

Bruksela, 1 kwietnia 2022 r.
(OR. fr)

7860/22
ADD 1

CYBER 108
COPEN 118
JAI 444
COPS 143
RELEX 429
JAIEX 30
TELECOM 138
POLMIL 82
CFSP/PESC 432
ENFOPOL 179
DATAPROTECT 95

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	29 marca 2022 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2022) 132 final
Dotyczy:	ZAŁĄCZNIK do zalecenia dotyczącego decyzji Rady upoważniającej do rozpoczęcia negocjacji dotyczących kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych

Delegacje otrzymują w załączeniu dokument COM(2022) 132 final.

Załącznik: COM(2022) 132 final



KOMISJA
EUROPEJSKA

Bruksela, dnia 29.3.2022 r.
COM(2022) 132 final

ANNEX

ZAŁĄCZNIK

do

zalecenia dotyczącego decyzji Rady

**upoważniającej do rozpoczęcia negocjacji dotyczących kompleksowej konwencji
międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii
informacyjno-komunikacyjnych w celach przestępczych**

ZAŁĄCZNIK

Jeśli chodzi o proces negocjacji, cele Unii powinny być następujące:

- 1) proces negocjacji powinien być otwarty, integracyjny i przejrzysty oraz oparty na współpracy w dobrej wierze;
- 2) proces negocjacji powinien umożliwiać znaczący udział wszystkich zainteresowanych stron, w tym społeczeństwa obywatelskiego, sektora prywatnego, środowisk akademickich i organizacji pozarządowych;
- 3) wszystkie uwagi otrzymane od każdego z członków Organizacji Narodów Zjednoczonych powinny być rozpatrywane na równych zasadach, aby zapewnić integracyjny charakter procesu;
- 4) proces negocjacji powinien opierać się na skutecznym i realistycznym programie prac.

Jeśli chodzi o ogólne cele negocjacji, cele Unii powinny być następujące:

- 5) konwencja powinna służyć jako skuteczny instrument, z którego organy ścigania przestępstw i organy sądowe będą mogły korzystać w międzynarodowej walce z cyberprzestępczością, a celem konwencji powinno być wniesienie wartości dodanej do współpracy międzynarodowej;
- 6) należy w pełni uwzględnić istniejące ramy sprawdzonych instrumentów i działań międzynarodowych i regionalnych, o których mowa w rezolucjach Zgromadzenia Ogólnego ONZ nr 74/247 i 75/282. W związku z tym konwencja powinna być zgodna z istniejącymi instrumentami międzynarodowymi, w szczególności z Konwencją Rady Europy o cyberprzestępczości z 2001 r. i jej protokołami, Konwencją Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej z 2000 r. i jej protokołami, a także innymi odpowiednimi instrumentami międzynarodowymi i regionalnymi, oraz stanowić uzupełnienie tych instrumentów. Konwencja nie powinna mieć wpływu na stosowanie tych instrumentów ani na dalsze przystępowanie do nich przez jakiekolwiek państwo, a także, w miarę możliwości, nie powinna zawierać niepotrzebnie powielanych postanowień;
- 7) należy w pełni uwzględnić prace i wyniki prac otwartej międzyrządowej grupy ekspertów w celu przeprowadzenia kompleksowego badania na temat cyberprzestępczości, zgodnie z rezolucją Zgromadzenia Ogólnego ONZ nr 75/282;
- 8) postanowienia Konwencji powinny zapewniać najwyższą możliwą ochronę praw człowieka. Państwa członkowskie UE powinny być w stanie przestrzegać prawa Unii, w tym podstawowych praw, wolności i zasad ogólnych prawa Unii zapisanych w traktatach Unii Europejskiej oraz w Karcie praw podstawowych. Postanowienia konwencji powinny być także zgodne z międzynarodowymi zobowiązaniami handlowymi UE i jej państw członkowskich.

Jeśli chodzi o treść negocjacji, cele Unii powinny być następujące:

- 9) konwencja powinna zawierać definicje przestępstw, które można popełnić wyłącznie przy użyciu systemów informatycznych;

- 10) konwencja powinna zawierać definicje przestępstw, które można popełnić bez użycia systemów informatycznych, ale których popełnienie w pewnych okolicznościach może być możliwe dzięki wykorzystaniu takich systemów, lecz tylko w przypadkach, gdy zaangażowanie systemów informatycznych w istotny sposób zmienia charakterystykę lub skutki przestępstw;
- 11) przestępstwa powinny zostać jasno i wąsko zdefiniowane w sposób neutralny pod względem technologicznym. Definicje te powinny być zgodne z definicjami zawartymi w innych stosownych konwencjach międzynarodowych lub regionalnych, zwłaszcza w dziedzinie przestępczości zorganizowanej lub cyberprzestępczości, oraz z międzynarodowymi standardami praw człowieka;
- 12) w konwencji należy przewidzieć przepisy dotyczące usiłowania popełnienia takich przestępstw oraz pomocnictwa w tym zakresie, odpowiedzialności osób prawnych za takie przestępstwa, przepisy dotyczące ustanowienia jurysdykcji w odniesieniu do takich przestępstw oraz przepisy dotyczące sankcji i środków związanych z takimi przestępstwami, zgodne z innymi odpowiednimi konwencjami międzynarodowymi lub regionalnymi, w szczególności w dziedzinie przestępczości zorganizowanej lub cyberprzestępczości, oraz z międzynarodowymi standardami praw człowieka;
- 13) w konwencji należy przewidzieć środki proceduralne w postępowaniu karnym, które umożliwią organom prowadzenie skutecznych dochodzeń w sprawach cyberprzestępstw, zamrożenie i konfiskatę dochodów pochodzących z takich przestępstw oraz zabezpieczenie lub uzyskanie elektronicznego materiału dowodowego dotyczącego wszelkich przestępstw w ramach postępowań przygotowawczych lub postępowań karnych, przy należyтым uwzględnieniu zasady proporcjonalności;
- 14) wspomniane środki proceduralne w postępowaniu karnym powinny zapewniać wystarczającą wartość dodaną w porównaniu z innymi odpowiednimi konwencjami międzynarodowymi lub regionalnymi, w szczególności w dziedzinie przestępczości zorganizowanej lub cyberprzestępczości, oraz powinny być zgodne z takimi konwencjami i z międzynarodowymi standardami praw człowieka;
- 15) środki proceduralne służące zabezpieczeniu lub uzyskaniu elektronicznego materiału dowodowego powinny zawierać jasną i wąską definicję rodzaju informacji, których dotyczą. Środki proceduralne dotyczące współpracy z podmiotami sektora prywatnego powinny zapewniać, aby obciążenia nakładane na takie podmioty były proporcjonalne oraz aby podmioty sektora prywatnego w pełni respektowały prawa człowieka swoich użytkowników. Konwencja powinna zapewniać dostawcom usług online (np. dostawcom usług internetowych) jasność prawa w ich kontaktach z organami ścigania państw stron konwencji. Środki proceduralne służące usuwaniu treści niezgodnych z prawem powinny odnosić się wyłącznie do treści niezgodnych z prawem, które można dostatecznie konkretnie i wąsko zdefiniować;
- 16) konwencja powinna przewidywać środki współpracy, które umożliwią organom różnych państw stron tego instrumentu skuteczną współpracę w celu prowadzenia postępowań przygotowawczych lub karnych w sprawie przestępstw określonych w tym instrumencie lub współpracę w celu zabezpieczenia lub uzyskania elektronicznego materiału dowodowego na popełnienie przestępstwa w ramach postępowania przygotowawczego lub postępowania karnego;
- 17) wspomniane środki współpracy powinny zapewniać wystarczającą wartość dodaną w porównaniu z innymi odpowiednimi konwencjami międzynarodowymi lub

regionalnymi, w szczególności w dziedzinie przestępczości zorganizowanej lub cyberprzestępczości, oraz być zgodne z takimi konwencjami i z międzynarodowymi standardami praw człowieka;

- 18) środki współpracy powinny podlegać warunkom przewidzianym w prawie wezwanej strony i przewidywać szerokie podstawy odmowy, takie jak zapewnienie ochrony praw podstawowych, w tym prawa do ochrony danych osobowych, także w kontekście przekazywania danych osobowych, oraz, w stosownych przypadkach, istnienie podwójnej karalności;
- 19) konwencja powinna przewidywać rygorystyczne warunki i mocne zabezpieczenia, które zagwarantują państwom członkowskim UE możliwość przestrzegania i ochrony podstawowych praw, wolności i ogólnych zasad prawa Unii zapisanych w traktatach Unii Europejskiej i w Karcie praw podstawowych, w tym w szczególności zasady proporcjonalności, gwarancji i praw procesowych, prawa do skutecznego środka zaskarżenia, domniemania niewinności, prawa do rzetelnego procesu sądowego oraz prawa do obrony osób, wobec których toczy się postępowanie karne, a także prawa do prywatności, prawa do ochrony danych osobowych i danych pochodzących z łączności elektronicznej podczas przetwarzania tych danych, w tym podczas przekazywania ich organom w państwach spoza Unii Europejskiej, oraz prawa do wolności wypowiedzi i informacji. Konwencja powinna gwarantować w szczególności, że państwa członkowskie UE będą w stanie spełnić wymogi dotyczące międzynarodowego przekazywania danych osobowych w rozumieniu dyrektywy (UE) 2016/680, rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE. Warunki i zabezpieczenia powinny również zapewniać ochronę praw człowieka i podstawowych wolności zgodnie z międzynarodowymi standardami praw człowieka. Dotyczy to całej konwencji, w tym środków proceduralnych i środków współpracy, także tych, które mogą znacząco ingerować w prawa osób fizycznych, jak np. zamrożenie i konfiskata dochodów pochodzących z przestępstw oraz ekstradycja;
- 20) konwencja powinna stanowić podstawę dla dobrowolnych środków budowania zdolności, aby wspierać państwa – również przez pomoc techniczną i szkolenia – w zwiększaniu ich zdolności do prowadzenia skutecznych postępowań przygotowawczych i karnych w sprawach dotyczących cyberprzestępstw oraz uzyskiwania elektronicznego materiału dowodowego na potrzeby postępowań przygotowawczych i karnych w sprawach dotyczących innych przestępstw. Rola UNODC w zakresie wdrażania takich środków powinna zostać jasno określona;
- 21) w konwencji należy uwzględnić pozycję osób fizycznych i prawnych jako ofiar cyberprzestępstw. Powinna ona zapewniać tym ofiarom cyberprzestępstw gwarancję otrzymania odpowiedniej pomocy, wsparcia i ochrony;
- 22) konwencja powinna stanowić podstawę dla praktycznych środków zapobiegania cyberprzestępczości, które powinny zostać jasno określone i być ściśle ograniczone, a także różnić się od środków proceduralnych w postępowaniu karnym, które mogłyby ingerować w prawa i wolności osób fizycznych lub prawnych.

Jeśli chodzi o funkcjonowanie konwencji, cele Unii powinny być następujące:

- 23) konwencja powinna chronić istniejące instrumenty na poziomie międzynarodowym i regionalnym oraz bieżącą współpracę międzynarodową w ogólnosięciowej walce z cyberprzestępczością. W szczególności państwa członkowskie Unii Europejskiej

będą mogły nadal stosować przepisy Unii Europejskiej w swoich wzajemnych stosunkach;

- 24) w konwencji należy przewidzieć odpowiedni mechanizm zapewniający jej wdrożenie, a także postanowienia końcowe, w tym dotyczące rozstrzygania sporów, podpisania, ratyfikacji, przyjęcia, zatwierdzenia i przystąpienia, wejścia w życie, zmiany, zawieszenia, wypowiedzenia oraz depozytariusza i języków, które to postanowienia w miarę możliwości i w stosownych przypadkach należy wzorować na postanowieniach innych odpowiednich konwencji międzynarodowych lub regionalnych, w szczególności w dziedzinie przestępczości zorganizowanej lub cyberprzestępczości;
- 25) konwencja powinna umożliwiać Unii Europejskiej stanie się jej stroną.