Rada
Unii Europejskiej

Bruksela, 2 grudnia 2021 r.
(OR. pl)

14614/21

Międzyinstytucjonalny numer referencyjny:
2021/0383 (NLE)

JAI 1333
COPEN 433
CYBER 321
ENFOPOL 483
TELECOM 453
EJUSTICE 106
MI 913
DATAPROTECT 277

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	25 listopada 2021 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2021) 719 final
Dotyczy:	Wniosek dotyczący DECYZJI RADY upoważniającej państwa członkowskie do ratyfikowania, w interesie Unii Europejskiej, drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego

Delegacje otrzymują w załączeniu dokument COM(2021) 719 final.

Zał.: COM(2021) 719 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 25.11.2021 r.
COM(2021) 719 final

2021/0383 (NLE)

Wniosek

DECYZJA RADY

upoważniająca państwa członkowskie do ratyfikowania, w interesie Unii Europejskiej, drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego

UZASADNIENIE

1. PRZEDMIOT WNIOSKU

Niniejszy wniosek dotyczy decyzji upoważniającej państwa członkowskie do ratyfikowania, w interesie Unii Europejskiej, drugiego protokołu dodatkowego w sprawie wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego do „budapeszteńskiej" Konwencji Rady Europy o cyberprzestępczości („protokół")[1]. Protokół służy zapewnieniu wspólnych zasad na szczeblu międzynarodowym w celu wzmocnienia współpracy w zakresie zwalczania cyberprzestępczości i gromadzenia materiału dowodowego w formie elektronicznej na potrzeby postępowań przygotowawczych lub karnych.

Niniejszy wniosek stanowi uzupełnienie odrębnego wniosku Komisji dotyczącego decyzji Rady Unii Europejskiej („Rada") upoważniającej państwa członkowskie do podpisania protokołu w interesie Unii Europejskiej.

Cyberprzestępczość nadal stanowi poważne wyzwanie dla naszego społeczeństwa. Niezależnie od starań organów ścigania i organów wymiaru sprawiedliwości cyberataki, w tym ataki z wykorzystaniem oprogramowania typu ransomware, nasilają się i stają się coraz bardziej złożone[2]. W szczególności ponadgraniczny charakter internetu sprawia, że dochodzenia w sprawie cyberprzestępstw mają niemal zawsze charakter transgraniczny, co wymaga ścisłej współpracy między organami w różnych państwach.

Elektroniczny materiał dowodowy odgrywa coraz większą rolę w postępowaniach przygotowawczych. Komisja szacuje, że obecnie organy ścigania i organy wymiaru sprawiedliwości potrzebują dostępu do elektronicznych materiałów dowodowych w 85 % postępowań przygotowawczych, w tym w postępowaniach dotyczących cyberprzestępczości[3]. Dowody dotyczące wszelkich przestępstw są w coraz większym stopniu przechowywane w formie elektronicznej przez usługodawców w zagranicznych jurysdykcjach, a skuteczna reakcja wymiaru sprawiedliwości w sprawach karnych wymaga odpowiednich środków umożliwiających uzyskanie takich dowodów w celu utrzymania praworządności.

Na całym świecie, na szczeblu krajowym, unijnym[4] i międzynarodowym, w tym za pośrednictwem protokołu, podejmowane są działania na rzecz poprawy transgranicznego dostępu do elektronicznego materiału dowodowego w postępowaniach przygotowawczych. Aby uniknąć konfliktów prawnych w przypadku ubiegania się o transgraniczny dostęp do elektronicznego materiału dowodowego, ważne jest zapewnienie kompatybilnych przepisów na szczeblu międzynarodowym.

2. KONTEKST WNIOSKU

2.1. Kontekst

„Budapeszteńska" Konwencja Rady Europy o cyberprzestępczości (CETS nr 185) („konwencja") ma na celu ułatwienie walki z przestępstwami, w których wykorzystuje się sieci komputerowe. Konwencja 1) zawiera przepisy harmonizujące elementy krajowego

[1] Tekst protokołu dołączony jest do niniejszego wniosku jako załącznik.
[2] Ocena zagrożenia poważną i zorganizowaną przestępczością w Unii Europejskiej z 2021 r. (EU SOCTA 2021).
[3] SWD(2018) 118 final.
[4] COM(2018)225 i 226 final.

prawa karnego materialnego dotyczące przestępstw i powiązane przepisy w dziedzinie cyberprzestępczości, 2) przewiduje uprawnienia w ramach krajowego prawa karnego procesowego niezbędne do dochodzenia i ścigania takich przestępstw, jak również innych przestępstw popełnianych przy użyciu systemu komputerowego lub gdy dowody mają postać elektroniczną, oraz 3) ma na celu ustanowienie szybkiego i skutecznego systemu współpracy międzynarodowej.

Do konwencji mogą przystąpić państwa członkowskie Rady Europy, a państwa niebędące członkami – na zaproszenie. Obecnie stronami konwencji jest 66 państw, w tym 26 państw członkowskich Unii Europejskiej[5]. Konwencja nie przewiduje możliwości przystąpienia do niej przez Unię Europejską. Unia Europejska ma jednak status obserwatora przy komitecie Konwencji o cyberprzestępczości (T-CY)[6].

Niezależnie od starań zmierzających do wynegocjowania nowej konwencji w sprawie cyberprzestępczości na szczeblu Organizacji Narodów Zjednoczonych[7], budapeszteńska Konwencja o cyberprzestępczości pozostaje główną wielostronną konwencją w sprawie walki z cyberprzestępczością. Unia konsekwentnie wspiera tę konwencję[8], również w ramach finansowania programów budowania zdolności[9].

W następstwie wniosków grupy ds. dowodów znajdujących się w chmurze[10] komitet Konwencji o cyberprzestępczości przyjął kilka zaleceń w celu sprostania – w tym w ramach negocjacji dotyczących drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy międzynarodowej – wyzwaniu, jakim jest fakt, że elektroniczny materiał dowodowy związany z cyberprzestępczością i innymi przestępstwami jest coraz częściej przechowywany przez usługodawców w zagranicznych jurysdykcjach, podczas gdy uprawnienia organów ścigania pozostają ograniczone do terytorium danego kraju. W czerwcu 2017 r. komitet Konwencji o cyberprzestępczości przyjął zakres zadań dotyczący przygotowania drugiego protokołu dodatkowego do konwencji w okresie od września 2017 r. do grudnia 2019 r.[11] W związku z potrzebą większej ilości czasu na sfinalizowanie rozmów, jak również z ograniczeniami wynikającymi z pandemii COVID-19 w 2020 i 2021 r. komitet Konwencji o cyberprzestępczości następnie dwukrotnie przedłużył zakres zadań: do grudnia 2020 r., a następnie do maja 2021 r.

W odpowiedzi na wezwanie Rady Europejskiej zawarte w konkluzjach z dnia 18 października 2018 r.[12] Komisja przyjęła w dniu 5 lutego 2019 r. zalecenie dotyczące decyzji Rady

---

5 Wszystkie z wyjątkiem Irlandii, która podpisała konwencję, ale jej nie ratyfikowała, niemniej jednak zobowiązała się do dążenia do przystąpienia.

6 Regulamin wewnętrzny komitetu Konwencji o cyberprzestępczości (T-CY (2013)25 rev), dostępny pod adresem www.coe.int/cybercrime

7 Rezolucja Zgromadzenia Ogólnego Narodów Zjednoczonych (ZO ONZ) 74/247 „Przeciwdziałanie wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych", grudzień 2019 r.

8 JOIN(2020) 81 final.

9 Zob. np. rozszerzone globalne działania na rzecz walki z cyberprzestępczością (GLACY)+, pod adresem https://www.coe.int/en/web/cybercrime/glacyplus

10 Sprawozdanie końcowe grupy ds. dowodów znajdujących się w chmurze przy komitecie Konwencji o cyberprzestępczości „Dostęp wymiaru sprawiedliwości w sprawach karnych do elektronicznego materiału dowodowego w chmurze: zalecenia do rozważenia przez komitet Konwencji o cyberprzestępczości" z dnia 16 września 2016 r.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690

12 https://www.consilium.europa.eu/pl/press/press-releases/2018/10/18/20181018-european-council-conslusions/

upoważniającej Komisję do uczestnictwa w imieniu Unii Europejskiej w negocjacjach w sprawie drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości[13]. Europejski Inspektor Ochrony Danych przyjął opinię dotyczącą zalecenia w dniu 2 kwietnia 2019 r.[14] Decyzją z dnia 6 czerwca 2019 r. Rada Unii Europejskiej upoważniła Komisję do uczestnictwa, w imieniu Unii Europejskiej, w negocjacjach w sprawie drugiego protokołu dodatkowego[15].

Jak wyrażono w strategii UE w zakresie unii bezpieczeństwa z 2020 r.[16], strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę z 2020 r.[17] oraz unijnej strategii zwalczania przestępczości zorganizowanej z 2021 r.[18], Komisja zobowiązała się do szybkiego i pomyślnego zakończenia negocjacji w sprawie protokołu. Parlament Europejski również uznał potrzebę zakończenia prac nad protokołem w swojej rezolucji z 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[19].

Komisja uczestniczyła, w imieniu Unii Europejskiej, w negocjacjach w sprawie protokołu, zgodnie z decyzją Rady Unii Europejskiej. Komisja konsekwentnie konsultowała się w sprawie stanowiska Unii ze specjalnym komitetem Rady ds. negocjacji.

Zgodnie z Porozumieniem ramowym w sprawie stosunków między Parlamentem Europejskim i Komisją Europejską[20] Komisja informowała również Parlament Europejski o negocjacjach za pomocą sprawozdań pisemnych i prezentacji ustnych.

Na posiedzeniu plenarnym komitetu Konwencji o cyberprzestępczości w dniu 28 maja 2021 r. komitet zatwierdził projekt protokołu na swoim szczeblu i przekazał projekt do przyjęcia przez Komitet Ministrów Rady Europy[21]. W dniu 17 listopada 2021 r. Komitet Ministrów Rady Europy przyjął protokół.

2.2. Drugi protokół dodatkowy

Protokół służy wzmocnieniu współpracy w zakresie zwalczania cyberprzestępczości i gromadzenia dowodów przestępstw w formie elektronicznej na potrzeby postępowań przygotowawczych lub karnych. W protokole uznaje się potrzebę zwiększonej i bardziej efektywnej współpracy między państwami oraz z sektorem prywatnym oraz większej jasności i pewności prawa dla usługodawców i innych podmiotów w odniesieniu do okoliczności, w których mogą oni odpowiadać na wnioski organów wymiaru sprawiedliwości w sprawach karnych innych stron o ujawnienie elektronicznego materiału dowodowego.

W protokole uznaje się również, że skuteczna współpraca transgraniczna na potrzeby wymiaru sprawiedliwości w sprawach karnych, w tym między organami sektora publicznego a podmiotami sektora prywatnego, wymaga skutecznych warunków i solidnych zabezpieczeń

---

[13] COM(2019) 71 final.
[14] Opinia EIOD dotycząca uczestnictwa w negocjacjach dotyczących drugiego protokołu dodatkowego do budapeszteńskiej konwencji o cyberprzestępczości, z dnia 2 kwietnia 2019 r., opinia 3/2019.
[15] Decyzja Rady o sygn. 9116/19.
[16] COM(2020) 605 final.
[17] JOIN(2020) 81 final.
[18] COM(2021) 170 final.
[19] Rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę.
[20] Sygnatura L 304/47.
[21] https://rm.coe.int/0900001680a2aa42

w zakresie ochrony praw podstawowych. W tym celu w protokole zastosowano podejście oparte na prawach oraz przewidziano warunki i zabezpieczenia zgodne z międzynarodowymi instrumentami dotyczącymi praw człowieka, w tym z Konwencją Rady Europy o ochronie praw człowieka i podstawowych wolności z 1950 r. W związku z tym, że elektroniczny materiał dowodowy często dotyczy danych osobowych, protokół zawiera również solidne zabezpieczenia w zakresie ochrony prywatności i danych osobowych.

Postanowienia, o których mowa w poniższych akapitach, mają szczególne znaczenie dla protokołu. Do protokołu dołączone jest szczegółowe sprawozdanie wyjaśniające. Chociaż sprawozdanie wyjaśniające nie stanowi instrumentu zapewniającego autorytatywną interpretację protokołu, ma ono na celu „naprowadzać Strony i pomagać im" w stosowaniu protokołu[22].

2.2.1. Postanowienia wspólne

Rozdział I protokołu zawiera postanowienia wspólne. W art. 2 określono zakres stosowania protokołu, zgodnie z zakresem konwencji: ma on zastosowanie do szczególnych postępowań przygotowawczych lub karnych dotyczących przestępstw związanych z systemami i danymi komputerowymi oraz do gromadzenia dowodów przestępstw w formie elektronicznej.

W art. 3 zawarto definicje dotyczące „organów centralnych", „właściwych organów", „sytuacji nadzwyczajnych", „danych osobowych" i „Strony przekazującej". Definicje te mają zastosowanie do protokołu wraz z definicjami zawartymi w konwencji.

W art. 4 określono języki, w których strony powinny składać nakazy, wnioski lub zgłoszenia na podstawie protokołu.

2.2.2. Działania w ramach współpracy

Rozdział II protokołu obejmuje działania służące zacieśnieniu współpracy. Po pierwsze, art. 5 ust. 1 stanowi, że strony współpracują na podstawie protokołu w najszerszym możliwym zakresie. W art. 5 ust. 2–5 określono zastosowanie działań wymienionych w protokole w odniesieniu do istniejących traktatów lub porozumień o wzajemnej pomocy. Art. 5 ust. 7 stanowi, że działania przewidziane w rozdziale II nie ograniczają współpracy między stronami, ani z usługodawcami i podmiotami, prowadzonej na podstawie innych obowiązujących umów, porozumień, praktyk lub prawa krajowego.

Art. 6 stanowi podstawę bezpośredniej współpracy między właściwymi organami jednej strony a podmiotami świadczącymi usługi rejestracji nazw domen na terytorium innej strony w zakresie ujawniania danych dotyczących rejestracji nazw domen.

Art. 7 stanowi podstawę bezpośredniej współpracy między właściwymi organami jednej strony a usługodawcami drugiej strony w zakresie ujawniania danych abonenta.

Art. 8 stanowi podstawę zacieśnionej współpracy między organami w zakresie ujawniania danych komputerowych.

Art. 9 stanowi podstawę współpracy między organami w zakresie ujawniania danych komputerowych w sytuacjach nadzwyczajnych.

---

[22] Zob. pkt 2 sprawozdania wyjaśniającego do protokołu.

Art. 10 stanowi podstawę wzajemnej pomocy prawnej w sytuacjach nadzwyczajnych.

Art. 11 stanowi podstawę współpracy w formie wideokonferencji.

Art. 12 stanowi podstawę prowadzenia wspólnych dochodzeń i działania wspólnych zespołów dochodzeniowo-śledczych.

2.2.3. Zabezpieczenia

W protokole zastosowano podejście oparte na prawach oraz przewidziano w nim szczególne warunki i zabezpieczenia, z których część włączono do szczególnych działań zacieśniających współpracę, jak również do rozdziału III protokołu. Art. 13 protokołu zobowiązuje strony do zapewnienia, by uprawnienia i procedury podlegały odpowiedniemu poziomowi ochrony praw podstawowych, co zgodnie z art. 15 konwencji zapewnia stosowanie zasady proporcjonalności.

Art. 14 protokołu przewiduje ochronę danych osobowych, określonych w art. 3 protokołu, zgodnie z Protokołem zmieniającym Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (CETS 223) (Konwencja 108+) i prawem Unii.

Na tej podstawie w art. 14 ust. 2–15 określono podstawowe zasady ochrony danych, w tym zasadę celowości, podstawę prawną, jakość danych oraz zasady mające zastosowanie do przetwarzania szczególnych kategorii danych, obowiązki mające zastosowanie do administratorów (w tym dotyczące zatrzymywania danych, prowadzenia rejestrów, bezpieczeństwa oraz w zakresie dalszego przekazywania danych), egzekwowalne prawa jednostki (w tym dotyczące zgłaszania, dostępu, poprawiania danych i zautomatyzowanego podejmowania decyzji), niezależny i skuteczny nadzór sprawowany przez co najmniej jeden organ, a także administracyjne i sądowe środki ochrony prawnej. Zabezpieczenia obejmują wszystkie formy współpracy określone w protokole, z dostosowaniami, w razie potrzeby, w celu uwzględnienia szczególnych cech współpracy bezpośredniej (np. w kontekście zgłaszania naruszeń). Wykonywanie niektórych praw indywidualnych można opóźnić, ograniczyć lub można odmówić ich wykonywania, jeżeli jest to konieczne i proporcjonalne do osiągnięcia ważnych celów interesu publicznego, w szczególności w celu zapobieżenia zagrożeniu dla trwających dochodzeń związanych ze ściganiem przestępstw, co jest również zgodne z prawem Unii.

Art. 14 protokołu należy również odczytywać w powiązaniu z art. 23 protokołu. Art. 23 zwiększa skuteczność zabezpieczeń zawartych w protokole, stanowiąc, że komitet Konwencji o cyberprzestępczości oceni wdrażanie i stosowanie środków przyjętych w ustawodawstwie krajowym w celu nadania skuteczności postanowieniom protokołu. W szczególności w art. 23 ust. 3 wyraźnie stwierdzono, że wdrożenie przez strony art. 14 zostanie ocenione po wyrażeniu przez dziesięć stron konwencji zgody na podporządkowanie się protokołowi.

Jako dalsze zabezpieczenie, zgodnie z art. 14 ust. 15, w przypadku gdy strona posiada istotne dowody na to, że inna strona systematycznie lub istotnie narusza zabezpieczenia określone w protokole, może zawiesić przekazywanie danych osobowych tej stronie po przeprowadzeniu konsultacji (co nie jest wymagane w pilnych przypadkach). Wszelkie dane osobowe przekazane przed zawieszeniem są nadal traktowane zgodnie z protokołem.

Ponadto, biorąc pod uwagę wielostronny charakter protokołu, w art. 14 ust. 1 lit. b) i c) protokołu zezwala się stronom w ich stosunkach dwustronnych na uzgodnienie, pod pewnymi

warunkami, alternatywnych sposobów zapewnienia ochrony danych osobowych przekazywanych na podstawie protokołu. Chociaż zabezpieczenia określone w art. 14 ust. 2–15 mają domyślnie zastosowanie do stron otrzymujących dane osobowe, na podstawie art. 14 ust. 1 lit. b) strony związane wzajemnie umową międzynarodową ustanawiającą kompleksowe ramy ochrony danych osobowych zgodnie z mającymi zastosowanie wymogami prawodawstwa tych stron mogą również opierać się na tych ramach. Dotyczy to na przykład Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (w odniesieniu do tych stron, które zezwalają na przekazywanie danych innym stronom na podstawie tej konwencji) lub umowy ramowej między UE a Stanami Zjednoczonymi (w zakresie jej stosowania, tj. w odniesieniu do przekazywania danych osobowych między organami oraz, w połączeniu ze szczególnym porozumieniem w sprawie przekazywania danych między Stanami Zjednoczonymi a UE, w odniesieniu do bezpośredniej współpracy między organami a usługodawcami). Ponadto na podstawie art. 14 ust. 1 lit. c) strony mogą również wspólnie postanowić, że przekazywanie danych osobowych odbywa się na podstawie innych umów lub porozumień między zainteresowanymi stronami. W przypadku państw członkowskich UE takie alternatywne umowy lub porozumienia mogą być podstawą przekazywania danych na podstawie protokołu tylko wtedy, gdy takie przekazywanie danych jest zgodne z wymogami unijnych przepisów o ochronie danych, a mianowicie z przepisami rozdziału V dyrektywy (UE) 2016/680 (dyrektywa o ochronie danych w sprawach karnych) oraz (w odniesieniu do bezpośredniej współpracy między organami i usługodawcami na podstawie art. 6 i 7 protokołu) rozdziału V rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych).

2.2.4. Postanowienia końcowe

Rozdział IV protokołu zawiera postanowienia końcowe. Między innymi w art. 15 ust. 1 lit. a) zapewniono możliwość odmiennego uregulowania przez strony stosunków w kwestiach określonych w protokole, zgodnie z art. 39 ust. 2 konwencji. Art. 15 ust. 1 lit. b) zapewnia państwom członkowskim UE będącym stronami protokołu możliwość dalszego stosowania prawa Unii we wzajemnych stosunkach. Art. 15 ust. 2 stanowi również, że do protokołu stosuje się art. 39 ust. 3 Konwencji.

W art. 16 ust. 3 wskazano, że protokół wejdzie w życie po wyrażeniu przez pięć stron konwencji zgody na podporządkowanie się protokołowi.

Art. 19 ust. 1 stanowi, że strony mogą zgłaszać zastrzeżenia zgodnie z art. 7 ust. 9 lit. a) i b), art. 8 ust. 13 i art. 17. Art. 19 ust. 2 stanowi, że strony mogą składać oświadczenia zgodnie z art. 7 ust. 2 lit. b) i ust. 8, art. 8 ust. 11, art. 9 ust. 1 lit. b) i ust. 5, art. 10 ust. 9, art. 12 ust. 3 i art. 18 ust. 2. Art. 19 ust. 3 stanowi, że strona przedkłada oświadczenia, zgłoszenia lub komunikaty określone w art. 7 ust. 5 lit. a) i e), art. 8 ust. 4 i 10 lit. a) i b), art. 14 ust. 7 lit. c) i ust. 10 lit. b) oraz art. 17 ust. 2.

Art. 23 ust. 1 stanowi podstawę do konsultacji między stronami, w tym za pośrednictwem komitetu Konwencji o cyberprzestępczości, zgodnie z art. 46 konwencji. Art. 23 ust. 2 stanowi również podstawę oceny stosowania i wdrażania postanowień protokołu. W art. 23 ust. 3 zagwarantowano, że ocena stosowania i wdrażania art. 14 dotyczącego ochrony danych rozpocznie się po wyrażeniu przez dziesięć stron zgody na podporządkowanie się protokołowi.

2.3. Prawo i polityka Unii w tej dziedzinie

Dziedzina regulowana protokołem jest w dużej mierze objęta wspólnymi zasadami opartymi na art. 82 ust. 1 i art. 16 TFUE. Obecne ramy prawne Unii Europejskiej obejmują

w szczególności instrumenty dotyczące egzekwowania prawa i współpracy wymiarów sprawiedliwości w sprawach karnych, takie jak dyrektywa 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, Konwencja o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej oraz decyzja ramowa Rady 2002/465/WSiSW w sprawie wspólnych zespołów dochodzeniowo-śledczych. W stosunkach zewnętrznych Unia Europejska zawarła szereg porozumień dwustronnych z państwami trzecimi, takich jak Porozumienie o wzajemnej pomocy prawnej między Unią Europejską a Stanami Zjednoczonymi Ameryki, między Unią Europejską a Japonią oraz między Unią Europejską a Norwegią i Islandią. Obecne ramy prawne Unii Europejskiej obejmują również rozporządzenie (UE) 2017/1939 wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej („EPPO"). Państwa członkowskie uczestniczące we wzmocnionej współpracy powinny zapewnić, aby EPPO mogła, w ramach wykonywania swoich kompetencji przewidzianych w art. 22, 23 i 25 rozporządzenia (UE) 2017/1939, dążyć do współpracy na podstawie protokołu w taki sam sposób jak prokuratorzy krajowi tych państw członkowskich. Te instrumenty i porozumienia odnoszą się w szczególności do art. 8, 9, 10, 11 i 12 protokołu.

Ponadto Unia przyjęła szereg dyrektyw, które wzmacniają prawa procesowe podejrzanych i oskarżonych[23]. Instrumenty te odnoszą się w szczególności do art. 6, 7, 8, 9, 10, 11, 12 i 13 protokołu. Jeden szczególny zestaw zabezpieczeń dotyczy ochrony danych osobowych, która jest prawem podstawowym zapisanym w traktatach UE i w Karcie praw podstawowych Unii Europejskiej. Dane osobowe mogą być przetwarzane wyłącznie zgodnie z rozporządzeniem (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) i dyrektywą (UE) 2016/680 (dyrektywa o ochronie danych w sprawach karnych). Podstawowe prawo każdej osoby do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się obejmuje – jako zasadniczy element – poszanowanie prywatności komunikowania się. Dane pochodzące z łączności elektronicznej mogą być przetwarzane wyłącznie zgodnie z dyrektywą 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej). Instrumenty te odnoszą się w szczególności do art. 14 protokołu.

Art. 14 ust. 2–15 protokołu przewiduje odpowiednie zabezpieczenia w zakresie ochrony danych w rozumieniu unijnych przepisów o ochronie danych, w szczególności art. 46 ogólnego rozporządzenia o ochronie danych i art. 37 dyrektywy o ochronie danych w sprawach karnych, a także stosownego orzecznictwa Trybunału Sprawiedliwości. Zgodnie

[23] Dyrektywa Parlamentu Europejskiego i Rady 2010/64/UE z dnia 20 października 2010 r. w sprawie prawa do tłumaczenia ustnego i tłumaczenia pisemnego w postępowaniu karnym, Dz.U. L 280 z 26.10.2010, s. 1; dyrektywa Parlamentu Europejskiego i Rady 2012/13/UE z dnia 22 maja 2012 r. w sprawie prawa do informacji w postępowaniu karnym, Dz.U. L 142 z 1.6.2012, s. 1; dyrektywa Parlamentu Europejskiego i Rady 2013/48/UE z dnia 22 października 2013 r. w sprawie prawa dostępu do adwokata w postępowaniu karnym i w postępowaniu dotyczącym europejskiego nakazu aresztowania oraz w sprawie prawa do poinformowania osoby trzeciej o pozbawieniu wolności i prawa do porozumiewania się z osobami trzecimi i organami konsularnymi w czasie pozbawienia wolności, Dz.U. L 294 z 6.11.2013, s. 1; dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1919 z dnia 26 października 2016 r. w sprawie pomocy prawnej z urzędu dla podejrzanych i oskarżonych w postępowaniu karnym oraz dla osób, których dotyczy wniosek w postępowaniu dotyczącym europejskiego nakazu aresztowania, Dz.U. L 297 z 4.11.2016, s. 1; dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/800 z dnia 11 maja 2016 r. w sprawie gwarancji procesowych dla dzieci będących podejrzanymi lub oskarżonymi w postępowaniu karnym, Dz.U. L 132 z 21.5.2016, s. 1; dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/343 z dnia 9 marca 2016 r. w sprawie wzmocnienia niektórych aspektów domniemania niewinności i prawa do obecności na rozprawie w postępowaniu karnym, Dz.U. L 65 z 11.3.2016, s. 1; dyrektywa Parlamentu Europejskiego i Rady 2012/13/UE z dnia 22 maja 2012 r. w sprawie prawa do informacji w postępowaniu karnym.

z wymogami prawa Unii[24] oraz w celu zagwarantowania skuteczności zabezpieczeń określonych w art. 14 protokołu państwa członkowskie powinny zapewnić powiadamianie osób, których dane zostały przekazane, z zastrzeżeniem pewnych ograniczeń, np. aby nie zagrozić trwającym dochodzeniom. Art. 14 ust. 11 lit. c) protokołu stanowi dla państw członkowskich podstawę do spełnienia tego wymogu.

Aby zachować zgodność art. 14 ust. 1 protokołu z unijnymi przepisami o ochronie danych konieczne jest również, aby państwa członkowskie rozważyły następujące kwestie w odniesieniu do możliwych alternatywnych sposobów zapewnienia odpowiedniej ochrony danych osobowych przekazywanych na podstawie protokołu. W odniesieniu do innych umów międzynarodowych ustanawiających kompleksowe ramy ochrony danych osobowych zgodnie z mającymi zastosowanie wymogami prawodawstwa zainteresowanych stron, zgodnie z art. 14 ust. 1 lit. b) państwa członkowskie powinny wziąć pod uwagę, że w przypadku bezpośredniej współpracy umowa ramowa pomiędzy UE a Stanami Zjednoczonymi musi zostać uzupełniona dodatkowymi zabezpieczeniami – które należy zapewnić w szczególnych porozumieniach dotyczących przekazywania danych między Stanami Zjednoczonymi a UE/jej państwami członkowskimi – które uwzględniają wyjątkowe wymogi dotyczące przekazywania elektronicznego materiału dowodowego bezpośrednio przez usługodawców, a nie pomiędzy organami[25].

Ponadto na podstawie art. 14 ust. 1 lit. b) protokołu państwa członkowskie powinny uznać, że w przypadku państw członkowskich UE, które są stronami Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, konwencja ta sama w sobie nie stanowi odpowiedniej podstawy dla transgranicznego przekazywania danych na podstawie protokołu innym stronom tej konwencji. W tym względzie należy zwrócić uwagę na ostatnie zdanie art. 14 ust. 1 Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[26].

Ponadto w odniesieniu do innych umów lub porozumień na podstawie art. 14 ust. 1 lit. c) państwa członkowskie powinny pamiętać, że mogą działać na podstawie takich innych umów lub porozumień wyłącznie wtedy, gdy Komisja Europejska przyjęła decyzję stwierdzającą odpowiedni stopień ochrony na podstawie art. 45 ogólnego rozporządzenia o ochronie danych

---

[24] Zob. opinia 1/15 Trybunału Sprawiedliwości (wielka izba), ECLI:EU:C:2017:592, pkt 220. Zob. również wkład EROD do konsultacji w sprawie projektu drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (konwencja budapeszteńska), 13 listopada 2019 r., s. 6 („Właściwe organy krajowe, którym przyznano dostęp do danych, muszą powiadomić osoby, których dane dotyczą, zgodnie z mającymi zastosowanie procedurami krajowymi, gdy tylko takie powiadomienie nie będzie już zagrażać dochodzeniu prowadzonemu przez te organy. […] Powiadomienie jest niezbędne, aby umożliwić zainteresowanym osobom skorzystanie m.in. z przysługującego im prawa do środka ochrony prawnej i do ochrony danych w związku z przetwarzaniem ich danych").

[25] Dlatego też w decyzji Rady z dnia 21 maja 2019 r. upoważniającej do rozpoczęcia negocjacji w celu zawarcia porozumienia między Unią Europejską a Stanami Zjednoczonymi Ameryki w sprawie transgranicznego dostępu do dowodów elektronicznych na potrzeby współpracy wymiarów sprawiedliwości w sprawach karnych (9114/19) określono wytyczne negocjacyjne zawierające szereg dodatkowych zabezpieczeń w zakresie ochrony danych. W szczególności wytyczne negocjacyjne stanowią, że „[p]orozumienie powinno uzupełnić umowę ramową dodatkowymi zabezpieczeniami, które uwzględnią poziom wrażliwości poszczególnych kategorii przedmiotowych danych oraz szczególne wymagania dotyczące przekazywania dowodów elektronicznych bezpośrednio przez dostawców usług, a nie za pośrednictwem organów", a także przekazywania dowodów od właściwych organów bezpośrednio do dostawców usług.

[26] Zob. również sprawozdanie wyjaśniające do Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, 10 października 2018 r., pkt 106–107.

(UE) 2016/679 lub art. 36 dyrektywy (UE) 2016/680 o ochronie danych w sprawach karnych w odniesieniu do danego państwa trzeciego, która obejmuje odpowiednie przekazywanie danych, albo jeżeli taka inna umowa lub takie porozumienie zapewniają odpowiednie zabezpieczenia w zakresie ochrony danych zgodnie z art. 46 ogólnego rozporządzenia o ochronie danych lub art. 37 ust. 1 lit. a) dyrektywy o ochronie danych w sprawach karnych.

Należy wziąć pod uwagę nie tylko prawo Unii w obecnym brzmieniu w danej dziedzinie, ale także jego przyszłe zmiany, o ile jest to możliwe do przewidzenia w czasie analizy. Dziedzina objęta protokołem ma bezpośrednie znaczenie dla przewidywalnych przyszłych zmian w prawie Unii. W tym kontekście należy odnotować wnioski Komisji z kwietnia 2018 r. w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego[27]. Instrumenty te odnoszą się w szczególności do art. 6 i 7 protokołu.

Komisja, uczestnicząc w negocjacjach w imieniu Unii, zapewniła, aby protokół był w pełni zgodny z prawem Unii i wynikającymi z niego obowiązkami państw członkowskich. W szczególności Komisja zapewniła, by postanowienia protokołu umożliwiały państwom członkowskim przestrzeganie podstawowych praw, wolności i ogólnych zasad prawa Unii zapisanych w traktatach UE i Karcie praw podstawowych, w tym proporcjonalności, praw procesowych, domniemania niewinności i prawa do obrony osób, wobec których toczy się postępowanie karne, a także prywatności oraz ochrony danych osobowych i danych pochodzących z łączności elektronicznej w trakcie przetwarzania takich danych, w tym przekazywania danych organom ścigania w państwach spoza Unii Europejskiej, a także wszelkich obowiązków spoczywających w tym względzie na organach ścigania i organach sądowych. Komisja uwzględniła również opinię Europejskiego Inspektora Ochrony Danych[28] i Europejskiej Rady Ochrony Danych[29].

Ponadto Komisja dopilnowała, aby postanowienia protokołu i wnioski Komisji dotyczące elektronicznego materiału dowodowego były ze sobą zgodne, w tym z uwzględnieniem zmian projektu aktu ustawodawczego w toku dyskusji ze współprawodawcami, a także aby protokół nie prowadził do kolizji przepisów. W szczególności Komisja dopilnowała, by protokół zawierał odpowiednie zabezpieczenia w zakresie ochrony danych i prywatności, które umożliwiają usługodawcom UE wywiązanie się z obowiązków wynikających z unijnych przepisów o ochronie danych i prywatności w zakresie, w jakim protokół stanowi podstawę prawną dla przekazywania danych w odpowiedzi na nakazy lub wnioski wydane przez organ państwa spoza UE będącego stroną protokołu, wymagające od administratora lub podmiotu przetwarzającego z UE ujawnienia danych osobowych lub danych pochodzących z łączności elektronicznej.

2.4. Zastrzeżenia, oświadczenia, zgłoszenia i komunikaty oraz inne kwestie

Protokół stanowi podstawę do korzystania przez strony z pewnych zastrzeżeń oraz do składania oświadczeń, przekazywania zgłoszeń lub komunikatów w odniesieniu do

[27] COM(2018) 225 i 226 final.

[28] Opinia EIOD dotycząca uczestnictwa w negocjacjach dotyczących drugiego protokołu dodatkowego do budapeszteńskiej konwencji o cyberprzestępczości, z dnia 2 kwietnia 2019 r., opinia 3/2019.

[29] W tym „wkład EROD do konsultacji w sprawie projektu drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (konwencja budapeszteńska) z dnia 13 listopada 2019 r.”; „oświadczenie nr 02/201 w sprawie nowego projektu przepisów drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (konwencja budapeszteńska) przyjęte 2 lutego 2021 r.”; „wkład EROD w 6. rundę konsultacji w sprawie projektu drugiego protokołu dodatkowego do budapeszteńskiej Konwencji Rady Europy o cyberprzestępczości z dnia 4 maja 2021 r.”.

niektórych artykułów. Państwa członkowskie powinny przyjąć jednolite podejście do niektórych zastrzeżeń i oświadczeń, zgłoszeń i komunikatów określonych w załączniku do niniejszej decyzji. Aby zapewnić zgodność wdrażania protokołu z prawem Unii, państwa członkowskie UE powinny zająć następujące stanowisko w odniesieniu do tych zastrzeżeń i oświadczeń. W przypadku gdy protokół stanowi podstawę dla innych zastrzeżeń, oświadczeń, zgłoszeń lub komunikatów, niniejszy wniosek upoważnia państwa członkowskie do rozpatrywania i zgłaszania własnych zastrzeżeń, oświadczeń, zgłoszeń lub komunikatów.

Aby zapewnić zgodność postanowień protokołu z odpowiednimi przepisami i politykami Unii, państwa członkowskie nie powinny korzystać z możliwości zgłoszenia zastrzeżeń na podstawie art. 7 ust. 9 lit. a)[30] i b)[31]. Ponadto państwa członkowskie powinny złożyć oświadczenie zgodnie z art. 7 ust. 2 lit. b)[32] oraz dokonać zgłoszenia zgodnie z art. 7 ust. 5 lit. a)[33]. Brak tych zastrzeżeń oraz złożenie oświadczenia i dokonanie zgłoszenia są istotne dla zapewnienia zgodności protokołu z wnioskami ustawodawczymi Komisji dotyczącymi elektronicznego materiału dowodowego, w tym z uwzględnieniem zmian projektu aktu ustawodawczego w toku dyskusji ze współprawodawcami.

Ponadto, aby zapewnić jednolite stosowanie protokołu przez państwa członkowskie UE we współpracy ze stronami niebędącymi państwami członkowskimi UE, zachęca się państwa członkowskie do niekorzystania z zastrzeżenia na podstawie art. 8 ust. 13[34], również dlatego, że takie zastrzeżenie miałoby skutek wzajemny[35]. Państwa członkowskie powinny złożyć oświadczenie zgodnie z art. 8 ust. 4, aby zapewnić skuteczność nakazów w przypadku, gdy potrzebne są dodatkowe informacje uzupełniające, np. dotyczące okoliczności danej sprawy w celu oceny proporcjonalności i konieczności[36].

Zachęca się również państwa członkowskie do powstrzymania się od składania oświadczeń na podstawie art. 9 ust. 1 lit. b)[37] w celu zapewnienia skutecznego stosowania protokołu.

Państwa członkowskie powinny przekazywać komunikaty zgodnie z art. 7 ust. 5 lit. e)[38], art. 8 ust. 10 lit. a) i b)[39], art. 14 ust. 7 lit. c) oraz ust. 10 lit. b), aby zapewnić ogólne skuteczne stosowanie protokołu[40].

---

[30] Umożliwienie stronom zastrzeżenia prawa do niestosowania art. 7 (ujawnianie danych abonenta).

[31] Umożliwienie stronom zastrzeżenia prawa do niestosowania art. 7 (ujawnianie danych abonenta) do niektórych rodzajów numerów dostępu, jeżeli byłoby to niezgodne z podstawowymi zasadami ich krajowego systemu prawnego.

[32] Umożliwienie stronom oświadczenia, że nakaz na podstawie art. 7 ust. 1 (ujawnianie danych abonenta) musi być wydany przez prokuratora lub inny organ sądowy bądź pod nadzorem prokuratora lub innego organu sądowego, lub też wydany w inny sposób pod niezależnym nadzorem.

[33] Umożliwienie stronom powiadomienia Sekretarza Generalnego Rady Europy, że w przypadku wydania nakazu na podstawie art. 7 ust. 1 (ujawnianie danych abonenta) w odniesieniu do usługodawcy na terytorium danej strony strona ta wymaga, w każdym przypadku lub w określonych okolicznościach, jednoczesnego zgłoszenia nakazu oraz przekazania informacji uzupełniających i streszczenia faktów związanych z postępowaniem przygotowawczym lub karnym.

[34] Umożliwienie stronom zastrzeżenia prawa do niestosowania art. 8 (wykonywanie nakazów innej strony) w odniesieniu do danych o ruchu.

[35] Zob. pkt 147 sprawozdania wyjaśniającego do protokołu, który stanowi, że „Strona, która zastrzega sobie prawo do niestosowania tego artykułu, nie jest uprawniona do wydawania nakazów dotyczących danych o ruchu innym stronom na podstawie [art. 8] ust. 1".

[36] Umożliwienie stronom oświadczenia, że wymagane są dodatkowe informacje uzupełniające w celu wykonania nakazów wydanych na podstawie art. 8 ust. 1 (wykonywanie nakazów innej strony).

[37] Umożliwienie stronom oświadczenia, że nie będą wykonywać wniosków na podstawie art. 9 ust. 1 lit. a) (niezwłoczne ujawnienie danych komputerowych w sytuacjach nadzwyczajnych) dotyczących wyłącznie ujawnienia danych abonenta.

Ponadto państwa członkowskie powinny wdrożyć niezbędne środki zgodnie z art. 14 ust. 11 lit. c) w celu zapewnienia, aby stronę otrzymującą informowano w momencie przekazywania danych o wynikającym z prawa Unii obowiązku zawiadomienia osoby, której dane dotyczą[41], oraz aby strona ta otrzymała odpowiednie dane kontaktowe, umożliwiające jej poinformowanie właściwego organu w państwie członkowskim UE po ustaniu ograniczeń dotyczących poufności i gdy istnieje możliwość przekazania zawiadomienia.

2.5. Uzasadnienie wniosku

Protokół wejdzie w życie po wyrażeniu przez pięć stron zgody na podporządkowanie się protokołowi zgodnie z postanowieniami art. 16 ust. 1 i 2. Ceremonia podpisania protokołu ma się odbyć w marcu 2022 r.

Państwa członkowskie UE powinny poczynić niezbędne kroki w celu zapewnienia szybkiego wejścia w życie protokołu i jego szybkiej ratyfikacji, co jest istotne z uwagi na szereg czynników.

Po pierwsze, protokół zapewni organom ścigania i organom sądowym lepsze przygotowanie do uzyskiwania elektronicznego materiału dowodowego niezbędnego do prowadzenia postępowań przygotowawczych. Ze względu na rosnące znaczenie elektronicznego materiału dowodowego w postępowaniach przygotowawczych istnieje pilna potrzeba, by organy ścigania i organy sądowe dysponowały właściwymi instrumentami umożliwiającymi uzyskanie dostępu do elektronicznego materiału dowodowego, tak aby mogły skutecznie zwalczać przestępczość w internecie.

Po drugie, protokół zapewni, aby takie środki służące uzyskaniu dostępu do elektronicznego materiału dowodowego wykorzystywano w sposób umożliwiający państwom członkowskim poszanowanie praw podstawowych, w tym praw procesowych w sprawach karnych, prawa do prywatności i prawa do ochrony danych osobowych. Wobec braku jasnych zasad na szczeblu międzynarodowym istniejące praktyki mogą stanowić wyzwanie w kontekście pewności prawa, przejrzystości, rozliczalności oraz poszanowania praw podstawowych i gwarancji proceduralnych osób podejrzanych w postępowaniach przygotowawczych.

Po trzecie, protokół rozwiąże kwestię kolizji praw – która dotyka zarówno organy, jak i usługodawców z sektora prywatnego i inne podmioty – i pozwoli jej zapobiegać, dzięki zapewnieniu kompatybilnych przepisów na szczeblu międzynarodowym dotyczących transgranicznego dostępu do elektronicznego materiału dowodowego.

---

[38] Umożliwienie stronom przekazywania danych kontaktowych organu wyznaczonego do otrzymywania zgłoszeń na podstawie art. 7 ust. 5 lit. a) oraz wykonywania działań opisanych w art. 7 ust. 5 lit. b), c) i d) (ujawnianie danych abonenta).

[39] Umożliwienie stronom przekazywania danych kontaktowych organów wyznaczonych do wydawania i przyjmowania nakazów na podstawie art. 8 (wykonywanie nakazów innej strony). Zgodnie z wymogami rozporządzenia (UE) 2017/1939 państwa członkowskie, które uczestniczą we wzmocnionej współpracy w zakresie ustanowienia Prokuratury Europejskiej, uwzględniają Prokuraturę Europejską w zawiadomieniu.

[40] Umożliwienie stronom przekazania informacji o organie lub organach, które należy odpowiednio zawiadomić w przypadku incydentu bezpieczeństwa lub z którymi należy się skontaktować w celu ubiegania się o uprzednie zezwolenie w przypadku dalszego przekazywania danych innemu państwu lub organizacji międzynarodowej.

[41] Zob. przypis 24 powyżej.

Po czwarte, protokół pozwoli uwydatnić, jak duże jest w dalszym ciągu znaczenie konwencji jako głównych wielostronnych ram walki z cyberprzestępczością. Będzie to miało kluczowe znaczenie w procesie wynikającym z rezolucji Zgromadzenia Ogólnego Narodów Zjednoczonych (ZO ONZ) 74/247 z grudnia 2019 r. „Przeciwdziałanie wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych", w której ustanowiono otwarty międzyrządowy komitet ekspertów *ad hoc* w celu opracowania kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych.

3. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- *Podstawa prawna*

Kompetencja Unii do stanowienia prawa w sprawach dotyczących ułatwiania współpracy między organami sądowymi lub równoważnymi organami w ramach ścigania karnego i wykonywania orzeczeń wynika z art. 82 ust. 1 TFUE. Kompetencja Unii w sprawach dotyczących ochrony danych osobowych wynika z art. 16 TFUE.

Zgodnie z art. 3 ust. 2 TFUE Unia ma wyłączną kompetencję do zawierania umów międzynarodowych w zakresie, w jakim ich zawarcie może wpływać na wspólne zasady UE lub zmieniać ich zakres. Postanowienia protokołu należą do dziedziny objętej w znacznym stopniu wspólnymi zasadami określonymi w sekcji 2.3 powyżej.

Protokół wchodzi zatem w zakres wyłącznej kompetencji zewnętrznej Unii. Ratyfikacja protokołu przez państwa członkowskie w interesie Unii może zatem nastąpić na podstawie art. 16, art. 82 ust. 1 i art. 218 ust. 6 TFUE.

- *Pomocniczość (w przypadku kompetencji niewyłącznych)*

Nie dotyczy.

- *Proporcjonalność*

Cele Unii w odniesieniu do niniejszego wniosku przedstawione w sekcji 2.5 powyżej można osiągnąć jedynie poprzez zawarcie wiążącej umowy międzynarodowej przewidującej niezbędne środki współpracy przy jednoczesnym zapewnieniu odpowiedniej ochrony praw podstawowych. Protokół przyczynia się do osiągnięcia tego celu. Postanowienia protokołu ograniczają się do tego, co jest konieczne do osiągnięcia jego głównych celów. Działania jednostronne nie stanowią alternatywy, ponieważ nie stanowiłyby wystarczającej podstawy do współpracy z państwami niebędącymi członkami UE i nie mogłyby zapewnić niezbędnej ochrony praw podstawowych. Ponadto przystąpienie do umowy wielostronnej, takiej jak wynegocjowany przez Unię protokół, jest skuteczniejsze niż podejmowanie negocjacji z poszczególnymi państwami niebędącymi członkami UE na poziomie dwustronnym. Przy założeniu, że wszystkie 66 stron konwencji, jak również przyszłe nowe strony konwencji ratyfikują protokół, protokół ten zapewni wspólne ramy prawne współpracy państw członkowskich UE z najważniejszymi partnerami międzynarodowymi w walce z przestępczością.

- ***Wybór instrumentu***

Nie dotyczy.

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

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

Nie dotyczy.

- *Konsultacje z zainteresowanymi stronami*

Rada Europy zorganizowała sześć rund konsultacji publicznych w związku z negocjacjami w sprawie protokołu: w lipcu i listopadzie 2018 r., w lutym i listopadzie 2019 r., w grudniu 2020 r. oraz w maju 2021 r.[42] Strony uwzględniły uwagi otrzymane w ramach tych konsultacji.

Komisja, pełniąc rolę negocjatora w imieniu Unii, prowadziła również wymianę poglądów z organami ochrony danych oraz zorganizowała w latach 2019 i 2021 ukierunkowane spotkania konsultacyjne z organizacjami społeczeństwa obywatelskiego, usługodawcami i stowarzyszeniami branżowymi. Komisja wzięła pod uwagę informacje otrzymane w wyniku tych wymian.

- *Gromadzenie i wykorzystanie wiedzy eksperckiej*

W trakcie negocjacji Komisja stale konsultowała się ze specjalnym komitetem Rady ds. negocjacji zgodnie z decyzją Rady Unii Europejskiej z dnia 6 czerwca 2019 r. upoważniającą Komisję do udziału w negocjacjach w imieniu Unii, co dało ekspertom z państw członkowskich możliwość wniesienia wkładu w proces formułowania stanowiska Unii. Wielu ekspertów z państw członkowskich również uczestniczyło w negocjacjach, w uzupełnieniu udziału Komisji w imieniu Unii. Przeprowadzono także konsultacje z zainteresowanymi stronami (zob. powyżej).

- *Ocena skutków*

W latach 2017–2018 przeprowadzono ocenę skutków, która towarzyszyła wnioskom Komisji w sprawie elektronicznego materiału dowodowego[43]. W tym kontekście negocjacje dotyczące porozumienia w sprawie drugiego protokołu dodatkowego do budapeszteńskiej Konwencji o cyberprzestępczości stanowiły element preferowanego wariantu. Istotne skutki przedstawiono ponadto w niniejszym uzasadnieniu.

- *Sprawność regulacyjna i uproszczenie*

Protokół może mieć wpływ na niektóre kategorie usługodawców, w tym małe i średnie przedsiębiorstwa (MŚP), ponieważ mogą oni podlegać wnioskom i nakazom dotyczącym przedstawienia elektronicznego materiału dowodowego na podstawie protokołu. Obecnie jednak usługodawcy ci często już podlegają takim wnioskom za pośrednictwem innych istniejących kanałów, czasami przekazywanym przez różne organy, w tym na podstawie konwencji[44], innych traktatów o pomocy prawnej lub innych ram, w tym opartych na porozumieniu zainteresowanych stron polityk w zakresie zarządzania internetem[45]. Ponadto

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations

[43] SWD(2018) 118 final.

[44] Zob. np. wytyczne nr 10 komitetu Konwencji o cyberprzestępczości z dnia 1 marca 2017 r. w sprawie nakazów przekazania informacji o abonencie (art. 18 Konwencji o cyberprzestępczości).

[45] Zob. np. rezolucja Zarządu Internetowej Korporacji ds. Nadanych Nazw i Numerów (ICANN) z dnia 15 maja 2019 r. w sprawie zaleceń dotyczących tymczasowej specyfikacji danych rejestracyjnych gTLD, dostępna pod adresem www.icann.org

usługodawcy, w tym MŚP, skorzystają również z jasnych ram prawnych na szczeblu międzynarodowym oraz wspólnego podejścia wszystkich stron protokołu.

- *Prawa podstawowe*

Instrumenty współpracy przewidziane w protokole mogą mieć wpływ na prawa podstawowe, w przypadku gdy dane danej osoby można uzyskać w kontekście postępowania karnego, w tym np. na prawo do rzetelnego procesu sądowego, prawo do prywatności i prawo do ochrony danych osobowych. W protokole zastosowano podejście oparte na prawach oraz przewidziano warunki i zabezpieczenia zgodne z międzynarodowymi instrumentami dotyczącymi praw człowieka, w tym z Konwencją Rady Europy o ochronie praw człowieka i podstawowych wolności z 1950 r. W protokole przewidziano w szczególności określone zabezpieczenia w zakresie ochrony danych. W razie potrzeby protokół stanowi również podstawę dla stron do zgłaszania pewnych zastrzeżeń, przedstawiania oświadczeń lub dokonywania zgłoszeń oraz zawiera podstawy do odmowy współpracy w odpowiedzi na wniosek w szczególnych sytuacjach. Zapewnia to zgodność protokołu z Kartą praw podstawowych Unii Europejskiej.

5. WPŁYW NA BUDŻET

Wniosek nie ma wpływu na budżet Unii. Państwa członkowskie mogą ponieść jednorazowe koszty związane z wdrożeniem protokołu, a organy państw członkowskich mogą ponieść wyższe koszty w związku z oczekiwanym wzrostem liczby spraw.

6. ELEMENTY FAKULTATYWNE

- *Plany wdrożenia i monitorowanie, ocena i sprawozdania*

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

W odniesieniu do monitorowania Komisja będzie brała udział w posiedzeniach komitetu Konwencji o cyberprzestępczości, ponieważ Unia Europejska ma status obserwatora przy tym komitecie.

2021/0383 (NLE)

Wniosek

DECYZJA RADY

upoważniająca państwa członkowskie do ratyfikowania, w interesie Unii Europejskiej, drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16, art. 82 ust. 1 i art. 218 ust. 6,

uwzględniając wniosek Komisji Europejskiej,

uwzględniając zgodę Parlamentu Europejskiego,

a także mając na uwadze, co następuje:

(1) W dniu 9 czerwca 2019 r. Rada upoważniła Komisję do udziału, w imieniu Unii, w negocjacjach w sprawie drugiego protokołu dodatkowego do budapeszteńskiej Konwencji Rady Europy o cyberprzestępczości.

(2) Tekst drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego („protokół") został przyjęty przez Komitet Ministrów Rady Europy w dniu 17 listopada 2021 r. i ma zostać otwarty do podpisu w marcu 2022 r.

(3) Postanowienia protokołu należą do dziedziny objętej w znacznym stopniu wspólnymi zasadami w rozumieniu art. 3 ust. 2 TFUE, w tym instrumentami ułatwiającymi współpracę wymiarów sprawiedliwości w sprawach karnych, zapewniającymi minimalne standardy praw procesowych, a także zabezpieczenie ochrony danych i prywatności.

(4) Komisja przedłożyła również wnioski ustawodawcze dotyczące rozporządzenia w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych (COM(2018) 225 final) oraz dyrektywy ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych (COM(2018) 226 final), zawierające wymóg kierowania transgranicznych europejskich nakazów wydania dowodów i zabezpieczenia dowodów bezpośrednio do przedstawiciela usługodawcy w innym państwie członkowskim.

(5) Uczestnicząc w negocjacjach w imieniu Unii, Komisja zapewniła zgodność drugiego protokołu dodatkowego z odpowiednimi wspólnymi zasadami Unii Europejskiej.

(6) Szereg zastrzeżeń, oświadczeń, zgłoszeń i komunikatów ma istotne znaczenie dla zapewnienia zgodności protokołu z prawem i politykami Unii, a także jednolitego stosowania protokołu przez państwa członkowskie UE w ich stosunkach ze stronami spoza UE oraz skutecznego stosowania protokołu.

(7) Biorąc pod uwagę, że w protokole przewidziano szybkie procedury usprawniające transgraniczny dostęp do elektronicznego materiału dowodowego i wysoki poziom zabezpieczeń, jego wejście w życie przyczyni się do walki z cyberprzestępczością i innymi formami przestępczości na szczeblu światowym poprzez ułatwienie współpracy między państwami członkowskimi UE będącymi stronami protokołu a państwami spoza UE będącymi stronami protokołu, zapewni wysoki poziom ochrony osób fizycznych oraz rozwiąże kwestię kolizji praw.

(8) Biorąc pod uwagę, że w protokole przewidziano odpowiednie zabezpieczenia zgodnie z wymogami dotyczącymi międzynarodowego przekazywania danych osobowych na podstawie rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680, jego wejście w życie przyczyni się do propagowania unijnych standardów ochrony danych na szczeblu światowym, ułatwi przepływ danych między państwami członkowskimi UE będącymi stronami protokołu a państwami spoza UE będącymi stronami protokołu, a także zapewni przestrzeganie przez państwa członkowskie UE ich zobowiązań wynikających z unijnych przepisów o ochronie danych.

(9) Szybkie wejście w życie potwierdzi również status budapeszteńskiej Konwencji Rady Europy jako głównych wielostronnych ram walki z cyberprzestępczością.

(10) Unia Europejska nie może zostać stroną protokołu, ponieważ zarówno protokół, jak i Konwencja Rady Europy o cyberprzestępczości są otwarte wyłącznie dla państw.

(11) Państwa członkowskie należy zatem upoważnić do ratyfikowania protokołu w ramach wspólnego działania w interesie Unii Europejskiej.

(12) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu […] r.

(13) [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.]

[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 powiadomiła [pismem z dnia … r.] o chęci uczestniczenia w przyjęciu i stosowaniu niniejszej decyzji.]

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

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Państwa członkowskie niniejszym upoważnia się do ratyfikowania, w interesie Unii Europejskiej, drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego („protokół”).

Artykuł 2

Przy ratyfikacji protokołu państwa członkowskie przedkładają zastrzeżenia, oświadczenia, zgłoszenia lub komunikaty określone w załączniku.

Artykuł 3

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Artykuł 4

Niniejsza decyzja zostaje opublikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 5

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Rady
Przewodniczący