów ds. wydobycia ropy naftowej i gazu ziemnego ze złóż podmorskich.

Rosnące i coraz bardziej złożone uzależnienie świadczenia usług finansowych od procesów cyfrowych wymaga również zwiększenia poziomu cyberbezpieczeństwa w **sektorze finansowym**. Mimo że bezpieczeństwo systemów ICT uznaje się za integralną część zarządzania ryzykiem w przypadku podmiotów finansowych, to jednak fakt ten nie został jeszcze w pełni odzwierciedlony w unijnym otoczeniu regulacyjnym w obszarze usług finansowych. W dniu 24 września 2020 r. Komisja przyjęła pakiet dotyczący strategii w zakresie finansów cyfrowych[11], którego wyraźnym celem jest rozwiązanie problemu wyzwań i ryzyka towarzyszących transformacji cyfrowej, promowanie odporności, ochrona danych osobowych i odpowiedni nadzór ostrożnościowy. Pakiet ten obejmuje wniosek ustawodawczy dotyczący operacyjnej odporności cyfrowej[12] w celu zapewnienia, aby obowiązywały zabezpieczenia mające na celu łagodzenie cyberataków i innych zagrożeń[13]. Inicjatywa ta przyczynia się do budowania silnego i dynamicznego

[8] C(2019) 2400.

[9] Dz.U. L 158 z 14.6.2019, s. 1.

[10] Bezpieczeństwo energetyczne: dobre praktyki w zakresie przeciwdziałania zagrożeniom związanym z pandemią (SWD(2020) 104).

[11] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[12] COM(2020) 595.

[13] We wniosku określono spójny poziom bazowy wymogów dotyczących zarządzania ryzykiem związanym z systemami ICT, zgłaszania incydentów ICT organom sprawującym nadzór finansowy, testowania

europejskiego sektora finansów cyfrowych i tym samym do wzmacniania zdolności Europy do zwiększenia otwartej strategicznej autonomii w obszarze usług finansowych, a co za tym idzie, przyczynia się do zwiększenia zdolności w zakresie regulowania i nadzorowania systemu finansowego w celu ochrony europejskiej stabilności finansowej.

W sytuacjach nadzwyczajnych o dużej skali wysoki poziom współzależności między sektorami i państwami wymaga skoordynowanego działania w celu zapewnienia szybkiego i skutecznego reagowania, a także lepszego zapobiegania podobnym sytuacjom w przyszłości i większej gotowości na takie sytuacje. W ramach zmiany decyzji w sprawie Unijnego Mechanizmu Ochrony Ludności[14] Komisja zaproponowała[15] określenie **celów** i **zaplanowanie scenariuszy w zakresie odporności na klęski i katastrofy** ze szczególnym uwzględnieniem budowania długoterminowej międzysektorowej odporności na klęski i katastrofy o charakterze transgranicznym. Zaproponowane nowe podejście dotyczące budowania odporności stanowi uzupełnienie prac prowadzonych na szczeblu krajowym w zakresie zarządzania ryzykiem związanym z klęskami i katastrofami. W dniu 26 listopada Rada osiągnęła porozumienie w sprawie mandatu negocjacyjnego, by skuteczniej zapobiegać klęskom i katastrofom, zwiększyć gotowość na wypadek ich wystąpienia i lepiej na nie reagować, na podstawie wniosku Komisji z dnia 2 czerwca 2020 r.[16]

Pandemia COVID-19 uwidoczniła wpływ kryzysu zdrowotnego na bezpieczeństwo na szczeblu unijnym i światowym, a także uwydatniła potrzebę zwiększenia działań w zakresie planowania gotowości i reagowania na epidemie i inne poważne transgraniczne zagrożenia zdrowia. W sporządzonym przez Komisję pakiecie z dnia 11 listopada 2020 r. pt. „**Tworzenie Europejskiej Unii Zdrowotnej**: Zwiększenie odporności UE" określono dalsze działania służące przeciwdziałaniu transgranicznym zagrożeniom zdrowia. Pozwoliłoby to na wzmocnienie ram dotyczących transgranicznej współpracy w zakresie wszystkich zagrożeń zdrowia. Pakiet objął trzy wnioski ustawodawcze: przegląd przepisów dotyczących poważnych transgranicznych zagrożeń zdrowia oraz wzmocnienie Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) i Europejskiej Agencji Leków (EMA). Wnioski te wspólnie stworzą solidne i racjonalne pod względem kosztów ramy lepiej zabezpieczające zdolność UE i państw członkowskich do reagowania na przyszłe kryzysy zdrowotne.

Kluczowe znaczenie dla ochrony najważniejszych unijnych i krajowych aktywów cyfrowych ma stworzenie kanału **bezpiecznej komunikacji** na potrzeby infrastruktury krytycznej. Wsparcie w tym zakresie obejmuje rozwój infrastruktury sieciowej na potrzeby bezpiecznej i odpornej rządowej łączności satelitarnej jako elementu unijnego programu kosmicznego.

2. ***Cyberbezpieczeństwo***

---

cyfrowego i wymiany informacji. Ponadto we wniosku wymaga się, aby zewnętrzni dostawcy usług ICT podlegali ramom nadzoru w skali europejskiej.

[14] Decyzja nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

[15] COM(2020) 220.

[16] Wniosek dotyczący zmiany decyzji nr 1313/2013/EU w sprawie Unijnego Mechanizmu Ochrony Ludności – mandat do negocjacji z Parlamentem Europejskim.

Transformacja cyfrowa przynosi wyraźne korzyści, ale jednocześnie w nieuchronny sposób wiąże się z równie wyraźnym wzrostem potencjalnej podatności na zagrożenia[17]. Infrastruktura krytyczna często stanowi cel coraz bardziej wyrafinowanych cyberataków[18]. **Cyberbezpieczeństwo** musi zatem stanowić przedmiot zainteresowania nie tylko decydentów, ale również każdego, kto pracuje lub komunikuje się za pośrednictwem internetu.

Aby zwiększyć zaufanie do produktów, procesów i usług cyfrowych oraz ich bezpieczeństwo, w drodze aktu o cyberbezpieczeństwie z czerwca 2019 r. utworzono **unijne ramy certyfikacji cyberbezpieczeństwa**. Komisja zwróciła się do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) o przygotowanie dwóch programów certyfikacji cyberbezpieczeństwa; prace nad ich sporządzeniem są na zaawansowanym etapie. W prace te zaangażowane są również krajowe organy ds. certyfikacji cyberbezpieczeństwa, przedstawiciele przemysłu, konsumenci, jednostki akredytujące, organy normalizacyjne i jednostki certyfikujące, a także Europejska Rada Ochrony Danych.

Jednym z tych programów jest program **usług w chmurze** wspierający bezpieczny i wiarygodny rynek usług w chmurze. Jest to kluczowy element **europejskiej strategii w zakresie danych** przyjętej w lutym 2020 r.[19] Program ten stworzyłby wspólny poziom bazowy dotyczący bezpieczeństwa usług w chmurze w różnych sektorach w oparciu o najwyższy wspólny mianownik spośród istniejących (europejskich i międzynarodowych) norm, programów i praktyk. Będzie to kluczowy element swobodnego przepływu danych w UE[20]. Program ten będzie również sprzyjał przyjmowaniu technologii chmury poprzez zapewnienie użytkownikom, w szczególności małym i średnim przedsiębiorstwom i administracji publicznej, zrozumiałej gwarancji w odniesieniu do poziomu bezpieczeństwa w związku z korzystaniem z chmury.

---

17 ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. [Krajobraz zagrożeń w 2020 r.: cyberataki stają się coraz bardziej wyrafinowane, lepiej ukierunkowane, powszechniejsze i coraz częściej pozostają niewykryte].

18 Od czasu wybuchu pandemii agencje UE i państwa członkowskie obserwują znaczny wzrost cyberataków, w tym cyberataków wymierzonych w sektor opieki zdrowotnej.

19 COM(2020) 66.

20 Rozporządzenie (UE) 2018/1807.

Jak wskazano w strategii w zakresie unii bezpieczeństwa, w kontekście infrastruktury 5G uruchamianej obecnie w całej UE istnieje niebezpieczeństwo, że ewentualne systemowe zakłócenia o dużej skali mogą mieć szczególnie dotkliwe skutki, ponieważ wiele usług o krytycznym znaczeniu będzie potencjalnie uzależnionych od sieci 5G. W rezultacie państwa członkowskie podjęły wspólne działania w celu opracowania i wprowadzenia odpowiednich środków bezpieczeństwa. W związku z zaleceniem Komisji dotyczącym **cyberbezpieczeństwa sieci 5G** z marca 2019 r.[21] państwa członkowskie przeprowadziły krajowe oceny ryzyka, na podstawie których sporządzono sprawozdanie dotyczące unijnej skoordynowanej oceny ryzyka[22]. Zidentyfikowano w nim wyzwania w dziedzinie bezpieczeństwa związane z sieciami 5G. Na tej podstawie w dniu 29 stycznia 2020 r. grupa współpracy ds. bezpieczeństwa sieci i informacji[23] opublikowała **unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G**[24] obejmujący niezbędne środki strategiczne i techniczne. Zestaw zawiera środki służące zaostrzeniu wymogów w zakresie bezpieczeństwa w odniesieniu do operatorów sieci ruchomych, zapewnieniu różnorodności dostawców na potrzeby poszczególnych operatorów sieci ruchomych, ocenie profilu ryzyka dostawców oraz stosowaniu ograniczeń w odniesieniu do dostawców uznanych za stwarzających wysokie ryzyko. Komisja będzie wspierać wdrażanie tego zestawu narzędzi, w pełni korzystając z posiadanych kompetencji i środków, jakimi dysponuje[25], w tym w ramach przepisów dotyczących telekomunikacji i cyberbezpieczeństwa, koordynacji w zakresie normalizacji, a także ogólnounijnej certyfikacji; oraz unijnych ram monitorowania bezpośrednich inwestycji zagranicznych[26].

W lipcu 2020 r. grupa współpracy ds. bezpieczeństwa sieci i informacji opublikowała sprawozdanie z postępu prac w zakresie wdrażania środków przewidzianych w zestawie narzędzi[27]. W sprawozdaniu tym odnotowano, że znaczna większość państw członkowskich już przyjęła środki zalecane w ramach zestawu narzędzi lub jest w trakcie ich wdrażania. W przypadkach, w których wdrażanie znajdowało się na mniej zaawansowanym etapie, środki te obejmowały ograniczanie ryzyka uzależnienia od dostawców wysokiego ryzyka oraz rozwój strategii przewidujących korzystanie z usług wielu dostawców zarówno na szczeblu przedsiębiorstw, jak i na szczeblu krajowym.

W ciągu ostatnich kilku miesięcy instytucje Unii i państwa członkowskie reagowały na podwyższony poziom ryzyka w cyberprzestrzeni spowodowanego **kryzysem związanym z COVID-19**, intensyfikując wymianę informacji i zwiększając poziom gotowości na potencjalny cyberkryzys. Rozwinięto współpracę na szczeblu unijnym w ramach kluczowych forów (grupa współpracy ds. bezpieczeństwa sieci i informacji oraz sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)), a także

---

[21] COM(2019) 2335.

[22] Sprawozdanie dotyczące unijnej skoordynowanej oceny ryzyka związanego z cyberbezpieczeństwem w sieciach 5G.

[23] Grupę współpracy ds. bezpieczeństwa sieci i informacji ustanowiono w celu zapewnienia współpracy strategicznej i wymiany informacji w dziedzinie cyberbezpieczeństwa między państwami członkowskimi UE.

[24] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[25] COM(2020) 50.

[26] Rozporządzenie (UE) 2019/452. Rozporządzenie to zawiera wyraźne odniesienia do „infrastruktury krytycznej” (a także „technologii krytycznych”) w ramach szerszego terminu „czynniki, które mogą być brane pod uwagę przez państwa członkowskie lub Komisję” w ocenie ewentualnego wpływu inwestycji.

[27] Sprawozdanie z postępów poczynionych przez państwa członkowskie we wdrażaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G.

w ramach nowych form koordynacji i narzędzi do wymiany informacji[28]. We wrześniu 2020 r. odbyło się drugie ćwiczenie symulacyjne w zakresie planu działania na poziomie operacyjnym (Blue OLEx)[29], w ramach którego uruchomiono również sieć organizacji łączności w zakresie cyberkryzysów (CyCLONe) tworzoną przez państwa członkowskie, która zajmie się dalszym wdrażaniem planu działania na rzecz szybkiego reagowania na transgraniczne incydenty lub kryzysy cybernetyczne na dużą skalę[30].

W globalnej cyberprzestrzeni cyberataki i zagrożenia często pochodzą spoza UE. Aby skutecznie radzić sobie z tymi wyzwaniami, UE i państwa członkowskie współpracują w celu zwiększenia międzynarodowego bezpieczeństwa i stabilności w cyberprzestrzeni, promowania odpowiedzialnego zachowania państw, zwiększenia globalnej odporności i podnoszenia świadomości na temat zagrożeń dla cyberbezpieczeństwa i szkodliwych działań w cyberprzestrzeni, w tym wraz z międzynarodowymi partnerami[31]. W dniu 30 kwietnia 2020 r. wysoki przedstawiciel opublikował oświadczenie wydane w imieniu Unii Europejskiej, w którym potępił szkodliwe zachowania w cyberprzestrzeni i wyraził solidarność z ofiarami[32].

W dniu 30 lipca 2020 r. Rada przyjęła **pierwsze w historii unijne sankcje związane z cyberatakami** nałożone na sześć osób fizycznych i trzy podmioty odpowiedzialne za cyberataki lub w nie zaangażowane. Chodzi m.in. o niedoszły do skutku cyberatak na OPCW (Organizację ds. Zakazu Broni Chemicznej) oraz ataki ogólnie znane pod nazwami „WannaCry", „NotPetya" oraz „Operation Cloud Hopper". W dniu 22 października 2020 r. Rada zastosowała sankcje wobec kolejnych dwóch osób fizycznych i jednego podmiotu odpowiedzialnych za cyberatak skierowany przeciwko niemieckiemu parlamentowi federalnemu lub zaangażowanych w ten atak. Decyzje te podjęto w odpowiedzi na ciągłe sygnały ze strony UE i państw członkowskich dotyczące konieczności zapobiegania szkodliwym działaniom w cyberprzestrzeni, eliminowania ich, zniechęcania do nich i reagowania na nie, w tym poprzez wykorzystanie systemu sankcji związanych z cyberatakami w ramach zestawu narzędzi dla dyplomacji cyfrowej z 2017 r.[33]

---

[28] Instytucje i organy Unii zgromadzone w grupie zadaniowej ds. cyberbezpieczeństwa w czasie pandemii COVID-19 wprowadziły cotygodniowe sprawozdania orientacyjne i analizy sytuacji w poszczególnych sektorach. ENISA i Europol rozpoczęły kampanie dotyczące zachowania cyberbezpieczeństwa w czasie pandemii COVID-19. CERT-UE wydał wytyczne dotyczące tworzenia bezpiecznych wirtualnych sieci prywatnych. Latem 2019 r. grupa współpracy ustanowiła nowy obszar prac poświęcony cyberbezpieczeństwu w sektorze zdrowia, a Komisja i ENISA uruchomiły unijne centrum wymiany i analizy informacji zdrowotnych.

[29] https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

[30] C(2017) 6100.

[31] UE promuje strategiczne ramy dotyczące zapobiegania konfliktom oraz stabilności i współpracy w cyberprzestrzeni, w tym w ramach udziału UE w dyskusjach na forum Organizacji Narodów Zjednoczonych dotyczących tematyki cyberbezpieczeństwa. Dwa ważne procesy to Otwarta Grupa Robocza ds. Rozwoju Technologii Teleinformatycznych w kontekście Bezpieczeństwa Międzynarodowego oraz grupa ekspertów rządowych ds. promocji odpowiedzialnego zachowania państw w cyberprzestrzeni w kontekście bezpieczeństwa międzynarodowego. Podejmowane kwestie obejmują wpływ prawa międzynarodowego, wdrożenie uzgodnionych niewiążących i dobrowolnych norm dotyczących odpowiedzialnego zachowania państw oraz środków budowy zaufania, a także rozwój wdrażania za sprawą ukierunkowanego budowania zdolności.

[32] https://www.consilium.europa.eu/pl/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/

[33] Decyzje Rady (WPZiB) 2020/1127, 2020/1537 oraz 2020/651 w ramach 9916/17.

Postępy poczyniono również w zakresie negocjacji między współprawodawcami dotyczących nowych przepisów wywozowych ograniczających sprzedaż towarów służących do cyberinwigilacji światowym reżimom łamiącym prawa człowieka[34]. Po przyjęciu tych przepisów nastąpi wzrost rozliczalności, konkurencyjności i przejrzystości w zakresie handlu produktami podwójnego zastosowania[35]. Proponowane zmiany, konieczne ze względu na rozwój technologiczny i rosnące zagrożenia dla bezpieczeństwa, obejmują nowe kryteria przyznawania lub odmawiania pozwoleń na wywóz niektórych produktów.

3. Ochrona przestrzeni publicznej

Jak uznano w programie działań UE na rzecz walki z terroryzmem[36], ochrona przestrzeni publicznej poprzez budowanie odporności na zagrożenia dla bezpieczeństwa pozostaje kluczowym elementem prac na rzecz rzeczywistej i skutecznej unii bezpieczeństwa. Komisja współpracuje z szerokim gronem zainteresowanych stron z sektora publicznego i prywatnego w celu opracowania wytycznych oraz zapewnienia praktycznego wsparcia i finansowania[37], zgodnie z **Planem działania na rzecz wspierania ochrony przestrzeni publicznej z 2017 r.**[38] oraz zbiorem dobrych praktyk w zakresie wspierania ochrony przestrzeni publicznej z 2019 r.[39] Zgodnie z programem działań UE na rzecz walki z terroryzmem Komisja zwiększy swoje wsparcie dla władz lokalnych i regionalnych, które odgrywają kluczową rolę w ochronie przestrzeni publicznej i zapobieganiu radykalizacji postaw. Będzie to obejmowało opracowanie protokołu UE w sprawie bezpieczeństwa i odporności miast, określającego podstawowe zasady i cele dla władz lokalnych działających w tych obszarach.

W związku z tym, że ataki terrorystyczne coraz częściej są wymierzone w **miejsca kultu**, szczególny nacisk kładzie się na współpracę między organami publicznymi a przywódcami i zgromadzeniami religijnymi, aby poprawić poziom świadomości w zakresie bezpieczeństwa i pomóc we wdrażaniu dobrych praktyk i szkoleń w miejscach kultu. Proste środki mogą decydować o życiu lub śmierci. W październiku 2019 r. obiektem ataku terrorystycznego stała się synagoga w Halle. Dzięki wzmocnionym drzwiom, alarmowi napadowemu i kamerom bezpieczeństwa udało się uratować ludzkie życia.

W celu dalszego wspierania zwiększonego bezpieczeństwa w przestrzeni publicznej, w szczególności w miejscach kultu, Komisja udostępniła w 2020 r. środki w wysokości 20 mln EUR na projekty prowadzone przez zainteresowane strony.

Komisja pracuje również nad reagowaniem na **pojawiające się zagrożenia dla przestrzeni publicznej**, w tym **na systemy bezzałogowego statku powietrznego** (SBSP). Bezzałogowe statki powietrzne stwarzają wprawdzie znaczne możliwości gospodarcze

---

[34] COM(2016) 616. Wniosek Komisji ma na celu zmianę i przekształcenie rozporządzenia nr 428/2009, które ustanawia wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

[35] Jest to ogromna grupa towarów, materiałów, oprogramowania i technologii, które mogą być stosowane zarówno w celach cywilnych, jak i wojskowych.

[36] COM(2020) 795.

[37] Wezwanie do ochrony FBW w 2019 r. obejmowało „Secu4All", opracowanie kompleksowego cyklu szkoleń dla władz lokalnych w celu zapewnienia obywatelom bezpiecznego środowiska miejskiego, oraz „DroneWISE" w celu zwiększenia gotowości pierwszych respondentów do zwalczania wrogich bezzałogowych statków powietrznych. W 2020 r. uruchomiony zostanie nowy program na rzecz ochrony przestrzeni publicznej, na który przeznaczony zostaną środki w wysokości 12 mln EUR.

[38] COM(2017) 612.

[39] SWD(2019) 140.

i możliwości zatrudnienia, ale stanowią również znaczne zagrożenie dla przestrzeni publicznej, infrastruktury krytycznej i innych wrażliwych miejsc, takich jak zakłady karne. Najnowsze przepisy UE[40] w tej dziedzinie zmniejszają to ryzyko, zwiększając bezpieczeństwo eksploatacji bezzałogowych statków powietrznych. Od stycznia 2021 r. operatorzy bezzałogowych statków powietrznych będą również zobowiązani do rejestracji w organach krajowych. System ten może zostać uzupełniony **ramami regulacyjnymi dotyczącymi U-space**, europejskiego systemu zarządzania bezzałogowymi systemami powietrznymi[41], w celu zapewnienia bezpieczniejszej i pewniejszej eksploatacji bezzałogowych statków powietrznych. Łącznie działania te utrudnią osobom fizycznym latanie bezzałogowymi statkami powietrznymi w strefach ograniczonych oraz pomogą w identyfikacji i ściganiu przestępców.

Komisja pracuje również nad wspieraniem organów ścigania, operatorów infrastruktury krytycznej, organizatorów imprez masowych i innych zainteresowanych stron w przeciwdziałaniu wykorzystywaniu bezzałogowych statków powietrznych w sposób niewspółpracujący, np. Komisja współpracuje z Agencją Unii Europejskiej ds. Bezpieczeństwa Lotniczego w celu opracowania **dobrych praktyk pomagających zainteresowanym stronom z portów lotniczych** w reagowaniu na incydenty związane z nieuprawnionym korzystaniem z bezzałogowych statków powietrznych, ułatwia bardziej zharmonizowane **działania w zakresie testowania środków zaradczych** w całej UE oraz opracowuje praktyczny podręcznik dla zainteresowanych stron, koncentrujący się na kontekście miejskim.

Jesienna szkoła cyfrowa UE na rzecz ochrony przestrzeni publicznej, zorganizowana przez Wspólne Centrum Badawcze Komisji w październiku 2020 r., zgromadziła ponad 200 urbanistów oraz publicznych i prywatnych operatorów w przestrzeni publicznej. Podczas sesji przeanalizowano szeroki zakres tematów, takich jak sposoby ochrony przed wybuchami w powietrzu i taranowaniem statków powietrznych, łagodzenie zagrożeń stwarzanych przez wrogie bezzałogowe statki powietrzne w środowisku miejskim oraz wykorzystanie technologii nadzoru i wykrywania.

Komisja nadal aktywnie wspiera również **partnerstwo na rzecz bezpieczeństwa w przestrzeni publicznej**, zainicjowane w styczniu 2019 r. w ramach agendy miejskiej dla UE, które opublikowało nowy plan działania[42] na rzecz walki z zagrożeniami dla bezpieczeństwa w miastach na różnych szczeblach zarządzania. Działania te obejmują utworzenie ram dla narzędzia samooceny, opracowanie zaleceń dotyczących kształtowania polityki, wielopoziomowego zarządzania i finansowania, innowacje za pomocą inteligentnych rozwiązań i technologii, w tym koncepcji bezpieczeństwa w fazie projektowania, zapobiegania i włączenia społecznego. Partnerstwo rozpocznie teraz fazę realizacji.

Wsparcie na rzecz poprawy bezpieczeństwa w przestrzeni publicznej na poziomie lokalnym zapewniono również w ramach czwartego zaproszenia do składania wniosków dotyczących innowacyjnych działań miejskich. Wybrano trzy miasta, które testują nowe rozwiązania w zakresie bezpieczeństwa miejskiego (Pireus w Grecji, Tampere w Finlandii

---

[40] Rozporządzenie wykonawcze Komisji (UE) 2019/947.

[41] Komisja może przedstawić w tym celu rozporządzenie wykonawcze, które zostałoby przyjęte w ramach procedury sprawdzającej z udziałem komitetu ds. bezpieczeństwa lotniczego.

[42] Plan działania został przyjęty i jest dostępny na stronie Futurium: https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0

i Turyn we Włoszech), korzystając ze środków z Europejskiego Funduszu Rozwoju Regionalnego.

Jeżeli chodzi o reagowanie, Komisja opracowała również europejskie ramy mające na celu zwiększenie gotowości i zdolności reagowania na katastrofy skutkujące masowym występowaniem oparzeń, wykorzystując ogólne europejskie możliwości w zakresie opieki nad pacjentami z oparzeniami dzięki współpracy na szczeblu UE. Unijny Mechanizm Ochrony Ludności może zostać wykorzystany do wspierania dużej liczby pacjentów z poważnymi oparzeniami poprzez zapewnienie dostępu do łóżek w specjalistycznych ośrodkach leczenia oparzeń, specjalistów ds. oceny oparzeń oraz poprzez zapewnienie zdolności do prowadzenia ewakuacji medycznej.

III DZIAŁANIE W OBLICZU ZMIENIAJĄCYCH SIĘ ZAGROŻEŃ

1. Cyberprzestępczość

Przestępcy często wykorzystują niedociągnięcia w zakresie cyberbezpieczeństwa. W czasie kryzysu związanego z COVID-19 jest to widoczne bardziej niż kiedykolwiek. Nastąpił wzrost liczby „klasycznych" cyberprzestępstw z użyciem złośliwego oprogramowania i oprogramowania typu ransomware (tj. w celu kradzieży danych osobowych i płatniczych lub szantażowania ofiar), a także wzrost rozpowszechniania się nowych stron internetowych wabiących użytkowników do instalowania złośliwego oprogramowania. Ponadto doszło do cyberataków na infrastrukturę ochrony zdrowia i infrastrukturę badawczą polegających na zamykaniu systemów ICT, z możliwością odblokowania jedynie po zapłaceniu okupu lub udostępnieniu informacji na temat rozwoju szczepionek[43]. Zaobserwowano również znaczny wzrost przypadków niegodziwego traktowania dzieci w celach seksualnych oraz ilości materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych[44].

Skuteczna reakcja na cyberprzestępczość wymaga solidnych ram w zakresie postępowań przygotowawczych i ścigania przestępstw, a kluczowym pierwszym krokiem jest pełna transpozycja i wdrożenie dyrektywy dotyczącej **ataków na systemy informatyczne**[45]. Komisja monitoruje działania Bułgarii, Włoch, Portugalii i Słowenii po wszczęciu

[43] Ocena zagrożenia wykorzystaniem internetu przez zorganizowane grupy przestępcze (IOCTA) z 2020 r., październik 2020 r.

[44] Sprawozdanie na temat wykorzystywania izolacji: sprawcy i ofiary niegodziwego traktowania dzieci w celach seksualnych w internecie w czasie pandemii COVID-19, Europol, 19.6.2020.

[45] Dyrektywa 2013/40/UE.

postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego w 2019 r. Konieczne są również postępy we wdrażaniu **dyrektywy z 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych dzieci**[46]. Obszary, w których nadal konieczne jest podjęcie działań, obejmują zapobieganie, prawo karne materialne, pomoc, środki wsparcia i ochrony dla dzieci będących ofiarami. W 2018 r. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 25 państwom członkowskim[47].

W dniu 24 lipca 2020 r. Komisja przyjęła **strategię UE na rzecz skuteczniejszej walki z niegodziwym traktowaniem dzieci w celach seksualnych**[48], której celem jest zapewnienie skutecznej reakcji UE na przestępstwo niegodziwego traktowania dzieci w celach seksualnych. Pojawiło się również szczególne wyzwanie, ponieważ od dnia 21 grudnia 2020 r. niektóre usługi łączności online, takie jak poczta elektroniczna lub usługi przesyłania wiadomości, będą objęte zakresem stosowania dyrektywy o prywatności i łączności elektronicznej i zostaną objęte zmienionymi definicjami w Europejskim kodeksie łączności elektronicznej. W związku z tym istnieje wyraźne ryzyko, że dostawcy tych usług, którzy podejmują dziś pewne ważne dobrowolne działania w celu wykrywania, zwalczania i zgłaszania przypadków niegodziwego traktowania dzieci w celach seksualnych w internecie, będą musieli zaprzestać tych działań. Komisja wystąpiła zatem z wnioskiem w sprawie **rozporządzenia**[49] umożliwiającego kontynuację tych dobrowolnych działań pod pewnymi warunkami do czasu znalezienia długoterminowego rozwiązania legislacyjnego. Komisja pracuje nad wnioskiem dotyczącym takiego rozwiązania, którego przyjęcie planowane jest na 2021 r.

W ramach europejskiej sieci centrów ds. cyberbezpieczeństwa i centrów kompetencji w dziedzinie innowacji i operacji utworzono **Sojusz na rzecz cyberobrony w związku z COVID-19** w celu opracowania innowacyjnych podejść do zwalczania przestępstw związanych z COVID-19. W kwietniu 2020 r. utworzono specjalną platformę EIC COVID[50], która ma łączyć społeczeństwo obywatelskie, innowatorów, partnerów i inwestorów w całej Europie w celu opracowywania innowacyjnych rozwiązań.

Aby zapewnić skuteczniejsze ściganie przestępstw oraz ze względu na duże znaczenie informacji i dowodów elektronicznych w postępowaniach przygotowawczych, organy ścigania i organy wymiaru sprawiedliwości powinny szybko uzyskiwać dostęp do takich informacji i dowodów w celu prowadzenia postępowań przygotowawczych. Kwestię tę uznano we wspólnym oświadczeniu unijnych ministrów spraw wewnętrznych z dnia 13 listopada 2020 r.[51] Europol, Eurojust i Europejska Sieć Sądowa opublikowały w dniu 1 grudnia 2020 r. swoje drugie „sprawozdanie na temat sytuacji w UE w zakresie dowodów cyfrowych (SIRIUS)". W sprawozdaniu tym podkreślono większe znaczenie elektronicznych materiałów dowodowych w postępowaniach przygotowawczych[52].

---

[46] Dyrektywa 2011/93/UE.

[47] Hiszpanii, Portugalii, Włochom, Niderlandom, Szwecji, Malcie, Litwie, Słowacji, Bułgarii, Rumunii, Niemcom, Austrii, Belgii, Czechom, Estonii, Grecji, Finlandii, Francji, Chorwacji, Węgrom, Irlandii, Luksemburgowi, Łotwie, Polsce i Słowenii.

[48] COM(2020) 607.

[49] COM(2020) 568.

[50] Komisja, wraz z Europejską Radą ds. Innowacji i państwami członkowskimi, była gospodarzem paneuropejskiego wydarzenia EUvsVirus Hackathon + Matchathon https://covid-eic.easme-web.eu/

[51] Wspólne oświadczenie unijnych ministrów spraw wewnętrznych w sprawie ostatnich ataków terrorystycznych w Europie, 13.11.2020, 12634/20.

[52] Zgodnie ze sprawozdaniem liczba wniosków transgranicznych złożonych przez organy UE do dostawców usług online znacznie wzrosła w 2019 r., przy czym zdecydowana większość z nich została złożona

W odniesieniu do wniosków Komisji dotyczących **transgranicznego dostępu do elektronicznego materiału dowodowego**[53] z kwietnia 2018 r. Parlament Europejski nie określił jeszcze swojego stanowiska, dlatego też negocjacje między współprawodawcami nie zostały jeszcze rozpoczęte. Opóźnienia w przyjęciu tych wniosków hamują prace organów ścigania i organów wymiaru sprawiedliwości, jak również komplikują bieżące działania na rzecz ustanowienia kompatybilnych zasad dotyczących transgranicznego dostępu do elektronicznych materiałów dowodowych w drodze negocjacji międzynarodowych[54].

Na szczeblu międzynarodowym Komisja uczestniczy, w imieniu UE, w trwających negocjacjach dotyczących drugiego protokołu dodatkowego do **budapeszteńskiej konwencji Rady Europy o cyberprzestępczości**. Protokół ten zapewniłby właściwym organom ścigania rozszerzone, daleko idące narzędzia współpracy transgranicznej w zakresie prowadzenia dochodzeń i ścigania cyberprzestępczości i innych poważnych form przestępczości, w tym bezpośredniej współpracy z dostawcami usług. Ponieważ większość z tych wzmocnionych i zacieśnionych sposobów współpracy będzie opierać się na wymianie danych osobowych, istotne jest, by przyszły protokół przewidywał odpowiednie gwarancje ochrony danych, nie tylko z punktu widzenia praw podstawowych, ale również w celu zapewnienia pewności prawa, wzajemnego zaufania i skuteczności operacyjnej współpracy organów ścigania.

Negocjacje powinny zakończyć się w 2021 r. Równolegle, w związku z mandatem otrzymanym przez Radę ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w ubiegłym roku, Komisja negocjuje **umowę między UE a Stanami Zjednoczonymi w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego**. Dzięki usunięciu kolizji przepisów i zapewnieniu wspólnych zasad i zabezpieczeń uzupełniłoby to proponowane wewnętrzne przepisy UE dotyczące bezpośredniej współpracy transgranicznej z usługodawcami. W dniu 25 września 2019 r. rozpoczęły się formalne negocjacje i od tego czasu przeprowadzono już kilka rund negocjacyjnych. Wynik negocjacji zależy jednak w dużej mierze od postępów osiągniętych w zakresie wewnętrznych przepisów dotyczących elektronicznego materiału dowodowego.

Jeżeli chodzi o **zatrzymywanie i wykorzystywanie danych do celów egzekwowania prawa**, po wyroku w sprawie Tele2/Watson z 2016 r.[55] Komisja podjęła działania następcze w postaci konsultacji ekspertów z odpowiednimi dostawcami usług, policją i organami wymiaru sprawiedliwości, społeczeństwem obywatelskim, organami ochrony danych, środowiskiem akademickim i agencjami UE. Rozważania zostały również poparte

---

w Niemczech (37,7 % wniosków), we Francji (17,9 %) i w Zjednoczonym Królestwie (16,4 %). Liczba wniosków o dostęp do danych elektronicznych wzrosła dwukrotnie w Polsce i prawie trzykrotnie w Finlandii. Ponadto liczba wniosków o ujawnienie informacji w trybie pilnym wzrosła niemal o połowę w ciągu jednego roku.

53 COM(2018) 226 i COM(2018) 225.

54 Np. Zgromadzenie Ogólne ONZ (ZO ONZ) przyjęło w dniu 27 grudnia 2019 r. rezolucję 74/247 w sprawie „Przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych", ustanawiającą otwarty międzyrządowy komitet ekspertów *ad hoc*, którego zadaniem jest opracowanie kompleksowej konwencji międzynarodowej w sprawie cyberprzestępczości. UE nie popiera utworzenia nowego międzynarodowego instrumentu prawnego dotyczącego cyberprzestępczości, ponieważ konwencja budapeszteńska o cyberprzestępczości zapewnia już kompleksowe wielostronne ramy prawne. W lipcu 2020 r. państwa członkowskie ONZ zgodziły się wstrzymać pierwsze działania: UE wniosła wkład w ten proces w oparciu o wspólne stanowisko (dok. 7677/2/20).

55 Wyrok w sprawach połączonych C-203/15 i C-698/15, Tele2 Sverige AB oraz Watson i in., 21 grudnia 2016 r.

badaniem dotyczącym praktyk w zakresie zatrzymywania danych stosowanych przez dostawców usług łączności elektronicznej oraz potrzeb i praktyk organów ścigania w zakresie dostępu do danych, określeniem odpowiednich wyzwań technologicznych oraz przeglądem krajowych ram prawnych[56]. W wyniku tych prac zwrócono uwagę na potrzebę zapewnienia organom ścigania dostępu do danych w celu umożliwienia im skuteczniejszego wykonywania zadań.

W dniu 6 października 2020 r. Trybunał Sprawiedliwości wydał wyroki[57] w sprawie przepisów krajowych Belgii, Francji i Zjednoczonego Królestwa regulujących zatrzymywanie i przekazywanie danych komunikacyjnych niedotyczących treści oraz dostęp do takich danych do celów egzekwowania prawa i bezpieczeństwa narodowego. Komisja oceni dostępne możliwości zapewnienia identyfikacji i śledzenia terrorystów i innych przestępców, przy jednoczesnym poszanowaniu prawa Unii zgodnie z wykładnią Trybunału Sprawiedliwości, uwzględniając również inne sprawy toczące się przed Trybunałem w tej dziedzinie.

Innym ważnym elementem w walce z cyberprzestępczością są działania na rzecz zapewnienia dostępności i dokładności danych rejestracyjnych nazw domen internetowych („**informacje WHOIS**"), zgodnie z działaniami Internetowej Korporacji ds. Nadanych Nazw i Numerów (ICANN). Dyskusje mają na celu zagwarantowanie, że podmioty legalnie ubiegające się o dostęp, w tym organy ścigania i operatorzy zajmujący się cyberbezpieczeństwem, uzyskają skuteczny dostęp do ogólnych danych rejestracyjnych domen najwyższego poziomu, przy pełnym poszanowaniu obowiązujących przepisów o ochronie danych. Ostateczne zalecenia dotyczące nowej polityki WHOIS zostały opublikowane w dniu 10 sierpnia 2020 r. i są obecnie poddawane przeglądowi, przed podjęciem decyzji przez zarząd ICANN. Komisja przeanalizuje wnioski z przeglądu i rozważy, czy w wystarczającym stopniu odzwierciedlają one ochronę danych i względy interesu publicznego związane z zapewnieniem skutecznego dostępu organom ścigania i operatorom w obszarze cyberbezpieczeństwa.

2. Nowoczesne egzekwowanie prawa

W związku z tym, że technologia w dalszym ciągu kształtuje niemal każdy sektor społeczeństwa, w tym bezpieczeństwo, organy ścigania i wymiar sprawiedliwości muszą być w stanie nadążyć za zmianami. Włączenie sztucznej inteligencji, technologii dużych zbiorów danych i obliczeń wielkiej skali do polityki bezpieczeństwa, nie osłabiając jednocześnie skutecznej ochrony praw podstawowych, ma zasadnicze znaczenie dla zwiększenia bezpieczeństwa i ochrony.

Komisja pracuje obecnie nad kilkoma kluczowymi zagadnieniami[58]. W dniu 25 listopada 2020 r. Komisja przedstawiła wniosek dotyczący[59] aktu w sprawie zarządzania danymi, stanowiącego ramy dla ułatwionego udostępniania i ponownego wykorzystywania danych osobowych i nieosobowych do celów innowacji i rozwoju. Obejmuje to przemysł i organy publiczne za pośrednictwem wirtualnych lub fizycznych przestrzeni danych sektorowych. Na mocy takiego aktu krajowe organy ścigania zyskałyby dostęp do danych przechowywanych w innych przestrzeniach danych na potrzeby ich własnych celów

[56] https://data.europa.eu/doi10.2837/26288

[57] Wyroki w sprawie C-623/17, Privacy International, oraz w sprawach połączonych C-511/18, La Quadrature du Net i in., C-512/18, French Data Network i in., oraz C-520/18, Ordre des barreaux francophones et germanophone i in.

[58] W tym nad strategią UE w zakresie danych (zob. powyżej).

[59] COM(2020) 767.

w zakresie innowacji. Jednocześnie dostęp do danych przechowywanych przez krajowe organy ścigania i organy bezpieczeństwa nie byłby dozwolony, chyba że zezwoli na to prawo Unii lub prawo krajowe. Krajowe organy ścigania odpowiedzialne za bezpieczeństwo mogą zyskać również na tym, jeżeli poszczególne osoby, których dane dotyczą, udostępniają swoje dane dobrowolnie dla wspólnego dobra, wyłącznie w celu prowadzenia badań naukowych.

Trwają również prace nad przygotowaniem nowej inicjatywy w sprawie **sztucznej inteligencji (AI)**, w następstwie opublikowania białej księgi w sprawie sztucznej inteligencji[60]. Uznając możliwości, jakie oferuje technologia sztucznej inteligencji w zakresie zwiększenia bezpieczeństwa i dobrobytu obywateli i całego społeczeństwa, w białej księdze określono również szereg zagrożeń – takich jak zagrożenia dla cyberbezpieczeństwa, zagrożenia dla bezpieczeństwa osobistego lub utrata łączności. Główne obawy, jakie wyrażali uczestnicy konsultacji publicznych, dotyczyły możliwości naruszenia przez sztuczną inteligencję praw podstawowych oraz ryzyka, że sztuczna inteligencja może prowadzić do dyskryminacyjnych wyników[61]. W komunikacie w sprawie budowania zaufania do sztucznej inteligencji ukierunkowanej na człowieka[62] Komisja podkreśliła potrzebę uodpornienia systemów sztucznej inteligencji zarówno na jawne ataki, jak i na bardziej subtelne próby manipulacji danymi lub algorytmami, a także potrzebę podjęcia kroków w celu ograniczenia tego ryzyka.

Szyfrowanie odgrywa zasadniczą rolę w zapewnieniu solidnego cyberbezpieczeństwa i skutecznej ochrony praw podstawowych, takich jak prawo do prywatności, w tym poufności komunikacji, oraz ochrony danych osobowych, a także w zapewnieniu zaufania do usług i produktów opartych na technologiach szyfrowania, takich jak rozwiązania w zakresie tożsamości cyfrowej. Jednocześnie szyfrowanie może również zostać wykorzystane do ukrywania przestępstw przed organami ścigania i organami wymiaru sprawiedliwości, co utrudnia dochodzenie, wykrywanie i ściganie. Państwa członkowskie wchodzące w skład Rady wezwały do przyjęcia rozwiązań, które umożliwią organom ścigania i organom wymiaru sprawiedliwości uzyskanie zgodnego z prawem dostępu do elektronicznego materiału dowodowego, przy pełnym poszanowaniu prywatności, ochrony danych i gwarancji sprawiedliwego procesu[63]. Komisja będzie współpracować z państwami członkowskimi w celu określenia rozwiązań prawnych, operacyjnych i technicznych umożliwiających zgodny z prawem dostęp do informacji elektronicznych w zaszyfrowanych środowiskach, które zapewniają bezpieczeństwo łączności.

Praktyczne kroki w tym kierunku obejmują **platformę deszyfrującą** w Europolu, która ma pomóc organom ścigania w uzyskaniu zgodnego z prawem dostępu do zaszyfrowanych informacji zawartych w urządzeniach skonfiskowanych w trakcie postępowań przygotowawczych[64]. Europejska grupa ds. szkolenia i edukacji w zakresie cyberprzestępczości opracowała pilotażowe moduły szkoleniowe, które zostaną wykorzystane w pracach Agencji ds. Szkolenia w Dziedzinie Ścigania (CEPOL). W państwach członkowskich utworzono sieć punktów wiedzy specjalistycznej w zakresie

[60] COM(2020) 65.
[61] Odpowiednio 90 % i 87 % respondentów uważa te obawy za ważne lub bardzo ważne.
[62] COM(2019) 168.
[63] ST 13084 2020 – Rezolucja Rady w sprawie szyfrowania – Bezpieczeństwo dzięki szyfrowaniu i bezpieczeństwo pomimo szyfrowania.
[64] Ten projekt o wartości 6 mln EUR jest również objęty wsparciem ze strony Wspólnego Centrum Badawczego Komisji.

szyfrowania w celu wymiany najlepszych praktyk i wiedzy specjalistycznej oraz wspierania rozwoju zestawu narzędzi technicznych i praktycznych.

System cyfrowej wymiany elektronicznego materiału dowodowego będzie stanowił narzędzie bezpiecznej, szybkiej i skutecznej transgranicznej wymiany europejskich nakazów dochodzeniowych, wniosków o wzajemną pomoc i elektronicznych materiałów dowodowych . Należy go stopniowo ulepszać i rozszerzać na inne instrumenty współpracy sądowej w sprawach karnych, a jego przyszły zakres zostanie określony we wniosku ustawodawczym w sprawie transformacji cyfrowej procedur współpracy sądowej zaplanowanym na 2021 r.[65]

3. Zwalczanie nielegalnych treści w internecie

Radykalizacja prowadząca do brutalnego ekstremizmu i terroryzmu to zjawisko wielowymiarowe i transgraniczne, które zyskało na szybkim rozwoju internetu. Internet nadal służy do radykalizacji i werbowania osób znajdujących się w trudnej sytuacji. W lipcu działająca w ramach Europolu unijna jednostka ds. zgłaszania podejrzanych treści w internecie usunęła 2 000 linków do treści o charakterze terrorystycznym – w tym podręczników i samouczków na temat przeprowadzania ataków. Dowody na to, że internet odgrywa rolę w radykalizacji postaw i rozgłaszaniu informacji na temat przestępstw popełnionych przez osoby uczestniczące w atakach we Francji i w Austrii, jeszcze bardziej podkreślają potrzebę istnienia jasnych ram legislacyjnych służących zapobieganiu rozpowszechniania treści o charakterze terrorystycznym w internecie, przy jednoczesnym utrzymaniu skutecznych zabezpieczeń w zakresie ochrony praw podstawowych. W ostatnich tygodniach nabrały tempa negocjacje między Parlamentem Europejskim a Radą w sprawie proponowanego **rozporządzenia w sprawie treści o charakterze terrorystycznym w internecie**[66]. Aby rozwiązać problem treści o charakterze terrorystycznym, w tym treści przyczyniających się do radykalizacji, negocjacje te muszą koniecznie zakończyć się ustanowieniem, w szczególności, nowego i skutecznego instrumentu operacyjnego obejmującego nakazy usunięcia służące do transgranicznego usuwania treści o charakterze terrorystycznym w terminie do godziny od otrzymania takiego nakazu.

Jednocześnie **Forum UE ds. Internetu** nadal pełni rolę katalizatora działań, stanowiąc istotną platformę współpracy państw członkowskich i branży w celu zapobiegania rozprzestrzenianiu się treści o charakterze terrorystycznym w internecie i przeciwdziałania wpływowi radykalizujących przekazów. Forum pracuje nad opracowaniem wykazu referencyjnego symboli i grup zakazanych w państwach członkowskich, który można by wykorzystać do kształtowania polityki moderacji treści na platformie.

Forum UE ds. Internetu rozszerza zakres swoich działań, aby objąć nim również **niegodziwe traktowanie dzieci w internecie w celach seksualnych**. Forum zapewni również wspólną przestrzeń służącą do wymiany najlepszych praktyk i identyfikacji przeszkód, na jakie napotykają zarówno podmioty prywatne, jak i publiczne, aby zwiększyć wzajemne zrozumienie i wspólnie poszukiwać rozwiązań. Umożliwia ono również koordynację polityczną na wysokim szczeblu w celu maksymalnego zwiększenia skuteczności i efektywności działań. W ramach Forum UE ds. Internetu, w skład którego wchodzą przedstawiciele środowisk akademickich, przemysłu, organów publicznych

[65] Komunikat w sprawie transformacji cyfrowej wymiaru sprawiedliwości w UE, COM(2020) 710, z dnia 2 grudnia 2020 r.

[66] COM(2018) 640.

i organizacji społeczeństwa obywatelskiego, stworzono techniczny proces ekspercki mający na celu określenie i wstępną ocenę możliwych rozwiązań technicznych służących wykrywaniu i zgłaszaniu przypadków niegodziwego traktowania dzieci w celach seksualnych w ramach pełni szyfrowanej komunikacji elektronicznej. Takie rozwiązania techniczne nie powinny osłabiać szyfrowania. Podejście to stanowi uzupełnienie innych elementów zwalczania niegodziwego traktowania dzieci w celach seksualnych zarówno w internecie, jak i poza nim, jak opisano powyżej.

Komisja kontynuowała również dzielenie się unijną wiedzą fachową i doświadczeniem w ramach niezależnego komitetu doradczego będącego częścią nowo utworzonego **Globalnego Internetowego Forum Przeciwdziałania Terroryzmowi** oraz w ramach współprzewodniczenia, wraz z firmą Microsoft, grupie roboczej ds. reagowania kryzysowego. Wraz z Europolem Komisja w dalszym ciągu wspierała państwa członkowskie we wdrażaniu **unijnego protokołu kryzysowego.** W dniu 23 listopada 2020 r. unijna jednostka ds. zgłaszania podejrzanych treści w internecie zorganizowała drugie ćwiczenie symulacyjne, którego celem było przygotowanie wytycznych mających poprawić reagowanie operacyjnego i koordynację w czasie rzeczywistym między państwami członkowskimi i dostawcami usług online.

W czerwcu 2020 r. Komisja opublikowała wyniki ostatniego monitorowania wdrażania **Kodeksu postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie**[67]. Wynika z nich, że przedsiębiorstwa informatyczne – średnio – sprawdzają 90 % zgłoszonych treści w ciągu 24 godzin i usuwają 71 % treści uznanych za nielegalne nawoływanie do nienawiści. Stwierdzono jednak również niedociągnięcia w zakresie przejrzystości i informacji zwrotnej dla użytkowników. Doświadczenia zdobyte podczas wdrażania kodeksu postępowania w ciągu ostatnich czterech lat wykorzystano również w rozważaniach na temat sposobów rozwiązania problemu nielegalnych treści w internecie przy jednoczesnym zapewnieniu ochrony wolności wypowiedzi w ramach przygotowywanego wniosku dotyczącego aktu prawnego o usługach cyfrowych. W orędziu o stanie Unii z 2020 r. przewodnicząca von der Leyen zapowiedziała również, że do końca 2021 r. Komisja zaproponuje rozszerzenie wykazu przestępstw na szczeblu UE zawartego w art. 83 ust. 1 TFUE o przestępstwa z nienawiści i przestępstwa nawoływania do nienawiści[68].

4. *Zagrożenia hybrydowe*

Uznając zmieniający się charakter zagrożeń hybrydowych, Rada ustanowiła w lipcu 2019 r. **Horyzontalną Grupę Roboczą ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym**. Jej głównym celem jest wspieranie strategicznej i horyzontalnej koordynacji między państwami członkowskimi w dziedzinie odporności państwa i społeczeństwa, a także poprawa komunikacji strategicznej i zwalczanie dezinformacji. Prace obejmowały działania następcze w związku z badaniami na temat zagrożeń hybrydowych[69], jak również analizę poświęconą w szczególności kwestiom zagrożeń hybrydowych i dezinformacji w sąsiadujących krajach partnerskich.

---

[67] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_pl

[68] Przedstawiono je bardziej szczegółowo również w strategii na rzecz równości osób LGBTIQ na lata 2020–2025 (COM(2020) 698).

[69] Działanie 1, Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym z 2016 r., zob. JOIN/2016/018.

Działalność Horyzontalnej Grupy Roboczej przedstawiono w sprawozdaniu rocznym przyjętym w dniu 14 września 2020 r.

W grudniu 2019 r. Rada przyjęła konkluzje w sprawie dodatkowych wysiłków na rzecz zwiększenia odporności i zwalczania zagrożeń hybrydowych[70], w których wezwała do przyjęcia kompleksowego podejścia do bezpieczeństwa i przeciwdziałania zagrożeniom hybrydowym, wymagającego prowadzenia prac we wszystkich odnośnych sektorach polityki w bardziej strategiczny, skoordynowany i spójny sposób. W lipcu 2020 r. podjęto dwa kluczowe działania następcze. Po pierwsze, służby Komisji i ESDZ przygotowały **wykaz działań i dokumentów dotyczących reakcji UE na zagrożenia hybrydowe**[71]. Wykaz zawiera ogólny spis działań związanych z przeciwdziałaniem zagrożeniom hybrydowym na poziomie UE oraz odpowiadających im dokumentów programowych. Stanowi on punkt wyjścia do stworzenia platformy internetowej o ograniczonym dostępie stanowiącej punkt kompleksowej obsługi w odniesieniu do wszystkich działań związanych z zagrożeniami hybrydowymi, dokumentów programowych i legislacyjnych, a także odpowiednich badań. Po drugie, w ostatnim rocznym **sprawozdaniu w sprawie przeciwdziałania zagrożeniom hybrydowym**[72] przeanalizowano wdrażanie obejmujące kwestie orientacji sytuacyjnej, budowania odporności, gotowości i reagowania kryzysowego, a także współpracy międzynarodowej, w szczególności współpracy UE i NATO w zakresie przeciwdziałania zagrożeniom hybrydowym. Chociaż w sprawozdaniu odnotowano pewne postępy w zakresie koordynacji na szczeblu UE, bezprecedensowa skala i różnorodność zagrożeń hybrydowych wymaga obecnie podjęcia dalszych kroków na szczeblu UE w celu płynnego połączenia wymiaru zewnętrznego i wewnętrznego oraz wsparcia wysiłków państw członkowskich na rzecz przeciwdziałania zagrożeniom hybrydowym i wzmocnienia ich odporności.

Jednocześnie trwają prace nad wdrożeniem środków określonych w nowej strategii w zakresie bezpieczeństwa w celu uwzględnienia zagrożeń hybrydowych w głównym nurcie kształtowania polityki, opracowania platformy internetowej o ograniczonym dostępie, ustanowienia wyjściowych poziomów odporności sektorowej, a także usprawnienia przepływu informacji, aby jeszcze bardziej zwiększyć orientację sytuacyjną[73]. Podstawę tych prac stanowi **Komórka UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych** ustanowiona w ramach Centrum Analiz Wywiadowczych UE (INTCEN), która pozostaje centralnym punktem UE do spraw oceny zagrożeń hybrydowych. Komórka opracowała już ponad 180 pisemnych sprawozdań na temat zagrożeń hybrydowych i zagrożeń dla cyberbezpieczeństwa. Jednym z projektów Komórki ds. Syntezy Informacji o Zagrożeniach Hybrydowych jest **analiza tendencji w zakresie zagrożeń hybrydowych**[74], która jest źródłem danych dotyczących następujących zagadnień: cykliczna analiza działań hybrydowych prowadzonych przez nowe podmioty;

---

[70] Konkluzje Rady 14972/19.

[71] SWD(2020) 152, wspólny dokument roboczy służb, Wykaz działań służących zwiększeniu odporności na zagrożenia hybrydowe i przeciwdziałaniu im.

[72] SWD(2020) 153, wspólny dokument roboczy służb, Sprawozdanie w sprawie wdrażania wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym z 2016 r. oraz wspólnego komunikatu z 2018 r. w sprawie zwiększenia odporności i wzmocnienia zdolności reagowania na zagrożenia hybrydowe.

[73] Na przykład w dniu 26 listopada 2020 r. Wspólne Centrum Badawcze zaproponowało nowe ramy mające na celu zwiększenie świadomości na temat zagrożeń: https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats

[74] Analiza tendencji w zakresie zagrożeń hybrydowych to narzędzie przeznaczone do stosowania wraz z systemami krajowymi w celu monitorowania skali i intensywności zagrożeń hybrydowych w dziedzinach: politycznej/dyplomatycznej, wojskowej, gospodarczej, informacyjnej, wywiadowczej, cybernetycznej, społecznej, energetycznej i infrastrukturalnej.

obce działania wywiadowcze przeciwko państwom członkowskim, instytucjom, partnerom i interesom UE oraz hybrydowe wykorzystywanie pandemii COVID-19 przez podmioty państwowe i niepaństwowe.

Współpraca UE–NATO (na podstawie kompleksowych ram przewidzianych we wspólnych deklaracjach z Warszawy i z Brukseli z 2016 r. i 2018 r.) stała się jeszcze bardziej intensywna, co podkreślono w piątym sprawozdaniu z postępu prac z czerwca 2020 r., i objęła kontakty między personelem organizacji oraz konkretne rezultaty w dziedzinie zagrożeń hybrydowych, cyberobrony i budowania zdolności[75]. Należy koniecznie opracować jednolitą metodykę dla wszystkich sektorów na potrzeby prac nad wyjściowymi poziomami odporności na zagrożenia hybrydowe, aby ograniczyć ryzyko rozdrobnienia i powielania polityk, narzędzi i działań. We współpracę tę zaangażowane było również Europejskie Centrum Doskonałości ds. Zwalczania Zagrożeń Hybrydowych w Helsinkach. Współpracę z NATO zintensyfikowano podczas kryzysu związanego z COVID-19, m.in. w zakresie dezinformacji związanej z pandemią i przeciwdziałania wrogim działaniom informacyjnymi.

Ogólnie rzecz biorąc, pandemia COVID-19 uwidoczniła szybko zmieniające się zagrożenia związane z **dezinformacją** i rzeczywiste zagrożenie dla życia ludzkiego[76]. W dniu 10 czerwca 2020 r. Komisja i wysoki przedstawiciel przyjęli **wspólny komunikat w sprawie zwalczania dezinformacji na temat COVID-19**[77], aby wskazać konkretne zagrożenia związane z dezinformacją wokół COVID-19 oraz działania, jakie należy podjąć. Wiązało się to z podjęciem działań przez główne platformy internetowe w celu opracowania strategii przeciwdziałania tym zagrożeniom oraz z intensyfikacją monitorowania działań platform, jak również ze specjalną współpracą za pośrednictwem zarządzanego przez ESDZ systemu wczesnego ostrzegania. Pandemia spowodowała wzmożenie starań na rzecz rozwiązania problemu dezinformacji i zwiększenia świadomości społecznej. W pierwszej połowie 2020 r. w publicznej bazie danych **EUvsDisinfo** dotyczącej przypadków dezinformacji dodano 1 963 nowych przypadków dezinformacji prokremlowskiej, z czego blisko jedna trzecia dotyczyła infodemii związanej z COVID-19. Od połowy marca do końca kwietnia 2020 r. stronę odwiedzało ponad 10 000 osób dziennie, a ogólna liczba odwiedzających wzrosła o 400 % w porównaniu z tym samym okresem w 2019 r. Reakcja UE obejmowała ukierunkowane kampanie informacyjne[78] i udzielanie sprawdzonych informacji na temat pandemii.

Zdobyte doświadczenie wykorzystano przy opracowywaniu **europejskiego planu działania na rzecz demokracji** przyjętego w dniu 2 grudnia 2020 r.[79] W planie tym określono kluczowe kroki mające na celu wzmocnienie odporności unijnej struktury demokratycznej dzięki wspieraniu wolnych i uczciwych wyborów, rozwiązywaniu problemów, z którymi zmagają się wolne i niezależne media, oraz zwalczaniu

---

[75] Współpracę między personelem w dziedzinie cyberbezpieczeństwa i cyberobrony dodatkowo zintensyfikowano dzięki pracom dotyczącym spójnych koncepcji i doktryn, ćwiczeniom, wymianie informacji i wzajemnym briefingom.

[76] Rzeczywiste konsekwencje obejmowały podpalenia infrastruktury telekomunikacyjnej i wprowadzające w błąd informacje na temat zdrowia, które miały bezpośrednie skutki.

[77] JOIN(2020) 8, wspólny komunikat, Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom.

[78] Na przykład rozpoczęto kampanię „Pomyśl, zanim udostępnisz” („Think before you share”) w celu zapewnienia porad dotyczących sposobu ograniczania rozprzestrzeniania się dezinformacji wśród młodych odbiorców i środowisk opiniotwórczych w krajach Partnerstwa Wschodniego UE, którą wyświetlono na platformach mediów społecznościowych ponad 500 000 razy.

[79] COM(2020) 790.

dezinformacji. Ten ostatni aspekt przewiduje wykorzystanie planu działania na rzecz zwalczania dezinformacji z 2018 r.[80] jako podstawy zintensyfikowanej działalności UE na rzecz przeciwdziałania dezinformacji oraz opracowania sposobu zaangażowania kluczowych zainteresowanych stron w ramach społeczeństwa obywatelskiego, jak również sektora prywatnego. Wymaga również podjęcia dalszych działań związanych z **kodeksem postępowania w zakresie zwalczania dezinformacji** po przeprowadzeniu we wrześniu 2020 r. oceny skuteczności kodeksu[81]. Kodeks stanowi ważny i konieczny etap na drodze do utworzenia bardziej przejrzystego i rozliczalnego ekosystemu platform internetowych, ale byłby bardziej skuteczny, gdyby definicje były bardziej ujednolicone i wdrażane w spójniejszy sposób oraz gdyby podjęto więcej działań w określonych obszarach, takich jak mikrotargetowanie. Innym kluczowym narzędziem, którym obecnie dysponuje UE, jest **Europejskie Obserwatorium Mediów Cyfrowych**, które rozpoczęło działalność w czerwcu 2020 r. Skupia ono najważniejsze zainteresowane strony zajmujące się kwestią dezinformacji, w tym weryfikatorów informacji i pracowników naukowych.

IV OCHRONA EUROPEJCZYKÓW PRZED TERRORYZMEM I PRZESTĘPCZOŚCIĄ ZORGANIZOWANĄ

1. *Terroryzm i radykalizacja postaw*

Ostatnie ataki po raz kolejny pokazały, że zagrożenie terrorystyczne w UE jest nadal wysokie. W dniu 16 października 2020 r. w Conflans-Sainte-Honorine zamordowano nauczyciela, a w dniu 29 października w kościele Notre-Dame w Nicei zabito trzy osoby. W dniu 2 listopada w Wiedniu w wyniku ataku terrorystycznego zginęły cztery osoby, a 23 osoby zostały ranne. W dniu 13 listopada Rada przyjęła wspólną deklarację ministrów spraw wewnętrznych UE w sprawie ostatnich ataków terrorystycznych we Francji i w Austrii[82]. Te ostatnie ataki inspirowane przez dżihadystów zbiegają się z rosnącym zagrożeniem ze strony brutalnych prawicowych ekstremistów i innych form terroryzmu.

Aby bardziej wesprzeć państwa członkowskie w walce z terroryzmem i radykalizacją, Komisja przyjmuje dziś **agendę antyterrorystyczną dla UE**[83]. Agenda ta opiera się na istniejącej polityce i instrumentach i wzmocni ramy UE w celu dalszej poprawy w zakresie przewidywania zagrożeń i ryzyka, zapobiegania radykalizacji i brutalnemu ekstremizmowi, ochrony ludzi i infrastruktury, w tym dzięki zabezpieczeniu granic zewnętrznych oraz przeprowadzaniu skutecznych działań następczych po atakach. Przedstawiono w niej również dalsze działania na rzecz poprawy egzekwowania prawa i współpracy sądowej oraz wykorzystania technologii i wymiany istotnych informacji w ramach UE, w tym z osobami przeprowadzającymi kontrole na granicach zewnętrznych. Kluczowe znaczenie ma nadal wdrażanie i egzekwowanie przepisów.

Istotnym elementem zwalczania terroryzmu jest zapobieganie. Działania UE w dziedzinie **zapobiegania radykalizacji postaw** opierają się na solidnym doświadczeniu zdobytym dotychczas w zakresie wspierania osób działających na pierwszej linii i decydentów. W dniu 24 listopada Komisja przyjęła nowy **plan działania na rzecz integracji i włączenia społecznego**[84]. Niezwykle istotnym elementem zwalczania radykalizacji jest

[80] JOIN(2018) 36, wspólny komunikat, Plan działania na rzecz zwalczania dezinformacji.
[81] SWD(2020) 180.
[82] Wspólne oświadczenie unijnych ministrów spraw wewnętrznych w sprawie ostatnich ataków terrorystycznych w Europie, 13.11.2020, 12634/20.
[83] COM(2020) 795.
[84] COM(2020) 758.

wzmożenie działań na rzecz zbliżenia społeczności. Społeczeństwo, które jest bardziej spójne i integracyjne, może pomóc w zapobieganiu rozprzestrzeniania się ideologii ekstremistycznych, które mogą prowadzić do terroryzmu i brutalnego ekstremizmu. Wsparcie na rzecz **sieci upowszechniania wiedzy o radykalizacji postaw** obejmuje kolejną umowę na kwotę 30 mln EUR od stycznia 2020 r. na kolejne cztery lata obejmującą pomoc dla osób działających w terenie, a także dodatkowe wsparcie dla decydentów i naukowców. Te i inne instrumenty, takie jak **Forum UE ds. Internetu**, umożliwią Komisji zajęcie się działaniami priorytetowymi wskazanymi w ramach kierunków strategicznych na 2021 r. dotyczących skoordynowanego podejścia UE do zapobiegania radykalizacji postaw, opracowanych wspólnie z państwami członkowskimi. Uzupełniają je działania w ramach agendy antyterrorystycznej dla UE, mające na celu przeciwdziałanie ideologiom ekstremistycznym w internecie, zintensyfikowanie działań prowadzonych w zakładach karnych oraz w zakresie resocjalizacji i reintegracji, w tym dotyczących zagranicznych bojowników terrorystycznych, a także zwiększenie wsparcia dla podmiotów lokalnych i budowanie bardziej odpornych społeczności.

Przyjęta w marcu 2017 r. **dyrektywa w sprawie zwalczania terroryzmu**[85] jest głównym instrumentem wymiaru sprawiedliwości w sprawach karnych na szczeblu UE służącym do zwalczania terroryzmu. W dyrektywie określono minimalne standardy dotyczące definiowania przestępstw terrorystycznych i związanych z terroryzmem oraz sankcji, jednocześnie zapewniając ofiarom terroryzmu prawo do ochrony, wsparcia i pomocy. W dniu 30 września 2020 r. Komisja przyjęła sprawozdanie [86]dotyczące oceny środków, które państwa członkowskie wprowadziły celem wykonania dyrektywy. Stwierdzono w nim, że transpozycja do prawa krajowego przyczyniła się do zaostrzenia podejścia do terroryzmu stosowanego w systemach wymiaru sprawiedliwości w sprawach karnych w państwach członkowskich oraz wzmocnienia praw przysługujących ofiarom terroryzmu, ale pozostają pewne luki. Na przykład nie wszystkie państwa członkowskie uznają w swoim prawie krajowym za przestępstwa wszystkie czyny wymienione w dyrektywie jako przestępstwa terrorystyczne, a także nie wszystkie wprowadziły przepisy mające na celu uznanie za przestępstwo podróży w celach terrorystycznych oraz nie wszystkie odniosły się do problemu finansowania terroryzmu, jak również udzielania wsparcia ofiarom. Sprawozdanie z oceny dyrektywę zostanie przyjęte w późniejszym okresie w 2021 r.

UE kontynuuje działania mające na celu wspieranie państw członkowskich w uniemożliwianiu terrorystom dostępu do środków służących do przeprowadzania ataków i pomoc we wdrażaniu przepisów. Przyjęte w czerwcu 2019 r. rozporządzenie w sprawie wprowadzania do obrotu i stosowania **prekursorów materiałów wybuchowych**[87] zacznie obowiązywać od dnia 1 lutego 2021 r. Aby pomóc organom krajowym i sektorowi prywatnemu w wykonywaniu rozporządzenia, Komisja opublikowała w czerwcu 2020 r. szereg wytycznych[88]. Ponadto w czerwcu 2020 r. Komisja stworzyła program[89] służący do monitorowania wyników, rezultatów i skutków rozporządzenia.

---

85 Dyrektywa (UE) 2017/541.
86 COM(2020) 619.
87 Rozporządzenie (UE) 2019/1148.
88 Zawiadomienie Komisji – Wytyczne dotyczące wykonania rozporządzenia (UE) 2019/1148 w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, Dz.U. C 210/1 z 24.6.2020.
89 SWD(2020) 114 final.

W listopadzie 2019 r. Komisja wezwała państwa członkowskie do oceny realizacji planu działania z 2017 r. na rzecz zwiększania gotowości na wypadek **chemicznych, biologicznych, radiologicznych i jądrowych zagrożeń dla bezpieczeństwa**[90]. Ogólnie stwierdzono, że większość działań wdrożono. Na początku 2020 r. Komisja przygotowała we współpracy z ekspertami krajowymi wykaz chemikaliów wysokiego ryzyka budzących obawy. Stanowiło to podstawę do nawiązania współpracy z producentami sprzętu w celu poprawy zdolności w zakresie wykrywania. Niedawno Komisja rozpoczęła badanie dotyczące możliwości ograniczenia dostępności niektórych z tych chemikaliów. Trwają również prace w ramach Unijnego Mechanizmu Ochrony Ludności oraz rozmowy z państwami członkowskimi na temat dodatkowych zdolności reagowania w związku z zagrożeniami CBRJ w dziedzinie odkażania, wykrywania, nadzoru i monitorowania, a także składowania.

W dniu 12 października 2020 r. Rada podjęła decyzję o przedłużeniu obowiązywania systemu sankcji ograniczających rozprzestrzenianie i stosowanie broni chemicznej o rok[91], umożliwiając UE nałożenie środków ograniczających na osoby i podmioty zaangażowane w opracowywanie i stosowanie broni chemicznej. W dniu 14 października 2020 r. Rada nałożyła środki ograniczające na sześć osób fizycznych i jeden podmiot zamieszanych w próbę zabójstwa Aleksieja Nawalnego, którego otruto toksycznym środkiem paralityczno-drgawkowym z grupy „nowiczok" w dniu 20 sierpnia 2020 r. w Rosji[92].

Do identyfikacji siatek terrorystycznych niezbędne są również **informacje finansowe**, ponieważ terroryści potrzebują środków finansowych do przemieszczania się, szkolenia i zakupu sprzętu, a działania w zakresie **przeciwdziałania finansowaniu terroryzmu** stanowią kluczowy element postępowań w sprawach dotyczących terroryzmu. Do najważniejszych kwestii należą pełne wykorzystanie istniejących narzędzi i danych wywiadowczych, właściwe wdrożenie standardów uzgodnionych na szczeblu międzynarodowym oraz stawienie czoła zmieniającym się wyzwaniom związanym z nowymi technologiami i platformami mediów społecznościowych[93] (zob. poniżej).

Celem ataków terrorystycznych była i pozostaje sieć **transportowa**. Działania UE obejmują podejście do ochrony sektora lotniczego oparte na ocenie ryzyka[94]. Poważnym zagrożeniem dla lotnictwa cywilnego są strefy konfliktu, przy czym zasadnicze znaczenie dla ograniczenia ryzyka ma wymiana informacji i ocen ryzyka[95]. Unijny system ostrzeżeń o **ocenie ryzyka dotyczącego stref konfliktu** uznano za najlepszą praktykę, a międzynarodowe normy w zakresie wymiany informacji włączono do prawodawstwa UE[96]. Dzięki doświadczeniom zdobytym w dziedzinie lotnictwa cywilnego Komisja rozszerzyła podejście oparte na ocenie ryzyka na inne rodzaje transportu. Wdrażanie

---

90 COM(2017) 610 final.

91 Decyzja Rady (WPZiB) 2020/1466 z dnia 12 października 2020 r. zmieniająca decyzję (WPZiB) 2018/1544.

92 Decyzja Rady (WPZiB) 2020/1482 z dnia 14 października 2020 r. i rozporządzenie wykonawcze Rady (UE) 2020/1480.

93 Zgodnie z ustaleniami UE z listopada 2019 r. poczynionymi na konferencji ministerialnej „No Money For Terror" w sprawie przeciwdziałania finansowaniu terroryzmu, której gospodarzem była Australia.

94 Zintegrowany proces przeprowadzania oceny ryzyka w zakresie ochrony lotnictwa w UE stanowi wsparcie w procesie podejmowania decyzji w obszarze bezpieczeństwa lotniczego transportu towarów, norm ochrony lotnictwa i ryzyka dla lotnictwa cywilnego wynikającego ze stref konfliktu.

95 Tragiczne zestrzelenie samolotu linii Ukraine International Airlines, którym odbywał się lot 752, w dniu 8 stycznia 2020 r. dodatkowo potwierdziło znaczenie wymiany informacji i oceny ryzyka dla bezpieczeństwa lotnictwa cywilnego.

96 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32019R1583

unijnego planu działania na rzecz **bezpieczeństwa kolei**[97] znajduje się na zaawansowanym etapie, przy czym w procesie tym wykorzystuje się wiedzę fachową unijnej platformy pasażerów w ruchu kolejowym, specjalnej grupy ekspertów ustanowionej przez Komisję. W sektorze morskim podejście oparte na ocenie ryzyka jest powszechnie znane i stosowane, a Komisja współpracuje z państwami członkowskimi i zainteresowanymi stronami w celu zwiększenia bezpieczeństwa pasażerów. Kwestię tę uwzględniono w **strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego** oraz związanym z nią **planie działania**, zmienionym w 2018 r., który również obejmuje wymiar bezpieczeństwa i obrony. Określono to w najnowszym sprawozdaniu z realizacji przyjętym i opublikowanym w dniu 23 października 2020 r.[98]

Europol za pośrednictwem **Europejskiego Centrum ds. Zwalczania Terroryzmu (ECTC)** udziela wsparcia państwom członkowskim w prowadzeniu dochodzeń dotyczących terroryzmu. Liczba wniosków o udzielenie wsparcia operacyjnego składanych przez państwa członkowskie do Europejskiego Centrum ds. Zwalczania Terroryzmu nadal wzrastała i obecnie Centrum to uczestniczy niemal w każdym poważnym dochodzeniu w sprawie zwalczania terroryzmu. W 2019 r. Europol wspierał ogółem 632 różnych operacji w obszarze zwalczania terroryzmu. Śledczy z państw członkowskich w coraz większym stopniu cenią tę współpracę – ich poziom zadowolenia wzrósł z 8/10 w 2018 r. do 9,1/10 w 2019 r. W 2019 r. Europejskie Centrum ds. Zwalczania Terroryzmu koordynowało dni wspólnego działania łącznie 18 razy[99].

Eurojust również udzielił wsparcia w 116 dochodzeniach w sprawie terroryzmu w latach 2019 i 2020. W wyniku obecnie prowadzonych prac zostanie sporządzony wniosek ustawodawczy w sprawie wymiany informacji na temat spraw dotyczących terroryzmu transgranicznego na potrzeby rozwoju sądowego rejestru antyterrorystycznego uruchomionego w 2019 r.[100], jak również rozszerzenia prac w obszarze prawicowych i lewicowych grup ekstremistycznych.

W dniu 30 lipca 2020 r. Rada dokonała ostatniej aktualizacji unijnej listy osób, grup i podmiotów podlegających środkom ograniczającym mającym na celu zwalczanie terroryzmu. Najnowsza lista obejmuje 14 osób i 21 podmiotów. Tego samego dnia Rada nałożyła środki ograniczające na jedną osobę objętą systemem sankcji mających na celu zwalczanie terroryzmu ISIL (Daisz)/Al-Kaidy. Obecnie system ten, którego ważność przedłużono o jeden rok w dniu 19 października 2020 r.[101], obejmuje pięć niezależnie umieszczonych osób.

Istotny element polityki zwalczania terroryzmu dotyczy zagrożeń, jakie stwarzają **zagraniczni bojownicy terrorystyczni,** obecnie działający w Syrii i Iraku. Przy pełnym poszanowaniu podstawowej odpowiedzialności państw członkowskich za te kwestie, wsparcie i koordynacja na poziomie UE pomagają państwom członkowskim w sprostaniu wspólnym wyzwaniom: ściganiu sprawców przestępstw terrorystycznych, zapobieganiu

---

97 COM(2018) 470 final.

98 Sprawozdanie służb Komisji, Europejskiej Służby Działań Zewnętrznych i Europejskiej Agencji Obrony w sprawie realizacji zmienionego planu działania dotyczącego strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego, SWD(2020) 252.

99 Roczne skonsolidowane sprawozdanie z działalności z 2019 r., Europol, 9.6.2020.

100 Administratorem sądowego rejestru antyterrorystycznego jest Eurojust, który zapewnia całodobowe wsparcie krajowym organom wymiaru sprawiedliwości. Tego rodzaju scentralizowane informacje powinny pomóc prokuratorom w bardziej aktywnej koordynacji i w wykrywaniu podejrzanych lub sieci będących przedmiotem dochodzeń w konkretnych sprawach o potencjalnych skutkach transgranicznych.

101 Decyzje Rady (WPZiB) 2020/1132, 2020/1126 i 2020/1516.

niewykrytym wjazdom do strefy Schengen oraz reintegracji i resocjalizacji powracających zagranicznych bojowników terrorystycznych. Na przykład Komisja ściśle współpracuje z państwami członkowskimi i głównymi krajami partnerskimi, aby zapewnić wymianę dowodów gromadzonych w rejonach konfliktów i ich skuteczne wykorzystywanie do identyfikacji, wykrywania na granicach UE i ścigania. W memorandum w sprawie dowodów z rejonów konfliktów z 2020 r.[102] opublikowanym przez Eurojust wykazano, że chociaż pozyskiwanie takich danych i zapewnianie, aby spełniały one kryteria dopuszczalności dowodów, stwarza wiele wyzwań, mogą one pomóc w postawieniu osób podejrzanych o terroryzm przed wymiarem sprawiedliwości.

Komisja ułatwia także prowadzenie dialogu z państwami członkowskimi i podmiotami prowadzącymi działalność humanitarną w celu przedstawienia kompleksowego i faktycznego przeglądu sytuacji w obozach w północno-wschodniej Syrii, w których znajdują się członkowskie rodzin zagranicznych bojowników terrorystycznych z Europy. Szczególną uwagę poświęca się sytuacji dzieci przebywających w obozach syryjskich. Komisja pomaga państwom członkowskim również w wymianie doświadczeń dotyczących krajowych środków i mechanizmów służących lepszemu zarządzaniu **resocjalizacją i reintegracją** powracających zagranicznych bojowników terrorystycznych, a także dzieci. Ponadto sieć upowszechniania wiedzy o radykalizacji postaw prowadzi wizyty studyjne i udziela zindywidualizowanych porad w celu lepszego sprostania wyzwaniom dotyczącym skazanych osób powracających, w szczególności po zwolnieniu z zakładu karnego, jak również roli rodzin i społeczności lokalnych w staraniach na rzecz reintegracji.

Partnerstwa i współpraca z państwami trzecimi i partnerami z sąsiedztwa UE na rzecz zwalczania terroryzmu również ma zasadnicze znaczenie dla zwiększenia bezpieczeństwa w UE i lepszego powiązania wewnętrznego i zewnętrznego wymiaru unijnej polityki bezpieczeństwa. Rada zaapelowała o dalsze wzmocnienie zaangażowania UE w działania zewnętrzne w zakresie zwalczania terroryzmu[103] z naciskiem na Bałkany Zachodnie, Afrykę Północną i Bliski Wschód, Sahel, Róg Afryki i Azję. Prace te są prowadzone przy pełnym wykorzystaniu narzędzi z zakresu działań zewnętrznych, w tym dialogów na wysokim szczeblu dotyczących zwalczania terroryzmu oraz sieci 17 **ekspertów ds. bezpieczeństwa i zwalczania terroryzmu**[104] rozmieszczonych w delegaturach Unii, którzy nieustannie udzielają wsparcia, ułatwiając współpracę i promując budowanie zdolności. Obecnie rozważa się możliwość wzmocnienia i rozszerzenia tej sieci.

We wspólnym planie działania dla **Bałkanów Zachodnich** w zakresie zwalczania terroryzmu z 2018 r. i towarzyszących mu porozumieniach dwustronnych zawartych w 2019 r. z każdym z partnerów[105] skoncentrowano się na regionie o zasadniczym znaczeniu dla realizacji wspólnych celów z zakresu bezpieczeństwa i ochronie osób mieszkających w UE. Podczas Forum ministerialnego UE-Bałkany Zachodnie dotyczącego wymiaru sprawiedliwości i spraw wewnętrznych w dniu 22 października 2020 r. UE

[102] https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0

[103] Konkluzje Rady (8868/20) w sprawie działań zewnętrznych UE w zakresie przeciwdziałania terroryzmowi i brutalnemu ekstremizmowi oraz zwalczania tych zjawisk (16 czerwca 2020 r.).

[104] W Algierii, Bośni i Hercegowinie (ekspert regionalny dla Bałkanów Zachodnich), w Czadzie (ekspert regionalny dla Sahelu), w Etiopii (urzędnik łącznikowy przy Unii Afrykańskiej), w Indonezji (ekspert regionalny dla Azji Południowo-Wschodniej i urzędnik łącznikowy przy Forum Regionalnym ASEAN), w Iraku, Jordanii, Kenii (ekspert regionalny dla Rogu Afryki), w Kirgistanie (ekspert regionalny dla Azji Środkowej), w Libanie, Libii, Maroku, Nigerii, Pakistanie, Arabii Saudyjskiej, Tunezji i Turcji.

[105] Serbia, Macedonia Północna, Bośnia i Hercegowina, Kosowo*, Albania i Czarnogóra.

i Bałkany Zachodnie potwierdziły swoje zobowiązanie do realizacji celów określonych we wspólnych planach działania po 2020 r.[106] Współpraca z Bałkanami Zachodnimi obejmuje zarządzanie trwającymi powrotami zagranicznych bojowników terrorystycznych i członków ich rodzin, a także dalszą integrację w ramach działań na rzecz przeciwdziałania radykalizacji postaw. UE podtrzymuje również regularną współpracę w zakresie zwalczania terroryzmu z **Bliskim Wschodem, Afryką Północną i Azją Środkową**[107]. Współpraca z **Azją Środkową** koncentruje się na niwelowaniu zagrożeń chemicznych, biologicznych, radiologicznych i jądrowych. W dniu 25 czerwca 2020 r. odbyło się posiedzenie Wspólnego Komitetu Współpracy **UE-Rady Współpracy Państw Zatoki**, na którym omówiono takie kwestie jak zwalczanie radykalizacji postaw i przeciwdziałanie finansowaniu terroryzmu i praniu pieniędzy, a także cyberbezpieczeństwo i współpraca z Europolem. UE współpracowała z NATO nad pierwszym w historii audytem dotyczącym zagrożeń chemicznych, biologicznych, radiologicznych i jądrowych w jednym z państw Zatoki Perskiej przeprowadzonym pod koniec 2019 r. Ogółem pod koniec 2019 r. przeznaczono około 465 mln EUR na bieżące projekty w zakresie zwalczania terroryzmu i przeciwdziałania brutalnemu ekstremizmowi poza UE, co stanowi wzrost o 15 % w stosunku do roku poprzedniego.

UE nadal pogłębia również współpracę z **Organizacją Narodów Zjednoczonych** w zakresie zwalczania terroryzmu[108], w szczególności z Biurem Narodów Zjednoczonych ds. Przeciwdziałania Terroryzmowi i Zarządem Wykonawczym Komitetu Antyterrorystycznego, w tym poprzez coroczne dialogi na wysokim szczeblu, a ostatnio aktywnie uczestnicząc w wirtualnym tygodniu zwalczania terroryzmu zorganizowanym przez Organizację Narodów Zjednoczonych latem 2020 r. Ponadto Komisja uważnie śledziła rozważania na temat zmiany definicji przestępstw terrorystycznych w Konwencji **Rady Europy** o zapobieganiu terroryzmowi, zachęcając do ścisłego dostosowania jej do definicji określonych w prawie Unii. Kontynuowano owocną współpracę w obszarze zwalczania terroryzmu i materiałów chemicznych, biologicznych, radiologicznych i jądrowych między **NATO** i UE, wymieniając informacje na temat budowania zdolności, aby uniknąć powielania i zapewnić komplementarność.

2. Zwalczanie przestępczości zorganizowanej

Przestępczość zorganizowana rozwija się – staje się coraz bardziej transgraniczna i przenosi się do internetu.

---

[106] Wspólne oświadczenie prasowe: https://www.consilium.europa.eu/en/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf

[107] Działania na rzecz zwalczania terroryzmu podkreślono na przykład w nowej strategii UE wobec Azji Środkowej.
*Użycie tej nazwy nie wpływa na stanowiska w sprawie statusu Kosowa i jest zgodne z rezolucją Rady Bezpieczeństwa ONZ 1244/1999 oraz z opinią Międzynarodowego Trybunału Sprawiedliwości w sprawie Deklaracji niepodległości Kosowa.

[108] W 2019 r. podpisano ramy współpracy na rzecz zwalczania terroryzmu między UE i Organizacją Narodów Zjednoczonych https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

Europol, Ocena zagrożenia poważną i zorganizowaną przestępczością (SOCTA, 2017)

Działania Komisji obejmują zwalczanie środków odurzających, nielegalnej broni palnej, przeciwdziałanie przestępstwom finansowym, nielegalnemu przywozowi dóbr kultury, handlowi ludźmi czy przestępstwom przeciwko środowisku, co zapewnia wsparcie organom ścigania i organom wymiaru sprawiedliwości w państwach członkowskich, a także partnerom w sąsiedztwie. Współpraca z państwami trzecimi, w szczególności leżącymi w sąsiedztwie, takimi jak państwa Bałkanów Zachodnich, i organizacjami międzynarodowymi, w tym z Biurem Narodów Zjednoczonych ds. Narkotyków i Przestępczości[109], również odegrała w tym kontekście znaczącą rolę[110].

W 2019 r. **Europejskie Centrum Zwalczania Poważnej i Zorganizowanej Przestępczości przy Europolu** otrzymało i przetworzyło niemal 55 000 wkładów operacyjnych, co stanowi wzrost o 12 % w porównaniu z 2018 r. Jeżeli chodzi o liczbę operacji, na rzecz których udzielono wsparcia, Centrum pomagało państwom przy 726 sprawach[111]. Zasadnicze znaczenie ma również pełna transpozycja we wszystkich państwach członkowskich unijnych ram legislacyjnych dotyczących przestępczości zorganizowanej[112], za pośrednictwem których dąży się do harmonizacji prawa państw członkowskich w zakresie kryminalizacji przestępstw związanych z udziałem w organizacji przestępczej i w których określono kary za te przestępstwa. Komisja przeprowadziła badanie w celu przeanalizowania sposobów na ulepszenie tych przepisów. Dalsze etapy intensyfikacji zwalczania przestępczości zorganizowanej w UE zostaną opracowane wraz z agendą UE na rzecz walki z przestępczością zorganizowaną, która ma zostać przyjęta w pierwszym kwartale 2021 r.

Zabezpieczenie i konfiskata dochodów z przestępstwa jest jednym z najskuteczniejszych sposobów walki z przestępczością zorganizowaną. Nowy **Europejski Ośrodek ds. Przestępczości Gospodarczej i Finansowej** utworzony w czerwcu 2020 r. przy Europolu zapewni większe wsparcie operacyjne udzielane organom państw członkowskich i UE w obszarze przestępstw finansowych i gospodarczych oraz będzie promował systematyczne prowadzenie dochodzeń finansowych. Wspierając starania UE na rzecz skuteczniejszego wykrywania, zabezpieczania i konfiskowania mienia pochodzącego z przestępstwa, w czerwcu 2020 r. Rada przyjęła konkluzje w sprawie usprawniania

[109] Dialog wysokiego szczebla między UE i UNODC odbył się w dniu 8 grudnia 2020 r.
[110] Zgodnie ze stanem na koniec 2019 r. na bieżące działania w zakresie przestępczości zorganizowanej prowadzone poza UE przeznaczono około 830 mln EUR.
[111] Roczne skonsolidowane sprawozdanie z 2019 r., Europol, czerwiec 2020 r.
[112] Decyzja ramowa 2008/841.

dochodzeń finansowych w celu zwalczania poważnej i zorganizowanej przestępczości[113]. W 2021 r. Komisja dokona przeglądu prawodawstwa w sprawie zabezpieczenia i konfiskaty dochodów z przestępstwa[114] oraz biur ds. odzyskiwania mienia[115].

Zwalczanie przestępczości zorganizowanej wymaga zabezpieczeń, aby zapewnić skuteczne działanie organów ścigania w niezbędnych granicach, takich jak ochrona danych osobowych. Dyrektywa o ochronie danych w sprawach karnych z 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych związanych z przestępstwami[116] zabezpiecza prawo podstawowe do ochrony danych osobowych w przypadku wykorzystywania danych osobowych przez organy ścigania w sprawach karnych do celów egzekwowania prawa. Gwarantuje ona należytą ochronę danych osobowych ofiar, świadków i osób podejrzanych oraz ułatwia współpracę transgraniczną w zakresie zwalczania przestępczości i terroryzmu. Termin na dokonanie transpozycji dyrektywy o ochronie danych w sprawach karnych upłynął w dniu 6 maja 2018 r. Dotychczas większość państw członkowskich przyjęła ustawodawstwo transponujące tę dyrektywę. Nadal toczą się jednak niektóre postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego[117]. Obecnie Komisja ocenia zgodność krajowych przepisów transponujących z dyrektywą.

Zwalczanie nielegalnych środków odurzających

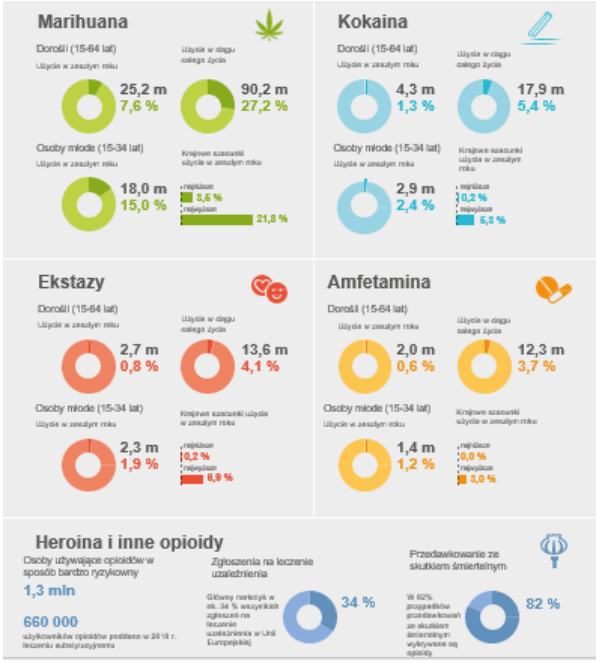
W lipcu 2020 r. Komisja przyjęła nową **Agendę i plan działania UE w zakresie środków odurzających na lata 2021–2025**[118] będące kontynuacją obecnych strategii antynarkotykowych UE[119]**.** Określono w nich ramy polityczne i priorytetowe obszary działania na kolejnych pięć lat. Agenda dotyczy głównie: 1) wzmocnionych środków bezpieczeństwa przeciwko nielegalnemu obrotowi środkami odurzającymi, od zorganizowanych grup przestępczych po zarządzanie granicami zewnętrznymi oraz nielegalną dystrybucję i produkcję; 2) wzmożonego zapobiegania, w tym podnoszenia świadomości w zakresie niepożądanych skutków używania środków odurzających, w szczególności na temat związku między ich używaniem a przemocą i innymi formami przestępczości; oraz 3) przeciwdziałania szkodom związanym z używaniem narkotyków za pośrednictwem dostępu do leczenia, ograniczenia ryzyka i szkód oraz zrównoważonego podejścia do kwestii używania środków odurzających w więzieniach. W dniu 30 listopada 2020 r. Komisja przyjęła również ocenę polityki UE w sprawie prekursorów narkotyków, w której stwierdzono, że konieczne są dodatkowe działania, aby uniemożliwić zorganizowanym grupom przestępczym w UE dostęp do chemikaliów, których potrzebują do produkcji nielegalnych narkotyków syntetycznych[120].

[113] Konkluzje Rady 8927/20.
[114] Dyrektywa 2014/42/UE.
[115] Decyzja Rady 2007/845/WSiSW.
[116] Dyrektywa (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych związanych z przestępstwami.
[117] Trzy państwa członkowskie (Niemcy, Słowenia i Hiszpania) nie zgłosiły jeszcze pełnej transpozycji mimo postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego. Komisja wniosła jedną sprawę dotyczącą braku transpozycji do Trybunału Sprawiedliwości, a w maju 2020 r. skierowała uzupełniające uzasadnione opinie do pozostałych dwóch państw członkowskich, które nie dokonały pełnej transpozycji dyrektywy.
[118] COM(2020) 606.
[119] Strategia antynarkotykowa UE na lata 2013–2020 i Plan działania UE w zakresie środków odurzających na lata 2017–2020.
[120] COM(2020) 768 z dnia 30 listopada 2020 r.

UE finansowała również konkretne projekty na rzecz wzmocnienia zwalczania środków odurzających, takie jak Europejskie Forum Społeczeństwa Obywatelskiego ds. Narkotyków. W Europejskim raporcie narkotykowym z 2020 r. sporządzonym przez Europejskie Centrum Monitorowania Narkotyków i Narkomanii opublikowanym w dniu 22 września 2020 r.[121] przedstawiono najnowsze tendencje w zakresie używania środków odurzających i tendencje na rynku środków odurzających w całej UE oraz w Turcji i Norwegii. Z raportu wynika, że nastąpił wzrost dostępności kokainy przy rekordowo wysokim poziomie konfiskat wynoszącym 181 ton, niemal podwojonej ilości skonfiskowanej heroiny – 9,7 tony – oraz dużej dostępności środków odurzających o wysokiej czystości w UE. Przeanalizowano w nim także pojawienie się nowych syntetycznych opioidów o szczególnie niepokojącym wpływie na zdrowie i odniesiono się do wyzwań wywołanych przez pandemię COVID-19.

Działania na rzecz zwalczania środków odurzających prowadzone są na kilku różnych poziomach. **Jesienią 2017 r. przyjęto pakiet legislacyjny dotyczący nowych substancji psychoaktywnych**[122] i zaczął on w pełni obowiązywać w listopadzie 2018 r. Wobec pięciu państw członkowskich nadal toczą się postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego[123]. Przyjęto już pierwszy akt delegowany, w którym uznano nową substancję psychoaktywną (izotonitazen) za narkotyk[124].

Na **arenie międzynarodowej** UE aktywnie działała w Komisji ds. Środków Odurzających[125] przy Organizacji Narodów Zjednoczonych, w szczególności w celu zaktualizowania klasyfikacji nowych substancji psychoaktywnych[126], a także zmiany klasyfikacji konopi i pochodnych konopi[127]. Nawiązanie dwóch nowych dialogów z Chinami i Iranem w sprawie środków odurzających zostało zatwierdzone przez Radę[128], a Europejskie Centrum Monitorowania Narkotyków i Narkomanii poczyniło postępy w zakresie uzgodnień roboczych z państwami trzecimi[129].



Zwalczanie przestępstw finansowych

[121] Europejski raport narkotykowy z 2020 r.: tendencje i zmiany, EMCDDA, 22.9.2020.
[122] Rozporządzenie (UE) 2017/2101 i dyrektywa (UE) 2017/2103.
[123] Austria, Finlandia, Irlandia, Portugalia i Słowenia.
[124] C/2020/5897; Dz.U. L 379 z 13.11.2020, s. 55.
[125] Organ zarządzający Biura Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC).
[126] COM(2019) 631.
[127] COM(2019) 624 i COM(2020) 659.
[128] W wyniku szczytu UE–Chiny, który odbył się w dniach 16–17 lipca 2018 r. w Pekinie, zawarto porozumienie w sprawie rozpoczęcia corocznego dialogu między UE a Chinami w sprawie środków odurzających. W dniu 30 października 2019 r. Coreper potwierdził warunki przyszłego dialogu. W dniu 5 marca 2020 r. Rada zatwierdziła nawiązanie nowego dialogu między UE a Iranem dotyczącego środków odurzających.
[129] Opinia Komisji w sprawie projektu uzgodnienia roboczego z Kosowem przyjęta w dniu 14 kwietnia 2020 r., i z Serbią – w dniu 16 grudnia 2019 r.

Aby wzmocnić zwalczanie przestępstw finansowych oraz prania pieniędzy, przyjęto nowe prawodawstwo. W 2019 r. przyjęto dyrektywę ułatwiającą korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania, która umożliwiła udzielanie dostępu do krajowych scentralizowanych rejestrów rachunków bankowych organom ścigania i biurom ds. odzyskiwania mienia na potrzeby zwalczania poważnych przestępstw. Dyrektywa ta ma również na celu poprawienie współpracy między organami ścigania i jednostkami analityki finansowej (FIU) oraz ułatwienie wymiany informacji między FIU. W czerwcu 2020 r. Komisja opublikowała sprawozdanie pt. „Odzyskiwanie i konfiskata mienia: Przestępstwa nigdy nie mogą się opłacać”[130]. Zwrócono w nim uwagę na możliwość większej harmonizacji systemów odzyskiwania mienia[131] w celu aktualizacji przepisów UE dotyczących odzyskiwania mienia i zwiększenia zdolności organów krajowych w zakresie zwalczania przestępczości zorganizowanej. W drodze badania zewnętrznego rozpoczęto dalszą analizę kwestii odzyskiwania mienia. Od dnia 19 grudnia 2020 r. zacznie obowiązywać rozporządzenie w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty[132] i znacząco wzmocni ono współpracę między państwami członkowskimi.

W maju 2020 r. Komisja przyjęła **plan działania na rzecz kompleksowej unijnej polityki zapobiegania praniu pieniędzy i finansowaniu terroryzmu**[133] w celu wzmocnienia ram UE. W dniu 5 listopada Rada przyjęła konkluzje w sprawie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[134], w których w szczególności wezwała Komisję do prowadzenia prac nad przyjęciem jednolitego zbioru przepisów, ustanowieniem niezależnego organu nadzoru i mechanizmu koordynacji jednostek analityki finansowej. Zgodnie z konkluzjami Rady w sprawie usprawniania dochodzeń finansowych[135] Komisja ocenia również konieczność integracji scentralizowanych rejestrów rachunków bankowych, co znacząco przyspieszyłoby uzyskiwanie dostępu przez jednostki analityki finansowej i organy ścigania do informacji o rachunkach bankowych. Jednocześnie nadal dąży się do zapewnienia skutecznego wdrożenia najnowszych norm UE przez państwa członkowskie. Przepisy na podstawie 5. dyrektywy w sprawie przeciwdziałania praniu pieniędzy mają na celu zapewnienie wyższego poziomu przejrzystości korporacyjnych struktur własnościowych. Termin transpozycji upłynął w dniu 1 stycznia 2020 r. i Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego wobec 16 państw członkowskich[136]. Kolejnym istotnym instrumentem jest nowe rozporządzenie w sprawie kontroli środków pieniężnych[137] przyjęte w październiku 2018 r. i mające zastosowanie od dnia 3 czerwca 2021 r. Usprawni ono istniejący system kontroli środków pieniężnych wwożonych do UE lub wywożonych z UE, a przepisy wykonawcze są opracowywane.

Jeżeli chodzi o wymiar zewnętrzny, kontynuowane są starania w celu wsparcia krajów partnerskich w przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. W tym kontekście ESDZ i delegatury Unii odgrywają zasadniczą rolę w promowaniu i wspieraniu

[130] COM(2020) 2017.
[131] W tym ocenę dyrektywy 2014/42/UE i decyzji Rady 2007/845/ WSiSW.
[132] Rozporządzenie (UE) 2018/1805.
[133] C(2020) 2800 final.
[134] Konkluzje Rady 12608/20.
[135] Konkluzje Rady 8927/20.
[136] Austrii, Belgii, Cypru, Czech, Grecji, Węgier, Estonii, Irlandii, Luksemburga, Niderlandów, Polski, Portugalii, Rumunii, Słowacji, Słowenii, Hiszpanii, jak również Zjednoczonego Królestwa.
[137] Rozporządzenie (UE) 2018/1672.

współpracy politycznej z państwami trzecimi oraz organizacjami międzynarodowymi, takimi jak Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF).

W uzupełnieniu tych prac Komisja uruchomiła globalny instrument na rzecz wsparcia krajów partnerskich poza UE w celu wprowadzenia skutecznych ram przeciwdziałania praniu pieniędzy/zwalczania finansowania terroryzmu zgodnych z normami międzynarodowymi. Celem tego działania, którego koszt wynosi 20 mln EUR, jest zachęcanie do współpracy między organami finansowymi i organami wymiaru sprawiedliwości na szczeblu krajowym, regionalnym i międzynarodowym.

Walka z korupcją

Korupcja sama w sobie jest przestępstwem i kluczowym czynnikiem umożliwiającym przestępczość zorganizowaną. Zapobieganie korupcji i walka z nią będą podlegać regularnemu monitorowaniu i ocenie w ramach przepisów państw członkowskich w oparciu o nowo ustawiony **mechanizm praworządności**[138]. W dniu 30 września 2020 r. przyjęto pierwsze ogólnounijne sprawozdanie na temat praworządności[139]. Wykazano w nim, że wiele państw członkowskich posiada wysokie standardy praworządności, ale nadal istnieją poważne wyzwania. Sprawozdanie obejmuje wszystkie państwa członkowskie wraz z obiektywnymi i faktycznymi rocznymi ocenami w celu rozwinięcia większej świadomości i zrozumienia zmian w poszczególnych państwach członkowskich w miarę ich zachodzenia, aby móc zidentyfikować ryzyko, opracować możliwe rozwiązania oraz ukierunkować wsparcie na wczesnym etapie. Na tym etapie **Prokuratura Europejska** (EPPO) będzie przeciwdziałać przestępstwom przeciwko budżetowi UE w uczestniczących, na tym etapie, 22 państwach UE. Będzie ona miała prawo do prowadzenia śledztw w odniesieniu do osób dopuszczających się przestępstw przeciwko budżetowi UE, takich jak oszustwa, korupcja lub poważne transgraniczne oszustwa związane z VAT, a także do ścigania takich osób i stawiania ich przed sądem. EPPO powinna rozpocząć działanie w pierwszym kwartale 2021 r.[140]

Obecnie Komisja dokonuje oceny transpozycji do prawa krajowego przepisów określonych w **dyrektywie w sprawie zwalczania nadużyć na szkodę interesów finansowych Unii za pośrednictwem prawa karnego**[141] i wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko państwom członkowskim, które nie zgłosiły pełnej transpozycji[142]. W 2021 r. Komisja przyjmie sprawozdanie oceniające zakres, w jakim państwa członkowskie przyjęły niezbędne środki, aby wdrożyć dyrektywę.

Walka z nielegalnym handlem dobrami kultury

Głównym celem **rozporządzenia w sprawie wprowadzania i przywozu dóbr kultury**[143], które przyjęto w czerwcu 2019 r., jest zapobieganie przywozowi do Unii dóbr kultury

[138] W ramach europejskiego mechanizmu praworządności zapewnia się proces dialogu na temat praworządności między Komisją a państwami członkowskimi, a także Radą i Parlamentem Europejskim oraz parlamentami narodowymi, społeczeństwem obywatelskim i innymi zainteresowanymi stronami. Rdzeniem tego nowego procesu są sprawozdania na temat praworządności.

[139] COM(2020) 580.

[140] Decyzja wykonawcza Rady, w której wyznaczono prokuratorów europejskich, weszła w życie w dniu 29 lipca 2020 r. Prokuratorzy europejscy tworzą kolegium, które odbyło swoje pierwsze posiedzenie w dniu 28 września 2020 r. Wkrótce EPPO przyjmie ustalenia robocze z Europolem, Eurojustem i OLAF-em.

[141] Dyrektywa (UE) 2017/1371.

[142] Postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego toczą się obecnie przeciwko Austrii, Irlandii, i Rumunii.

[143] Rozporządzenie (UE) 2019/880.

nielegalnie wywiezionych z ich państwa pochodzenia. Aby zapewnić prawidłowe wykonanie wspomnianego rozporządzenia, Komisja przygotowuje obecnie przyjęcie przepisów wykonawczych, w tym w odniesieniu do scentralizowanego systemu elektronicznego dotyczącego przywozu dóbr kultury, które umożliwią przechowywanie i wymianę informacji między państwami członkowskimi, a także niezbędne formalności dotyczące przywozu[144]. Ogólny zakaz wejdzie w życie przed końcem 2020 r., co zapewni systemom celnym państw członkowskich środek prawny do kontrolowania przesyłek, które mogą zawierać dobra kultury nielegalnie wywiezione z ich państwa pochodzenia, i podejmowania działań w odniesieniu do takich przesyłek.

Walka z nielegalnym handlem bronią palną

Dnia 24 lipca 2020 r. Komisja opublikowała **nowy plan działania UE w sprawie nielegalnego handlu bronią palną na lata 2020–2025**[145]. Podczas konferencji ministerialnej Ministerstw Spraw Zagranicznych i Ministerstw Spraw Wewnętrznych UE i Bałkanów Zachodnich na wysokim szczeblu, która miała miejsce dnia 31 stycznia 2020 r., podkreślono potrzebę dalszych działań ukierunkowanych na zwalczanie nielegalnego handlu bronią palną. Plan działania obejmuje konkretne działania mające na celu usprawnienie kontroli prawnej nad bronią palną, poprawę wiedzy na temat zagrożeń związanych z bronią palną oraz poprawę współpracy w zakresie egzekwowania prawa i współpracy międzynarodowej z naciskiem na Europę Południowo-Wschodnią. Komisja podjęła działania służące zapewnieniu pełnej transpozycji przez państwa członkowskie dyrektywy w sprawie kontroli nabywania i posiadania broni przyjętej w maju 2017 r.[146] 10 państw członkowskich wciąż nie zgłosiło jednak jeszcze pełnej transpozycji dyrektywy[147], a znaczna większość państw członkowskich nie transponowała jeszcze przepisów wykonawczych z nią związanych. W rezultacie Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego[148]. Komisja ocenia także szczegółowo zgłoszone krajowe środki wykonawcze, a w pierwszej połowie 2021 r. złoży sprawozdanie z wdrażania dyrektywy. Komisja rozpoczęła także ocenę ewentualnej modernizacji ram prawnych dotyczących środków w zakresie przywozu, wywozu i tranzytu broni palnej[149].

---

[144] System dotyczący przywozu dóbr kultury należy ustanowić najpóźniej do dnia 28 czerwca 2025 r. Komisja przyjęła pierwsze sprawozdanie z postępu prac nad opracowaniem systemu dotyczącego przywozu dóbr kultury. [COM(2020) 342].

[145] COM(2020) 608: ten nowy plan działania łączy w sobie francusko-niemiecką inicjatywę na rzecz Bałkanów Zachodnich pt. „Plan działania na rzecz trwałego rozwiązania kwestii nielegalnego posiadania i niewłaściwego wykorzystywania BSiL oraz amunicji do niej do 2024 r.”.

[146] Dyrektywa (UE) 2017/853. Kluczowe były także dwie dyrektywy wykonawcze z dnia 16 stycznia 2019 r., w których przewidziano specyfikacje techniczne dotyczące oznakowania oraz broni sygnałowej i alarmowej.

[147] Są to: Czechy, Dania, Hiszpania, Cypr, Luksemburg, Węgry, Polska, Słowenia, Słowacja i Szwecja.

[148] W odniesieniu do tej dyrektywy toczy się 25 postępowań (przeciwko Austrii, Belgii, Bułgarii, Cyprowi, Czechom, Danii, Niemcom, Estonii, Grecji, Hiszpanii, Finlandii, Francji, Węgrom, Irlandii, Litwie, Luksemburgowi, Łotwie, Malcie, Niderlandom, Polsce, Portugalii, Rumunii, Szwecji, Słowenii i Słowacji oraz przeciwko Zjednoczonemu Królestwu), a w odniesieniu do dyrektyw wykonawczych – 34 postępowania (w odniesieniu do dyrektywy 2019/68 – przeciwko Austrii, Belgii, Bułgarii, Cyprowi, Czechom, Niemcom, Grecji, Hiszpanii, Finlandii, Chorwacji, Węgrom, Irlandii, Włochom, Luksemburgowi, Polsce, Rumunii, Szwecji, Słowenii i Zjednoczonemu Królestwu; w odniesieniu do dyrektywy 2019/69 – przeciwko Bułgarii, Cyprowi, Czechom, Grecji, Hiszpanii, Finlandii, Chorwacji, Węgrom, Irlandii, Włochom, Luksemburgowi, Niderlandom, Polsce, Rumunii, Szwecji, Słowenii oraz Zjednoczonemu Królestwu).

[149] Zgodnie z rozporządzeniem (UE) nr 258/2012.

Walka z handlem ludźmi

W strategii w zakresie unii bezpieczeństwa podkreślono potrzebę opracowania nowego strategicznego podejścia do wyeliminowania handlu ludźmi w kontekście Agendy na rzecz zwalczania przestępczości zorganizowanej. Ponadto, jak określono w art. 20 dyrektywy w sprawie zapobiegania handlowi ludźmi[150], Komisja opublikowała w październiku 2020 r. swoje trzecie sprawozdanie w sprawie postępów w dziedzinie zwalczania handlu ludźmi[151].

Świadczy to o postępach we współpracy transnarodowej, transgranicznym egzekwowaniu przepisów i działaniach operacyjnych w zakresie sądownictwa; tworzeniu krajowych i transnarodowych mechanizmów ukierunkowanej pomocy dla ofiar oraz opracowywaniu bazy wiedzy na temat zjawiska handlu ludźmi. Państwa członkowskie w coraz większym stopniu wykorzystują unijne agencje do celów wymiany informacji i prowadzenia wspólnych działań, a wspólne zespoły śledcze do zwalczania handlu ludźmi zarówno w UE, jak i poza jej granicami[152]. Współpraca operacyjna przyniosła wymierne rezultaty, zwłaszcza w ramach europejskiej multidyscyplinarnej platformy przeciwko zagrożeniom przestępstwami. W 2019 r. wyniki tych działań były następujące: 825 aresztowań oraz identyfikacja 8 824 podejrzanych i 1 307 potencjalnych ofiar, w tym 69 dzieci. Zidentyfikowano lub zlikwidowano 94 zorganizowane grupy przestępcze zaangażowane w te przestępstwa oraz zamrożono 1,5 mln EUR środków na rachunkach bankowych, w przedsiębiorstwach i domenach internetowych. Podczas Europejskiego Dnia Przeciwdziałania Handlowi Ludźmi przypadającego dnia 18 października 2020 r. Komisja opublikowała badanie na temat

[150] Dz.U. L 101 z 15.4.2011, s. 1.

[151] COM(2020) 661 final. Komunikat uzupełniony badaniem w zakresie gromadzenia danych dotyczących handlu ludźmi w UE w latach 2017–2018.

[152] Na przykład Europejski Urząd ds. Pracy współpracował z Europolem w celu zwalczania handlu ludźmi w UE powiązanego ze wszystkimi formami wykorzystywania, w tym wykorzystywaniem seksualnym i wyzyskiem pracowników, a także wszelkimi formami handlu dziećmi. Współpraca ta jest także formą uznania protokołu Międzynarodowej Organizacji Pracy dotyczącego pracy przymusowej (P29). Protokół ten stanowi podstawową normę dotyczącą pracy, w której określa się pracę przymusową jako przestępstwo; odnosi się on do zapobiegania pracy przymusowej, ochrony ofiar, kompensaty i współpracy międzynarodowej w zakresie obecnych form pracy przymusowej, w tym w związku z handlem ludźmi.

kosztów handlu ludźmi oraz badanie na temat krajowych i ponadnarodowych mechanizmów ukierunkowanej pomocy[153].

Przemyt migrantów

Europejskie Centrum Zwalczania Przemytu Migrantów zgłosiło stały wzrost, jeżeli chodzi o działania związane z **przemytem migrantów**, głównie na Bałkanach Zachodnich i w państwach sąsiadujących, a także w ramach wtórnych przepływów migrantów na obszarze UE. W 2019 r. Europol przyczynił się do wykrycia 14 218 podejrzanych działających w obszarze przemytu migrantów[154]. W maju 2020 r. Eurojust uruchomił grupę dyskusyjną prokuratorów zajmujących się kwestią przemytu migrantów; jest to ważna platforma umożliwiająca regularne spotkania najważniejszych przedstawicieli sądownictwa z państw członkowskich UE na szczeblu krajowym oraz wspierająca ich wspólną reakcję operacyjną[155].

Walka z przestępstwami przeciwko środowisku

Przestępstwa przeciwko środowisku obejmują czyny, które naruszają przepisy dotyczące ochrony środowiska i powodują lub mogą powodować szkody lub ryzyko dla środowiska i zdrowia ludzkiego[156]. Jednymi z najważniejszych **przestępstw przeciwko środowisku** są nielegalna emisja lub uwalnianie substancji do atmosfery, wody lub gleby, nielegalny handel dziką fauną i florą, nielegalny handel substancjami zubożającymi warstwę ozonową oraz nielegalne przemieszczanie lub składowanie odpadów. W przeprowadzonej niedawno ocenie dyrektywy w sprawie przestępstw przeciwko środowisku[157] wykazano, że postępom w opracowywaniu europejskich ram nie towarzyszyły znaczące efekty w terenie, w tym pod względem lepszej współpracy transgranicznej i wyrównania poziomu sankcji we wszystkich państwach członkowskich. W szczególności nie przyczyniła się ona do wzrostu liczby wyroków skazujących oraz nakładania bardziej odstraszających sankcji w państwach członkowskich. W związku z tym podjęto decyzję o przeprowadzeniu przeglądu dyrektywy do końca 2021 r.

W dniach 29–30 października 2019 r. Eurojust – wraz z Europejską Siecią Prokuratorów ds. Przestępczości przeciwko Środowisku (ENPE) – zorganizował konferencję pt. „Współpraca międzynarodowa w walce z przestępstwami przeciwko środowisku", której celem było zwiększanie świadomości i promowanie współpracy transgranicznej w odniesieniu do przestępstw przeciwko środowisku wśród prokuratorów i innych praktyków w UE i poza jej granicami.

Obecnie trwa ocena przyjętego w 2016 r. Planu działania przeciwko nielegalnemu handlowi dziką fauną i florą. Szczególnym działaniem jest projekt trwający do stycznia 2021 r. i ukierunkowany na nielegalny handel dziką fauną i florą w UE i przez jej teren z wykorzystaniem internetu i usług dostarczania przesyłek, którego celem jest zwalczanie i likwidowanie sieci cyberprzestępczości dotyczącej dzikiej fauny i flory[158].

---

[153] Badania na temat kosztów gospodarczych, społecznych i ludzkich handlu ludźmi oraz przegląd funkcjonowania krajowych i ponadnarodowych mechanizmów ukierunkowanej pomocy państw członkowskich są dostępne pod adresem: https://ec.europa.eu/anti-trafficking

[154] Europejskie Centrum Zwalczania Przemytu Migrantów, 4. roczne sprawozdanie z działalności, 15 maja 2020 r.

[155] http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx

[156] Dyrektywa 2008/99/WE w sprawie ochrony środowiska poprzez prawo karne.

[157] SWD(2020) 259 final.

[158] https://wwf.be/fr/wildlife-cybercrime/

V. SILNY EUROPEJSKI EKOSYSTEM BEZPIECZEŃSTWA

Rzeczywista i skuteczna unia bezpieczeństwa musi być wspólnym przedsięwzięciem wszystkich grup społecznych. Uczestniczyć w niej muszą rządy, organy ścigania, sektor prywatny, system oświaty i szkolnictwa i sami obywatele. Należy zapewnić im odpowiednie narzędzia i wzajemne połączenia w celu budowania gotowości i odporności dla wszystkich, w szczególności osób w najtrudniejszej sytuacji, ofiar oraz świadków.

1. Współpraca i wymiana informacji

Jednym z najważniejszych sposobów, w jaki UE może przyczynić się do ochrony obywateli, jest ułatwianie skutecznej współpracy podmiotów odpowiedzialnych za bezpieczeństwo. Współpraca i wymiana informacji to potężne narzędzia do walki z przestępczością i terroryzmem, z zagrożeniami takimi jak te dotyczące cyberbezpieczeństwa, oraz dążenia do sprawiedliwości. W celu wspierania wymiany danych między organami ścigania i organami wymiaru sprawiedliwości wdrożono szereg narzędzi.

Dziś Komisja przyjmuje zmieniony mandat dla **Europolu**[159], aby wprowadzić do jego pracy szereg ukierunkowanych usprawnień. Zapewni to Europolowi lepsze możliwości, jeżeli chodzi o radzenie sobie ze zmieniającym się charakterem przestępstw popełnianych za pośrednictwem internetu, a także z przestępstwami finansowymi. Pozwoli to wzmocnić współpracę z sektorem prywatnym oraz dostosować przepisy dotyczące ochrony danych osobowych do istniejących przepisów UE.

Europol oraz inne agencje UE takie jak Frontex, CEPOL i Eurojust, przy wsparciu ze strony Komisji, w dalszym ciągu rozwijają unijny cykl polityki odnoszący się do poważnej i zorganizowanej przestępczości międzynarodowej – **europejską multidyscyplinarną platformę przeciwko zagrożeniom przestępstwami** (EMPACT)[160]. Współpraca w ramach EMPACT stale okazuje się skutecznym narzędziem zwalczania przestępczości zorganizowanej w całej Europie, tak jak na przykład podczas dni wspólnego działania we wrześniu, w październiku i listopadzie 2020 r.[161] Pokazuje to wyraźnie, jaka jest wartość współpracy. Współpraca ta przyczynia się także do osiągania mniej wymiernych celów takich jak: lepszy obraz sytuacji na podstawie danych wywiadowczych, szkolenia i budowanie zdolności, zapobieganie, współpraca z partnerami spoza UE oraz walka z przestępczością internetową[162]. Na podstawie niezależnej oceny w ramach cyklu polityki

---

[159] COM (2020) 796.

[160] EMPACT to unijne narzędzie współpracy policyjnej, którego celem jest przeciwdziałanie najważniejszym zagrożeniom dla bezpieczeństwa UE przez wzmocnienie współpracy między właściwymi służbami państw członkowskich, instytucjami oraz agencjami Unii, a także państwami trzecimi i organizacjami. EMPACT łączy różne zainteresowane strony (podejście wielodyscyplinarne), aby usprawniać i wzmacniać współpracę między państwami członkowskimi, instytucjami oraz agencjami Unii, a także państwami trzecimi i organizacjami, uwzględniając sektor prywatny.

[161] Dni wspólnego działania EMPACT: „operacja BOSPHORUS" – przechwycono 1 776 sztuk broni palnej (2–11 listopada); dni wspólnego działania „Mobile 3" – odzyskano ponad 350 skradzionych samochodów i ponad 1 000 skradzionych samochodowych części zamiennych (12–13 października); „Dni wspólnego działania przeciwko handlowi ludźmi w celach wyzysku pracowników" – funkcjonariusze zidentyfikowali 715 potencjalnych ofiar wyzysku pracowników (14–20 września); „Dni wspólnego działania przeciwko przestępczości w Europie Południowo-Wschodniej" – 51 sztuk różnego rodzaju broni i 47 kilogramów różnych rodzajów narkotyków (wrzesień).

[162] Wszystkie szczegółowe arkusze informacyjne dotyczące wyników wraz z danymi, w podziale na unijne priorytety dotyczące przestępczości w ramach EMPACT, można znaleźć pod adresem: https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf, dok. 7623/20, 5 maja 2020 r.

UE na lata 2018–2021/EMPACT w 2020 r.[163] wykazano, że współpraca w ramach EMPACT jest coraz bardziej istotna i skuteczna, jeżeli chodzi o najpilniejsze zagrożenia, jakie tworzą zorganizowane grupy przestępcze. Wartość dodana wynika z zapewnienia platformy współpracy, która umożliwia państwom członkowskim osiągnięcie lepszych wyników w walce z poważną i zorganizowaną przestępczością, niż byłoby to możliwe w przypadku indywidualnej walki z tym problemem. W ocenie zaznaczono także możliwości i wymieniono zalecenia dotyczące dalszego rozwijania tego bardzo pożytecznego narzędzia współpracy w kolejnym cyklu na lata 2022–2025.

W 2021 r. Komisja uruchomi inicjatywę dotyczącą **unijnego kodeksu współpracy policyjnej**, aby usprawnić, poprawić, rozwinąć, zmodernizować i ułatwić współpracę w zakresie egzekwowania przepisów między właściwymi agencjami krajowymi. Będzie to dla państw członkowskich ogromne wsparcie w ich walce z poważną i zorganizowaną przestępczością oraz terroryzmem.

Niezbędna jest także współpraca między **policją a innymi kluczowymi organami ścigania**, a także z agencjami takimi jak organy celne. Unijne **organy celne** pełnią kluczową rolę, jeżeli chodzi o zapewnianie bezpieczeństwa granic zewnętrznych i łańcucha dostaw, a tym samym przyczyniają się do bezpieczeństwa wewnętrznego Unii Europejskiej. Nowe i zmieniające się zagrożenia dotyczą najważniejszych powiązań między organami celnymi a organami ścigania, co podkreśla w szczególności wartość w postaci „wykrywania/zapobiegania", jaką niosą za sobą kontrole celne, a także wiodącą rolę organów celnych w odniesieniu do towarów. Komisja wspiera współpracę między organami celnymi a Europolem[164], która będzie miała bezpośredni wpływ na działania w dziedzinach obejmujących broń palną, przestępstwa przeciwko środowisku, finansowanie działań przestępczych i cyberprzestępstw, a także zachęca do tej współpracy. Organy celne uczestniczą obecnie w kilku zorganizowanych przez Europol działaniach przeciwko poważnej i międzynarodowej zorganizowanej przestępczości[165], a także w szkoleniach CEPOL. Działania te pomagają w promowaniu i dalszym rozwijaniu współpracy między agencjami oraz w usprawnianiu interakcji między kluczowymi podmiotami.

Silne i skuteczne systemy informacyjne są niezbędne, aby usprawnić wymianę informacji między organami wymiaru sprawiedliwości a organami ścigania w całej UE. Również **System Informacyjny Schengen (SIS)** wzmocniono za pośrednictwem zaktualizowanych przepisów, które eliminują potencjalne luki poprzez ustanowienie dodatkowych kategorii ostrzeżeń, rozszerzenie wykazu obiektów, w odniesieniu do których można wprowadzać ostrzeżenia, a także poprzez umożliwienie wprowadzania

[163] W konkluzjach Rady z dnia 27 marca 2017 r. w sprawie kontynuacji cyklu polityki unijnej dotyczącej poważnej i zorganizowanej przestępczości międzynarodowej na lata 2018–2021 przewidziano przeprowadzenie niezależnej oceny (7704/17).

[164] Zob. na przykład plan działania Grupy Roboczej ds. Współpracy Celnej. Najważniejsze obszary na lata 2020–2021 obejmują: zwiększoną obecność funkcjonariuszy celnych w biurach łącznikowych w Europolu, bezpośredni dostęp organów celnych do aplikacji sieci bezpiecznej wymiany informacji (SIENA) Europolu, lepszą reprezentację funkcjonariuszy celnych w jednostkach krajowych Europolu oraz udział szefów policji i organów celnych w Europejskiej Konwencji Szefów Policji.

[165] Przestępstwa dotyczące akcyzy/oszustwa związane z VAT, nielegalny handel bronią palną, przestępstwa przeciwko środowisku, finansowanie działań przestępczych, walka z niegodziwym traktowaniem dzieci w celach seksualnych.

nowych rodzajów danych[166]. Nowe przepisy weszły w życie w dniu 28 grudnia 2018 r. i powinny być w pełni operacyjne do grudnia 2021 r.[167]

Podobnie w 2019 r. do **europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS)** dodano dodatkowy system umożliwiający skuteczną wymianę informacji z rejestrów karnych dotyczących obywateli państw trzecich skazanych w UE (ECRIS-TCN). Obecnie trwają prace nad technicznym rozwojem i wdrożeniem tego nowego scentralizowanego systemu, a jego wejście w życie zaplanowano na 2023 r.

Dnia 24 lipca 2020 r. Komisja przyjęła sprawozdanie dotyczące przeglądu dyrektywy w sprawie danych dotyczących przelotu pasażera (PNR)[168], dokonując przeglądu pierwszych dwóch lat stosowania dyrektywy w sprawie PNR[169]. Ze wspomnianego sprawozdania wynika, że prace nad ogólnounijnym systemem PNR są mocno zaawansowane. Wykorzystywanie danych PNR ma kluczowe znaczenie w walce z terroryzmem oraz poważną i zorganizowaną przestępczością i już przyniosło wymierne rezultaty. Tylko jedno państwo członkowskie nie zgłosiło jeszcze Komisji dokonania pełnej transpozycji[170]. Dnia 3 grudnia 2020 r. Komisja przesłała uzasadnioną opinię w związku z brakiem powiadomienia o dokonaniu pełnej transpozycji dyrektywy.

Dnia 9 września 2020 r. Komisja opublikowała ocenę **dyrektywy w sprawie danych pasażera przekazywanych przed podróżą** z 2004 r.[171] W ocenie tej podkreślono szereg niedociągnięć i niespójności, które zostaną uwzględnione podczas zbliżającego się przeglądu bieżących ram legislacyjnych. Innym kluczowym instrumentem, który podlega dalszej ocenie, są **decyzje w sprawie konwencji z Prüm**[172], które mają zostać rozpatrzone w świetle zmian operacyjnych, zmian w zakresie technologii, kryminalistyki i ochrony danych.

Współpraca musi także sięgać poza granice UE, aby zaangażować **najważniejsze państwa trzecie w walkę z terroryzmem i przestępczością zorganizowaną**. Dnia 13 maja 2020 r. Rada zezwoliła na otwarcie negocjacji z Nową Zelandią w odniesieniu do wymiany danych osobowych między Europolem a Nową Zelandią. Trwają negocjacje z Turcją, jednak nie osiągnięto żadnych postępów w negocjacjach dotyczących wymiany danych osobowych w celu zwalczania poważnych przestępstw i terroryzmu z Algierią, Egiptem, Izraelem, Jordanią, Libanem, Marokiem, Tunezją. Ponadto dnia 19 listopada 2020 r. Komisja przyjęła zalecenie dotyczące decyzji Rady w sprawie zezwolenia na otwarcie negocjacji dotyczących porozumienia między Unią Europejską a dziesięcioma państwami trzecimi w sprawie współpracy między Eurojustem a tymi państwami trzecimi w odniesieniu do wymiany danych osobowych[173].

Jeżeli chodzi o **współpracę międzynarodową w zakresie wymiany danych PNR** do celów zwalczania terroryzmu i poważnej przestępczości, Rada zezwoliła na rozpoczęcie

[166] Rozporządzenie (UE) 2018/1860, rozporządzenie (UE) 2018/1861, rozporządzenie (UE) 2018/1862.
[167] SIS zostanie zaktualizowany także zgodnie z zaproponowanymi zmianami w rozporządzeniu w sprawie Europolu (COM(2020) XXX).
[168] COM(2020) 305.
[169] Dyrektywa (UE) 2016/681.
[170] Słowenia.
[171] SWD(2020) 174.
[172] Ramy z Prüm umożliwiają automatyczną wymianę danych dotyczących DNA, odcisków palców i danych rejestracyjnych pojazdów między organami ścigania. Opublikowano wstępną ocenę skutków.
[173] Proponuje się następujące państwa trzecie: Algieria, Armenia, Bośnia i Hercegowina, Egipt, Izrael, Jordania, Liban, Maroko, Tunezja i Turcja, COM(2020) 743 final.

negocjacji z Japonią w sprawie podpisania umowy PNR[174]. W międzyczasie *finalizowane są* **wspólne oceny istniejących umów między UE a USA i UE a Australią**. Komisja rozpoczęła również proces przeglądu swojego obecnego ogólnego podejścia do przekazywania danych PNR do państw trzecich[175].

Komisja współpracuje również z ONZ w celu zwiększenia zdolności krajów partnerskich do zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania, poprzez gromadzenie i analizowanie danych dotyczących pasażerów, zarówno danych pasażera przekazywanych przed podróżą, jak i danych dotyczących przelotu pasażera.

Komisja zaangażowała się w proces ułatwiania przekazywania danych dotyczących przelotu pasażera zgodnie z wymogami prawnymi UE w ramach nowych norm dotyczących danych PNR[176] przyjętych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO)[177]. Dnia 23 czerwca 2020 r. Rada Organizacji Międzynarodowego Lotnictwa Cywilnego przyjęła nowe normy i zalecane metody postępowania (SARPs) dotyczące danych PNR[178], a umawiające się strony mają czas do dnia 30 stycznia 2021 r. na poinformowanie ICAO o wszelkich różnicach między krajowymi praktykami regulacyjnymi a nowymi normami i zalecanymi metodami postępowania dotyczącymi danych PNR.

2. Znaczenie silnych granic zewnętrznych

Nowoczesne i skuteczne zarządzanie granicami zewnętrznymi ma kluczowe znaczenie dla zapewnienia bezpieczeństwa obywateli Unii. Zaangażowanie wszystkich właściwych podmiotów w celu jak najlepszego wykorzystania służb granicznych i zapewnienia im odpowiednich narzędzi może mieć rzeczywisty wpływ na zapobieganie przestępczości transgranicznej i terroryzmowi. W nowym pakcie o migracji i azylu[179] podkreślono również potrzebę solidnego i sprawiedliwego zarządzania granicami zewnętrznymi, obejmującego kontrole tożsamości, stanu zdrowia i bezpieczeństwa. Jest to część kompleksowego podejścia pokazującego, jak polityka w zakresie migracji, azylu, integracji i zarządzania granicami zależy od postępów na wszystkich frontach.

W nowym pakcie podkreślono, że skuteczna strefa Schengen jest niezbędna dla polityki migracyjnej, a także ma poważne konsekwencje dla bezpieczeństwa. Kwestię tę omówiono podczas pierwszego forum Schengen, które odbyło się dnia 30 listopada 2020 r. Przedstawiciele państw członkowskich i Parlamentu Europejskiego zgodzili się, że ważne jest, aby Schengen skutecznie służyło obywatelom pod względem swobodnego przepływu, a także pod względem bezpieczeństwa. Proces ten zostanie uwzględniony w nowej strategii dotyczącej strefy Schengen, która zostanie przedstawiona w 2021 r. Mechanizm oceny i monitorowania dorobku Schengen jest kluczowym narzędziem zapewniającym wzajemne zaufanie oraz gwarantującym lepsze i spójne wdrażanie dorobku Schengen, w tym jego

---

[174] 18 lutego 2020 r.

[175] Plan działania dotyczący zewnętrznego wymiaru polityki UE w zakresie danych dotyczących przelotu pasażera, dostępny pod adresem: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-

[176] Decyzja Rady (UE) 2019/2107.

[177] Rezolucja Rady Bezpieczeństwa ONZ nr 2396 (2017).

[178] Określane jako poprawka 28 do załącznika 9 (Ułatwienia) do Konwencji o międzynarodowym lotnictwie cywilnym („konwencja chicagowska").

[179] COM(2020) 609.

wpływ na bezpieczeństwo. Był to ważny temat sprawozdania przyjętego w dniu 25 listopada[180], przedstawiającego stan wdrażania dorobku Schengen oraz podsumowującego funkcjonowanie mechanizmu oceny i monitorowania dorobku Schengen.

Rozporządzenia w sprawie interoperacyjności[181] mają skutkować tym, że istniejące oraz nowe lub zmodernizowane systemy informacyjne UE w obszarze bezpieczeństwa, zarządzania granicami i migracjami będą współpracowały ze sobą w bardziej inteligentny i skuteczniejszy sposób. Interoperacyjność systemów informacyjnych UE poprawi skuteczność i efektywność kontroli na granicach zewnętrznych, przyczyni się do zapobiegania imigracji nieuregulowanej, a także do wysokiego poziomu bezpieczeństwa. Zapewni cenne dodatkowe narzędzie dla organów ścigania i służb granicznych[182]. Państwa członkowskie, państwa stowarzyszone w ramach Schengen oraz odpowiednie agencje Unii (eu-LISA, Europejska Agencja Straży Granicznej i Przybrzeżnej oraz Europol) muszą być gotowe, a Komisja monitoruje przygotowania i gotowość, aby zapewnić pełne wdrożenie do końca 2023 r.

Dnia 8 Grudnia 2020 r. współprawodawcy osiągnęli wstępne porozumienie w sprawie wniosku dotyczącego **aktualizacji wizowego systemu informacyjnego[183]**.

Nadal konieczne jest jednak przyjęcie niektórych kluczowych aktów prawnych. Parlament Europejski musi sfinalizować swoją gotowość do współpracy z Radą w sprawie zmian[184] dotyczących europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS)[185].

Powiązania między odpowiednimi systemami informacyjnymi do analizy ryzyka związanego z bezpieczeństwem mają kluczowe znaczenie dla zwiększenia bezpieczeństwa. Wzmocnienie **współpracy między organami celnymi i organami zarządzającymi granicami** oraz synergii między ich **systemami informacyjnymi** zgodnie z odpowiednimi mechanizmami kontroli i równowagi, w tym ochroną danych osobowych i przepisami dotyczącymi prywatności, jest priorytetem planu działania z dnia 28 września 2020 r. na rzecz wprowadzenia unii celnej na kolejny poziom[186] W ramach wstępnej oceny przeprowadzonej przez Komisję wraz z ekspertami policyjnymi i celnymi z państw członkowskich zalecono w szczególności połączenie Systemu Informacyjnego Schengen (SIS) i danych Europolu z systemem kontroli importu 2 w ramach UKC (ICS2)[187], a obecnie zostanie rozpoczęte studium wykonalności.

Rozporządzenie w sprawie Europejskiej Straży Granicznej i Przybrzeżnej[188] weszło w życie w grudniu 2019 r. i zapewnia istotny przegląd potencjału i narzędzi UE służących wzmocnieniu granic zewnętrznych UE. Pozwoli to znacznie zwiększyć wkład granic w bezpieczeństwo. Nowy mandat wzmacnia zdolność Fronteksu do wspierania państw

[180] SWD(2020) 327 final.
[181] Rozporządzenie (UE) 2019/817 i rozporządzenie (UE) 2019/818.
[182] Istniejące systemy: System Informacyjny Schengen (SIS), wizowy system informacyjny (VIS), Eurodac i przyszłe systemy: system wjazdu/wyjazdu, europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS), europejski system przekazywania informacji z rejestrów karnych dotyczących obywateli państw trzecich (ECRIS-TCN).
[183] COM(2019) 12.
[184] COM(2019) 3 final oraz COM(2019) 4 final.
[185] Rozporządzenie (UE) 2018/1240 i rozporządzenie (UE) 2018/1241.
[186] COM(2020) 581.
[187] System wyprzedzającej informacji o towarach wykorzystywany do wczesnej oceny ryzyka dla bezpieczeństwa wszystkich przepływów towarów przekraczających granicę zewnętrzną.
[188] Rozporządzenie (UE) 2019/1896.

członkowskich w zarządzaniu granicami zewnętrznymi i powrotami oraz rozszerza możliwości współpracy z państwami trzecimi. Trwają prace mające na celu zapewnienie gotowości stałej służby Europejskiej Straży Granicznej i Przybrzeżnej do jej pierwszego rozmieszczenia z dniem 1 stycznia 2021 r.

W czerwcu 2019 r. UE wprowadziła **zaostrzone normy dotyczące zabezpieczeń dowodów tożsamości**, aby ułatwić swobodny przepływ obywateli Unii i jednocześnie ograniczyć oszustwa dotyczące tożsamości[189]. Państwa członkowskie są zobowiązane do rozpoczęcia wydawania dowodów osobistych i dokumentów pobytowych zgodnie z nowymi normami dotyczącymi zabezpieczeń od sierpnia 2021 r. Większość z nich jest obecnie w trakcie dostosowywania swoich projektów dokumentów do wymogów rozporządzenia.

3. Wspieranie badań naukowych i innowacji w dziedzinie bezpieczeństwa

Badania nad bezpieczeństwem i promowanie innowacji stanowią podstawę skoordynowanej odpowiedzi UE na złożone wyzwania i pozwalają na podjęcie konkretnych kroków w celu ograniczenia ryzyka. Unia bezpieczeństwa jest jednym z czterech obszarów priorytetowych w ramach programu prac 2018–2020 dla programu **„Horyzont 2020”**[190], który odpowiada za 50 % wszystkich funduszy publicznych na badania nad bezpieczeństwem w UE. W 2019 r. zaproszenia do podjęcia badań nad bezpieczeństwem w ramach programu „Horyzont 2020” skutkowały wyborem 42 projektów, które miały otrzymać w sumie 253 mln EUR z finansowania unijnego. Prace obejmą ochronę infrastruktury, zwiększenie odporności na klęski żywiołowe, zwalczanie przestępczości i terroryzmu oraz zabezpieczenie granic zewnętrznych, jak również poprawę bezpieczeństwa cyfrowego. Orientacyjny budżet dostępny na projekty w 2020 r. wynosi 265 mln EUR. Obejmuje to zaproszenie do składania wniosków w zakresie sztucznej inteligencji o wartości 20 mln EUR, które wesprze europejskie organy ścigania w zwiększaniu zdolności w zakresie AI, uzupełnieniu niedoboru kwalifikacji w tym zakresie oraz pobudzeniu współpracy. Prace przygotowywane w ramach nowego programu ramowego w zakresie badań „Horyzont Europa” będą wspierać wdrażanie strategii UE w zakresie unii bezpieczeństwa, jak również zarządzanie granicami i wymiar bezpieczeństwa w ramach nowego paktu o migracji i azylu, polityki UE w zakresie zmniejszania ryzyka związanego z klęskami żywiołowymi oraz strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego[191].

Finansowane przez UE badania nad bezpieczeństwem okazały się również skuteczne w promowaniu współpracy i wspieraniu praktyków w dziedzinie bezpieczeństwa podczas pandemii COVID-19[192]. Wsparcie obejmuje narzędzia do wspólnej oceny i badania ryzyka i zagrożeń epidemiologicznych oraz związanych z przestępczością.

Aby zapewnić wykorzystanie **innowacyjnych projektów**, agencje UE muszą wpisać się w istniejący krajobraz badań naukowych i innowacji w dziedzinie bezpieczeństwa.

---

[189] Rozporządzenie (UE) 2019/1157.

[190] UE przeznaczyła środki finansowe w wysokości około 91 mln EUR na projekty zwiększające ochronę infrastruktury, w tym połączone zagrożenia dla cyberbezpieczeństwa i zagrożenia fizyczne, usprawnione i szybkie reagowanie na incydenty oraz lepszą wymianę informacji.

[191] W ramach programu „Horyzont Europa” klaster 3 będzie służył w szczególności wsparciu priorytetu politycznego Komisji – Promowanie naszego europejskiego stylu życia, a także Europejskiego Zielonego Ładu i Europy na miarę ery cyfrowej.

[192] Z działaniami w ramach programu „Horyzont 2020” wspierającymi reakcję na pandemię można zapoznać się na stronie internetowej: https://www.researchgate.net/publication/341287556

W następstwie posiedzenia Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w październiku 2019 r. agencje UE i Wspólne Centrum Badawcze Komisji tworzą obecnie **europejskie centrum innowacji na rzecz bezpieczeństwa wewnętrznego** na podstawie istniejących mandatów prawnych, które ma służyć jako sieć współpracy ich innowacyjnych laboratoriów. Centrum będzie mechanizmem koordynacyjnym wspierającym uczestniczące podmioty w dzieleniu się informacjami i wiedzą, tworzeniu wspólnych projektów oraz upowszechnianiu ustaleń i opracowanych rozwiązań technologicznych istotnych dla bezpieczeństwa wewnętrznego[193].

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji stanowią odpowiedź Europy na wspieranie innowacji i polityki przemysłowej w dziedzinie cyberbezpieczeństwa. Mają one na celu wzmocnienie europejskich zdolności w zakresie cyberbezpieczeństwa, ochronę gospodarki i społeczeństwa przed cyberatakami, utrzymanie doskonałości badawczej oraz wzmocnienie konkurencyjności UE. Obecnie trwają rozmowy trójstronne.

4. Podnoszenie umiejętności i świadomości

Świadomość kwestii związanych z bezpieczeństwem oraz nabywanie umiejętności radzenia sobie z potencjalnymi zagrożeniami są niezbędne do budowania bardziej odpornego społeczeństwa charakteryzującego się lepszym przygotowaniem przedsiębiorstw, administracji i osób fizycznych. Istotny jest również dostęp ofiar do przysługujących im praw.

Pracownicy organów ścigania i wymiaru sprawiedliwości

Ograniczenia związane z COVID-19 miały poważny wpływ na CEPOL, która była zobowiązana do anulowania wszystkich planowanych działań stacjonarnych od marca 2020 r. Te szczególne okoliczności spowodowały również rosnący popyt na usługi online; w pierwszych czterech miesiącach roku Agencja odnotowała 30-procentowy wzrost aktywności wirtualnej i 100-procentowy wzrost liczby użytkowników online. Wśród priorytetowych obszarów szkoleniowych na lata 2019–2021[194] znajduje się zwalczanie nielegalnej imigracji, terroryzmu, handlu ludźmi i cyberprzestępczości oraz niegodziwego traktowania dzieci w celach seksualnych. Komisja przygotowuje obecnie ocenę CEPOL-u, która ma zostać zakończona do lipca 2021 r.

Ogół społeczeństwa

W 2018 r. w Dniu Bezpiecznego Internetu uruchomiono kampanię #SaferInternet4EU. Działania te dotarły do niemal 63 milionów osób w UE w ciągu ostatnich 2 lat i obejmują nagrody, wsparcie dla nauczycieli oraz higienę cyberbezpieczeństwa. Sieć centrów bezpieczniejszego internetu zapewniła ponad 1 800 nowych zasobów obejmujących takie tematy jak fałszywe informacje, cyberprzemoc, troska o prywatność, nagabywanie dzieci dla celów seksualnych i higiena cyberbezpieczeństwa.

[193] Dnia 21 lutego 2020 r. Stały Komitet Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego potwierdził deklarację misji, główne cechy, zadania i zarządzanie europejskim centrum innowacji na rzecz bezpieczeństwa wewnętrznego.

[194] Ocena strategicznych potrzeb szkoleniowych Unii Europejskiej (STNA) na lata 2018–2021 sprawozdanie UE-STNA, CEPOL.

W październiku 2020 r. odbył się 8. Europejski **Miesiąc Cyberbezpieczeństwa** mający na celu promowanie bezpieczeństwa w internecie w UE. Tegoroczna kampania miała na celu rozwiązanie problemów związanych z bezpieczeństwem, wynikających z transformacji cyfrowej życia codziennego przyspieszonej przez pandemię COVID-19. W ramach kampanii promującej podejście „Pomyśl, zanim klikniesz" („Think Before U Click") zwrócono uwagę na różne tematy związane z cyberbezpieczeństwem, aby pomóc użytkownikom w identyfikacji zagrożeń dla cyberbezpieczeństwa i przygotowaniu się na te zagrożenia. Trwają przygotowania do europejskiego wyzwania dotyczącego cyberbezpieczeństwa w 2021 r. w Pradze.

Kluczowym narzędziem pomagającym ofiarom cyberprzestępczości jest „No More Ransom"[195], bezpłatne repozytorium narzędzi rozszyfrowujących, które pomaga ofiarom w walce bez płacenia hakerom. Narzędzie to – wspierane przez Centrum ds. Walki z Cyberprzestępczości Europolu, które w lipcu 2020 r. obchodziło swoją czwartą rocznicę powstania – od czasu uruchomienia zarejestrowało ponad 4,2 mln odwiedzających ze 188 państw. Dzięki niemu żądany okup o szacowanej wartości 632 mln USD nie trafił ostatecznie do kieszeni przestępców.

Dnia 1 lipca 2020 r. Komisja przedstawiła **europejski program na rzecz umiejętności**[196] służący zrównoważonej konkurencyjności, sprawiedliwości społecznej i odporności. Wyznaczono w nim ambitne cele ilościowe dotyczące poprawy istniejących umiejętności i szkoleń w zakresie nowych umiejętności, które mają zostać osiągnięte w ciągu najbliższych 5 lat. Obejmuje to specjalne działania mające na celu zwiększenie liczby absolwentów nauk ścisłych, technologii, inżynierii, sztuki i matematyki potrzebnych w nowatorskich dziedzinach, takich jak cyberbezpieczeństwo. Dnia 10 listopada 2020 r., podczas piątej edycji Europejskiego Tygodnia Umiejętności Zawodowych 2020, Komisja zainicjowała pakt na rzecz umiejętności. Promuje on wspólne działania mające na celu maksymalizację wpływu inwestycji w poprawę istniejących umiejętności i szkolenia w zakresie nowych umiejętności. Wraz z paktem ogłoszono pierwsze europejskie partnerstwa na rzecz umiejętności w trzech obszarach: motoryzacji, mikroelektroniki i lotnictwa oraz obrony.

Dnia 30 września 2020 r. Komisja przyjęła zestaw strategii politycznych, które będą miały istotny wpływ na rozwój długoterminowego potencjału UE w zakresie umiejętności dotyczących bezpieczeństwa. **Plan działania w dziedzinie edukacji cyfrowej na lata 2021–2027**[197] będzie stanowił siłę napędową wysokowydajnego ekosystemu edukacji cyfrowej o zwiększonych kompetencjach w zakresie transformacji cyfrowej[198]. Tego samego dnia przyjęto komunikat w sprawie **europejskiego obszaru edukacji** do 2025 r.[199], w którym główny nacisk położono na umiejętności podstawowe oraz cyfrowe. W komunikacie w sprawie nowej **europejskiej przestrzeni badawczej**[200] wytyczono drogę do poprawy sytuacji w zakresie badań naukowych i innowacji w Europie oraz przyspieszenia procesu transformacji UE w kierunku przywództwa cyfrowego a także do zwalczania wszelkich form przemocy ze względu na płeć w organizacjach zajmujących się badaniami naukowymi i innowacjami.

[195] https://www.nomoreransom.org/
[196] COM(2020) 274.
[197] COM(2020) 624.
[198] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf
[199] COM(2020) 625.
[200] COM(2020) 628.

Program Erasmus+ również przyczynia się do zwalczania radykalizacji postaw poprzez projekty służące walce z radykalizacją, brutalnym ekstremizmem, dotyczące włączenia społecznego, informacji wprowadzających w błąd oraz fałszywych informacji[201]. Przykładem takich działań jest projekt narzędzia do oceny ryzyka radykalizacji w więzieniach, którego celem jest zwiększenie kompetencji pracowników pierwszego kontaktu w zakresie rozpoznawania, zgłaszania i interpretowania oznak radykalizacji oraz odpowiedniego reagowania[202]. Projekt No Hate BootCamp pomógł osobom pracującym z młodzieżą stać się „ambasadorami przeciwko mowie nienawiści" w swoich społecznościach lokalnych.

Sama Komisja stara się zaangażować społeczeństwo w refleksję nad polityką bezpieczeństwa UE. Działania na szczeblu UE stały się bardziej widoczne i dostępne dla obywateli dzięki nowej **stronie internetowej dotyczącej europejskiej strategii bezpieczeństwa**[203]. Uruchomiono kilka **konsultacji publicznych**, zapewniając obywatelom możliwość bezpośredniego wpływania na kształtowanie polityki.

Wszystkie ofiary przestępstw mają prawo do wsparcia i ochrony, ale ofiary najpoważniejszych przestępstw, takich jak terroryzm lub wykorzystywanie seksualne dzieci, wymagają szczególnej uwagi. Dnia 24 czerwca 2020 r. Komisja przyjęła swoją pierwszą w historii **Strategię UE w zakresie praw ofiar (na lata 2020–2025)**[204]. Dotyczy ona ofiar wszystkich przestępstw, ale zwraca się w niej szczególną uwagę na osoby najbardziej narażone, w tym ofiary terroryzmu, dzieci będące ofiarami wykorzystywania seksualnego oraz ofiary handlu ludźmi. Dnia 22 września 2020 r. Komisja zorganizowała konferencję wysokiego szczebla na temat praw ofiar, podczas której zainaugurowała **platformę praw ofiar**, aby promować bardziej horyzontalne podejście do praw ofiar[205]. Komisja mianowała również swojego pierwszego w historii **koordynatora ds. praw ofiar**, aby wspierać spójność i skuteczność w zakresie praw ofiar.

Jeżeli chodzi o **ofiary terroryzmu**, w styczniu 2020 r. utworzono unijne centrum wiedzy specjalistycznej dla ofiar terroryzmu, które ma oferować organom krajowym i organizacjom wspierającym ofiary wiedzę fachową, wskazówki i wsparcie. Promuje ono wymianę najlepszych praktyk i dzielenie się wiedzą fachową wśród praktyków i specjalistów w wymiarze transgranicznym. Nie ma ono na celu oferowania bezpośredniej pomocy poszczególnym ofiarom terroryzmu, lecz wspieranie struktur krajowych w zapewnianiu profesjonalnej pomocy i wsparcia, w tym wytycznych, które mają zostać opublikowane w 2020 r. Unijne centrum jest projektem pilotażowym, który potrwa dwa lata. Prezydencja w Radzie UE pracuje nad wsparciem centrum poprzez sieć pojedynczych krajowych punktów kontaktowych ds. ofiar terroryzmu.

---

[201] Do tej pory sfinansowano około 80 projektów obejmujących kwestie związane z radykalizacją postaw, ponad sto projektów dotyczących sposobów zapobiegania cyberprzemocy i jej zwalczania oraz ponad sto projektów dotyczących edukacji w zakresie krytycznego i etycznego korzystania z internetu z myślą o zwalczaniu dezinformacji cyfrowej.

[202] http://www.r2pris.org/

[203] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_pl

[204] COM(2020) 258.

[205] Platforma pozwoli po raz pierwszy zrzeszyć główne podmioty na szczeblu UE, w tym europejską sieć dotyczącą praw ofiar, europejską sieć krajowych punktów kontaktowych ds. kompensat, Koordynatora UE ds. Zwalczania Terroryzmu, odpowiednie agencje, takie jak Eurojust, Agencja Praw Podstawowych Unii Europejskiej, Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania, Europejski Instytut ds. Równości Kobiet i Mężczyzn, a także przedstawicieli społeczeństwa obywatelskiego.

VI PODSUMOWANIE

Strategię w zakresie unii bezpieczeństwa wprowadzono w celu zapewnienia kompleksowego i dynamicznego podejścia. Niedawne ataki terrorystyczne ponownie pokazały, w jaki sposób UE musi być w stanie reagować, wzmacniając naszą odporność i zdolność reagowania poprzez modernizację i skuteczne wykorzystanie kluczowych narzędzi, które są do naszej dyspozycji. Wskazały one również na potrzebę pełnego zaangażowania wszystkich podmiotów we wspólne podejście, tak aby państwa członkowskie, instytucje Unii, sektor prywatny, organizacje pozarządowe i sami obywatele mogli odegrać rolę w budowaniu bazy bezpieczeństwa, która będzie wystarczająco silna i elastyczna, by osiągnąć rezultaty. To spójne i konsekwentne podejście jest również najlepszym sposobem na zapewnienie ochrony praw podstawowych w ramach promowania naszego europejskiego stylu życia.

W niniejszym sprawozdaniu przedstawiono obecne liczne kierunki prac, ale także sposób, w jaki należy utrzymać osiągniętą dynamikę. Celem zaprezentowanej dziś agendy antyterrorystycznej dla UE jest wzmocnienie europejskich ram walki z terroryzmem poprzez określenie kolejnych niezbędnych kroków: przewidywania terroryzmu i zapobiegania terroryzmowi, ochrony obywateli i infrastruktury oraz gotowości do reagowania, mając na uwadze powiązanie między bezpieczeństwem wewnętrznym a zewnętrznym. Obecnie zacieśniliśmy już współpracę, prowadzimy więcej działań przeciwko radykalizacji oraz mamy więcej narzędzi, które pozwalają pozbawiać terrorystów środków do ataku. Teraz należy pójść o krok dalej. Znamienne w tym kontekście jest zapewnienie przyjęcia nowych przepisów dotyczących treści o charakterze terrorystycznym w internecie, przy czym priorytetem jest osiągnięcie porozumienia w tym roku. Komisja wzywa również państwa członkowskie do przyspieszenia wdrażania całego uzgodnionego prawodawstwa. Zapewnienie bezpieczeństwa obywateli Unii jest wspólnym obowiązkiem, a podejmowanie wspólnych działań musi stanowić zbiorową ambicję ukierunkowaną na bezpieczniejszą Europę.