KOMISJA
EUROPEJSKA

Bruksela, dnia 16.7.2025 r.
COM(2025) 415 final

2025/0230 (NLE)

Wniosek

DECYZJA RADY

w sprawie podpisania, w imieniu Unii Europejskiej, Konwencji Narodów Zjednoczonych przeciwko cyberprzestępczości; wzmocnienie współpracy międzynarodowej w zakresie zwalczania określonych przestępstw popełnianych za pomocą systemów technologii informacyjno-komunikacyjnych oraz wymiany materiału dowodowego w formie elektronicznej w odniesieniu do poważnych przestępstw

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Kontekst wniosku

Celem niniejszego wniosku jest uzyskanie od Rady Unii Europejskiej („Rada”) upoważnienia dla Komisji Europejskiej („Komisja”) do podpisania, w imieniu Unii Europejskiej, konwencji Narodów Zjednoczonych przeciwko cyberprzestępczości („konwencja”)[(1)].

Komisja przedstawi także wniosek dotyczący decyzji Rady upoważniającej Komisję do zawarcia konwencji w imieniu Unii Europejskiej. Obydwa wnioski stanowią kontynuację zobowiązania Komisji zawartego w komunikacie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego[(2)].

Cyberprzestępczość stanowi coraz większe zagrożenie dla bezpieczeństwa obywateli i przedsiębiorstw w Unii Europejskiej (UE)[(3)]. Według opracowanej przez Europol oceny zagrożenia zorganizowaną przestępczością internetową w ciągu ostatnich 10 lat zagrożenia stwarzane przez cyberprzestępczość gwałtownie wzrosły pod względem skali, intensywności i możliwości wyrządzania szkód[(4)]. Cyberprzestępcy wykorzystują powstające technologie, takie jak sztuczna inteligencja (AI) do automatyzacji ataków, inżynierii społecznej i omijania zabezpieczeń, dzięki czemu cyberataki stały się bardziej skalowalne i skuteczne. Recesja gospodarcza, niestabilność geopolityczna i pogłębiające się nierówności na świecie zwiększyły zachęty dla osób fizycznych do angażowania się w cyberprzestępczość motywowaną finansowo[(5)]. Nadal rośnie liczba i skala przestępstw wykorzystujących cyberprzestrzeń, takich jak oszustwa internetowe i niegodziwe traktowanie dzieci w celach seksualnych. Szacuje się, że w 2024 r. straty spowodowane oszustwami internetowymi wyniosły 1,03 bln EUR[(6)]. Liczba zgłoszeń dotyczących niegodziwego traktowania dzieci w celach seksualnych na całym świecie wzrosła z 1 mln w 2010 r. do prawie 36 mln w 2023 r., z czego 1,3 mln przypadków miało miejsce w UE[(7)].

Cyberprzestępczość jest zjawiskiem globalnym i pozbawionym granic, a zacieśnienie współpracy międzynarodowej w zakresie jej zwalczania od ponad dziesięciu lat jest priorytetem dla państw na całym świecie. W szczególności ponadgraniczny charakter internetu sprawia, że dochodzenia w sprawie cyberprzestępstw mają niemal zawsze charakter

---

(1) Tekst konwencji zostanie załączony do wniosku dotyczącego decyzji Rady w sprawie zawarcia konwencji, w imieniu Unii Europejskiej.

(2) Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego; COM(2025) 148 final.

(3) W 2023 r. ataki z użyciem oprogramowania szantażującego, wykorzystywanie seksualne dzieci i oszustwa internetowe nadal były najbardziej groźnymi przejawami cyberprzestępczości w Unii Europejskiej (UE). Niektórzy cyberprzestępcy atakujący UE mieli siedzibę w UE, podczas gdy inni woleli działać spoza jej granic, ukrywając swoje nielegalne operacje i środki finansowe w państwach trzecich. Internet Organised Crime Threat Assessment (IOCTA) [„Ocena zagrożenia wykorzystaniem internetu przez zorganizowane grupy przestępcze (IOCTA)”], 2024.

(4) Internet Organised Crime Threat Assessment (IOCTA) [„Ocena zagrożenia wykorzystaniem internetu przez zorganizowane grupy przestępcze (IOCTA)”], 2024.

(5) Ocena zagrożenia poważną i zorganizowaną przestępczością (SOCTA), 2025.

(6) Global State of Scams Report 2025 (GASA) [„Sprawozdanie na temat globalnego obrazu oszustw w 2025 r. (GASA)”].

(7) Krajowe Centrum ds. Zaginionych i Wykorzystywanych Dzieci, https://www.missingkids.org/cybertiplinedata.

transgraniczny, co wymaga ścisłej współpracy między organami w różnych państwach. W ostatnich latach rośnie liczba krajów, z którymi konieczna jest współpraca, ponieważ cyberprzestępcy ukrywają się w dogodnych jurysdykcjach na całym świecie, aby dokonywać ataków na UE i jej kraje partnerskie.

Elektroniczny materiał dowodowy odgrywa coraz większą rolę w dochodzeniach, zarówno dotyczących przestępstw internetowych, jak i tradycyjnych, takich jak nielegalny obrót środkami odurzającymi, które często pozostawiają ślady w internecie, ponieważ przestępcy planują i koordynują swoją działalność w internecie i przy użyciu aplikacji. W wyniku badania przeprowadzonego przez Komisję stwierdzono, że już w 2018 r. organy ścigania i organy sądowe potrzebowały dostępu do elektronicznych materiałów dowodowych w co najmniej 85 % dochodzeń, w tym dochodzeń dotyczących cyberprzestępczości[(8)]. Dowody dotyczące wszelkich przestępstw są w coraz częściej w posiadaniu dostawców usług, którzy przechowują je w formie elektronicznej w zagranicznych jurysdykcjach. Co najmniej 55 % dochodzeń obejmuje wniosek o transgraniczny dostęp do materiału dowodowego[(9)]. Skuteczna reakcja wymiaru sprawiedliwości w sprawach karnych wymaga odpowiednich środków umożliwiających uzyskanie takich dowodów w celu utrzymania praworządności.

W związku z tym na szczeblu krajowym, unijnym[(10)] i międzynarodowym podejmowane są działania mające na celu poprawę wymiany elektronicznych materiałów dowodowych na potrzeby dochodzeń.

Konwencja stanowi część tych działań. Ustanawia ona wspólne zasady na szczeblu globalnym w celu usprawnienia współpracy w zakresie cyberprzestępczości i gromadzenia materiału dowodowego w formie elektronicznej do celów prowadzenia dochodzeń lub postępowań karnych, tworząc podstawę do współpracy z wieloma państwami, z którymi ani UE, ani jej państwa członkowskie nie zawarły umów, przy jednoczesnym zapewnieniu poszanowania prawa i wartości UE. Jest ona zgodna z obowiązującymi instrumentami UE i instrumentami międzynarodowymi oraz stanowi ich uzupełnienie.

Przebieg procedury

Konwencja Rady Europy o cyberprzestępczości z 2001 r. („konwencja budapesztańska”)[(11)] jest pierwszym traktatem międzynarodowym dotyczącym cyberprzestępczości. Ułatwia ona zwalczanie przestępstw popełnianych przy użyciu sieci komputerowych. Do konwencji budapesztańskiej mogą przystąpić państwa członkowskie Rady Europy, a państwa niebędące członkami – na zaproszenie. Do tej pory przystąpiło do niej 80 państw, w tym 26 państw członkowskich Unii Europejskiej. Drugi protokół dodatkowy[(12)] do konwencji

(8) SWD(2018) 118 final.

(9) SWD(2018) 118 final.

(10) 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.U. L 191 z 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj) oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz.U. L 191 z 28.7.2023, s. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

(11) CETS nr 185.

(12) CETS nr 224.

budapesztańskiej zawiera zaktualizowane przepisy dotyczące wymiany elektronicznego materiału dowodowego[13].

Unia Europejska i jej państwa członkowskie są również stronami dwóch głównych instrumentów Organizacji Narodów Zjednoczonych dotyczących wymiaru sprawiedliwości w sprawach karnych, które zostały przyjęte niemal powszechnie: Konwencji Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej (konwencja z Palermo)[14] oraz Konwencji Narodów Zjednoczonych przeciwko korupcji (UNCAC)[15].

Postanowienia nowej konwencji są dostosowane do tych trzech uznanych i powszechnie przyjętych instrumentów międzynarodowych oraz są z nimi zgodne.

Kwestie postępu technologii informacyjnych oraz szybkiego rozwoju nowych systemów telekomunikacyjnych i sieci komputerowych, a także wykorzystywania i nadużywania tych technologii w celach przestępczych znalazły się również w programie działań Organizacji Narodów Zjednoczonych (ONZ). 21 grudnia 2010 r. Zgromadzenie Ogólne ONZ przyjęło rezolucję nr 65/230, w której zwróciło się do Komisji ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości Sądownictwa Karnego o powołanie otwartej międzyrządowej grupy ekspertów w celu przeprowadzenia kompleksowego badania problemu cyberprzestępczości.

Zgromadzenie Ogólne ONZ przyjęło rezolucję 73/187 z dnia 17 grudnia 2018 r. w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych. W dniu 27 grudnia 2019 r. Zgromadzenie Ogólne ONZ przyjęło drugą

---

(13) Rada przyjęła decyzje upoważniające państwa członkowskie do podpisania i ratyfikowania drugiego protokołu dodatkowego w interesie UE: decyzja Rady (UE) 2022/722 z dnia 5 kwietnia 2022 r. upoważniająca państwa członkowskie do podpisania, w interesie Unii Europejskiej, Drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości dotyczącego wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego (Dz.U. L 134 z 11.5.2022, s. 15, ELI: http://data.europa.eu/eli/dec/2022/722/oj) oraz decyzja Rady (UE) 2023/436 z dnia 14 lutego 2023 r. upoważniająca państwa członkowskie do ratyfikowania, w interesie Unii Europejskiej, Drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości dotyczącego wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego, Dz.U. L 63 z 28.2.2023, s. 48, ELI: https://eur-lex.europa.eu/eli/dec/2023/436/oj).

(14) dokument A/55/383. UE podpisała konwencję z Palermo w dniu 12 grudnia 2000 r. i ratyfikowała ją w dniu 21 maja 2004 r., a także ratyfikowała protokoły w sprawie przemytu i handlu ludźmi. Zob. 2004/579/WE: decyzja Rady z dnia 29 kwietnia 2004 r. w sprawie zawarcia, w imieniu Wspólnoty Europejskiej, Konwencji Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej (Dz.U. L 261 z 6.8.2004, s. 69, ELI: https://eur-lex.europa.eu/eli/dec/2004/579/oj); 2006/616/WE: decyzja Rady z dnia 24 lipca 2006 r. w sprawie zawarcia w imieniu Wspólnoty Europejskiej Protokołu przeciwko przemytowi migrantów drogą lądową, morską i powietrzną, uzupełniającego Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, dotyczącą tych postanowień protokołu, które są objęte zakresem zastosowania art. 179 i 181a Traktatu ustanawiającego Wspólnotę Europejską (Dz.U. L 262 z 22.9.2006, s. 24, ELI: http://data.europa.eu/eli/dec/2006/616/oj) oraz 2006/619/WE: decyzja Rady z dnia 24 lipca 2006 r. w sprawie zawarcia w imieniu Wspólnoty Europejskiej Protokołu o zapobieganiu, zwalczaniu oraz karaniu za handel ludźmi, w szczególności kobietami i dziećmi, uzupełniającego Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, dotycząca tych postanowień protokołu, które są objęte zakresem zastosowania tytułu IV część III Traktatu ustanawiającego Wspólnotę Europejską (Dz.U. L 262 z 22.9.2006, s. 51, ELI: https://eur-lex.europa.eu/eli/dec/2006/619/oj).

(15) Zbiór Traktatów ONZ, tom 2349, nr 41; dokument A/58/422. UE podpisała UNCAC w dniu 15 września 2005 r. i ratyfikowała ją w dniu 12 listopada 2008 r. Zob. 2008/801/WE: decyzja Rady z dnia 25 września 2008 r. w sprawie zawarcia w imieniu Wspólnoty Europejskiej Konwencji Narodów Zjednoczonych przeciwko korupcji (Dz.U. L 287 z 29.10.2008, s. 1, ELI: https://eur-lex.europa.eu/eli/dec/2008/801/oj).

rezolucję, nr 74/247, w tej samej sprawie, ustanawiającą otwarty międzyrządowy komitet ekspertów *ad hoc* („komitet *ad hoc*") w celu opracowania kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych. W rezolucji określono, że komitet *ad hoc* ma w pełni uwzględnić obowiązujące instrumenty międzynarodowe oraz działania podejmowane na szczeblu krajowym, regionalnym i międzynarodowym w zakresie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych, w szczególności prace i wyniki prac otwartej międzyrządowej grupy ekspertów.

W dniu 24 maja 2022 r. Rada upoważniła Komisję do uczestnictwa, w imieniu Unii Europejskiej, w negocjacjach w sprawie konwencji[16]. Komisja uczestniczyła w negocjacjach zgodnie z decyzją Rady i kierowała się wytycznymi negocjacyjnymi określonymi w tej decyzji. Komisję wspierała Europejska Służba Działań Zewnętrznych (ESDZ). Komisja regularnie konsultowała się w sprawie stanowiska Unii ze specjalnym komitetem Rady ds. negocjacji i zapewniła zgodność konwencji z odpowiednim dorobkiem prawnym UE.

Zgodnie z Porozumieniem ramowym w sprawie stosunków między Parlamentem Europejskim i Komisją Europejską[17] Komisja informowała również Parlament Europejski o przebiegu negocjacji.

Komisja przekazywała także informacje Europejskiemu Inspektorowi Ochrony Danych (EIOD) i Europejskiej Radzie Ochrony Danych (ERPD) w trakcie negocjacji i po ich zakończeniu.

W okresie od 28 lutego 2022 r. do 9 sierpnia 2024 r. komitet *ad hoc* spotkał się osiem razy na formalnych sesjach. W międzyczasie odbyły się również sesje nieformalne oraz pięć posiedzeń międzysesyjnych, podczas których przeprowadzono konsultacje z wieloma różnymi zainteresowanymi stronami, w tym z globalnymi i regionalnymi organizacjami międzyrządowymi, organizacjami pozarządowymi, organizacjami społeczeństwa obywatelskiego, instytucjami akademickimi i sektorem prywatnym.

W dniu 8 sierpnia 2024 r. komitet *ad hoc* zatwierdził w drodze konsensusu projekt tekstu konwencji i towarzyszący mu projekt rezolucji Zgromadzenia Ogólnego ONZ. Zgromadzenie Ogólne ONZ przyjęło oba dokumenty na zasadzie konsensusu w dniu 24 grudnia 2024 r.[18] Konwencja ma zostać otwarta do podpisu w Hanoi (Wietnam) w dniu 25 października 2025 r., a następnie w siedzibie głównej Organizacji Narodów Zjednoczonych w Nowym Jorku do dnia 31 grudnia 2026 r.

Konwencja wejdzie w życie po wyrażeniu przez 40 państw-stron zgody na związanie się konwencją zgodnie z postanowieniami art. 65 ust. 1 i 2.

Zgodnie z ugruntowaną praktyką dotyczącą konwencji z Palermo i UNCAC konwencja stanowi, że regionalna organizacja integracji gospodarczej, taka jak Unia Europejska, może podpisać i ratyfikować konwencję, jeżeli co najmniej jedno z państw członkowskich ją podpisze i ratyfikuje.

Przyczyny wniosku

---

(16) Decyzja Rady (UE) 2022/895 z dnia 24 maja 2022 r. w sprawie upoważnienia do podjęcia negocjacji w imieniu Unii Europejskiej dotyczących kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych (Dz.U. L 155 z 8.6.2022, s. 42, ELI: https://eur-lex.europa.eu/eli/dec/2022/895/oj).

(17) Sygnatura L 304/47.

(18) Rezolucja przyjęta przez Zgromadzenie Ogólne ONZ w dniu 24 grudnia 2024 r.; A/RES/79/243.

Konwencja jest zgodna z celami Unii określonymi w strategii ProtectEU: europejskiej strategii bezpieczeństwa wewnętrznego z 2025 r. mającej na celu zwalczanie przestępczości i ułatwianie dostępu do dowodów cyfrowych w odniesieniu do wszystkich przestępstw za pomocą instrumentów międzynarodowych, takich jak przedmiotowa konwencja. Stanowi ona uzupełnienie obowiązujących instrumentów unijnych i międzynarodowych, których UE lub jej państwa członkowskie są stronami, takich jak konwencja budapesztańska Rady Europy, a tym samym przyczynia się do walki UE z przestępczością transgraniczną.

Po pierwsze, konwencja, jako instrument ONZ, ma szerszy zasięg pod względem członkostwa niż obowiązujące instrumenty unijne i międzynarodowe. Pod tym względem jest podobna do wcześniejszych instrumentów ONZ dotyczących współpracy w sprawach karnych, które niemal powszechnie przyjęto, takich jak konwencja z Palermo i UNCAC. Może zatem umożliwić wzmocnienie współpracy w zakresie walki z cyberprzestępczością w skali globalnej.

Po drugie, konwencja opiera się na postanowieniach konwencji budapesztańskiej dotyczących kryminalizacji, które mogą jeszcze bardziej wzmocnić współpracę w oparciu o wieloletnie i sprawdzone ramy prawne. Ponieważ konwencja została przyjęta niedawno, wprowadza ona również dalsze przepisy dotyczące kryminalizacji przestępstw, których liczba drastycznie wzrosła w ostatnich latach: oszustwa internetowe, nagabywanie lub uwodzenie dziecka przez internet w celu popełnienia wobec niego przestępstwa seksualnego oraz rozpowszechnianie intymnych obrazów bez zgody osoby, której dotyczą. Są one już kryminalizowane na szczeblu UE, ale jeszcze nie na szczeblu globalnym.

Po trzecie, konwencja umożliwia wymianę między organami jej państw-stron elektronicznego materiału dowodowego dotyczącego form poważnych przestępstw, których liczba również rośnie, w tym przestępstw związanych z terroryzmem i międzynarodową przestępczością zorganizowaną. To ograniczenie do poważnych przestępstw zawęża zakres stosowania mechanizmu wyłącznie do poważnych przypadków, co pomaga zapewnić proporcjonalność. Zapobiega również nadmiernemu obciążaniu organów krajowych wnioskami i odzwierciedla różne poziomy zaufania we współpracy istniejące na szczeblu międzynarodowym.

Po czwarte, konwencja uzupełnia obowiązujące instrumenty międzynarodowe, takie jak konwencja budapesztańska, uwzględniając środki proceduralne dotyczące ochrony ofiar i świadków, narzędzia służące odzyskiwaniu dochodów pochodzących z cyberprzestępczości oraz środki współpracy międzynarodowej w zakresie przekazywania osób skazanych i postępowań karnych, wspólnych dochodzeń i współpracy organów ścigania.

Po piąte, konwencja zawiera rozdział dotyczący pomocy technicznej i budowania potencjału, aby pomóc krajom rozwijającym się w budowaniu ich potencjału i umożliwić im wnoszenie wkładu w globalną walkę z cyberprzestępczością.

Po szóste, konwencja zobowiązuje państwa-strony konwencji do poszanowania praw człowieka, w tym praw i gwarancji proceduralnych w postępowaniu karnym (takich jak prawo do rzetelnego procesu sądowego, prawo do obrony, prawo do kontroli sądowej lub innej niezależnej kontroli) oraz prawa do ochrony danych osobowych w odniesieniu do każdego środka przewidzianego w konwencji. Z uwagi na uniwersalny charakter konwencji i w uznaniu istniejących różnic w poziomie ochrony praw człowieka na całym świecie, w konwencji zawarto postanowienia wykluczające jej stosowanie do popełniania naruszeń praw człowieka i dające państwom-stronom bezprecedensowe podstawy do odmowy współpracy z innymi stronami w takich przypadkach. Więcej informacji na ten temat można znaleźć w poniższych sekcjach „Spójność z przepisami obowiązującymi w tej dziedzinie polityki”, „Prawa podstawowe” i „Szczegółowe objaśnienia poszczególnych przepisów wniosku”. Dzięki tym postanowieniom konwencja jest pierwszym tego rodzaju dokumentem

zapewniającym tak kompleksową ochronę praw człowieka i gwarancje w tym zakresie. Po wejściu w życie konwencja stanie się punktem odniesienia dla przyszłych instrumentów międzynarodowych i przyczyni się do włączenia tych gwarancji praw człowieka do głównego nurtu globalnej współpracy w sprawach karnych.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Walka z cyberprzestępczością jest priorytetem Unii Europejskiej, co Rada uznała w swoich strategicznych wytycznych z 2024 r. dotyczących planowania ustawodawczego i operacyjnego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości,[19] a Komisja w opracowanej w 2025 r. strategii ProtectEU: europejskiej strategii bezpieczeństwa wewnętrznego, w której zapowiedziano działania UE mające na celu zwalczanie przestępczości internetowej i ułatwienie dostępu do dowodów cyfrowych w odniesieniu do wszystkich przestępstw, w tym za pośrednictwem międzynarodowych instrumentów wymiany informacji i dowodów, takie jak terminowe podpisanie i zawarcie konwencji.

Komisja uznaje potrzebę dalszego rozwoju i wzmacniania zdolności organów ścigania i organów wymiaru sprawiedliwości w tej dziedzinie oraz opracowania krajowych przepisów dotyczących cyberprzestępczości, jeżeli obowiązujące przepisy nie są wystarczające. Uznaje ona również potrzebę propagowania współpracy międzynarodowej w walce z cyberprzestępczością i wspiera szereg programów budowania potencjału w wielu krajach na całym świecie, w tym w krajach rozwijających się[20]. Komisja wspiera prace otwartej międzyrządowej grupy ekspertów, Komisji ONZ ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości Sądownictwa Karnego, Biura Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC), komitetu Budapesztańskiej Konwencji o cyberprzestępczości i innych organów.

Postanowienia konwencji są zgodne z przepisami i polityką UE w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych, współpracy policyjnej i ochrony danych, a także z odpowiednimi umowami dwustronnymi i wielostronnymi, których Unia Europejska jest już stroną.

Zastrzeżenia i notyfikacje

Konwencja nie zawiera osobnego postanowienia poświęconego zastrzeżeniom. Jednak w niektórych postanowieniach wyraźnie przewidziano możliwość zgłaszania zastrzeżeń (art. 11 ust. 3; art. 23 ust. 3 lit. a); art. 23 ust. 3 akapit końcowy; art. 42 ust. 5; art. 63 ust. 3 i 4) i w sposób dorozumiany dopuszcza się inne zastrzeżenia, o ile są one zgodne z art. 19 lit. c) Konwencji wiedeńskiej o prawie traktatów[21] i międzynarodowym prawem zwyczajowym, a zatem nie są niezgodne z przedmiotem i celem konwencji. W związku z tym konwencja dopuszcza znaczną elastyczność w odniesieniu do zastrzeżeń. Państwa członkowskie powinny przyjąć jednolite podejście do zastrzeżeń i notyfikacji, jak określono w załączniku I do niniejszej decyzji. Zastrzeżenia i notyfikacje powinny być zgodne z prawem Unii i prawem międzynarodowym publicznym i nie powinny być sprzeczne z przedmiotem i celem konwencji. Warunki i zabezpieczenia w zakresie praw człowieka uznane i przewidziane w niniejszej konwencji stanowią część jej przedmiotu i celu, a zatem nie podlegają zastrzeżeniom.

---

[19] Strategiczne wytyczne dotyczące planowania ustawodawczego i operacyjnego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, 28 listopada 2024 r., pkt 19.

[20] Zob. np. wzmocnione globalne działania na rzecz walki z cyberprzestępczością (GLACY-e), pod adresem https://www.coe.int/en/web/cybercrime/glacy-e.

[21] Zbiór Traktatów ONZ, tom 1155, nr 331.

- **Spójność z innymi politykami Unii**

Konwencja jest zgodna z odpowiednimi przepisami i polityką Unii Europejskiej w obszarach, które zostaną nią objęte (współpraca międzynarodowa i wzajemna pomoc prawna między organami publicznymi państw członkowskich oraz między organami państw członkowskich i organami państw trzecich, jak opisano w sekcji „Spójność z przepisami obowiązującymi w tej dziedzinie polityki") oraz z odpowiednimi umowami dwustronnymi i wielostronnymi, których Unia Europejska jest już stroną. Nie ma ona wpływu na inne obszary polityki Unii.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Podstawą wniosku jest art. 218 ust. 5 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). W art. 218 TFUE ustanowiono procedurę negocjowania i zawierania umów pomiędzy Unią Europejską a państwami trzecimi lub organizacjami międzynarodowymi. W szczególności, w myśl jego ust. 5, Rada, na wniosek Komisji pełniącej rolę negocjatora, przyjmuje decyzję upoważniającą do podpisania umowy w imieniu Unii Europejskiej.

Materialna podstawa prawna decyzji przyjętej w trybie art. 218 ust. 5 TFUE jest uzależniona głównie od celu i treści planowanej umowy międzynarodowej, której dotyczy stanowisko, jakie ma być zajęte w imieniu Unii. Jeżeli planowana umowa międzynarodowa ma dwojaki cel lub dwa elementy składowe, a jeden z tych celów lub elementów da się określić jako główny, zaś drugi ma jedynie poboczny charakter, decyzja przyjęta w trybie art. 218 ust. 5 TFUE musi mieć jedną materialną podstawę prawną, a mianowicie podstawę, której wymaga główny lub dominujący cel lub element składowy.

Jeżeli planowana umowa międzynarodowa ma jednocześnie wiele celów lub elementów składowych, które są nierozerwalnie powiązane, a żaden nie ma charakteru pobocznego w stosunku do pozostałych, materialna podstawa prawna decyzji przyjętej w trybie art. 218 ust. 5 TFUE musi – na zasadzie wyjątku – obejmować różne, odpowiadające tym celom i elementom podstawy prawne.

Jeżeli chodzi o sprawy dotyczące ułatwiania współpracy między organami sądowymi lub równoważnymi organami w ramach ścigania karnego i wykonywania orzeczeń, materialną podstawą prawną jest art. 82 ust. 1 TFUE. W odniesieniu do definicji przestępstw w dziedzinie cyberprzestępczości materialną podstawą prawną jest art. 83 ust. 1 TFUE. W odniesieniu do środków dotyczących współpracy organów ścigania materialną podstawą prawną jest art. 87 ust. 2 TFUE. W odniesieniu do ochrony danych osobowych materialną podstawą prawną jest art. 16 TFUE.

- **Kompetencja Unii**

Przedmiotem konwencji jest walka z cyberprzestępczością między innymi poprzez kryminalizację niektórych poważnych szkodliwych rodzajów zachowań i nawiązanie w tym celu współpracy międzynarodowej, w tym w odniesieniu do elektronicznego materiału dowodowego. Wchodzi to w zakres kompetencji dzielonych między Unią a państwami członkowskimi zgodnie z art. 4 ust. 2 lit. j) TFUE.

Niektóre postanowienia konwencji, w szczególności postanowienia dotyczące ochrony danych, wchodzą w zakres obszarów objętych w dużym stopniu wspólnymi przepisami, na które konwencja może mieć wpływ lub których zakres mógłby zostać zmieniony. W związku z tym, w odniesieniu do tych obszarów i zgodnie z art. 3 ust. 2 TFUE, Unia posiada wyłączną kompetencję zewnętrzną do podpisania konwencji.

Podpisanie konwencji przez Komisję Europejską w interesie Unii może zatem nastąpić na podstawie art. 16, art. 82 ust. 1, art. 83 ust. 1, art. 87 ust. 1 i art. 218 ust. 5 TFUE.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Działanie na poziomie UE służy promowaniu harmonijnego stosowania postanowień konwencji w państwach członkowskich UE i zapewnia jej zgodność z obowiązującymi i przyszłymi instrumentami UE. Ponadto działania UE w tej dziedzinie zwiększają łączną siłę oddziaływania i wpływ UE i jej państw członkowskich w ramach mechanizmów wdrażania konwencji, takich jak Konferencja Państw-Stron (art. 57), a także w przyszłych negocjacjach Protokołów (art. 62) do konwencji.

- **Proporcjonalność**

Cele Unii w odniesieniu do niniejszego wniosku przedstawione w sekcji „Przyczyny wniosku" powyżej można osiągnąć jedynie poprzez zawarcie wiążącej umowy międzynarodowej przewidującej niezbędne środki współpracy przy jednoczesnym zapewnieniu odpowiedniej ochrony praw podstawowych. Konwencja osiąga ten cel. Postanowienia konwencji ograniczają się do tego, co jest konieczne do osiągnięcia jej głównych celów i nie naruszają obowiązujących instrumentów UE lub instrumentów międzynarodowych, których UE jest stroną.

- **Wybór instrumentu**

Art. 218 ust. 5 TFUE stanowi, że Komisja lub Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, w zależności od przedmiotu planowanej umowy, przedkładają wnioski Radzie, która przyjmuje decyzję upoważniającą do podpisania umowy międzynarodowej. Biorąc pod uwagę przedmiot konwencji, Komisja powinna przedstawić odpowiedni wniosek.

3. WYNIKI OCEN *EX POST,* KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Oceny *ex post*/oceny adekwatności obowiązującego prawodawstwa**

Nie dotyczy

- **Konsultacje z zainteresowanymi stronami**

14 stycznia 2022 r. Komisja opublikowała na swojej stronie internetowej zaproszenie do zgłaszania uwag dotyczących tej inicjatywy, gdzie można było zgłaszać uwagi przez cztery tygodnie. Indywidualne odpowiedzi na zaproszenie do zgłaszania uwag opublikowano na stronie internetowej poświęconej konsultacjom. Uwagi te uwzględniono przy przygotowywaniu wniosku Komisji dotyczącego rozpoczęcia negocjacji w sprawie konwencji.

Aby zapewnić większą przejrzystość procesu, w rezolucji Zgromadzenia Ogólnego ONZ 75/282 określającej kwestie organizacyjne dotyczące komitet *ad hoc* zapewniono udział w sesjach merytorycznych przedstawicieli zainteresowanych światowych i regionalnych organizacji międzyrządowych, w tym przedstawicieli organów ONZ, wyspecjalizowanych agencji i funduszy, a także przedstawicieli komisji funkcjonalnych Rady Gospodarczej i Społecznej w charakterze obserwatorów. Ponadto rezolucja ta umożliwiła organizacjom pozarządowym (w tym globalnym i regionalnym organizacjom międzyrządowym, organizacjom pozarządowym, organizacjom społeczeństwa obywatelskiego, instytucjom akademickim i sektorowi prywatnemu) rejestrowanie się i udział w sesjach komitetu *ad hoc,* gdzie regularnie miały one możliwość przedstawiania swoich opinii podczas sesji plenarnych

poświęconych omawianym rozdziałom. Zgodnie z tą rezolucją odbyło się pięć międzysesyjnych sesji konsultacyjnych z zainteresowanymi stronami. Zainteresowane strony mogły również przedłożyć materiały pisemne, które opublikowano na stronie internetowej komitetu *ad hoc*.

Komisja, pełniąc rolę negocjatora, regularnie konsultowała się również z różnymi zainteresowanymi stronami przez cały czas trwania negocjacji i uwzględniała ich uwagi.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Podczas negocjacji Komisja, jako przedstawiciel Unii, konsultowała się ze specjalnym komitetem Rady ds. negocjacji zgodnie z decyzją Rady z dnia 24 maja 2022 r. upoważniającą Komisję do udziału w negocjacjach w imieniu Unii. Jako członkowie ONZ państwa członkowskie UE mogły uczestniczyć we wszystkich sesjach negocjacyjnych. W trakcie negocjacji Komisja konsultowała się z ich przedstawicielami w sprawie sformułowania stanowiska Unii. Komisja prowadziła również regularne konsultacje z zainteresowanymi stronami (zob. sekcja „Konsultacje z zainteresowanymi stronami" powyżej).

- **Ocena skutków**

Istotne skutki przedstawiono w niniejszym uzasadnieniu.

- **Sprawność regulacyjna i uproszczenie**

Konwencja może mieć wpływ na niektóre organy publiczne i kategorie dostawców usług. W związku z intensywniejszą współpracą międzynarodową w zakresie wymiany elektronicznych materiałów dowodowych w celu zwalczania cyberprzestępczości i przestępstw wykorzystujących cyberprzestrzeń może wzrosnąć liczba wniosków o udostępnienie elektronicznego materiału dowodowego, które organy centralne państw członkowskich UE odpowiedzialne za wzajemną pomoc prawną mogą otrzymywać od swoich odpowiedników w innych państwach-stronach konwencji, a następnie przekazywać, z zastrzeżeniem wszystkich mających zastosowanie przepisów i procedur krajowych, dostawcom usług mającym siedzibę w ich państwie. Jednocześnie ramy prawne współpracy międzynarodowej w zakresie cyberprzestępczości, które konwencja ustanawia na skalę globalną, a także zawarte w niej zabezpieczenia i warunki zapewnią dostawcom usług większą pewność prawa w odniesieniu do wniosków o dostęp do danych, z którymi mogą się spotkać w ramach współpracy między państwami w sprawach karnych.

- **Prawa podstawowe**

Konwencja określa zabezpieczenia umożliwiające państwom członkowskim UE przestrzeganie zobowiązań w zakresie praw człowieka wynikających z prawa międzynarodowego, unijnego i krajowego. Zabezpieczenia te zapobiegają również nadużywaniu tego instrumentu ONZ przez państwa-strony do popełniania lub uzasadniania naruszeń praw człowieka.

Postanowienia konwencji obejmują środki proceduralne i środki współpracy międzynarodowej w sprawach karnych, takie jak ekstradycja, wzajemna pomoc prawna i wymiana elektronicznego materiału dowodowego, które mogłyby kolidować z prawami podstawowymi, takimi jak prawo do wolności i do ochrony przed nieludzkim i poniżającym traktowaniem oraz prawo do prywatności i do ochrony danych osobowych. W konwencji zastosowano podejście oparte na prawach i przewidziano zarówno horyzontalne, jak i specyficzne dla danego kontekstu solidne warunki i zabezpieczenia w zakresie praw człowieka, które są zgodne z obowiązującymi międzynarodowymi instrumentami dotyczącymi praw człowieka i współpracy w sprawach karnych. W konwencji uwzględniono również te zagrożenia dla praw człowieka, które są nieodłącznie związane ze zwalczaniem

cyberprzestępczości i charakterem internetu. W odniesieniu do zobowiązań państw-stron w zakresie praw człowieka, w konwencji wielokrotnie odwołano się do „prawa międzynarodowego praw człowieka". To szerokie sformułowanie obejmuje zarówno instrumenty międzynarodowe, jak i międzynarodowe prawo zwyczajowe dotyczące praw człowieka, a tym samym zapewnia jak najszersze stosowanie międzynarodowych zobowiązań w zakresie praw człowieka w odniesieniu do wszystkich przyszłych stron konwencji, niezależnie od tego, czy są one stronami konkretnych międzynarodowych instrumentów dotyczących praw człowieka.

W art. 6 określono nadrzędny wymóg, aby państwa-strony przestrzegały przy wdrażaniu konwencji swoich zobowiązań wynikających z prawa międzynarodowego praw człowieka. Wykluczono w nim również możliwość interpretowania konwencji przez którekolwiek z państw-stron jako zezwalającej im na wykorzystanie tego instrumentu prawnego do ograniczania praw człowieka lub podstawowych wolności. Aby podkreślić ten obowiązek w kontekście cyfrowym, w którym ta konwencja funkcjonuje, w art. 6 ust. 2 zawarto również niewyczerpujący wykaz tych praw człowieka i podstawowych wolności, które mogą być bardziej narażone na potencjalne nadużycia w sferze cyfrowej, w tym wolności wypowiedzi, sumienia, opinii, religii lub przekonań, pokojowego zgromadzania się i zrzeszania się. Ten przepis horyzontalny, ze względu na swoje umiejscowienie i charakter, ma zastosowanie do całej konwencji i stanowi część jej przedmiotu i celu.

Również art. 21 ust. 4 jest przepisem horyzontalnym i dotyczy harmonizacji ścigania, orzekania i karania z tytułu przestępstw określonych w konwencji. Zawiera on wymóg, zgodnie z którym państwa-strony zapewniają, aby każda osoba ścigana za przestępstwa określone zgodnie z niniejszą konwencją korzystała ze wszystkich praw i gwarancji zgodnych z prawem krajowym i spójnych z mającymi zastosowanie zobowiązaniami międzynarodowymi państwa-strony, w tym z prawem do rzetelnego procesu sądowego i prawem do obrony.

W art. 24 zawarto horyzontalne warunki i zabezpieczenia dotyczące uprawnień i środków proceduralnych przewidzianych w konwencji zarówno na szczeblu krajowym, jak i międzynarodowym. Od państw-stron wymaga się zapewnienia, aby wykonywane przez nie uprawnienia proceduralne podlegały warunkom i zabezpieczeniom, które zapewniają ochronę praw człowieka, zgodnie z ich zobowiązaniami wynikającymi z prawa międzynarodowego praw człowieka oraz aby uwzględniały zasadę proporcjonalności. Takie warunki i zabezpieczenia mające zastosowanie do uprawnień i procedur przewidzianych w konwencji obejmują między innymi kontrolę sądową lub inną niezależną kontrolę, prawo do skutecznego środka odwoławczego (obejmującego kilka środków w odniesieniu do osób, których prawa człowieka zostały naruszone), podstawy uzasadniające zastosowanie oraz ograniczenie zakresu i czasu trwania uprawnień i procedur.

Art. 36 zawiera, po raz pierwszy w instrumencie ONZ dotyczącym wymiaru sprawiedliwości w sprawach karnych, przepis poświęcony ochronie danych osobowych. Ma on zastosowanie do wszelkich przypadków przekazywania danych osobowych na mocy konwencji. Przekazywanie takie może odbywać się wyłącznie zgodnie z prawem krajowym i zobowiązaniami wynikającymi z prawa międzynarodowego państwa-strony przekazującego dane. Zanim dane osobowe będą mogły zostać przekazane innemu państwu-stronie, państwa-strony mogą odmówić ich przekazania, jeżeli nie można ich udostępnić zgodnie z obowiązującymi przepisami o ochronie danych. Aby zapewnić zgodność ze swoim prawem krajowym dotyczącym ochrony danych osobowych i móc odpowiedzieć na wniosek o współpracę międzynarodową, państwo-strona może nałożyć na państwo wzywające odpowiednie warunki. Państwa-strony są zobowiązane do zapewnienia, aby dane osobowe otrzymane przez nie zgodnie z niniejszą konwencją, w ramach wniosku o współpracę

międzynarodową lub w odpowiedzi na wniosek, podlegały skutecznym i odpowiednim zabezpieczeniom w ich odpowiednich ramach prawnych. Państwa-strony mogą przekazywać otrzymane dane osobowe państwu trzeciemu lub organizacji międzynarodowej wyłącznie za uprzednią zgodą państwa-strony, które je pierwotnie przekazało, co może wymagać uzyskania zgody w formie pisemnej.

W konwencji przewidziano kompleksowe zabezpieczenia w odniesieniu do ekstradycji i wzajemnej pomocy prawnej. Państwa-strony mają możliwość odrzucenia wniosku o ekstradycję lub wzajemną pomoc prawną w przypadku braku podwójnej karalności (art. 37 ust. 1 i art. 40 ust. 8).

Konwencja zawiera dalsze podstawy odmowy współpracy, które są zgodne z obowiązującymi instrumentami międzynarodowymi. Art. 37 ust. 8 i 15, art. 40 ust. 8, 21 i 22 umożliwiają państwom-stronom odrzucenie wniosku o współpracę międzynarodową w wielu przypadkach, na przykład jeżeli wniosek o wzajemną pomoc prawną nie został złożony zgodnie z postanowieniami art. 40; jeżeli wezwane państwo-strona uzna, że wykonanie wniosku może naruszyć jego suwerenność, bezpieczeństwo, porządek publiczny lub inne podstawowe interesy (co często interpretuje się na szczeblu międzynarodowym jako obejmujące również względy związane z prawami człowieka); jeżeli prawo krajowe wezwanego państwa-strony zabrania organom tego państwa podjęcia działania, o które wnioskowano, w odniesieniu do jakiegokolwiek podobnego przestępstwa; jeżeli byłoby to sprzeczne z systemem prawnym wezwanego państwa-strony w zakresie wzajemnej pomocy prawnej; oraz jeżeli wezwane państwo-strona ma uzasadnione podstawy, by sądzić, że wniosek złożono w celu ścigania lub ukarania danej osoby ze względu na jej płeć, rasę, język, wyznanie, narodowość, pochodzenie etniczne lub poglądy polityczne, lub że pozytywne rozpatrzenie wniosku zaszkodziłoby sytuacji tej osoby z którejkolwiek z wymienionych przyczyn. Stosowanie tego ostatniego zabezpieczenia w odniesieniu do środków wzajemnej pomocy prawnej, takich jak wymiana elektronicznego materiału dowodowego, jest rzadkością w większości międzynarodowych instrumentów dotyczących współpracy w sprawach karnych. Stanowi ono ważną dodatkową gwarancję zapobiegającą wymierzaniu działań przeciwko osobom fizycznym, organizacjom sektora prywatnego, mediom lub organizacjom społeczeństwa obywatelskiego oraz ich aktywom. Zabezpieczenie to, pozostałe podstawy odmowy oraz wymóg podwójnej karalności umożliwiają państwom-stronom odmowę współpracy międzynarodowej w sprawach, które uznają za umotywowane politycznie.

Warunki i zabezpieczenia w zakresie praw człowieka uznane i przewidziane w niniejszej konwencji stanowią część jej przedmiotu i celu oraz są nierozerwalnie związane z uprawnieniami i procedurami w niej przewidzianymi. W związku z tym te warunki i zabezpieczenia nie mogą być przedmiotem zastrzeżeń.

Konwencja przewiduje również mechanizm okresowego przeglądu jej wdrażania przez Konferencję Państw-Stron (art. 57 ust. 5 lit. f)). Przegląd ten powinien obejmować wszystkie postanowienia konwencji, w tym jej warunki i zabezpieczenia, zgodnie z innymi obowiązującymi międzynarodowymi instrumentami i mechanizmami w tej samej dziedzinie.

4. WPŁYW NA BUDŻET

Wniosek nie ma wpływu na budżet Unii. Państwa członkowskie UE mogą ponieść jednorazowe koszty związane z wdrożeniem konwencji, a koszty ponoszone przez organy państw członkowskich mogą umiarkowanie wzrosnąć ze względu na oczekiwany wzrost liczby wniosków o współpracę międzynarodową.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Nie istnieje plan wdrożenia, ponieważ państwa członkowskie będą zobowiązane do wdrożenia konwencji po jej podpisaniu i ratyfikacji.

W odniesieniu do monitorowania Komisja będzie brała udział w posiedzeniach Konferencji Państw-Stron, na których Unia Europejska będzie uznawana za stronę konwencji i będzie mogła wykonywać prawo głosu, dysponując liczbą głosów równą liczbie państw członkowskich będących stronami konwencji w odniesieniu do przyjmowania poprawek i protokołów uzupełniających do konwencji. Komisja będzie regularnie informować Parlament Europejski o wynikach przeglądu i monitorowania wdrażania konwencji przez Konferencję Państw-Stron.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Celem konwencji jest wzmocnienie współpracy międzynarodowej w zakresie przestępstw określonych w konwencji oraz gromadzenia elektronicznego materiału dowodowego dotyczącego przestępstw określonych w konwencji i innych poważnych przestępstw do celów specjalnych dochodzeń lub postępowań karnych. W tym względzie konwencja ma również na celu promowanie pomocy technicznej i budowania potencjału, w szczególności z korzyścią dla krajów rozwijających się.

Przepisy ogólne (rozdział I (art. 1–6))

W rozdziale I określono ogólny zakres i cel konwencji, a także definicje stosowane w jej treści. W większości przypadków przepisy te są standardowymi sformułowaniami i zaczerpnięto je z konwencji budapesztańskiej oraz dwóch obowiązujących instrumentów ONZ dotyczących wymiaru sprawiedliwości w sprawach karnych (konwencja z Palermo i UNCAC).

W art. 2 zawarto definicje terminów, które są spójne z definicjami zawartymi w konwencji budapesztańskiej, jej drugim protokole dodatkowym oraz dwóch obowiązujących instrumentach ONZ dotyczących wymiaru sprawiedliwości w sprawach karnych (konwencja z Palermo i UNCAC). W porównaniu z tymi instrumentami do konwencji dodano tylko jedną nową definicję „danych dotyczących treści", która została zaczerpnięta z modelowej ustawy UNODC o wzajemnej pomocy prawnej w sprawach karnych[(22)] oraz z definicji zawartej w rozporządzeniu w sprawie elektronicznego materiału dowodowego[(23)].

W art. 3 określono zakres zastosowania konwencji jako obejmujący zapobieganie przestępstwom określonym zgodnie z niniejszą konwencją, prowadzenie dochodzeń w ich sprawie i ściganie ich, a także odzyskiwanie dochodów pochodzących z tych przestępstw. Zakres konwencji obejmuje również gromadzenie i udostępnianie dowodów w formie elektronicznej w ramach specjalnych dochodzeń lub postępowań karnych zgodnie z art. 23 i 35 (zob. dalsze szczegóły poniżej w sekcjach „Środki proceduralne i egzekwowanie prawa (rozdział IV (art. 23–34))" oraz „Współpraca międzynarodowa (rozdział V (art. 35–52))").

---

(22) Modelowa ustawa UNODC o wzajemnej pomocy prawnej w sprawach karnych (2007 r.), zmieniona przepisami dotyczącymi elektronicznego materiału dowodowego i stosowania specjalnych technik śledczych (2022 r.); E/CN.15/2022/CRP.6.

(23) Zob. rozporządzenie (UE) 2023/1543 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, art. 3 ust. 12.

Art. 4 stanowi, że przestępstwa określone w innych mających zastosowanie konwencjach i protokołach ONZ (których państwa-strony są stronami) powinny podlegać karze niezależnie od tego, czy zostały popełnione w internecie czy poza nim. W ustępie drugim ogranicza się zakres stosowania tego artykułu, podkreślając, że przepis ten nie stanowi podstawy prawnej do tworzenia nowych lub dodatkowych przestępstw poza tymi, które zostały określone w mających zastosowanie konwencjach i protokołach ONZ.

Art. 5 jest standardowym postanowieniem dotyczącym poszanowania zasady suwerenności, powielającym brzmienie odpowiednich postanowień konwencji z Palermo i UNCAC.

Art. 6 jest przepisem bezprecedensowym w porównaniu z dwoma instrumentami ONZ dotyczącymi wymiaru sprawiedliwości w sprawach karnych i konwencją budapesztańską. Zawiera on jasne określenie przedmiotu i celu konwencji oraz pełni funkcję ważnego zabezpieczenia przed jej niewłaściwym stosowaniem. W ustępie pierwszym określono nadrzędny cel ogólny, zgodnie z którym wszystkie środki podejmowane w celu wdrożenia konwencji muszą być zgodne z międzynarodowymi zobowiązaniami w zakresie praw człowieka podjętymi przez każde państwo-stronę. W ustępie drugim rozwinięto ten cel, potwierdzając, że konwencji nie można interpretować w sposób naruszający jakiekolwiek prawa człowieka, czy to ekonomiczne, społeczne i kulturalne, czy też obywatelskie i polityczne. Przepis ten zawiera niewyczerpujący wykaz praw uznawanych za szczególnie podatne na naruszenia za pomocą środków mających na celu zwalczanie cyberprzestępczości, takich jak wolność wypowiedzi, sumienia, opinii, religii lub przekonań, pokojowego zgromadzania się i zrzeszania się. W związku z tym zakres konwencji jest również ograniczony przez ten przepis, co zapobiega przyszłym próbom zbyt szerokiego stosowania przez państwa-strony środków dotyczących współpracy międzynarodowej przewidzianych w konwencji.

Kryminalizacja (rozdział II (art. 7–21))

W art. 7–17 określono harmonizację kryminalizacji czynów oraz elementów cyberprzestępstw i niektórych przestępstw wykorzystujących cyberprzestrzeń. Cyberprzestępstwa (art. 7–11) wzorowane są na przestępstwach określonych w konwencji budapesztańskiej. Przestępstwa wykorzystujące cyberprzestrzeń (art. 12–16) również zostały zainspirowane konwencją budapesztańską i m.in. harmonizują przestępstwa oszustwa związanego z systemami technologii informacyjno-komunikacyjnych (w tym scamem jako rodzajem oszustwa); przestępstwa związane z materiałami przedstawiającymi niegodziwe traktowanie dzieci w celach seksualnych w internecie; a także przestępstwa nagabywania w celu popełnienia przestępstwa seksualnego wobec dziecka oraz rozpowszechniania intymnych obrazów bez zgody osoby, której dotyczą. Wszystkie przestępstwa określone w konwencji wymagają dwóch zasadniczych elementów: umyślności oraz popełnienia czynu zabronionego bezprawnie. Pojęcie „bezprawnie” stanowi wymóg odpowiedzialności karnej uzależniony od kontekstu, który umożliwia państwom-stronom elastyczność w stosowaniu, zgodnie z ich prawem krajowym i zobowiązaniami międzynarodowymi. W tym względzie warunek „bezprawnie” ma na celu zapewnienie, aby na przykład postępowanie organów ścigania podczas prowadzenia dochodzenia w sprawie przestępstw lub postępowanie w celach bezpieczeństwa, naukowych, medycznych, artystycznych lub innych zgodnych z prawem, uzasadnionych lub dozwolonych celach było wyłączone z zakresu kryminalizacji. W tym względzie w art. 14 ust. 4 przewidziano wyraźne zwolnienie z kryminalizacji zachowania dzieci w odniesieniu do samodzielnie wygenerowanych materiałów przedstawiających je same lub produkowania, przekazywania lub posiadania za zgodą dzieci materiałów opisanych w art. 14 ust. 2 lit. a)–c), w przypadku gdy zachowania przedstawione w tych materiałach są zgodne z prawem krajowym i gdy takie materiały są przechowywane wyłącznie do prywatnego wykorzystania przez zaangażowane osoby i za ich obopólną zgodą.

Art. 17 zawiera wymóg kryminalizacji prania dochodów z przestępstwa i jest inspirowany odpowiednimi postanowieniami konwencji z Palermo i UNCAC. Zgodnie z uwagami interpretacyjnymi do poszczególnych artykułów konwencji, załączonymi do rezolucji w sprawie przyjęcia konwencji, zachowanie uznaje się za przestępstwo w rozumieniu art. 17 tylko wtedy, gdy leżący u podstaw czyn zabroniony związany z bardziej złożonym przestępstwem prania dochodów stanowi przestępstwo określone zgodnie z art. 7–16 konwencji.

W art. 18 powtórzono odpowiednie postanowienia konwencji z Palermo i UNCAC dotyczące ustanowienia wymogów minimalnych odpowiedzialności osób prawnych za przestępstwa określone zgodnie z niniejszą konwencją (tj. przestępstwa określone w art. 7–17). Taka odpowiedzialność wiąże się z udziałem osób prawnych w jednym z przestępstw skodyfikowanych w art. 7–17, z zastrzeżeniem tych samych wymogów, które mają zastosowanie do osób fizycznych polegających na „umyślnym i bezprawnym" popełnianiu przestępstwa oraz zgodnie z zasadami prawnymi każdego państwa-strony (ust. 1 i 2).

Art. 19 i 20 odzwierciedlają odpowiednie postanowienia konwencji z Palermo i UNCAC, przewidując wymogi minimalne dotyczące określania przestępstw z tytułu udziału, usiłowania i przygotowania do popełnienia oraz przedawnienia zgodnie z prawem krajowym państw stron oraz, w razie potrzeby, w odniesieniu do przestępstw określonych w konwencji. Chociaż przekazywanie przez internet i kontrolowanie w internecie danych, które mogą mieć znaczenie dla przestępstwa, opiera się na pomocy dostawców usług, dostawca usług, który nie ma zamiaru popełnienia przestępstwa, nie powinien ponosić odpowiedzialności na podstawie art. 19. W związku z tym dostawca usług nie ma obowiązku aktywnego monitorowania treści w celu uniknięcia odpowiedzialności karnej na mocy tego przepisu.

Art. 21 jest również inspirowany konwencją z Palermo i UNCAC i przewiduje wymogi minimalne dotyczące ścigania przestępstw, orzekania i sankcji w odniesieniu do przestępstw określonych zgodnie z konwencją. Ust. 4 zawiera wymóg, zgodnie z którym państwa-strony zapewniają, aby każda osoba ścigana za przestępstwa określone zgodnie z niniejszą konwencją korzystała ze wszystkich praw i gwarancji spójnych ze zobowiązaniami międzynarodowymi państw-stron, w tym z prawa do rzetelnego procesu sądowego i prawa do obrony.

Jurysdykcja (rozdział III (art. 22))

Art. 22 odzwierciedla również odpowiednie postanowienia konwencji z Palermo, UNCAC i konwencji budapesztańskiej oraz reguluje ustanowienie obowiązkowych i fakultatywnych form jurysdykcji w razie potrzeby w odniesieniu do przestępstw określonych zgodnie z konwencją.

Środki proceduralne i egzekwowanie prawa (rozdział IV (art. 23–34))

W art. 23 określono zakres uprawnień krajowych i środków proceduralnych umożliwiających współpracę międzynarodową: ma ona zastosowanie do specjalnych dochodzeń lub postępowań karnych dotyczących przestępstw określonych zgodnie z konwencją; innych przestępstw popełnionych za pośrednictwem systemu technologii informacyjno-komunikacyjnych, a także gromadzenia dowodów w formie elektronicznej dotyczących każdego przestępstwa. Zgodnie z notami interpretacyjnymi dotyczącymi poszczególnych artykułów konwencji, które zostały załączone do rezolucji w sprawie przyjęcia konwencji: „termin »dochodzenia« obejmuje sytuacje, w których na podstawie okoliczności faktycznych istnieją uzasadnione podstawy, by sądzić, że przestępstwo (w tym przestępstwo określone w art. 19 konwencji) zostało popełnione lub jest popełniane, w tym gdy takie dochodzenie ma na celu zapobieżenie popełnieniu lub udaremnienie popełnienia danego przestępstwa".

W związku z tym konwencja nie stanowi podstawy do współpracy międzynarodowej w zakresie celów prewencyjnych, a dane mogą być wymieniane tylko wtedy, gdy dotyczą konkretnego dochodzenia.

W art. 24 powtórzono, z kilkoma zmianami, odpowiednie brzmienie art. 15 konwencji budapesztańskiej. Przewidziano w nim nadrzędne warunki i zabezpieczenia w celu zapewnienia, aby uprawnienia i procedury określone w rozdziale IV podlegały odpowiedniemu poziomowi ochrony praw podstawowych, w tym stosowaniu zasady proporcjonalności. Takie warunki i zabezpieczenia obejmują między innymi kontrolę sądową lub inną niezależną kontrolę, prawo do skutecznego środka odwoławczego, podstawy uzasadniające zastosowanie oraz ograniczenie zakresu i czasu trwania takiego uprawnienia lub procedury. Warunki i zabezpieczenia ustanowione zgodnie z niniejszym artykułem mają ponadto zastosowanie na szczeblu krajowym do uprawnień i procedur określonych w rozdziale IV, zarówno do celów krajowych dochodzeń i postępowań karnych, jak i do celów prowadzenia współpracy międzynarodowej przez wezwane państwo-stronę zgodnie z rozdziałem V.

Art. 25–30 są wzorowane na odpowiednich uprawnieniach krajowych i środkach proceduralnych przewidzianych w konwencji budapesztańskiej. Są to: niezwłoczne zabezpieczenie przechowywanych danych elektronicznych; niezwłoczne zabezpieczenie i częściowe ujawnienie danych o ruchu; nakaz dostarczenia; przeszukanie i zajęcie przechowywanych danych elektronicznych; gromadzenie w czasie rzeczywistym danych o ruchu i przechwytywanie danych dotyczących treści.

Art. 31 odzwierciedla art. 31 UNCAC. Zobowiązuje on państwa-strony do przyjęcia środków umożliwiających zabezpieczenie, zajęcie i konfiskatę dochodów z przestępstwa.

Art. 32, inspirowany konwencją z Palermo i UNCAC, przewiduje możliwość utworzenia przez państwa-strony rejestru karnego w celu wykorzystania takich informacji w postępowaniu karnym dotyczącym przestępstwa określonego zgodnie z konwencją.

Art. 33 jest inspirowany konwencją z Palermo i zobowiązuje państwa-strony do podjęcia odpowiednich środków zgodnie z ich prawem krajowym w celu zapewnienia odpowiedniej ochrony świadkom.

Art. 34 jest inspirowany konwencją z Palermo i zobowiązuje państwa-strony, zgodnie z ich prawem krajowym, do podjęcia odpowiednich środków w celu zapewnienia odpowiedniej pomocy ofiarom, w szczególności ofiarom przestępstw, o których mowa w art. 14–16 konwencji. W art. 34 wymaga się również, aby podczas stosowania postanowień ust. 2–4 każde państwo-strona brało pod uwagę wiek, płeć oraz szczególne okoliczności i potrzeby ofiar, w tym szczególne okoliczności i potrzeby dzieci. W ust. 6 zachęca się państwa strony do podjęcia skutecznych kroków w celu zapewnienia zgodności z wnioskami o usunięcie lub uniemożliwienie dostępu do treści opisanych w art. 14 i 16 niniejszej konwencji w zakresie zgodnym z ich krajowymi ramami prawnymi.

Współpraca międzynarodowa (rozdział V (art. 35–52))

W art. 35 określono ogólne zasady i zakres współpracy międzynarodowej, która zobowiązuje państwa-strony do wzajemnej współpracy w celu prowadzenia dochodzeń w sprawie przestępstw określonych zgodnie z niniejszą konwencją, ścigania ich oraz gromadzenia i udostępniania elektronicznego materiału dowodowego dotyczącego tych przestępstw, a także gromadzenia i udostępniania elektronicznego materiału dowodowego dotyczącego wszelkich poważnych przestępstw zagrożonych karą pozbawienia wolności w maksymalnym wymiarze co najmniej czterech lat lub surowszą karą. W związku z tym zakres współpracy

międzynarodowej ogranicza się do przestępstw określonych zgodnie z konwencją oraz poważnych przestępstw z wyraźnym progiem karalności.

Art. 36 zawiera wyraźny przepis dotyczący ochrony danych osobowych. Przepis ten reguluje zasady przekazywania danych osobowych w ramach współpracy międzynarodowej. Przekazywanie może odbywać się wyłącznie zgodnie z prawem krajowym i zobowiązaniami wynikającymi z prawa międzynarodowego państwa-strony przekazującego dane. Państwa-strony mogą odmówić przekazania danych osobowych, jeżeli dane te nie mogą zostać dostarczone zgodnie z mającymi zastosowanie przepisami dotyczącymi ochrony danych osobowych. Dla UE oznacza to, że przed przekazaniem danych osobowych innemu państwu-stronie należy zastosować ważne zasady ochrony danych, w tym zasadę ograniczenia celu, minimalizacji danych, proporcjonalności i konieczności, zgodnie z Kartą praw podstawowych Unii Europejskiej. Państwa-strony mogą również dążyć do nałożenia odpowiednich warunków w celu osiągnięcia zgodności, aby odpowiedzieć na wniosek o przekazanie danych osobowych. Państwa-strony są zobowiązane do zapewnienia, aby dane osobowe otrzymane przez nie zgodnie z niniejszą konwencją podlegały skutecznym i odpowiednim zabezpieczeniom w ich odpowiednich ramach prawnych. Państwa-strony mogą przekazywać otrzymane dane osobowe państwu trzeciemu lub organizacji międzynarodowej wyłącznie za uprzednią zgodą państwa-strony, które je pierwotnie przekazało, co może wymagać uzyskania zgody w formie pisemnej.

Art. 37 jest inspirowany UNCAC i konwencją budapesztańską i zawiera szczegółowe zasady ekstradycji. Zgodnie z ust. 8 konwencja zezwala na odmowę ekstradycji na podstawie warunków określonych w prawie krajowym wezwanego państwa-strony. W ust. 15 ustanowiono kolejną podstawę odmowy wykonania wniosku o ekstradycję, jeżeli wniosek złożono w celu ścigania lub ukarania danej osoby ze względu na jej płeć, rasę, wyznanie, język, narodowość, pochodzenie etniczne lub poglądy polityczne, lub że pozytywne rozpatrzenie wniosku zaszkodziłoby sytuacji tej osoby z którejkolwiek z wymienionych przyczyn.

Art. 38 i 39 są inspirowane konwencją z Palermo i UNCAC i ustanawiają możliwość przekazywania osób skazanych i przekazywania postępowań karnych.

W art. 40 powtórzono postanowienia konwencji z Palermo, UNCAC i konwencji budapesztańskiej oraz określono szczegółowe przepisy dotyczące zasad i procedur dotyczących wzajemnej pomocy prawnej. W ust. 17 wymaga się, aby wnioski o wzajemną pomoc prawną były wykonywane zgodnie z prawem krajowym wezwanego państwa-strony. W ust. 19 zabrania się wzywającemu państwu-stronie przekazywania lub wykorzystywania informacji lub dowodów dostarczonych przez wezwane państwo-stronę na potrzeby dochodzeń, ścigania lub postępowań sądowych innych niż wymienione we wniosku, bez uzyskania uprzedniej zgody wezwanego państwa-strony. W ust. 8, 21 i 22 przewidziano wyczerpujące podstawy odmowy wykonania wniosków o wzajemną pomoc prawną opisane w sekcji „Prawa podstawowe”.

Art. 41, wzorowany na art. 35 konwencji budapesztańskiej, zobowiązuje państwa-strony do utworzenia sieci dostępnych przez całą dobę, siedem dni w tygodniu, w celu zapewnienia pomocy w specjalnych dochodzeniach, postępowaniach karnych lub postępowaniach sądowych dotyczących przestępstw określonych zgodnie z konwencją lub w gromadzeniu elektronicznego materiału dowodowego.

W art. 42–46 powtórzono art. 29–33 konwencji budapesztańskiej i określono szczegółowo konkretne rodzaje środków współpracy międzynarodowej w zakresie wzajemnej pomocy prawnej. Środki te obejmują: niezwłoczne zabezpieczenie przechowywanych danych elektronicznych; niezwłoczne ujawnianie zabezpieczonych danych o ruchu; dostęp do

przechowywanych danych elektronicznych; gromadzenie w czasie rzeczywistym danych o ruchu i przechwytywanie danych dotyczących treści. Jeżeli chodzi o najbardziej inwazyjne środki gromadzenia danych o ruchu w czasie rzeczywistym i przechwytywania danych dotyczących treści, państwa-strony mają bardziej ograniczony obowiązek „dołożenia starań" w celu udzielenia takiej pomocy. Obowiązek ten stanowi w istocie „zobowiązanie starannego działania" i w związku z tym w mniejszym stopniu ogranicza państwa-strony niż zobowiązania dotyczące innych środków wzajemnej pomocy prawnej, które wymagają współpracy z innymi państwami-stronami, chyba że nie spełniono obowiązujących warunków lub skorzystano z jednej z mających zastosowanie podstaw odmowy. Ponadto o pomoc w przechwytywaniu danych dotyczących treści można zwrócić się wyłącznie w przypadku poważnych przestępstw, w zakresie dozwolonym na mocy traktatów mających zastosowanie do państw stron lub na mocy ich prawa krajowego.

Art. 47 i 48 są inspirowane konwencją z Palermo i UNCAC i zachęca się w nich państwa-strony do współpracy w celu wzmocnienia działań organów ścigania w zwalczaniu przestępstw określonych zgodnie z konwencją oraz do ustanowienia wspólnych organów dochodzeniowych w tym samym celu.

Art. 49–52 są inspirowane konwencją z Palermo lub UNCAC i zawierają wymogi minimalne dotyczące środków konfiskaty, odzyskiwania i zwrotu dochodów lub mienia pochodzących z przestępstw określonych zgodnie z konwencją.

Środki zapobiegawcze (rozdział VI (art. 53))

W art. 53 zachęca się państwa-strony do dołożenia starań, zgodnie z podstawowymi zasadami ich systemów prawnych, w celu opracowania i wdrożenia lub utrzymania skutecznych i skoordynowanych polityk i najlepszych praktyk w celu ograniczenia istniejących lub przyszłych możliwości cyberprzestępczości za pomocą odpowiednich środków ustawodawczych, administracyjnych lub innych. Państwa-strony powinny promować aktywny udział odpowiednich osób i podmiotów spoza sektora publicznego, takich jak organizacje pozarządowe, organizacje społeczeństwa obywatelskiego, instytucje akademickie i podmioty sektora prywatnego, a także ogółu społeczeństwa, w odpowiednich aspektach zapobiegania przestępstwom określonym zgodnie z niniejszą konwencją. W ust. 3 przedstawiono niewyczerpujący i niewiążący wykaz środków zapobiegawczych. W ust. 3 lit. e) zawarto wyraźne odniesienie do środków zapobiegawczych uznających wkład legalnej działalności naukowców zajmujących się bezpieczeństwem, jeżeli mają one wyłącznie na celu zwiększenie i poprawę bezpieczeństwa produktów, usług i klientów dostawców usług.

Pomoc techniczna i wymiana informacji (rozdział VII (art. 54–56))

Art. 54–56 są inspirowane konwencją z Palermo lub UNCAC i zawierają postanowienia dotyczące udzielania pomocy technicznej, budowania potencjału i wymiany informacji, ze szczególnym uwzględnieniem interesów i potrzeb rozwijających się państw-stron.

Mechanizm wdrażania (rozdział VIII (art. 57–58))

Art. 57 i 58 są inspirowane UNCAC i zawierają szczegółowe informacje dotyczące Konferencji Państw-Stron, która będzie nadzorować wdrażanie konwencji i będzie uprawniona do opracowywania i przyjmowania protokołów uzupełniających do konwencji na podstawie art. 61 i 62 konwencji. Sekretarz Generalny Organizacji Narodów Zjednoczonych zapewnia usługi sekretariatu i zwołuje Konferencję Państw-Stron nie później niż rok po wejściu w życie konwencji. Od chwili zwołania będą się odbywały regularne posiedzenia Konferencji zgodnie z zasadami procedury przyjętej przez Konferencję.

Przepisy końcowe (rozdział IX (art. 59–68))

Rozdział IX konwencji zawiera przepisy końcowe. Między innymi art. 60 ust. 1 zapewnia państwom członkowskim UE będącym stronami konwencji możliwość dalszego stosowania prawa Unii we wzajemnych stosunkach. Umożliwia on również stronom konwencji budapesztańskiej i innych instrumentów międzynarodowych dalsze stosowanie tych instrumentów między sobą.

Art. 64 ust. 1 stanowi, że konwencja jest otwarta do podpisu dla wszystkich państw w Hanoi w październiku 2025 r., a następnie w siedzibie głównej Organizacji Narodów Zjednoczonych w Nowym Jorku do dnia 31 grudnia 2026 r. Zgodnie z ust. 2 konwencja jest również otwarta do podpisu przez regionalne organizacje integracji gospodarczej, takie jak Unia, pod warunkiem że co najmniej jedno państwo członkowskie podpisało konwencję zgodnie z ust. 1.

W art. 64 ust. 3 i art. 65 ust. 1 wskazano, że konwencja wchodzi w życie po wyrażeniu przez czterdzieści państw zgody na związanie się konwencją poprzez złożenie Sekretarzowi Generalnemu Organizacji Narodów Zjednoczonych dokumentów ratyfikacji, przyjęcia lub zatwierdzenia. Regionalne organizacje integracji gospodarczej, takie jak Unia, mogą złożyć dokumenty ratyfikacji, przyjęcia lub zatwierdzenia, jeżeli uczyniło to co najmniej jedno z ich państw członkowskich. W dokumencie ratyfikacji, przyjęcia, zatwierdzenia lub przystąpienia regionalna organizacja integracji gospodarczej określa zakres swoich kompetencji w odniesieniu do spraw uregulowanych w niniejszej Konwencji. Zgodnie z art. 64 ust. 4 do konwencji mogą przystąpić regionalne organizacje integracji gospodarczej, takie jak Unia, pod warunkiem że co najmniej jedno państwo członkowskie jest stroną konwencji. W chwili przystąpienia Unia deklaruje zakres swoich kompetencji w odniesieniu do spraw uregulowanych w niniejszej konwencji.

Zgodnie z art. 66 ust. 1 po upływie pięciu lat od wejścia konwencji w życie państwo-strona może zaproponować zmianę i przekazać ją Sekretarzowi Generalnemu Organizacji Narodów Zjednoczonych, który następnie przekaże proponowaną zmianę państwom-stronom oraz Konferencji Państw-Stron Konwencji w celu rozpatrzenia i podjęcia decyzji w sprawie propozycji. Na podstawie ust. 2 regionalne organizacje integracji gospodarczej, takie jak Unia, w sprawach podlegających ich kompetencji wykonują swoje prawo głosu dysponując liczbą głosów równą liczbie państw członkowskich będących stronami konwencji. Zmiana przyjęta zgodnie z ust. 1 podlega ratyfikacji, przyjęciu lub zatwierdzeniu przez państwa-strony.

W art. 61 i 62 określono przepisy dotyczące protokołów uzupełniających konwencję. W art. 61 ust. 2 zezwala się regionalnym organizacjom integracji gospodarczej, takim jak Unia, na przystąpienie do protokołu tylko wtedy, gdy organizacja ta jest stroną konwencji. Zgodnie z ust. 4 każdy protokół do konwencji jest interpretowany łącznie z konwencją, z uwzględnieniem celu tego protokołu. W art. 62 ust. 1 przewidziano, że do rozpatrzenia przez Konferencję Państw-Stron przyjęcia jakiegokolwiek protokołu uzupełniającego wymagane jest co najmniej sześćdziesiąt państw-stron. Artykuł ten stanowi również, że Konferencja Państw-Stron dołoży wszelkich starań, aby osiągnąć konsensus w sprawie każdego protokołu uzupełniającego, a dopiero po wyczerpaniu wszystkich starań, w ostateczności, w celu jego przyjęcia wymaga głosowania większością dwóch trzecich głosów państw-stron obecnych i głosujących na posiedzeniu Konferencji Państw-Stron. Zgodnie z art. 62 ust. 2 regionalne organizacje integracji gospodarczej, takie jak Unia, w sprawach podlegających ich kompetencji korzystają z prawa głosu na mocy niniejszego artykułu, dysponując liczbą głosów równą liczbie państw członkowskich będących stronami konwencji.

Na podstawie art. 67 ust. 2 regionalne organizacje integracji gospodarczej, takie jak Unia, przestają być stronami konwencji z chwilą jej wypowiedzenia przez wszystkie jej państwa członkowskie.

Rezolucji w sprawie przyjęcia konwencji towarzyszą noty interpretacyjne dotyczące art. 2, 17, 23 i 35. Chociaż takie noty interpretacyjne nie stanowią instrumentu zapewniającego autorytatywną interpretację konwencji, mają one służyć stronom jako wytyczne i pomóc stronom w jej stosowaniu. W notach interpretacyjnych przewodniczącego komitetu *ad hoc* ONZ rozesłanych podczas negocjacji poruszono również kilka kluczowych aspektów interpretacji. Na stronie internetowej komitetu *ad hoc* zamieszczono wszystkie propozycje i zmiany projektu tekstu konwencji przedstawione podczas negocjacji, dzięki czemu można uzyskać przydatne informacje na temat opracowywania kluczowych przepisów w tekście i co może mieć znaczenie dla jego interpretacji. Ponadto sprawozdanie wyjaśniające do konwencji budapesztańskiej[(24)] może również służyć państwom jako pomocne, choć nieformalne, źródło informacji na temat wielu przepisów inspirowanych konwencją budapesztańską, takich jak większość postanowień konwencji dotyczących kryminalizacji i uprawnień proceduralnych.

(24) Seria traktatów europejskich nr 185.

2025/0230 (NLE)

Wniosek

DECYZJA RADY

w sprawie podpisania, w imieniu Unii Europejskiej, Konwencji Narodów Zjednoczonych przeciwko cyberprzestępczości; wzmocnienie współpracy międzynarodowej w zakresie zwalczania określonych przestępstw popełnianych za pomocą systemów technologii informacyjno-komunikacyjnych oraz wymiany materiału dowodowego w formie elektronicznej w odniesieniu do poważnych przestępstw

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16, art. 82 ust. 1, art. 83 ust. 1 oraz art. 87 ust. 2, w związku z art. 218 ust. 5,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) W dniu 24 maja 2022 r. decyzją (UE) 2022/895 Rada upoważniła Komisję do uczestnictwa, w imieniu Unii Europejskiej, w negocjacjach dotyczących Konwencji Narodów Zjednoczonych przeciwko cyberprzestępczości.

(2) W dniu 24 grudnia 2024 r. Zgromadzenie Ogólne Narodów Zjednoczonych przyjęto tekst Konwencji Narodów Zjednoczonych przeciwko cyberprzestępczości; wzmocnienie współpracy międzynarodowej w zakresie zwalczania określonych przestępstw popełnianych za pomocą systemów technologii informacyjno-komunikacyjnych oraz wymiany materiału dowodowego w formie elektronicznej w odniesieniu do poważnych przestępstw („konwencja”); tekst konwencji ma zostać otwarty do podpisu w Hanoi (Wietnam) w dniu 25 października 2025 r., a następnie w siedzibie głównej Organizacji Narodów Zjednoczonych w Nowym Jorku do dnia 31 grudnia 2026 r.

(3) Konwencja jest zgodna z celami Unii Europejskiej w zakresie bezpieczeństwa, o których mowa w art. 67 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej, a mianowicie z zapewnieniem wysokiego poziomu bezpieczeństwa za pomocą środków zapobiegających przestępczości i zwalczających ją, a także za pomocą środków służących koordynacji i współpracy organów policyjnych i sądowych oraz innych właściwych organów, a także przez zbliżenie przepisów karnych.

(4) Postanowienia konwencji mają zastosowanie do specjalnych dochodzeń lub postępowań karnych dotyczących przestępstw określonych zgodnie z konwencją i dopuszczają wymianę danych wyłącznie w tym celu.

(5) Konwencja harmonizuje ograniczony zbiór jasno określonych przestępstw, zapewniając jednocześnie państwom-stronom niezbędną swobodę w celu uniknięcia nadmiernej kryminalizacji zgodnego z prawem postępowania.

(6) Konwencja ustanawia jedynie wymogi minimalne dotyczące odpowiedzialności osób prawnych za przestępstwa w niej określone i nie wymaga ustanowienia takiej odpowiedzialności karnej w sposób, który byłby niezgodny z zasadami prawnymi państwa-strony.

(7) Konwencja jest również zgodna z celami Unii Europejskiej w zakresie ochrony danych osobowych, prywatności i praw podstawowych, określonymi w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej oraz w Karcie praw podstawowych Unii Europejskiej.

(8) Konwencja przewiduje solidne zabezpieczenia w zakresie praw człowieka i wyklucza wszelkie interpretacje, które prowadziłyby do łamania praw człowieka lub podstawowych wolności, w szczególności wolności wypowiedzi, sumienia, opinii, religii lub przekonań, pokojowego zgromadzania się i zrzeszania się. Zabezpieczenia te zapewniają również możliwość odmowy współpracy międzynarodowej, jeżeli taka współpraca byłaby sprzeczna z prawem krajowym państw-stron lub gdyby taka odmowa była konieczna do uniknięcia dowolnych form dyskryminacji.

(9) W odniesieniu do uprawnień i środków proceduralnych zarówno na szczeblu krajowym, jak i międzynarodowym, konwencja przewiduje horyzontalne warunki i zabezpieczenia zapewniające ochronę praw człowieka, zgodnie ze zobowiązaniami państw-stron wynikającymi z prawa międzynarodowego praw człowieka, które uwzględniają zasadę proporcjonalności. Takie warunki i zabezpieczenia obejmują między innymi kontrolę sądową lub inną niezależną kontrolę, prawo do skutecznego środka odwoławczego, podstawy uzasadniające zastosowanie oraz ograniczenie zakresu i czasu trwania uprawnień i procedur.

(10) Konwencja zawiera specjalny przepis dotyczący ochrony danych osobowych, który zapewnia, aby przed przekazaniem danych osobowych innej państwu-stronie stosowane były ważne zasady ochrony danych, w tym zasady ograniczenia celu, minimalizacji danych, proporcjonalności i konieczności, zgodnie z Kartą praw podstawowych Unii Europejskiej.

(11) Uczestnicząc w negocjacjach w imieniu Unii, Komisja zapewniła zgodność konwencji z odpowiednimi zasadami Unii Europejskiej.

(12) Szereg zastrzeżeń i notyfikacji ma znaczenie dla zapewnienia zgodności konwencji z prawem i politykami Unii, a także jednolitego stosowania konwencji przez państwa członkowskie UE w ich stosunkach ze stronami spoza UE oraz skutecznego stosowania konwencji.

(13) Zastrzeżenia i notyfikacje, w odniesieniu do których wytyczne podano w załączniku I do niniejszej decyzji, pozostają bez uszczerbku dla wszelkich innych zastrzeżeń lub deklaracji, które państwa członkowskie mogą chcieć złożyć indywidualnie, jeżeli jest to dopuszczalne.

(14) Biorąc pod uwagę, że konwencja przewiduje procedury poprawiające transgraniczny dostęp do elektronicznego materiału dowodowego i wysoki poziom zabezpieczeń, przystąpienie do niej przyczyni się do zwiększenia spójności działań Unii Europejskiej na rzecz zwalczania cyberprzestępczości i innych form przestępczości na szczeblu globalnym. Ułatwi współpracę między państwami członkowskimi UE będącymi stronami konwencji a państwami niebędącymi członkami UE, które są stronami konwencji, przy jednoczesnym zapewnieniu wysokiego poziomu ochrony osób fizycznych.

(15) Zgodnie z art. 64 konwencja jest otwarta do podpisu dla Unii.

(16) Unia powinna stać się stroną konwencji wraz ze swoimi państwami członkowskimi, ponieważ zarówno Unia, jak i jej państwa członkowskie mają kompetencje w dziedzinach objętych konwencją. Niniejsza decyzja pozostaje bez uszczerbku dla podpisania konwencji przez państwa członkowskie zgodnie z ich procedurami wewnętrznymi.

(17) Szybkie podpisanie konwencji przez Unię Europejską zapewni ponadto jej znaczący głos na wczesnym etapie wdrażania tych nowych globalnych ram walki z cyberprzestępczością.

(18) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych; swoją opinię wydał on w dniu [...].

(19) [Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Irlandia powiadomiła [, *pismem z dnia* …,] o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej decyzji.]

ALBO

[Zgodnie z art. 1 i 2 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, bez uszczerbku dla art. 4 tego protokołu, Irlandia nie uczestniczy w przyjęciu niniejszej decyzji i nie jest nią związana ani jej nie stosuje.]

(20) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Królestwa Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Królestwo Danii nie uczestniczy w przyjęciu niniejszej decyzji i nie jest nią związana ani jej nie stosuje.

(21) Należy podpisać konwencję i zatwierdzić załączone zastrzeżenia i notyfikacje,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Niniejszym udziela się upoważnienia do podpisania w imieniu Unii Europejskiej Konwencji Narodów Zjednoczonych przeciwko cyberprzestępczości; wzmocnienie współpracy międzynarodowej w zakresie zwalczania określonych przestępstw popełnianych za pomocą systemów technologii informacyjno-komunikacyjnych oraz wymiany materiału dowodowego w formie elektronicznej w odniesieniu do poważnych przestępstw (zwaną dalej „konwencją”), z zastrzeżeniem jej zawarcia.

Tekst konwencji jest dołączony do niniejszej decyzji (załącznik II).

Artykuł 2

Niniejszym zatwierdza się zastrzeżenia i notyfikacje określone w załączniku I dołączonym do niniejszej decyzji.

Artykuł 3

Niniejsza decyzja wchodzi w życie następnego dnia po jej przyjęciu.

Sporządzono w Brukseli dnia r.

W imieniu Rady
Przewodniczący
[...]