

Bruksela, 9 czerwca 2016 r.
(OR. en)

10007/16

JAI 552
COPEN 195
DROIPEN 109
CYBER 67
JAIEX 61
EJUSTICE 121

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	9 czerwca 2016 r.
Do:	Delegacje

Nr poprz. dok.:	9579/16 + COR 1
-----------------	-----------------

Dotyczy:	Konkluzje Rady Unii Europejskiej dotyczące usprawnienia wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni – Konkluzje Rady (9 czerwca 2016 r.)
----------	---

Delegacje otrzymują w załączeniu konkluzje Rady dotyczące usprawnienia wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni, przyjęte przez Radę na jej 3473. posiedzeniu w dniu 9 czerwca 2016 r.

**Konkluzje Rady Unii Europejskiej dotyczące usprawnienia wymiaru sprawiedliwości
w sprawach karnych w cyberprzestrzeni**

ZDECYDOWANA uniemożliwić przestępcom stworzenie bezpiecznej przystani
w cyberprzestrzeni,

ODNOTOWUJĄC coraz większe skutki cyberprzestępczości, przestępczości wykorzystującej
cyberprzestrzeń lub wszelkiej innej działalności przestępczej, która zostawia ślad cyfrowy
w cyberprzestrzeni,

PODKREŚLAJĄC rosnące znaczenie dowodów elektronicznych w postępowaniach karnych
w odniesieniu do wszystkich rodzajów przestępstw, w szczególności terroryzmu,

PODKREŚLAJĄC znaczenie, jakie dla naszych gospodarek i społeczeństw ma ochrona
cyberprzestrzeni przed nadużyciami i działalnością przestępczą, i w związku z tym potrzebę, by
organy ścigania i organy sądowe dysponowały skutecznymi narzędziami dochodzenia i ścigania
przestępstw dotyczących cyberprzestrzeni,

PRZYPOMINAJĄC, że zwalczanie cyberprzestępczości jest jednym z priorytetów Europejskiej
agendy bezpieczeństwa z dnia 28 kwietnia 2015 r., która zawiera zobowiązanie Komisji do
dokonania przeglądu przeszkód w dochodzeniach dotyczących cyberprzestępczości, zwłaszcza
przepisów regulujących dostęp do dowodów i informacji,

PRZYWOŁUJĄC dyskusję ministrów sprawiedliwości na temat przyszłych wyzwań dla
skutecznego wymiaru sprawiedliwości w sprawach karnych w erze cyfrowej przeprowadzoną na
posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w grudniu 2015 r.¹,

PRZYWOŁUJĄC poparcie ministrów sprawiedliwości dla opracowania konkretnych elementów
wspólnego unijnego podejścia do jurysdykcji w cyberprzestrzeni, wyrażone na nieformalnym
posiedzeniu ministrów sprawiedliwości i spraw wewnętrznych w dniu 26 stycznia 2016 r.,

¹ Dok. 14369/15.

PRZYWOŁUJĄC wspólne oświadczenie ministrów sprawiedliwości i spraw wewnętrznych oraz przedstawicieli instytucji UE w sprawie zamachów terrorystycznych w Brukseli w dniu 22 marca 2016 r., w którym podkreślono potrzebę znalezienia w trybie priorytetowym sposobów szybszego i skuteczniejszego zabezpieczania i uzyskiwania dowodów elektronicznych przez zintensyfikowanie współpracy z państwami trzecimi i usługodawcami działającymi na terytorium europejskim w celu poprawy przestrzegania przepisów UE i państw członkowskich, a także przez zintensyfikowanie bezpośrednich kontaktów z organami ścigania, jak również potrzebę zidentyfikowania konkretnych środków służących zajęciu się tą skomplikowaną kwestią podczas posiedzenia Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w czerwcu²,

PRZYWOŁUJĄC komunikat z dnia 20 kwietnia 2016 r. do Parlamentu Europejskiego, Rady Europejskiej i Rady pt. „Realizacja europejskiej agendy bezpieczeństwa w celu zwalczania terroryzmu i utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa”, w ramach którego Komisja zobowiązała się do zaproponowania rozwiązań i zajęcia się problemami z uzyskiwaniem dowodów cyfrowych w związku z dochodzeniami karnymi,

ODNOTOWUJĄC sprawozdanie³ z konferencji dotyczącej jurysdykcji w cyberprzestrzeni, która odbyła się w dniach 7 i 8 marca 2016 r. w Amsterdamie, odzwierciedlające dyskusje na temat możliwych rozwiązań służących usprawnieniu dochodzeń w cyberprzestrzeni, w szczególności rozwiązań dotyczących procedur wzajemnej pomocy prawnej i współpracy z sektorem prywatnym, a także rozwiązań służących usprawnieniu dochodzeń w cyberprzestrzeni, w przypadku gdy lokalizacja danych lub pochodzenie cyberataków nie są (jeszcze) znane,

ODNOTOWUJĄC przyjęcie przez COSI zestawu zaleceń dotyczących poprawy współpracy operacyjnej w zakresie dochodzeń w cyberprzestrzeni⁴,

ODNOTOWUJĄC, że trwająca siódma runda ocen wzajemnych poświęcona praktycznemu wdrażaniu i funkcjonowaniu europejskich polityk dotyczących zapobiegania cyberprzestępczości i jej zwalczania stanowi ważny wkład w wysiłki na rzecz intensyfikacji walki z cyberprzestępczością,

² Dok. 7371/16.

³ Dok. 7323/16.

⁴ Dok. 8634/2/16 REV 2.

ODNOTOWUJĄC wyniki przeglądu umowy między UE i USA o wzajemnej pomocy prawnej⁵,

ODNOTOWUJĄC konkluzje Rady w sprawie europejskiej sieci sądowej ds. cyberprzestępczości⁶,

PRZYWOŁUJĄC Konwencję Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. oraz jej protokół dodatkowy, propagowane przez Unię jako globalne ramy odniesienia dla zwalczania cyberprzestępczości,

PRZYWOŁUJĄC dyrektywę 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, która ma na celu szybsze i skuteczniejsze prowadzenie dochodzeń transgranicznych w całej UE, tj. na podstawie zasady wzajemnego uznawania, a także dyrektywę 2013/40/UE dotyczącą ataków na systemy informatyczne, w której wezwano państwa członkowskie m.in. do zapewnienia funkcjonowania ich krajowych punktów kontaktowych w ramach istniejących całodobowych sieci współpracy,

UZNAJĄC, że choć instrumenty te zapewniają szersze możliwości w zakresie egzekwowania prawa w cyberprzestrzeni, nadal istnieją praktyczne i prawne przeszkody, również ze względu na szybki rozwój technologii, np. w przypadku gdy pochodzenie cyberataków lub lokalizacja dowodów elektronicznych nie są (jeszcze) znane lub są zmienne lub w przypadku gdy spreczne przepisy utrudniają współpracę z usługodawcami,

ODNOTOWUJĄC, że przestępczość wykorzystująca cyberprzestrzeń i cyberprzestępczość łamią podstawowe prawa i wolności oraz że konieczne jest zapewnienie pełnej ochrony tych praw i wolności,

UZNAJĄC, że wykorzystanie środków dochodzeniowych powinno służyć ochronie podstawowych praw i wolności i być zgodne z zasadami konieczności i proporcjonalności,

ODNOTOWUJĄC przyjęcie instrumentów unijnej reformy ochrony danych, w szczególności dyrektywy w sprawie ochrony danych w odniesieniu do 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 oraz w sprawie swobodnego przepływu takich danych,

⁵ Dok. 9291/16.

⁶ Dok. 10025/16.

ODNOTOWUJĄC sprawozdania transgranicznej grupy w ramach komitetu Konwencji o cyberprzestępczości z lat 2012 i 2013, w których stwierdzono, że niektóre kraje już realizują ponadgraniczny dostęp do danych w sposób wykraczający poza zakres konwencji budapeszteńskiej na mocy niejasnej podstawy prawnej,

UZNAJĄC, że państwa członkowskie mają uzasadniony interes, aby w dochodzeniach karnych ustalić co najmniej lokalizację dowodów elektronicznych lub pochodzenie cyberataku,

ZDECYDOWANA działać na rzecz utrzymania rządów prawa w cyberprzestrzeni,

RADA UE:

UZNAJE, że następujące wytyczne powinny mieć zastosowanie do przyszłych prac służących poprawie egzekwowania rządów prawa w cyberprzestrzeni oraz uzyskiwania dowodów elektronicznych w postępowaniach karnych:

- praktyczne rozwiązania mające na celu usprawnienie skutecznego prowadzenia postępowań karnych w cyberprzestrzeni powinny zapewniać pełne poszanowanie ram ochrony danych i praw podstawowych;
- należy rozważyć wzmocnienie współpracy z usługodawcami lub wszelkie inne porównywalne rozwiązania, które umożliwiają szybkie ujawnienie danych; można by przewidzieć mniej rygorystyczne procedury prawne służące uzyskiwaniu szczególnych kategorii danych, zwłaszcza danych abonentów; mogłoby to przynieść korzyści wszystkim zainteresowanym stronom;
- należy przyspieszyć i usprawnić procedury wzajemnej pomocy prawnej dotyczące danych elektronicznych; liczba wniosków o wzajemną pomoc prawną między właściwymi organami mogłaby zostać zmniejszona poprzez wzmocnienie współpracy z usługodawcami lub wszelkie inne porównywalne rozwiązania;

- procedury wzajemnego uznawania powinny być sprawnie stosowane do zapewnienia skutecznego zabezpieczania i uzyskiwania dowodów elektronicznych;
- należy rozważyć inne środki, na podstawie przeglądu łączników na potrzeby stwierdzenia jurysdykcji w zakresie egzekwowania przepisów⁷ w cyberprzestrzeni, w tym w przypadkach, gdy lokalizacja danych nie jest (jeszcze) znana lub jest zmienna.

UWAŻA, że należy współpracować z odpowiednimi państwami trzecimi i podmiotami prywatnymi, tak aby umożliwić połączenie skutków różnych środków w celu efektywnego egzekwowania prawa w cyberprzestrzeni.

UWAŻA, że wypracowanie wspólnego unijnego podejścia w zakresie usprawnienia wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni powinno być traktowane jako priorytet. Należy tego dokonać w sposób spójny z pracami prowadzonymi w ramach budapeszteńskiej konwencji Rady Europy.

STWIERDZA ZATEM, ŻE:

I. NALEŻY WZMOCNIĆ WSPÓŁPRACĘ Z USŁUGODAWCAMI.

W tym celu:

1. Wzywa się KOMISJĘ do opracowania wspólnych ram współpracy z usługodawcami w celu uzyskiwania szczególnych kategorii danych, zwłaszcza danych abonenta, jeżeli jest to dopuszczone przez ustawodawstwo państw trzecich, lub do opracowania innego porównywalnego rozwiązania pozwalającego na szybkie legalne ujawnianie takich danych⁸. Wzywa się Komisję, aby dokonała tego w porozumieniu z państwami członkowskimi i odpowiednimi państwami trzecimi oraz we współpracy z sektorem prywatnym.

⁷ Do celów niniejszych konkluzji termin „jurysdykcja w zakresie egzekwowania przepisów” odnosi się do kompetencji właściwych organów do podjęcia czynności dochodzeniowych. Zgodnie z tymi konkluzjami należy zbadać wspólne unijne podejście z myślą o usprawnieniu dochodzeń w cyberprzestrzeni w szczególnych sytuacjach, gdy istniejące ramy prawne są niewystarczające.

⁸ W przypadku gdy wniosek o przekazanie danych obejmuje transfer danych osobowych przez organ państwa członkowskiego, należy przestrzegać odnośnych przepisów o ochronie danych.

2. Takie rozwiązania powinny obejmować wspólnie uzgodnione wymogi, w tym wymogi konieczności i proporcjonalności wniosków, które są skierowane do usługodawców, aby umożliwić legalny dostęp do danych znajdujących się w ich posiadaniu. Powinny zapobiegać niespójnym interpretacjom, kolizji obowiązujących przepisów oraz zająć się kwestią nieujawniania wniosków o dane. Proponowane rozwiązania nie powinny zakłócać rozwiązań na poziomie krajowym.
3. W tym celu wzywa się KOMISJĘ, aby we współpracy z państwami członkowskimi przeanalizowała z usługodawcami możliwość użycia dostosowanych formularzy i narzędzi, o których mowa w sekcji II, w celu ułatwienia uwierzytelniania, zapewnienia szybkich procedur oraz zwiększenia przejrzystości i rozliczalności procesu zabezpieczania i uzyskiwania dowodów elektronicznych.

Wzywa się KOMISJĘ do przedstawienia sprawozdania oceniającego postępy w tej kwestii do grudnia 2016 r. oraz do przedstawienia rezultatów prac do czerwca 2017 r.

II. NALEŻY USPRAWNIĆ PROCEDURY WZAJEMNEJ POMOCY PRAWNEJ (ORAZ, W STOSOWNYCH PRZYPADKACH, WZAJEMNEGO UZNAWANIA)

W tym celu:

4. Wzywa się KOMISJĘ, aby we współpracy z PAŃSTWAMI CZŁONKOWSKIMI i, w razie potrzeby, państwami trzecimi poszukiwała w trybie priorytetowym rozwiązań służących szybszemu i skuteczniejszemu zabezpieczeniu i uzyskiwaniu dowodów elektronicznych przez usprawnienie stosowania procedury wzajemnej pomocy prawnej oraz, w stosownych przypadkach, wzajemnego uznawania.
5. W tym celu wzywa się KOMISJĘ, aby we współpracy z PAŃSTWAMI CZŁONKOWSKIMI, EUROJUSTEM i państwami trzecimi rozważyła sposoby dostosowania, w odpowiednich przypadkach, istniejących znormalizowanych formularzy i procedur służących składaniu wniosków dotyczących zabezpieczenia i uzyskiwania dowodów elektronicznych, oraz by wydała stosowne zalecenia.
6. Aby zwiększyć efektywne wykorzystywanie takich znormalizowanych formularzy i procedur służących uzyskiwaniu dowodów elektronicznych, wzywa się KOMISJĘ, aby we współpracy z PAŃSTWAMI CZŁONKOWSKIMI, EUROJUSTEM, CEPOLEM i, w razie potrzeby, państwami trzecimi, przy wykorzystaniu w stosownych przypadkach istniejących narzędzi elektronicznych oraz przy poszanowaniu kompetencji i kanałów komunikacji w ramach istniejących ram prawnych, opracowała:
 - bezpieczny portal internetowy używany do elektronicznych wniosków i odpowiedzi dotyczących dowodów elektronicznych oraz do odpowiednich procedur, w tym fakultatywnego wykorzystywania automatycznego tłumaczenia takich wniosków, jak również ich identyfikowania i śledzenia;
 - wytyczne i specjalne moduły szkoleniowe – we współpracy z Europejską Siecią Szkolenia Kadr Wymiaru Sprawiedliwości, europejską siecią sądową ds. cyberprzestępczości oraz, w razie potrzeby, organami państw trzecich – dotyczące skutecznego wykorzystywania obecnych ram, które są używane do zabezpieczenia i uzyskiwania dowodów elektronicznych, w tym wytyczne wyjaśniające, kiedy, zgodnie z obowiązującymi przepisami, korzystanie z instrumentów wzajemnej pomocy prawnej lub wzajemnego uznawania nie jest wymagane.

Wzywa się KOMISJĘ do przedstawienia sprawozdania śródkresowego z postępów w zakresie tych działań do grudnia 2016 r. oraz do przedstawienia rezultatów prac najpóźniej do czerwca 2017 r. KOMISJA jest proszona o przedstawienie portalu internetowego do grudnia 2017 r.

7. Wzywa się KOMISJĘ, aby we współpracy z PAŃSTWAMI CZŁONKOWSKIMI i, w razie potrzeby, z państwami trzecimi rozważyła dodatkowe działania w celu skuteczniejszego zabezpieczania i uzyskiwania dowodów elektronicznych poprzez wykorzystanie ram wzajemnej pomocy prawnej między UE a USA.
8. Wzywa się KOMISJĘ, aby – z myślą o pełnym stosowaniu dyrektywy 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych do celów zabezpieczania i uzyskiwania dowodów elektronicznych w UE – dalej monitorowała i wspierała państwa członkowskie w procesie transpozycji tej dyrektywy do dnia 22 maja 2017 r.
9. Wzywa się PAŃSTWA CZŁONKOWSKIE, aby:
 - ratyfikowały i w pełni wdrożyły Konwencję o cyberprzestępczości z dnia 23 listopada 2001 r.;
 - dokonały szybkiej transpozycji dyrektywy w sprawie europejskiego nakazu dochodzeniowego najpóźniej do dnia 22 maja 2017 r.;
 - zapewniły wystarczające zdolności do rozpatrywania wniosków o wzajemną pomoc prawną dotyczących dochodzeń w cyberprzestrzeni oraz zapewniły odpowiednie szkolenia dla personelu dotyczące sposobu rozpatrywania takich wniosków;
 - zoptymalizowały wykorzystanie istniejących całodobowych punktów kontaktowych oraz zwiększyły wykorzystanie wspólnych zespołów dochodzeniowo-śledczych, aby ułatwić wymianę informacji lub przyspieszyć procedurę wzajemnej pomocy prawnej.

III. NALEŻY DOKONAĆ PRZEGLĄDU JURYSDYKCJI W ZAKRESIE EGZEKWOWANIA PRZEPISÓW W CYBERPRZESTRZENI.

W tym celu:

10. Wzywa się KOMISJĘ, aby w świetle wskazówek politycznych udzielonych przez ministrów sprawiedliwości na posiedzeniu Rady w czerwcu 2016 r. i we współpracy z PAŃSTWAMI CZŁONKOWSKIMI, EUROJUSTEM i EUROPOLEM zbadała możliwości wypracowania wspólnego unijnego podejścia do jurysdykcji w zakresie egzekwowania przepisów w cyberprzestrzeni w sytuacjach, gdy istniejące ramy są niewystarczające, np. w sytuacjach, w których pewne systemy informatyczne są stosowane jednocześnie w wielu jurysdykcjach w celu popełnienia jednego przestępstwa, w sytuacjach, gdy dane dowody elektroniczne przemieszczają się między jurysdykcjami w krótkim czasie lub gdy stosowane są zaawansowane metody służące ukryciu lokalizacji dowodów elektronicznych lub działalności przestępczej, co prowadzi do „utraty lokalizacji”.⁹
11. Przy uwzględnieniu specyfiki każdej sytuacji podejście powinno określać:
 - jakie łączniki mogą być podstawą jurysdykcji w zakresie egzekwowania przepisów w cyberprzestrzeni;
 - czy, a jeśli tak, to jakie środki dochodzeniowe mogą być stosowane niezależnie od granic fizycznych.
12. Należy uwzględnić:
 - charakter i wagę przestępstw, które w innym przypadku mogłyby pozostać bezkarne;
 - możliwe podstawy jurysdykcji w zakresie egzekwowania przepisów, tzn. na podstawie łączników, takich jak na przykład lokalizacja siedziby usługodawcy, działalność gospodarcza usługodawcy w państwie prowadzącym dochodzenie, tzn. gdy usługodawca oferuje produkty lub usługi na terytorium państwa prowadzącego dochodzenie („powiązanie biznesowe”), miejsce zwykłego pobytu lub obywatelstwo osoby podejrzanej lub oskarżonej lub też lokalizacja osoby poszkodowanej;

⁹ To są jedynie przykłady. Wzywa się Komisję do przeanalizowania rozwiązań pozwalających na zajęcie się takimi lub podobnie poważnymi sytuacjami, które uzasadniłyby takie podejście.

- stosowanie i skuteczność nakazów krajowych opartych na takich możliwych łącznikach na potrzeby jurysdykcji w zakresie egzekwowania przepisów w cyberprzestrzeni;
- rozwiązanie w zakresie współpracy na rzecz bezpośredniego transgranicznego dostępu do danych bez pomocy technicznej;
- odpowiednie zabezpieczenia, takie jak ochrona praw i wolności podstawowych, danych osobowych oraz zasady proporcjonalności i pomocniczości, jako zasady przewodnie zastosowania środków dochodzeniowych służące zagwarantowaniu ich legalności;
- ewentualne analogie z innymi transgranicznymi systemami prawnymi, np. Traktatem o otwartych przestworzach i Konwencją o prawie morza, przepisami UE dotyczącymi ochrony danych i prawem konkurencji UE;
- wpływ takiego podejścia na istniejące ramy prawne.

Wzywa się KOMISJĘ do sporządzenia sprawozdania dotyczącego procesu opracowywania tego podejścia do grudnia 2016 r. i do przedstawienia wyników tej oceny do czerwca 2017 r. Ocena ta powinna obejmować szczegółowe elementy dotyczące wspólnego unijnego podejścia i propozycje dotyczące jego realizacji, w tym możliwość prowadzenia inicjatywy ustawodawczej w tym zakresie.
