Terroryzm – studia, analizy, prewencja, 2026, nr 9: 15–37

https://doi.org/10.4467/27204383TER.26.001.23784

Artykuł

Cyfrowa rewolucja polityki antyterrorystycznej UE w nowej Agendzie UE na rzecz zwalczania terroryzmu z 2026 roku

Digital revolution of the EU's counter-terrorism policy under the new EU Agenda for Combating Terrorism of 2026

PIOTR BURCZANIUK

https://orcid.org/0000-0002-6685-8769

Instytut Nauk Prawnych,
Uniwersytet Kardynała Stefana Wyszyńskiego

Abstrakt

Komisja Europejska opublikowała 26 lutego 2026 r. w formie komunikatu nową agendę Unii Europejskiej na rzecz zapobiegania terroryzmowi i zwalczania go, zastępując dokument o podobnym charakterze obowiązujący od 9 grudnia 2020 r. Jako główną przyczynę zmian wskazano konieczność realizacji przyjętej 1 kwietnia 2025 r. nowej europejskiej strategii bezpieczeństwa wewnętrznego ProtectEU. Podstawowym celem opracowania jest przybliżenie zakresu treściowego nowej agendy, ze zwróceniem uwagi na zaprezentowane w niej nowe podejście w kwestii zagrożeń terrorystycznych i brutalnego ekstremizmu, odchodzące stopniowo od klasycznych, fizycznych zagrożeń terrorystycznych na rzecz zagrożeń przyjmujących postać hybrydową lub zachodzących wyłącznie w środowisku cyfrowym. W analizie dokumentu skoncentrowano się na przedstawieniu zbudowanej w nim nowej mapy zagrożeń terrorystycznych, opartej na sześciu filarach obejmujących: przewidywanie zagrożeń, zapobieganie radykalizacji postaw, ochronę obywateli w internecie, ochronę obywateli w środowisku fizycznym, reagowanie na zagrożenia i ataki oraz współpracę

z partnerami międzynarodowymi. Omówiono kwestię miejsca tej agendy w systemie źródeł prawa europejskiego i skutku normatywnego, który z niego wynika. Przedstawiono również najważniejsze różnice w podejściu do zjawiska zwalczania terroryzmu i brutalnego ekstremizmu w starej i nowej agendzie.

Słowa kluczowe

terroryzm, brutalny ekstremizm, polityka bezpieczeństwa UE, Agenda UE 2026, ProtectEU, cyfryzacja bezpieczeństwa, nowe technologie w zwalczaniu terroryzmu

Abstract

On 26 February 2026, the European Commission published a new European Union Agenda for Preventing and Combating Terrorism in the form of communication, replacing a similar document that had been in force since 9 December 2020. The need to implement the new European Internal Security Strategy 'Protect EU' adopted on 1 April 2025 was cited as the main reason for the changes. The primary objective of the study is to outline the content of the new Agenda, with particular attention to the new approach presented therein regarding terrorist threats and violent extremism. The approach is gradually shifting away from traditional, physical terrorist threats in favour of threats that take a hybrid form or occur exclusively in the digital environment. The analysis of the document focuses on presenting the new map of terrorist threats outlined therein, based on six pillars encompassing: anticipating threats, preventing radicalisation, protecting citizens online, protecting citizens in the physical environment, responding to threats and attacks, as well as cooperation with international partners. The article pays particular attention to the issue of the Agenda's place within the system of European legal sources and the normative effect that arises from it. The most significant differences in the approach to combating terrorism and violent extremism in the old and new Agendas were also outlined.

Keywords

terrorism, violent extremism, EU security policy, EU Agenda 2026, ProtectEU, digitalisation of security, new technologies in the fight against terrorism

Agenda na rzecz zwalczania terroryzmu jako element strategii ProtectEU

W dniu 26 lutego 2026 r. Komisja Europejska (dalej: Komisja lub KE) opublikowała, w formie komunikatu adresowanego do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, nową agendę Unii Europejskiej pt. *ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska* (dalej: Agenda)[1]. Zastąpiła ona wcześniejszą agendę pt. *Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie*, opublikowaną przez KE 9 grudnia 2020 r.[2]

Zasadniczym celem artykułu jest krytyczna analiza założeń Agendy oraz wskazanie, w jaki sposób redefiniuje ona unijną politykę bezpieczeństwa wewnętrznego, przenosząc środek ciężkości z klasycznego (fizycznego) zwalczania terroryzmu na przeciwdziałanie zagrożeniom hybrydowym i cyfrowym. Główny problem badawczy artykułu można sprowadzić do pytania: w jaki sposób cyfryzacja, rozwój nowych technologii oraz zmiana środowiska geopolitycznego wpłynęły na ewolucję unijnej polityki antyterrorystycznej i czy rozwiązania przyjęte w Agendzie oznaczają trwałe przejście UE od modelu reaktywno-operacyjnego do modelu technologiczno-prewencyjnego?

W artykule połączono kilka podejść badawczych. Oparto się przede wszystkim na: metodzie dogmatyczno-prawnej, która posłużyła do egzegezy aktów prawnych prawa pierwotnego oraz pochodnego UE i orzecznictwa Trybunału Sprawiedliwości UE; metodzie komparatystycznej, wykorzystanej w podsumowaniu artykułu, oraz metodzie systemowo-instytucjonalnej, zastosowanej do opisu architektury bezpieczeństwa UE.

Prace nad Agendą zostały zainicjowane przez KE w ramach realizacji europejskiej strategii bezpieczeństwa wewnętrznego ProtectEU, opublikowanej 1 kwietnia 2025 r. (dalej: Strategia)[3]. Stanowi ona kompleksową

[1] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska*, COM(2026) 101 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52026DC0101 [dostęp: 28 IV 2026].

[2] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie*, COM(2020) 795 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0795 [dostęp: 28 IV 2026].

[3] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ProtectEU: europejska strategia bezpieczeństwa*

aktualizację podejścia UE do bezpieczeństwa wewnętrznego i opiera się na założeniu, że ochrona obywateli oraz stabilność przestrzeni wewnętrznej UE wymagają zintegrowanego i wielopoziomowego działania wszystkich podmiotów – instytucji unijnych, państw członkowskich, krajowych służb bezpieczeństwa i wywiadu, sektora prywatnego oraz społeczeństwa obywatelskiego.

Kluczowym elementem Strategii jest wzmocnienie zdolności UE do przewidywania zagrożeń przez rozwój analiz ryzyka, lepszą wymianę informacji oraz wykorzystanie danych pochodzących od agencji UE, przede wszystkim Europolu. Strategia kładzie nacisk również na zapobieganie zagrożeniom i zwalczanie ich, zwłaszcza terroryzmu, przestępczości zorganizowanej oraz cyberprzestępczości, przez rozbijanie siatek przestępczych, przeciwdziałanie radykalizacji, szczególnie w środowisku internetowym, oraz ograniczanie źródeł finansowania działalności przestępczej. Istotnym filarem Strategii jest także ochrona infrastruktury krytycznej, co ma zwiększyć odporność UE na sabotaż, ataki hybrydowe oraz zakłócenia technologiczne. Duże znaczenie przypisuje się wzmocnieniu cyberbezpieczeństwa i odporności systemów cyfrowych, które coraz częściej są celem działań przestępczych i destabilizacyjnych. W Strategii podkreśla się, że:

> (...) poziom zagrożenia terrorystycznego w Europie nadal rośnie. Kryzysy regionalne poza UE wywołują efekt domina, dając podmiotom terrorystycznym z całego spektrum ideologicznego nową motywację do werbowania, mobilizacji lub budowania swoich zdolności. Ich działania w zakresie radykalizacji i werbowania skierowane są w szczególności do najsłabszych grup naszych społeczeństw, a zwłaszcza do niektórych osób młodych. Podżegają do ataków w pojedynkę i powodują gwałtowny wzrost ekstremizmu antysystemowego, którego celem jest zakłócenie demokratycznego porządku prawnego[4].

Zwalczanie terroryzmu i brutalnego ekstremizmu staje się jednym z filarów Strategii. Poświęcono temu zagadnieniu pkt 6. Zakłada się wprowadzenie kompleksowego planu zwalczania terroryzmu, aby zapobiegać

wewnętrznego, COM(2025) 148 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX%3A52025DC0148 [dostęp: 28 IV 2026].

[4] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego*..., pkt 1.

radykalizacji postaw, zabezpieczać przestrzeń internetową i publiczną, ograniczać kanały finansowania i reagować na ataki, gdy do nich dojdzie.

Strategia, podobnie jak Agenda, nie definiuje pojęcia terroryzmu. Odwołuje się do definicji „przestępstwa terrorystycznego" w rozumieniu art. 3 *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW*. Zgodnie z nią są to (...) *przestępstwa, które ze względu na swój charakter lub kontekst mogą wyrządzić poważne szkody państwu lub organizacji międzynarodowej*, jeżeli zostają popełnione umyślnie i w tzw. celu terrorystycznym. Do szkód tych zalicza się:

a) poważne zastraszenie ludności,
b) bezprawne zmuszenie rządu lub organizacji międzynarodowej do podjęcia lub zaniechania jakiegoś działania,
c) poważną destabilizację lub zniszczenie podstawowych struktur politycznych, konstytucyjnych, gospodarczych lub społecznych danego państwa lub danej organizacji międzynarodowej.

Jednocześnie zwraca uwagę, że w regulacjach UE nie została przyjęta żadna prawna definicja brutalnego ekstremizmu. W Agendzie w przypisie dolnym podano jedynie, że (...) *akty brutalnego ekstremizmu to działania, które nie przekraczają progu określonego w definicji przestępstw terrorystycznych, jednak stanowią poważne zagrożenie bezpieczeństwa*[5].

W Strategii jako cztery podstawowe elementy zwalczania terroryzmu KE wskazała:

1) zapobieganie radykalizacji i ochronę osób w internecie – Komisja zakłada konieczność eliminowania pierwotnych przyczyn, a przede wszystkim zwraca uwagę na wykorzystywanie przez terrorystów i brutalnych ekstremistów platform internetowych do rozpowszechniania (zwłaszcza wśród osób małoletnich) terrorystycznych i innych szkodliwych treści, gromadzenia funduszy i werbowania. Kluczową rolę w przeciwdziałaniu rozprzestrzenianiu się w internecie treści o charakterze terrorystycznym odgrywa *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym*,

[5] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska...*

gdyż umożliwia szybkie usuwanie najbardziej odrażających i niebezpiecznych materiałów;

2) przeciwdziałanie finansowaniu terroryzmu – Komisja zwraca uwagę, że terroryści pozyskują środki na swoją działalność za pomocą kampanii finansowania społecznościowego, kryptoaktywów, neobanków lub platform płatności internetowych. Organy ścigania muszą wykrywać i badać te przepływy finansowe, co wymaga odpowiednich środków, narzędzi i wiedzy specjalistycznej;
3) ochrona przed atakami – prócz inwestycji w zapobieganie radykalizacji postaw ważnym elementem ochrony obywateli jest ograniczenie środków, za pomocą których terroryści i przestępcy mogą przeprowadzać ataki. Konieczne są działania zarówno w odniesieniu do narzędzi wykorzystywanych przez terrorystów, jak i ochrony celów zagrożonych atakiem, ze zwróceniem szczególnej uwagi na przestrzeń publiczną. Komisja wskazuje również na coraz większe zagrożenia bezpieczeństwa spowodowane wykorzystywaniem bezzałogowych statków powietrznych do szpiegostwa i ataków;
4) zagraniczni bojownicy terrorystyczni – Komisja wraz z Europolem założyła zacieśnienie współpracy z kluczowymi państwami trzecimi w celu uzyskania danych biograficznych i biometrycznych dotyczących osób mogących stanowić zagrożenie terrorystyczne, w tym zagranicznych bojowników terrorystycznych. Dane te mają być wprowadzone do Systemu Informacyjnego Schengen (Schengen Information System, SIS). Komisja zaznacza, jak ważne jest, aby państwa członkowskie korzystały ze wszystkich istniejących narzędzi, w tym SIS, a także usprawniały kontrole biometryczne i przeprowadzały na granicach zewnętrznych UE obowiązkowe i systematyczne kontrole wszystkich osób.

Jednym z najważniejszych działań w zakresie zwalczania terroryzmu i brutalnego ekstremizmu przewidzianych w Strategii było przyjęcie w 2025 r. nowej unijnej agendy na rzecz zapobiegania terroryzmowi i brutalnemu ekstremizmowi oraz ich zwalczania. Ostatecznie Agendę przyjęto 26 lutego 2026 r.

Miejsce Agendy w systemie źródeł prawnych UE

Podstawę prawną działań UE w zakresie zapobiegania terroryzmowi i zwalczania go stanowią przepisy Traktatu o funkcjonowaniu Unii Europejskiej (dalej: TFUE). W ramach regulacji obszaru przestrzeni wolności, bezpieczeństwa i sprawiedliwości (tytuł V) wskazano w nim wśród obowiązków UE, w art. 67 ust. 3 TFUE, nakaz dokładania (...) *starań, aby zapewnić wysoki poziom bezpieczeństwa za pomocą środków zapobiegających przestępczości, rasizmowi i ksenofobii oraz zwalczających te zjawiska, a także za pomocą środków służących koordynacji i współpracy organów policyjnych i sądowych oraz innych właściwych organów, a także za pomocą wzajemnego uznawania orzeczeń sądowych w sprawach karnych i, w miarę potrzeby, przez zbliżanie przepisów karnych*.

Podstawowym środkiem realizacji tego celu jest art. 83 TFUE. Przyznaje on Parlamentowi Europejskiemu i Radzie prawo stanowienia w drodze dyrektyw (...) *norm minimalnych odnoszących się do określania przestępstw oraz kar w dziedzinach szczególnie poważnej przestępczości o wymiarze transgranicznym, wynikające z rodzaju lub skutków tych przestępstw lub ze szczególnej potrzeby wspólnego ich zwalczania*. Do dziedzin tej przestępczości TFUE zalicza: terroryzm, handel ludźmi oraz seksualne wykorzystywanie kobiet i dzieci, nielegalny handel narkotykami, nielegalny handel bronią, pranie pieniędzy, korupcję, fałszowanie środków płatniczych, przestępczość komputerową i przestępczość zorganizowaną.

Uzupełniająco, zgodnie z art. 84 TFUE: *Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, mogą ustanowić środki w celu promowania i wspierania działania Państw Członkowskich w dziedzinie zapobiegania przestępczości, z wyłączeniem jakiejkolwiek harmonizacji przepisów ustawowych i wykonawczych Państw Członkowskich*. To właśnie na tej podstawie Parlament Europejski i Rada mogą przyjmować dokumenty o charakterze strategii i agend, które wyznaczają kierunki polityki, ale nie mają charakteru bezpośrednio wiążącego. Jednocześnie Traktat o Unii Europejskiej (dalej: TUE), w art. 17 TUE, wyznacza KE zadanie wspierania ogólnego interesu UE i podejmowania w tym celu odpowiednich inicjatyw.

Podsumowując, przyjmowanie strategii takich jak Agenda nie opiera się na jednej konkretnej podstawie prawnej, lecz na zespole norm traktatowych. Normy te:

- określają cel UE nakierowany na zapewnienie bezpieczeństwa (art. 67 TFUE),
- przyznają UE kompetencje w zwalczaniu terroryzmu (art. 83 TFUE),

– umożliwiają działania wspierające i strategiczne (art. 84 TFUE),
– nadają Komisji rolę inicjatora polityk UE (art. 17 TUE).

Warto również wskazać, że zgodnie z art. 4 ust. 2 zdanie trzecie TUE: (...) *w szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego*. Oznacza to, że działania UE – w tym strategie antyterrorystyczne – mają charakter wyłącznie koordynacyjny i wspierający, a nie zastępują polityk krajowych.

Na tych podstawach prawnych KE może przyjmować dokumenty strategiczne w postaci m.in. komunikatów COM (COM documents). Zawierają one oficjalne stanowiska, strategie, analizy i zapowiedzi działań legislacyjnych Komisji i odgrywają rolę tzw. *soft law* (prawa miękkiego). Rola i znaczenie takiego prawa wynikają głównie z orzecznictwa Trybunału Sprawiedliwości UE (TSUE). Podkreśla się w nim, że takie prawo nie ma mocy wiążącej, jednak nie może być całkowicie pomijane przy wykładni prawa UE[6]. Może być ono punktem odniesienia interpretacyjnego, szczególnie gdy doprecyzowuje politykę UE[7], i jednocześnie wiąże ono Komisję w zakresie jej własnej praktyki, chociaż nie jest formalnie wiążące dla państw członkowskich UE[8].

Mapa zagrożeń terrorystycznych według Agendy

Agendę otwiera wprowadzenie, w którym KE analizuje najważniejsze zagrożenia i podkreśla, że (...) *terroryzm i brutalny ekstremizm pozostają stałym wyzwaniem dla UE i jej państw członkowskich. Coraz silniejsze powiązania między terroryzmem a innymi obszarami przestępczości, elastyczniejsze sieci oraz sprawcy, którzy w mniejszym stopniu kierują się ideologią, a także zacierające się granice działalności on-line i na żywo stanowią szczególne wyzwanie przy definiowaniu i identyfikowaniu przestępstw terrorystycznych*[9].

---

[6] Por. Wyrok Trybunału (druga izba) z dnia 13 XII 1989 r. Salvatore Grimaldi przeciwko Fonds des maladies professionnelles. ECLI: EU:C:1989:646.

[7] Por. Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

[8] Por. Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. Dansk Rørindustri and Others v Commission of the European Communities. ECLI:EU:C:2005:408.

[9] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska...*, s. 1.

Jak wskazują autorzy tego dokumentu, liczba skoordynowanych i wielkoskalowych zamachów w UE zmniejszyła się w ostatnich latach, ale zagrożenie nie zniknęło, lecz ewoluowało, zarówno w zakresie podmiotowym, jak i ideologicznym. Rośnie liczba sprawców działających w pojedynkę oraz małych kilkuosobowych grup, których trzon stanowią często osoby małoletnie. W aspekcie motywacji ideologicznej podkreśla się, że (...) *podczas gdy terroryzm dżihadystyczny pozostaje najbardziej znaczącym i śmiertelnym zagrożeniem terrorystycznym, terroryści i brutalni ekstremiści kierują się coraz większą liczbą motywacji, nie zawsze związanych z konkretną ideologią, w tym odrzuceniem europejskich wartości demokratycznych, antysemityzmem lub nienawiścią antymuzułmańską*[10].

Ponadto KE zwraca uwagę, że na bezpieczeństwo w UE, w tym poziom zagrożeń terrorystycznych, wpływają zmieniające się otoczenie geopolityczne i konflikty zewnętrzne wobec UE, głównie w Strefie Gazy, a także – w kontekście wzrostu liczby działań sabotażowych i hybrydowych – trwająca rosyjska wojna napastnicza przeciwko Ukrainie. Unia Europejska stanęła w obliczu złożonych zagrożeń, których źródłem są zarówno grupy terrorystyczne, jak i zagraniczne podmioty państwowe i niepaństwowe. Podmioty te wzorują się na działaniach tradycyjnie przypisywanych grupom terrorystycznym, np. posługują się improwizowanymi urządzeniami zapalającymi w ładunkach lotniczych, dokonują cyberataków czy sabotażu infrastruktury krytycznej, ale również wykorzystują terrorystów i brutalnych ekstremistów jako popleczników. Powstają i utrzymują się powiązania między terroryzmem, przestępczością zorganizowaną i cyberprzestępczością. Wykorzystuje się w nich modele usług przestępczych oraz wspólne zasoby, głównie w zakresie werbowania, przestępcze platformy handlowe i podziemne sieci bankowe.

Istotnym elementem współczesnego terroryzmu jest jego silne powiązanie ze środowiskiem cyfrowym. Internet, media społecznościowe, platformy do gier online stały się kluczowymi narzędziami wykorzystywanymi przez organizacje o charakterze ekstremistycznym i jednostki o takich postawach do prowadzenia propagandy, rekrutacji nowych członków, a także do wymiany informacji i planowania działań. W Agendzie wskazuje się:

> Podmioty terrorystyczne koordynują plany na platformach komunikacyjnych wykorzystujących pełne szyfrowanie transmisji (E2EE) oraz finansują swoje sieci i ataki za pomocą kryptowalut, niewymienialnych

[10] Tamże.

> aktywów cyfrowych (NFT) i „cyfrowej hawali”[11]. Nadużywają generatywnej AI do tworzenia instrukcji przeprowadzania ataków. Technologia druku przestrzennego (np. do produkcji broni palnej) oraz zwiększone wykorzystanie systemów bezzałogowych statków powietrznych (SBSP/dronów) jeszcze bardziej zwiększają zagrożenie[12].

Komisja wskazuje, że opisane zagrożenia mają charakter transgraniczny. To oznacza, że żadne państwo członkowskie nie jest w stanie skutecznie przeciwdziałać im samodzielnie. Konieczne jest zatem wzmocnienie współpracy na poziomie unijnym i międzynarodowym. Nie można jednak przy tym zapominać – co podkreśla Komisja – o konieczności zachowania równowagi między zapewnieniem bezpieczeństwa a ochroną praw podstawowych. Działania antyterrorystyczne muszą być prowadzone zgodnie z wartościami UE, takimi jak demokracja, praworządność oraz poszanowanie praw człowieka. Jest to istotne z punktu widzenia zarówno legalności podejmowanych działań, jak i utrzymania do nich zaufania społecznego.

Sześć filarów walki z terroryzmem i brutalnym ekstremizmem

W punkcie drugim Agendy Komisja przedstawia kompleksową koncepcję przeciwdziałania terroryzmowi i brutalnemu ekstremizmowi opartą na systemie sześciu wzajemnie powiązanych filarów działania. Są to: 1) przewidywanie zagrożeń, 2) zapobieganie radykalizacji postaw, 3) ochrona użytkowników internetu, 4) ochrona ludzi w środowisku fizycznym, 5) reagowanie na zagrożenia i ataki, 6) współpraca z partnerami międzynarodowymi. Podejście to odzwierciedla przekonanie, że skuteczna polityka antyterrorystyczna nie może ograniczać się do reakcji na zdarzenia, lecz musi obejmować pełne spektrum działań – od identyfikacji zagrożeń, przez zapobieganie im, aż po reagowanie i odbudowę po ewentualnych atakach. Współczesne zagrożenia mają charakter dynamiczny, wielowymiarowy i często transgraniczny, co wymaga zintegrowanego podejścia angażującego różne poziomy zarządzania – lokalny, krajowy, unijny i międzynarodowy.

---

[11] Cyfrowa hawala to nieformalny system przekazywania wartości finansowej z wykorzystaniem narzędzi cyfrowych, działający poza tradycyjnym systemem bankowym i oparty na sieci zaufanych pośredników.

[12] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska…*, s. 3.

Przewidywanie zagrożeń

Komisja podkreśla, że (...) *bezpieczeństwo zaczyna się od skutecznego przewidywania i prognozowania*[13].

Przewidywanie zagrożeń ma stanowić fundament całej strategii i opierać się na gromadzeniu, analizie i wymianie informacji. Szczególną rolę w tym zakresie odgrywa współpraca między państwami członkowskimi oraz agencjami UE, w tym Single Intelligence Analysis Capacity[14], dostarczającym terminowych ocen zagrożeń, oraz Europolem, sporządzającym – na podstawie informacji otrzymanych od organów ścigania – regularne sprawozdania dotyczące tendencji. Dynamiczny i nieprzewidywalny charakter pojawiających się zagrożeń wymaga – zdaniem Komisji – wzmocnienia zdolności organów ścigania do przewidywania, aby móc lepiej określać pojawiające się zagrożenia i podejmować odpowiednie działania polityczne służące zwalczaniu terroryzmu.

Z kolei prognozowanie jest kluczowe z perspektywy identyfikacji zagrożeń i ma się opierać na dwóch elementach. Pierwszy z nich to wykorzystanie potencjału nowych technologii w zakresie egzekwowania prawa. Sztuczna inteligencja (ang. *artificial intelligence*, AI), uczenie maszynowe czy analiza dużych zbiorów danych to potencjał narzędziowy umożliwiający identyfikowanie wzorców zachowań oraz wykrywanie sygnałów ostrzegawczych, które mogą wskazywać na przygotowywanie ataków. Drugim elementem ma być przygotowanie na przeciwdziałanie wykorzystaniu przez terrorystów nowych technologii, takich jak AI, platformy internetowe, metody elektronicznego finansowania, głównie kryptoaktywa, czy stosowanie broni drukowanej w technologii 3D. Działania w ramach prognozowania mają się opierać na pracach Wspólnego Centrum Badawczego Komisji Europejskiej (Joint Research Centre), a podstawą ich finansowania ma być program „Horyzont Europa".

Analiza założeń tego filaru prowadzi do wniosku o przejściu z dotychczas prezentowanego w UE modelu reaktywnego na model prewencyjny, w którym działania są podejmowane jeszcze przed materializacją zagrożenia.

[13] Tamże, s. 4.

[14] SIAC – struktura łącząca cywilne EU INTCEN (European Union Intelligence and Situation Centre), czyli cywilną jednostkę wywiadowczą UE będącą częścią Europejskiej Służby Działań Zewnętrznych, z Military Intelligence Directorate (wydziałem wywiadu wojskowego) w ramach Sztabu Wojskowego UE (European Union Military Staff, EUMS).

Zapobieganie radykalizacji postaw

Komisja definiuje zapobieganie radykalizacji postaw jako (...) *zwalczanie jej przyczyn, zanim się one utrwalą*[15]. Drugi filar ma się opierać na czterech elementach:

1) opracowaniu zestawu narzędzi prewencyjnych z myślą o osobach małoletnich. Narzędzia te mają umożliwić wczesne wykrywanie, wzmacniać czynniki ochronne, budowanie odporności przez edukację i integrację społeczną, przede wszystkim małoletnich, a także wspierać rodziny i społeczności w bezpiecznym korzystaniu z internetu;
2) budowaniu odpornych społeczeństw, nakierowanym na ochronę wszystkich wspólnot wyznaniowych przed nienawiścią, dyskryminacją i przemocą. Działania KE będą koncentrować się na usprawnieniu, dzięki wykorzystaniu AI, wykrywania treści ekstremistycznych, tworzeniu wspólnych wskaźników zagrożenia oraz usprawnieniu współpracy między platformami, organami ścigania i naukowcami w celu identyfikacji propagandy generowanej przez AI i skoordynowanych kampanii nakierowanych na radykalizację postaw;
3) przeciwdziałaniu radykalizacji postaw w zakładach karnych i wśród osób je opuszczających oraz zarządzaniu powrotami zagranicznych bojowników terrorystycznych i członków ich rodzin. Podstawą ma być opracowanie narzędzi oceny ryzyka i zarządzania nim na etapie poprzedzającym wypuszczenie na wolność oraz wytycznych wspierających krajowe podejścia do zradykalizowanych osób opuszczających zakłady karne oraz osób powracających, połączone ze szkoleniami w zakresie resocjalizacji i reintegracji, ze szczególnym uwzględnieniem ochrony dzieci;
4) wsparciu ofiar terroryzmu przez upowszechnienie Europejskiego Dnia Pamięci o Ofiarach Terroryzmu oraz wsparciu stowarzyszeń ofiar przez propagowanie ich aktywnej roli w programach zapobiegania.

Instytucjonalnie działaniami w ramach filaru drugiego zajmuje się powołane w 2024 r. Europejskie Centrum Wiedzy na temat Zapobiegania Radykalizacji (EU Knowledge Hub on Prevention of Radicalisation). Centrum

[15] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska...*, s. 5.

opracowuje wytyczne, narzędzia, szkolenia i usługi wsparcia dla decydentów i praktyków.

Ochrona użytkowników internetu

Unia Europejska przyjęła najbardziej zaawansowane na świecie ramy regulacyjne ukierunkowane na zwalczanie działalności terrorystycznej w internecie, jednak zagrożenie to nadal się rozwija. W Agendzie wskazuje się: *Sieci ekstremistyczne szybko się dostosowują, wykorzystują powstające technologie oraz przenoszą swoją działalność z otwartych platform do zamkniętych czatów i usług szyfrowanych. Może to stwarzać poważne wyzwania w zakresie wykrywania planów terrorystycznych i zapobiegania ich realizacji, mapowania siatek terrorystycznych i ich zwolenników oraz prowadzenia postępowań przygotowawczych i sądowych w sprawie działalności terrorystycznej*[16].

Zgodnie z założeniem Komisji działania w tym filarze mają się skupiać na trzech zagadnieniach:

1) pełnym wykorzystaniu ram regulacyjnych do zwalczania w internecie treści o charakterze ekstremistycznym i terrorystycznym, m.in. przez opracowanie przez Europol europejskiej bazy danych w celu wymiany skrótów kryptograficznych (ang. *hash*), tj. bazy śladów cyfrowych odnoszących się do treści o charakterze terrorystycznym i brutalnych treści ekstremistycznych, co umożliwi państwom członkowskim i dostawcom usług hostingowych bezpieczne oznaczanie, dopasowywanie i usuwanie treści na różnych platformach;
2) współpracy z przemysłem, głównie dostawcami usług online, która będzie realizowana za pośrednictwem Forum UE ds. Internetu (European Internet Forum zrzesza ministerstwa państw członkowskich UE, organy ścigania, społeczeństwo obywatelskie i dostawców usług online, w tym platformy mediów społecznościowych) oraz przez działania wspólnie z Europejską Radą ds. Usług Cyfrowych (European Board for Digital Services) w celu zintensyfikowania zwalczania rozpowszechniania treści o charakterze terrorystycznym i brutalnych treści ekstremistycznych;
3) zapewnieniu skutecznego i skoordynowanego reagowania kryzysowego w internecie, przy założeniu przekształcenia dotychczasowego unijnego protokołu kryzysowego w unijne ramy reagowania kryzysowego online (włączone do Digital Services Act – unijnego

[16] Tamże, s. 8.

aktu o usługach cyfrowych). Państwa członkowskie będą mogły z nich korzystać w przypadku, gdy incydent prowadzi do zwiększonej aktywności w internecie związanej z atakiem.

Ochrona ludzi w środowisku fizycznym

Czwarty filar opiera się na zmienionym podejściu, zgodnie z którym podstawą jest działanie oparte na odporności. Zastąpiło ono działanie skoncentrowane na ochronie. Nastąpiło to wraz z przyjęciem w 2022 r. *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE* (dalej: dyrektywa CER). Jednocześnie UE zapewnia praktyczne wsparcie, którego podstawą są doradcy UE ds. zapewniania bezpieczeństwa. Ich zadaniem jest pomoc w ocenie podatności na zagrożenia i sugerowanie konkretnych usprawnień. Zgodnie z Agendą działania UE w analizowanym filarze mają się skupić na pięciu zagadnieniach:

1) utrudnianiu przemieszczania się terrorystów, głównie przez zapewnienie wysokiego poziomu ochrony granic zewnętrznych UE. Służą temu przede wszystkim wielkoskalowe systemy informatyczne: wjazdu/wyjazdu (Entry/Exit System, EES), informacji o podróży oraz zezwoleń na podróż (European Travel Information and Authorisation System, ETIAS), wizowy system informacyjny (Visa Information System, VIS) oraz ramy interoperacyjności. Dużymi wyzwaniami pozostają współpraca z państwami trzecimi nakierowana na uzyskanie biograficznych i biometrycznych danych osób mogących stanowić zagrożenie terrorystyczne i wprowadzenie tych danych do systemu SIS oraz rozbudowa procedury postępowania w sytuacji uzyskania „trafienia". Od czerwca 2026 r. ma funkcjonować tzw. kontrola przesiewowa[17]. Dzięki niej ma być łatwiejsza identyfikacja obywateli państw trzecich, którzy nielegalnie przekroczyli granice zewnętrzne lub nielegalnie przebywają na terytorium państw członkowskich bez poddania się kontroli wjazdu. Komisja podkreśla, że będzie propagować skuteczne powroty osób stanowiących zagrożenie bezpieczeństwa;

[17] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1356 z dnia 14 maja 2024 r. w sprawie wprowadzenia kontroli przesiewowej obywateli państw trzecich na granicach zewnętrznych oraz zmiany rozporządzeń (WE) nr 767/2008, (UE) 2017/2226, (UE) 2018/1240 i (UE) 2019/817*.

2) ograniczeniu dostępu do środków wykorzystywanych do przeprowadzania ataków przez harmonizację przepisów dotyczących kryminalizacji nielegalnego handlu bronią palną i innych przestępstw związanych z tą bronią, w tym nielegalnego tworzenia, posiadania i rozpowszechniania projektów na potrzeby wytwarzania broni palnej drukowanej w technologii 3D. Agenda zakłada również dokonanie przeglądu *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1148 z dnia 20 czerwca 2019 r. w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, zmieniającego rozporządzenie (WE) nr 1907/2006 i uchylającego rozporządzenie (UE) nr 98/2013* oraz przedstawienie w 2026 r. nowego planu działania na rzecz gotowości i reagowania w zakresie zagrożeń chemicznych, biologicznych, radiologicznych i nuklearnych (CBRN);
3) przeciwdziałaniu zagrożeniu stwarzanemu przez drony. Komisja podkreśla znaczenie zagrożenia związanego z wykorzystaniem nowych i powstających technologii, głównie dronów, przez podmioty terrorystyczne. Zwalczanie ma się opierać na strategii dotyczącej dronów 2.0[18] oraz planie działania UE w zakresie bezpieczeństwa dronów i zabezpieczeń antydronowych przedstawionym 11 lutego 2026 r.[19];
4) ochronie przestrzeni publicznej w Europie, przy czym jest konieczne uwzględnianie wymogów bezpieczeństwa już na etapie projektowania obszarów miejskich, przestrzeni publicznych i miejsc kultu. Powinno to znaleźć odzwierciedlenie w odpowiednich zobowiązaniach dla podmiotów eksploatujących przestrzeń publiczną, aby wdrażały środki bezpieczeństwa wynikające z analiz ryzyka. Organizacyjnie to zadanie zostaje powierzone wzmacnianemu Forum UE ds. Ochrony Przestrzeni Publicznych (EU Forum on the Protection of Public Spaces);

[18] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. „Strategia dotycząca dronów 2.0 na rzecz inteligentnego i zrównoważonego ekosystemu bezzałogowych statków powietrznych w Europie*, COM(2022) 652 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52022DC0652 [dostęp: 28 IV 2026].

[19] *Plan działania na rzecz ochrony przed dronami i zwalczania dronów,* Komisja Europejska, https://digital-strategy.ec.europa.eu/pl/policies/drone-security [dostęp: 28 IV 2026].

5) odporności podmiotów krytycznych oraz bezpieczeństwa transportu i łańcucha dostaw. Wiąże się to z rosnącymi obawami dotyczącymi możliwych incydentów w postaci kampanii hybrydowych i aktów sabotażu ze strony wrogich podmiotów państwowych i ich popleczników. W celu poprawy bezpieczeństwa KE rekomenduje pilne wdrożenie wspomnianej wcześniej dyrektywy CER oraz *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS2)*.

Reagowanie na zagrożenia i ataki

Piąty filar ma się opierać na szybkiej i skoordynowanej reakcji zapewnianej przez, wymagające wzmocnienia, organy ścigania i organy sądowe przy wsparciu Europolu i Eurojustu. Komisja zwraca uwagę także na konieczność podejmowania dalszych działań nakierowanych na wyeliminowanie luk w systemie zapobiegania finansowaniu terroryzmu.

Działania w ramach tego filaru mają się skoncentrować na trzech zagadnieniach:

1) zwalczaniu finansowania terroryzmu i brutalnego ekstremizmu. Komisja podkreśla, że globalny charakter usług finansowych wymaga aktywnej reakcji całej Europy na problem jego wykorzystywania do finansowania terroryzmu. Ma to istotne znaczenie również ze względu na nowe źródła finansowania, takie jak kryptoaktywa czy cyfrowa hawala (oraz internetowe usługi płatnicze). Za fundament prawny walki z finansowaniem terroryzmu Komisja uznaje pełne wdrożenie, przyjętego 30 maja 2024 r., pakietu UE dotyczącego przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (ang. *anti-money laundering and countering the financing of terrorism*, AML/CFT), obejmującego *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy i finansowania terroryzmu* (wejdzie w życie 10 lipca 2027 r.) oraz *Dyrektywę Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania*

terroryzmu, zmieniającą dyrektywę (UE) 2019/1937 oraz zmieniającą i uchylającą dyrektywę (UE) 2015/849. Komisja planuje też podjęcie prac nad stworzeniem ogólnounijnego systemu umożliwiającego wyszukiwanie danych finansowych w celu śledzenia środków finansowych należących do terrorystów i korzyści z przestępczości zorganizowanej. System miałby powstać do 2030 r. i obejmować transakcje wewnątrzunijne i transakcje w ramach jednolitego obszaru płatności w euro (ang. *single euro payments area*, SEPA), transfery kryptoaktywów, płatności online i elektroniczne transfery środków pieniężnych;

2) usprawnieniu działań organów ścigania przez wzmacnianie mandatu Europolu, zwłaszcza jego Europejskiego Centrum ds. Zwalczania Terroryzmu (European Counter Terrorism Centre, ECTC), jako głównego centrum informacji, technologii i innowacji dla organów ścigania;
3) zacieśnieniu współpracy sądowej przez pełne wdrożenie, przyjętego komunikatem Komisji z 24 czerwca 2025 r., planu działania na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych[20]. Decydującego znaczenia nabiera możliwość zabezpieczania i pozyskiwania dowodów bezpośrednio od usługodawców oferujących swoje usługi w UE, na mocy znajdującego zastosowanie od 18 sierpnia 2026 r. *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności*. Komisja zwraca uwagę na istotę firmowanego przez UE projektu SIRIUS, będącego unijnym systemem wsparcia dla organów ścigania w zdobywaniu ponad granicami państw dowodów z internetu[21].

[20] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan działania na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych*, COM(2025) 349 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52025DC0349 [dostęp: 29 IV 2026].

[21] *SIRIUS project*, Europol, 21 I 2026 r., https://www.europol.europa.eu/how-we-work/sirius-project [dostęp: 29 IV 2026].

Współpraca z partnerami międzynarodowymi

Ostatni filar zakłada konieczność zacieśnienia współpracy międzynarodowej, głównie przez działania Wysokiego Przedstawiciela i koordynatora UE ds. zwalczania terroryzmu.

Działania w ramach tego filaru mają się skoncentrować na czterech zagadnieniach:

1) środkach ograniczających służących zwalczaniu terroryzmu, przy czym podstawowe narzędzie rozbijania siatek terrorystycznych stanowi tzw. unijna lista terrorystów[22];
2) postępie w zakresie zawierania umów międzynarodowych, dla których największym wyzwaniem pozostaje nowy protokół zmieniający definicję przestępstw terrorystycznych w Konwencji Rady Europy o zapobieganiu terroryzmowi[23]. Po wejściu w życie ma on zapewnić dla ponad 40 państw ogólnoeuropejską definicję przestępstw terrorystycznych;
3) zacieśnianiu współpracy dwustronnej i regionalnej, a zwłaszcza wzmacnianiu współpracy z partnerami objętymi procesem rozszerzenia UE, a także na działaniach prowadzonych wobec konkretnych regionów, ze zwróceniem szczególnej uwagi na Bałkany Zachodnie, Bliski Wschód, w tym Syrię, oraz państwa afrykańskie;
4) wzmocnieniu roli UE przez koordynację i działania na forach wielostronnych Wysokiego Przedstawiciela, Komisji oraz koordynatora UE ds. zwalczania terroryzmu. Utrzymana ma zostać współpraca tematyczna z Radą Europy, Grupą Specjalną ds. Przeciwdziałania Praniu Pieniędzy (Financial Action Task Force), Interpolem i NATO.

[22] Oficjalny wykaz osób, grup i podmiotów uznanych przez UE za zaangażowane w działalność terrorystyczną formalnie funkcjonuje na mocy *Wspólnego stanowiska Rady z dnia 27 grudnia 2001 r. w sprawie zastosowania szczególnych środków w celu zwalczania terroryzmu (2001/931/WPZiB)*.

[23] Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), https://search.coe.int/cm/eng#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} [dostęp: 14 V 2026].

Agenda z 2026 roku a agenda z 2020 roku

Agenda z 2026 r., która została opracowana w celu realizacji nowej strategii bezpieczeństwa wewnętrznego ProtectEU opublikowanej 1 kwietnia 2025 r., czyni motywem przewodnim dostosowanie unijnej strategii walki z terroryzmem i brutalnym ekstremizmem do aktualnych zagrożeń. Ich charakter uległ, co podkreśla Komisja, zauważalnej zmianie – z klasycznych, fizycznych zagrożeń terrorystycznych na zagrożenia przyjmujące postać hybrydową lub występujące wyłącznie w środowisku cyfrowym. Podejście reaktywno-operacyjne zostaje więc zastąpione podejściem skupionym na działaniach proaktywnych, systemowych, w sferze cyfrowej.

Agenda z 2020 r. ujmowała zagrożenia terrorystyczne w sposób tradycyjny, jako działalność zorganizowanych grup, inspirowaną ideologicznie i realizowaną głównie „offline". Internet pojawiał się w niej wyłącznie jako jedno z narzędzi i nie stanowił centralnego pola zainteresowania. Nowa Agenda traktuje przestrzeń cyfrową jako główne środowisko występowania zagrożeń. Radykalizacja, rekrutacja, propaganda czy finansowanie coraz częściej odbywają się bowiem wyłącznie w środowisku wirtualnym, co powoduje, że zagrożenia są bardziej rozproszone, trudniejsze do wykrycia na wczesnym etapie oraz silnie powiązane z dezinformacją i manipulacją informacyjną. Agenda zakłada konieczność przejścia z podejścia skoncentrowanego na zwalczaniu konkretnej organizacji na podejście oscylujące wokół zarządzania dynamicznym, głównie cyfrowym, ekosystemem zagrożeń.

Zmieniło się również podejście do sposobu prowadzenia działań prewencyjnych. Poprzednia agenda koncentrowała się na przeciwdziałaniu radykalizacji m.in. za pomocą programów społecznych, monitorowania środowisk ryzyka oraz współpracy służb. W Agendzie z 2026 r. prewencja zostaje przeniesiona w dużej mierze do internetu, z naciskiem na wczesne wykrywanie treści ekstremistycznych, przeciwdziałanie ich algorytmicznemu wzmacnianiu, szybkie usuwanie oraz ograniczanie ich zasięgu. W ten sposób prewencja staje się bardziej technologiczna i zautomatyzowana, a w mniejszym stopniu opiera się na działaniach społecznych.

W poprzedniej agendzie technologie cyfrowe były narzędziem wyłącznie wspierającym działania (np. analizy danych, wymiany informacji). W nowej Agendzie technologie te stają się centralnym elementem strategii, nakierowanym głównie na wykorzystanie AI do identyfikacji zagrożeń, analizy dużych zbiorów danych (big data), automatyzacji procesów bezpieczeństwa czy rozwoju narzędzi predykcyjnych. Różnica polega więc na przejściu od poziomu wsparcia technologicznego do strategii opartej na technologii.

W obu dokumentach podkreśla się znaczenie współpracy, jednak w poprzedniej agendzie skupiono się wyłącznie na współpracy między państwami członkowskimi i agencjami UE, a w nowej rozszerzono ją o sektor prywatny, podmioty technologiczne oraz współpracę globalną. Współpraca ta staje się sieciowa i wielopoziomowa. W dokumencie z 2020 r. sektor prywatny (zwłaszcza platformy internetowe) był partnerem wspierającym działania państw. W Agendzie z 2026 r. rola tego sektora wyraźnie wzrasta. Platformy społecznościowe stają się współodpowiedzialne za bezpieczeństwo. Komisja oczekuje od nich aktywnego wykrywania i usuwania treści oraz wprowadzenia systemowych mechanizmów współpracy i nadzoru. Następuje przesunięcie z modelu dobrowolnej współpracy w stronę modelu współodpowiedzialności regulacyjnej.

Zauważalna jest również zmiana w podejściu do budowania odporności społeczeństwa. W strategii z 2020 r. ta odporność była ważna, ale traktowana raczej jako element uzupełniający. W nowej Agendzie stała się ona jednym z najważniejszych filarów, głównie w zakresie walki z dezinformacją, budowania świadomości cyfrowej oraz ograniczania w sieci podatności na radykalizację. Bezpieczeństwo nie dotyczy już tylko konkretnej instytucji, ale całego społeczeństwa jako systemu.

Podsumowując, trzeba pamiętać, że przyjęta Agenda stanowi de facto dokument o charakterze wyłącznie programowym. Realizacja zawartych w nim założeń ma być osiągnięta dzięki projektowanym lub już wdrażanym aktom prawnym UE oraz działaniom zorientowanym głównie na rozwijanie współpracy organów ścigania państw członkowskich UE oraz państw trzecich, w swoistej koordynacji wzmacnianego organizacyjnie, mającego realne funkcje wykonawcze, Europolu.

Bibliografia

Źródła internetowe

Plan działania na rzecz ochrony przed dronami i zwalczania dronów, Komisja Europejska, https://digital-strategy.ec.europa.eu/pl/policies/drone-security [dostęp: 28 IV 2026].

SIRIUS project, Europol, 21 I 2026 r., https://www.europol.europa.eu/how-we-work/sirius-project [dostęp: 29 IV 2026].

Akty prawne

Traktat o funkcjonowaniu Unii Europejskiej (DzU z 2004 r. nr 90 poz. 864).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy i finansowania terroryzmu (Dz. Urz. UE L 1624 z 19 VI 2024 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1356 z dnia 14 maja 2024 r. w sprawie wprowadzenia kontroli przesiewowej obywateli państw trzecich na granicach zewnętrznych oraz zmiany rozporządzeń (WE) nr 767/2008, (UE) 2017/2226, (UE) 2018/1240 i (UE) 2019/817 (Dz. Urz. UE L 1356 z 22 V 2024 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz. Urz. UE L 191/118 z 28 VII 2023 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz. Urz. UE L 172/79 z 17 V 2021 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1148 z dnia 20 czerwca 2019 r. w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, zmieniające rozporządzenie (WE) nr 1907/2006 i uchylające rozporządzenie (UE) nr 98/2013 (Dz. Urz. UE L 186/1 z 11 VII 2019 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca dyrektywę (UE) 2019/1937 oraz zmieniająca i uchylająca dyrektywę (UE) 2015/849 (Dz. Urz. UE L 1640 z 19 VI 2024 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333/164 z 27 XII 2022 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333/80 z 27 XII 2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz. Urz. UE L 88/6 z 31 III 2017 r.).

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan dla UE w dziedzinie zwalczania terroryzmu: przewidywanie, zapobieganie, ochrona i reagowanie, COM(2020) 795 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=-CELEX:52020DC0795 [dostęp: 28 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Plan działania na rzecz zgodnego z prawem i skutecznego dostępu organów ścigania do danych, COM(2025) 349 final, https://eu-r-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52025DC0349 [dostęp: 29 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. ProtectEU: Program zapobiegania terroryzmowi i zwalczania tego zjawiska, COM(2026) 101 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52026DC0101 [dostęp: 28 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. „Strategia dotycząca dronów 2.0 na rzecz inteligentnego i zrównoważonego ekosystemu bezzałogowych statków powietrznych w Europie", COM(2022) 652 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52022DC0652 [dostęp: 28 IV 2026].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego, COM(2025) 148 final, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX%3A52025DC0148 [dostęp: 28 IV 2026].

Wspólne stanowisko Rady z dnia 27 grudnia 2001 r. w sprawie zastosowania szczególnych środków w celu zwalczania terroryzmu (2001/931/WPZiB) – (Dz. Urz. UE L 344/93 z 28 XII 2001 r.).

Orzecznictwo

Wyrok Trybunału (druga izba) z 13 XII 1989 r. Salvatore Grimaldi przeciwko Fonds des maladies professionnelles. ECLI: EU:C:1989:646.

Opinion of Advocate General Van Gerven delivered on 15 October 1992. ECLI: EU:C:1992:393.

Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P. Dansk Rørindustri and Others v Commission of the European Communities. ECLI: EU:C:2005:408.

Inne dokumenty

Council of Europe Committee on Counter-Terrorism (CDCT) – Draft Protocol amending the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196), https://search.coe.int/cm/eng#{%22CoEIdentifier%22:[%220912594880264105%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} [dostęp: 14 V 2026].

Dr Piotr Burczaniuk

Doktor nauk prawnych, adiunkt w Katedrze Teorii i Filozofii Prawa na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie; radca prawny, członek Okręgowej Izby Radców Prawnych w Warszawie; legislator, członek Polskiego Towarzystwa Legislacji; ekspert ds. legislacji. Autor publikacji z zakresu teorii i filozofii prawa, prawa konstytucyjnego oraz prawa gospodarczego.

Kontakt: p.burczaniuk@uksw.edu.pl