

# DECYZJE

## 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**

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 82 ust. 1 i 2 oraz jego art. 83 ust. 1 w związku z art. 218 ust. 3 i 4,

uwzględniając zalecenie Komisji Europejskiej,

a także mając na uwadze, co następuje:

- (1) W dniu 27 grudnia 2019 r. Zgromadzenie Ogólne ONZ przyjęło rezolucję nr 74/247 dotyczącą przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych, w której ustanowiono otwarty międzyrządowy komitet ekspertów *ad hoc*, reprezentatywny dla wszystkich regionów, w celu opracowania kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych.
- (2) Unia przyjęła już zasady obejmujące niektóre, ale nie wszystkie elementy, które prawdopodobnie należy uwzględnić w celu włączenia do kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych. Zasady te obejmują w szczególności instrumenty dotyczące prawa karnego materialnego <sup>(1)</sup>, współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych <sup>(2)</sup> i minimalnych norm w zakresie praw

---

<sup>(1)</sup> Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW, (Dz.U. L 335 z 17.12.2011, s. 1); dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8); dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/713 z dnia 17 kwietnia 2019 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zastępująca decyzję ramową Rady 2001/413/WSiSW (Dz.U. L 123 z 10.5.2019, s. 18).

<sup>(2)</sup> Akt Rady z dnia 29 maja 2000 r. ustanawiający zgodnie z art. 34 Traktatu o Unii Europejskiej Konwencję o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (Dz.U. C 197 z 12.7.2000, s. 1); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.U. L 295 z 21.11.2018, s. 138); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53); decyzja ramowa Rady 2002/465/WSiSW z dnia 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych (Dz.U. L 162 z 20.6.2002, s. 1); decyzja ramowa Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów (Dz.U. L 328 z 15.12.2009, s. 42); dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dz.U. L 130 z 1.5.2014, s. 1).

procesowych<sup>(3)</sup>, a także gwarancje ochrony danych i prywatności<sup>(4)</sup>. Ponadto, ponieważ wnioski ustawodawcze w dodatkowych powiązanych dziedzinach zostały już przedstawione i omówione, należy je również uwzględnić w zakresie, w jakim mają one na celu zwiększenie skuteczności unijnych ram prawnych.

- (3) Z tego względu kompleksowa konwencja międzynarodowa w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych może wpłynąć na niektóre zasady Unii lub zmienić ich zakres stosowania.
- (4) W celu ochrony integralności prawa Unii oraz zapewnienia spójności przepisów prawa międzynarodowego i prawa Unii konieczne jest, aby w kwestiach wchodzących w zakres kompetencji Unii określonych w Traktatach i w odniesieniu do których Unia przyjęła zasady w negocjacjach dotyczących kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych uczestniczyła Komisja wraz z państwami członkowskimi.
- (5) W dniu 22 marca 2021 r. Rada przyjęła konkluzje w sprawie unijnej strategii cyberbezpieczeństwa na cyfrową dekadę. Rada przypominała w nich, że kilka aspektów negocjacji dotyczących kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych może dotyczyć wspólnej polityki zagranicznej i bezpieczeństwa, podkreślając, że „popiera i promuje budapeszteńską Konwencję o cyberprzestępczości i bieżące prace nad drugim Protokołem dodatkowym do tej konwencji”. Ponadto nadal angażuje się w wielostronną wymianę poglądów na temat cyberprzestępczości, w tym w ramach procesów związanych z Radą Europy, Biurem Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC) i Komisją ds. Zapobiegania Przestępczości i Wymiaru Sprawiedliwości Sądownictwa Karnego (CCPCJ), aby zapewnić usprawnioną współpracę międzynarodową ukierunkowaną na przeciwdziałanie cyberprzestępczości, w tym wymianę najlepszych praktyk i wiedzy technicznej oraz wspieranie rozwijania zdolności, jednocześnie zapewniając poszanowanie, promowanie i ochronę praw człowieka i podstawowych wolności.
- (6) Niniejsza decyzja nie powinna naruszać określonego w Traktatach podziału kompetencji między Unią a jej państwami członkowskimi, udziału państw członkowskich w negocjacjach dotyczących kompleksowej międzynarodowej konwencji w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych oraz wszelkich późniejszych decyzji o zawarciu, podpisaniu lub ratyfikowaniu takiej konwencji.
- (7) Wytyczne negocjacyjne określone w addendum do niniejszej decyzji są skierowane do Komisji i w stosownych przypadkach, w zależności od przebiegu negocjacji, mogą zostać zmienione lub rozwinięte.
- (8) Zgodnie z zasadą lojalnej współpracy Komisja i państwa członkowskie powinny ściśle współpracować w trakcie procesu negocjacyjnego, w tym poprzez regularne kontakty z ekspertami i przedstawicielami państw członkowskich w Nowym Jorku i Wiedniu.

<sup>(3)</sup> 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).

<sup>(4)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1); dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89); dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz.U. L 337 z 18.12.2009, s. 11).

- (9) 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 18 maja 2022 r. <sup>(9)</sup>.
- (10) 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 (TUE) i do Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), bez uszczerbku dla art. 4 tego protokołu, Irlandia nie uczestniczy w przyjęciu niniejszej decyzji i nie jest nią związana ani jej nie stosuje.
- (11) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i do TFUE, Dania nie uczestniczy w przyjęciu niniejszej decyzji i nie jest nią związana ani jej nie stosuje.

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

#### Artykuł 1

1. Komisja zostaje niniejszym upoważniona do podjęcia negocjacji w imieniu Unii, w kwestiach wchodzących w zakres kompetencji Unii określonych w Traktatach i w odniesieniu do których Unia przyjęła zasady, dotyczące kompleksowej konwencji międzynarodowej w sprawie przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych.

2. Negocjacje są prowadzone na podstawie wytycznych negocjacyjnych Rady określonych w addendum do niniejszej decyzji i w stosownych przypadkach, w zależności od przebiegu negocjacji, mogą zostać zmienione lub rozwinięte.

#### Artykuł 2

Negocjacje są prowadzone w konsultacji z Grupą Roboczą ds. Współpracy w Sprawach Karnych, która zostaje niniejszym wyznaczona jako specjalny komitet w rozumieniu art. 218 ust. 4 TFUE.

Komisja regularnie składa specjalnemu komitetowi, o którym mowa w akapicie pierwszym, sprawozdania na temat kroków podjętych na podstawie niniejszej decyzji i regularnie konsultuje się z nim.

Gdy tylko Rada wyrazi takie życzenie, Komisja złoży jej – również na piśmie – sprawozdanie z przebiegu i wyników negocjacji.

W zakresie, w jakim przedmiot negocjacji wchodzi w zakres kompetencji zarówno Unii, jak i jej państw członkowskich, Komisja i państwa członkowskie ściśle współpracują w procesie negocjacji, dążąc do zapewnienia jedności w reprezentowaniu Unii i jej państw członkowskich na arenie międzynarodowej.

#### Artykuł 3

Niniejsza decyzja wraz z addendum zostanie podana do wiadomości publicznej niezwłocznie po jej przyjęciu.

#### Artykuł 4

Niniejsza decyzja skierowana jest do Komisji.

---

<sup>(9)</sup> Opinia z dnia 18 maja 2022 r. (dotychczas nieopublikowana w Dzienniku Urzędowym).

Sporządzono w Brukseli dnia 24 maja 2022 r.

*W imieniu Rady*  
*Przewodniczący*  
B. LE MAIRE

---

## ADDENDUM

**WYTYCZNE DO NEGOCJACJI DOTYCZĄCYCH KOMPLEKSOWEJ KONWENCJI MIĘDZYNARODOWEJ W SPRAWIE PRZECIWDZIAŁANIA WYKORZYSTYWANIU TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH W CELACH PRZESTĘPCZYCH**

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 przedstawicieli społeczeństwa obywatelskiego, sektora prywatnego, środowisk akademickich i organizacji pozarządowych.
- (3) 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 zapewniać wysoki poziom ochrony praw człowieka i podstawowych wolności, jednocześnie służąc organom ścigania i organom sądowym jako skuteczny instrument ogólnowiatowej walki z cyberprzestępczością; jej celem powinno być promowanie i wzmacnianie środków służących skuteczniejszemu i efektywniejszemu zapobieganiu cyberprzestępczości i jej zwalczaniu, a także promowanie i ułatwianie współpracy międzynarodowej, zapewnianie wysokiego poziomu ochrony praw ofiar oraz wspieranie budowania zdolności i pomocy technicznej w walce z cyberprzestępczością.
- (6) Należy w pełni uwzględnić istniejące ramy wypróbowanych 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 jest zgodna z istniejącymi instrumentami międzynarodowymi, w szczególności z Konwencją Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej z 2000 r. i jej protokołami, Konwencją Narodów Zjednoczonych przeciwko korupcji z 2003 r., „budapeszteńską” Konwencją Rady Europy o cyberprzestępczości z 2001 r. i jej protokołami, jak również z innymi odpowiednimi instrumentami międzynarodowymi i regionalnymi, w szczególności dotyczącymi ochrony praw człowieka i podstawowych wolności. Konwencja nie powinna mieć wpływu na stosowanie tych istniejących 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 i podstawowych wolności. Państwa członkowskie UE powinny być w stanie przestrzegać prawa międzynarodowego i 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 komputerowych.
- (10) Pod warunkiem zagwarantowania wystarczających warunków i zabezpieczeń oraz odpowiedniej ochrony praw człowieka i podstawowych wolności, w drodze wyjątku od zasady określonej w pkt 9, konwencja mogłaby zawierać definicje przestępstw, które mogą zostać popełnione bez użycia systemów komputerowych, ale które mogą być umożliwiające przy użyciu systemów komputerowych w pewnych okolicznościach, ale tylko w przypadkach, gdy użycie systemów komputerowych w istotny sposób zmienia cechy lub skutki przestępstw.
- (11) Przestępstwa powinny zostać jasno i wąsko zdefiniowane w sposób neutralny pod względem technologicznym. Definicje powinny być zgodne z definicjami zawartymi w innych stosownych konwencjach międzynarodowych lub regionalnych, zwłaszcza w dziedzinie cyberprzestępczości, oraz z międzynarodowymi standardami praw człowieka i podstawowymi wolnościami.

- (12) W konwencji należy przewidzieć przepisy dotyczące pomocnictwa oraz, w stosownych przypadkach, usiłowania popełnienia takich przestępstw, odpowiedzialności osób prawnych i fizycznych za takie przestępstwa, przepisy dotyczące ustanowienia jurysdykcji w odniesieniu do takich przestępstw oraz przepisy dotyczące skutecznych, proporcjonalnych i odstraszających 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) Konwencja powinna przewidywać środki proceduralne w postępowaniu karnym umożliwiające organom skuteczne prowadzenie dochodzeń w sprawie cyberprzestępczości, które to środki w postępowaniu karnym – w przypadku gdy przewidziano wystarczające zabezpieczenia – mogłyby obejmować środki mające na celu zabezpieczenie lub uzyskanie elektronicznego materiału dowodowego dotyczącego wszelkich przestępstw w ramach dochodzenia lub postępowania karnego, oraz, w przypadku gdy dodatkowo istnieje wykazana potrzeba i wartość dodana, środki mające na celu zamrożenie i konfiskatę korzyści pochodzących z takich przestępstw, z należyтым uwzględnieniem zasad proporcjonalności, legalności i konieczności, ochrony praw dotyczących poszanowania prywatności i ochrony danych osobowych.
- (14) Wspomniane proceduralne środki w postępowaniu karnym nie powinny być sprzeczne 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 i z podstawowymi wolnościami.
- (15) Środki proceduralne służące zabezpieczeniu lub uzyskaniu elektronicznego materiału dowodowego powinny zawierać jasną i wąską definicję rodzaju danych, 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 przepisy chroniące 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 są dostatecznie konkretnie i wąsko zdefiniowane w konwencji.
- (16) Konwencja powinna przewidywać środki współpracy umożliwiające organom różnych państw będących stronami instrumentu skuteczną współpracę poprzez wzajemną pomoc prawną, w tym poprzez ustanowienie punktów kontaktowych, do celów dochodzeń lub postępowań karnych dotyczących przestępstw określonych w tym instrumencie. Może również przewidywać takie środki współpracy do celów zabezpieczenia lub uzyskania elektronicznego materiału dowodowego dotyczącego wszelkich przestępstw w ramach dochodzenia lub postępowania karnego, pod warunkiem że na mocy prawa krajowego państw środki te podlegają dostatecznym warunkom i zabezpieczeniom zapewniającym odpowiednią ochronę praw człowieka i podstawowych wolności.
- (17) Wspomniane środki współpracy powinny być zgodne z innymi odpowiednimi konwencjami międzynarodowymi lub regionalnymi, w szczególności w dziedzinie przestępczości zorganizowanej lub cyberprzestępczości, oraz nie powinny być sprzeczne z takimi konwencjami, z międzynarodowymi standardami praw człowieka i z podstawowymi wolnościami.
- (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 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 zasad proporcjonalności, legalności i konieczności dotyczących przestępstw i kar, 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, prawa do niebicia ponownie sądzonym lub ukaranym w postępowaniu karnym za to samo przestępstwo, 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.

- (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) Konwencja powinna zapewniać ofiarom cyberprzestępstw gwarancję otrzymania odpowiedniej pomocy, wsparcia, ochrony oraz dostęp do kompensaty.
- (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 ogólnosiwiatowej walce z cyberprzestępczością. W szczególności państwa członkowskie Unii Europejskiej powinny nadal być w stanie 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 rozstrzygnięcia 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.

Ogólnie, negocjacje powinny przebiegać następująco:

- (26) Komisja powinna dążyć do zapewnienia spójności konwencji z odpowiednimi przepisami i politykami Unii, a także ze zobowiązaniami Unii wynikającymi z innych stosownych umów wielostronnych.
- (27) Komisja powinna prowadzić negocjacje w imieniu Unii w kwestiach, które zgodnie z Traktami wchodzą w zakres jej kompetencji oraz w odniesieniu do których Unia przyjęła przepisy.
- (28) Negocjacje, w tym każda runda negocjacji, muszą być przygotowane z dużym wyprzedzeniem. W tym celu Komisja powinna poinformować Radę o planowanym harmonogramie i kwestiach będących przedmiotem negocjacji oraz jak najszybciej przekazać odnośne informacje.
- (29) Zgodnie z zasadą lojalnej współpracy Komisja i państwa członkowskie powinny ściśle współpracować w trakcie procesu negocjacyjnego, w tym poprzez regularne kontakty z ekspertami i przedstawicielami państw członkowskich w Wiedniu i Nowym Jorku.
- (30) Sesje negocjacyjne powinno poprzedzać posiedzenie Grupy Roboczej ds. Współpracy Sądowej w Sprawach Karnych mające na celu określenie kluczowych kwestii, sformułowanie opinii i udzielenie wskazówek, w tym, w stosownych przypadkach, formułowanie oświadczeń i zastrzeżeń.
- (31) Po każdej sesji negocjacyjnej Komisja powinna składać Grupie Roboczej ds. Współpracy Sądowej w Sprawach Karnych sprawozdanie z wyników negocjacji, w tym w formie pisemnej.
- (32) Komisja powinna informować Radę i konsultować się z Grupą Roboczą ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych w sprawie wszelkich istotnych kwestii, które mogą zostać podjęte w trakcie negocjacji.