

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Streszczenie opinii Europejskiego Inspektora Danych Osobowych w sprawie wniosków dotyczących europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych

(Pełny tekst niniejszej opinii jest dostępny w wersji angielskiej, francuskiej i niemieckiej na stronie internetowej EIOD www.edps.europa.eu)

(2020/C 32/04)

W kwietniu 2018 r. Komisja przedłożyła dwa wnioski – jeden dotyczący rozporządzenia i jeden dotyczący dyrektywy – w celu ustanowienia ram prawnych, które ułatwiłyby i przyspieszyłyby policji i organom wymiaru sprawiedliwości zabezpieczanie elektronicznego materiału dowodowego w sprawach transgranicznych i uzyskiwanie dostępu do niego. Od tego czasu Rada przyjęła tzw. podejścia ogólne w sprawie wniosków, a Parlament Europejski przedstawił kilka dokumentów roboczych. Swoją opinię wydała Europejska Rada Ochrony Danych. Na szczeblu międzynarodowym można było zaobserwować działania związane z tymi zagadnieniami, w szczególności rozpoczęcie negocjacji w sprawie międzynarodowej umowy dotyczącej transgranicznego dostępu do elektronicznego materiału dowodowego, a także prace nad drugim protokołem dodatkowym do konwencji o cyberprzestępczości. W niniejszej opinii EIOD pragnie przekazać unijnemu prawodawcy nowe przemyślenia na potrzeby dalszych prac nad wnioskami, uwzględniając opisany powyżej rozwój sytuacji.

W dzisiejszym świecie, który ulega zmianom pod wpływem nowych technologii, czas miewa często szczególne znaczenie dla umożliwienia organom uzyskania danych niezbędnych do realizacji ich misji. Jednocześnie nawet przy prowadzeniu śledztw w sprawach krajowych organy ścigania coraz częściej mają do czynienia z „sytuacjami transgranicznymi”, ponieważ korzystano po prostu z usług zagranicznego usługodawcy, a informacje są przechowywane elektronicznie w innym państwie członkowskim. EIOD popiera cel, jakim jest zapewnienie skutecznych narzędzi dostępnych organom ścigania w celu prowadzenia śledztw i ścigania przestępstw, a w szczególności przyjmuje z zadowoleniem cele wniosków, jakimi są przyspieszenie i usprawnienie dostępu do danych w sprawach transgranicznych poprzez uproszczenie procedur w obrębie UE.

Jednocześnie EIOD pragnie podkreślić, że wszelkie inicjatywy w tej dziedzinie muszą być podejmowane z pełnym poszanowaniem Karty praw podstawowych UE oraz unijnych ram ochrony danych osobowych, co jest niezbędne dla zapewnienia istnienia wszystkich koniecznych zabezpieczeń. W szczególności skuteczna ochrona praw podstawowych w procesie transgranicznego gromadzenia dowodów elektronicznych wymaga większego zaangażowania organów wymiaru sprawiedliwości w egzekwującym państwie członkowskim. Powinny być one systematycznie angażowane w ten proces od możliwie wczesnych etapów, mieć możliwość weryfikowania zgodności nakazów z Kartą praw podstawowych UE oraz obowiązek powołania się na tej podstawie na przesłanki do odmowy.

Ponadto w projektowanym rozporządzeniu należy doprecyzować definicje kategorii danych, zapewniając ich spójność z innymi definicjami kategorii danych występującymi w prawie Unii. EIOD zaleca również ponowną ocenę równowagi między różnymi typami przestępstw, dla których możliwe jest wydanie europejskiego nakazu wydania dowodów, a kategoriami danych z uwzględnieniem odpowiedniego orzecznictwa Trybunału Sprawiedliwości UE.

Co więcej, EIOD formułuje konkretne zalecenia dotyczące kilku aspektów wniosków w sprawie elektronicznego materiału dowodowego, które wymagają dopracowania, a można wśród nich wymienić: autentyczność i poufność nakazów i przesyłanych danych; ograniczone zabezpieczanie na podstawie europejskich nakazów zabezpieczania dowodów; obowiązujące ramy ochrony danych; prawa osób, których dane dotyczą; osoby, których dane dotyczą korzystające z immunitetów i przywilejów; przedstawiciele prawni; terminy na realizację europejskich nakazów zabezpieczenia dowodów oraz możliwość sprzeciwienia się nakazowi przez usługodawców.

Wreszcie EIOD zwraca się o doprecyzowanie kwestii zależności między projektowanym rozporządzeniem a przyszłymi umowami międzynarodowymi. Projektowane rozporządzenie powinno zapewniać utrzymanie wysokiego poziomu ochrony danych w UE i stanowić punkt odniesienia przy negocjowaniu międzynarodowych umów w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego.

1. WPROWADZENIE I INFORMACJE OGÓLNE

1. W dniu 17 kwietnia 2018 r. Komisja opublikowała dwa wnioski ustawodawcze (zwane dalej „wnioskami”), którym towarzyszyła ocena skutków⁽¹⁾, obejmująca:
 - wniosek dotyczący rozporządzenia w sprawie⁽²⁾ europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych (zwany dalej „projektowanym rozporządzeniem”),
 - wniosek dotyczący dyrektywy ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych⁽³⁾ (zwany dalej „projektowaną dyrektywą”).
2. Projektowane rozporządzenie będzie istniało równoległe do dyrektywy 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (zwanej dalej „dyrektywą w sprawie europejskiego nakazu dochodzeniowego”) ⁽⁴⁾, która ma na celu ułatwienie procesu gromadzenia dowodów na terytorium innego państwa członkowskiego i obejmuje każdego rodzaju gromadzenie dowodów, w tym dowodów elektronicznych⁽⁵⁾. Wszystkie państwa członkowskie, które brały udział w przyjmowaniu dyrektywy w sprawie europejskiego nakazu dochodzeniowego⁽⁶⁾ miały czas na wdrożenie jej do krajowego porządku prawnego do maja 2017 r. ⁽⁷⁾.
3. W dniu 26 września 2018 r. Europejska Rada Ochrony Danych⁽⁸⁾ (zwana dalej „EROD”) przyjęła opinię⁽⁹⁾ w sprawie przedłożonych wniosków.
4. W dniu 7 grudnia 2018 r. i 8 marca 2019 r. Rada przyjęła podejście ogólne odpowiednio w sprawie projektowanego rozporządzenia⁽¹⁰⁾ i projektowanej dyrektywy⁽¹¹⁾. Parlament Europejski opublikował serię dokumentów roboczych.
5. Europejski Inspektor Ochrony Danych (zwany dalej „EIOD”) z zadowoleniem przyjmuje fakt, że służby Komisji nieformalnie zwróciły się do niego o wydanie opinii przed przyjęciem wniosków. Również z zadowoleniem EIOD przyjmuje fakt odwołania się do jego opinii w motywie 66 projektowanego rozporządzenia oraz motywie 24 projektowanej dyrektywy.
6. W dniu 5 lutego 2019 r. Komisja przyjęła dwa zalecenia dotyczące decyzji Rady: zalecenie dotyczące decyzji upoważniającej do rozpoczęcia negocjacji w celu zawarcia porozumienia między Unią Europejską a Stanami Zjednoczonymi Ameryki Północnej w sprawie transgranicznego dostępu do dowodów elektronicznych na potrzeby współpracy wymiarów sprawiedliwości w sprawach karnych⁽¹²⁾ oraz zalecenie dotyczące upoważnienia Komisji do uczestnictwa w negocjacjach w sprawie drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (CETS nr 185) (zwanej dalej „konwencją o cyberprzestępczości”) ⁽¹³⁾. Dwa wspomniane zalecenia były przedmiotem dwóch opinii wydanych przez EIOD⁽¹⁴⁾. Zarówno negocjacje ze Stanami Zjednoczonymi, jak i te toczące się w Radzie Europy, są ze sobą ściśle powiązane.
7. W lutym 2019 r. Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego skierowała podobne pisma do EIOD i EROD, wnioskując o ocenę prawną oddziaływania amerykańskiej ustawy CLOUD⁽¹⁵⁾, którą Kongres przyjął w marcu 2018 r., na europejskie ramy ochrony danych osobowych. W dniu 12 lipca 2019 r. EIOD i EROD przyjęły wspólną odpowiedź na ten wniosek, przedstawiając wstępną ocenę⁽¹⁶⁾.
8. W dniu 3 października 2019 r. Zjednoczone Królestwo i Stany Zjednoczone podpisały umowę dwustronną w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego w celu zwalczania poważnych przestępstw⁽¹⁷⁾. Jest to pierwsza umowa zawarta na szczeblu władzy wykonawczej umożliwiająca amerykańskim usługodawcom realizowanie wniosków o dane z obcego państwa zgodnie z amerykańską ustawą CLOUD Act.

Niniejsza opinia obejmuje obydwie wnioski, przy czym większy nacisk położono w niej na projektowane rozporządzenie. Zgodnie z misją EIOD w opinii skoncentrowano się na prawie do prywatności i ochronie danych osobowych, a jej celem jest zachowanie spójności względem opinii EROD 23/2018 i uzupełnienie jej przy jednoczesnym uwzględnieniu podejść ogólnych Rady i dokumentów roboczych Parlamentu Europejskiego.

5. WNIOSKI

70. EIOD popiera cel, jakim jest zapewnienie skutecznych narzędzi dostępnych organom ścigania i organom wymiaru sprawiedliwości w celu prowadzenia śledztw i ścigania przestępstw w świecie ulegającym zmianom pod wpływem nowych technologii. Jednocześnie EIOD chce zapewnić, aby działania to było w pełni zgodne z kartą praw podstawowych UE oraz dorobkiem prawnym Unii w zakresie ochrony danych. Projektowane rozporządzenie wymagałoby przechowywania i przekazywania danych osobowych w obrębie Unii Europejskiej i poza nią między właściwymi organami

państw członkowskich, podmiotami prywatnymi, a w niektórych przypadkach – organami państw trzecich. Wiązałoby się to z ograniczeniem dwóch podstawowych praw, jakimi są poszanowanie życia prywatnego i ochrona danych osobowych, gwarantowanych przez art. 7 i 8 Karty praw podstawowych Unii Europejskiej. Aby tego rodzaju ograniczenia były zgodne z prawem, muszą spełniać warunki określone w art. 52 ust. 1 Karty, a szczególnie warunek konieczności.

71. EIOD uważa, że należałoby prowadzić dalszą ocenę rozwiązań alternatywnych, które zapewniłyby większe środki bezpieczeństwa przy jednoczesnym zapewnieniu osiągnięcia tych samych celów.
72. Po drugie, EIOD zauważa, że projektowane rozporządzenie obejmuje już szereg gwarancji proceduralnych. Tym niemniej EIOD wyraża zaniepokojenie faktem, że ważny obowiązek kontroli zgodności zaświadczenia europejskiego nakazu wydania dowodów i zaświadczenia europejskiego nakazu zabezpieczenia dowodów z Kartą praw podstawowych UE powierzono usługodawcom i zaleca włączenie w tę kontrolę, na możliwie szybkim etapie procesu gromadzenia elektronicznego materiału dowodowego, organów wymiaru sprawiedliwości wyznaczonych przez wykonujące państwo członkowskie.
73. EIOD zaleca zapewnienie większej spójności między definicjami kategorii danych z elektronicznego materiału dowodowego a istniejącymi definicjami szczególnych kategorii danych przewidzianych prawem Unii oraz ponowne rozważenie kwestii kategorii danych dostępu lub objęcie dostępu do tego rodzaju danych podobnymi warunkami, jakie mają zastosowanie w przypadku dostępu do kategorii danych dotyczących transakcji i danych dotyczących treści. W projektowanym rozporządzeniu określono jasno i bezpośrednio definicje każdej z kategorii danych w celu zapewnienia pewności prawnej dla wszystkich zaangażowanych zainteresowanych stron. EIOD zaleca również zmianę projektowanej definicji kategorii danych abonenta w celu jej większego doprecyzowania.
74. Ponadto zaleca również ponowną ocenę równowagi między rodzajami przestępstw, w odniesieniu do których można wydać europejskie nakazy wydania i zabezpieczenia dowodów a objętymi kategoriami danych z uwzględnieniem odpowiedniego orzecznictwa TSUE. W szczególności możliwość wydania europejskiego nakazu wydania i zabezpieczenia dowodów w celu pozyskania danych dotyczących transakcji i danych dotyczących treści należy ograniczyć do poważnych przestępstw. EIOD przychyłaby się do określenia zamkniętego katalogu konkretnych poważnych przestępstw, w odniesieniu do których możliwe jest wydanie europejskiego nakazu wydania i zabezpieczenia dowodów w celu pozyskania danych dotyczących transakcji i danych dotyczących treści, co zwiększyłoby również pewność prawa dla wszystkich zaangażowanych zainteresowanych stron.
75. EIOD formułuje również zalecenia służące zapewnieniu poszanowania danych i prywatności przy osiągnięciu celu szybkiego gromadzenia materiału dowodowego na potrzeby konkretnego postępowania karnego. Zalecenia te dotyczą głównie bezpieczeństwa transmisji danych między wszystkimi zaangażowanymi zainteresowanymi stronami, autentyczności nakazów i zaświadczeń oraz ograniczonego zabezpieczania danych na podstawie europejskiego nakazu zabezpieczenia dowodów.
76. Poza uwagami ogólnymi i głównymi zaleceniami wspomnianymi powyżej EIOD formułuje w niniejszej opinii dodatkowe zalecenia dotyczące następujących aspektów wniosków:
 - odniesienia się do obowiązujących ram ochrony danych osobowych,
 - praw osób, których dane dotyczą (większej przejrzystości i prawa do środka ochrony prawnej),
 - osób, których dane dotyczą, korzystających z immunitetów i przywilejów,
 - powołania przedstawicieli prawnych na potrzeby gromadzenia materiału dowodowego w sprawach karnych,
 - terminu na realizację europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów i przedstawienie materiału dowodowego,
 - możliwości sprzeciwienia się nakazom przez usługodawców na określonych podstawach.
77. Wreszcie EIOD ma świadomość szerszego kontekstu, w jakim przedkładano wnioski, jak również dwóch przyjętych decyzji Rady: jednej dotyczącej drugiego protokołu dodatkowego do konwencji Rady Europy o cyberprzestępczości, a jednej dotyczącej rozpoczęcia negocjacji ze Stanami Zjednoczonymi. Zwraca się o doprecyzowanie kwestii zależności między projektowanym rozporządzeniem a umowami międzynarodowymi. EIOD wyraża gotowość do konstruktywnej współpracy w celu zapewnienia spójności i zgodności ostatecznych tekstów z unijnymi ramami ochrony danych osobowych.

Bruksela, dnia 6 listopada 2019 r.

Wojciech Rafał WIEWIÓROWSKI
Zastępca Inspektora

(¹) Dokument roboczy służb Komisji: Ocena skutków, SWD(2018) 118 final (zwana dalej „oceną skutków”), dostępna na stronie: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=SWD%3A2018%3A118%3AFIN>.

(²) Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady 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.

- (³) Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych, COM(2018) 226 final.
- (⁴) 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; zob. art. 23 projektowanego rozporządzenia.
- (⁵) Dyrektywa w sprawie europejskiego nakazu dochodzeniowego przewiduje ścisłą współpracę organu wydającego nakaz w jednym państwie członkowskim i organu egzekwującego nakaz w innym państwie członkowskim, czy też – stosownie do przypadku – współpracę za pośrednictwem organów centralnych powołanych przez zainteresowane państwa członkowskie. Ma ona na celu usprawnienie i przyspieszenie tej współpracy poprzez zapewnienie standardowych formularzy i ścisłych terminów oraz usunięcie kilku przeszkód współpracy transgranicznej, przykładowo: „[o]rgan wydający może wydać END w celu zastosowania wszelkich czynności służących tymczasowemu zapobieżeniu zniszczeniu, przekształceniu, usunięciu, przekazaniu lub pozbyciu się przedmiotu, który może być wykorzystany jako dowód” oraz „Organ wykonujący podejmuje decyzję co do zastosowania tego środka tymczasowego i informuje o niej tak szybko, jak to możliwe, a jeśli jest to wykonalne — w ciągu 24 godzin od otrzymania END” (art. 32); ponadto przy wykonaniu END w celu zidentyfikowania osób posiadających abonament na określony numer telefonu lub adres IP nie ma zastosowania wymóg podwójnej karalności (art. 10 ust. 2 lit. e) w związku z art. 11 ust. 2).
- (⁶) Wszystkie państwa członkowskie UE z wyjątkiem Danii i Irlandii.
- (⁷) Wszystkie państwa członkowskie wdrożyły dyrektywę w sprawie europejskiego nakazu dochodzeniowego do swoich przepisów krajowych w 2017 r. lub 2018 r. Zob. status wdrożenia Europejskiej Sieci Sądowej: https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?l=PL&CategoryId=120.
- (⁸) EROD ustanowiona art. 68 RODO jest następcą grupy roboczej ustanowionej na podstawie art. 29 uchylonej dyrektywy 95/46/WE. EROD, podobnie jak dawniej Grupa Robocza Art. 29, składa się z przedstawicieli krajowych organów ochrony danych i EIOD.
- (⁹) Opinia 23/2018 z dnia 26 września 2018 r. w sprawie wniosków Komisji dotyczących europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych (art. 70 ust. 1 lit. b) (zwana dalej „opinią EROD 23/2018”), dostępna na stronie: https://edpb.europa.eu/sites/edpb/files/files/file1/evidence_opinion_final_en.pdf.
- (¹⁰) <https://www.consilium.europa.eu/pl/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/>.
- (¹¹) <https://www.consilium.europa.eu/pl/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/>.
- (¹²) Zalecenie dotyczące decyzji Rady 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, COM(2019) 70 final.
- (¹³) Zalecenie dotyczące decyzji Rady upoważniającej do uczestnictwa w negocjacjach w sprawie drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (CETS nr 185), COM(2019) 71 final Do dnia dzisiejszego konwencję Rady Europy o wzmocnieniu współpracy międzynarodowej w zwalczaniu przestępczości i elektronicznych materiałów dowodowych podpisały wszystkie państwa członkowskie UE, a niemal wszystkie już ją ratyfikowały. Proces ratyfikowania konwencji o cyberprzestępczości toczy się nadal w Irlandii i Szwecji. Konwencja o cyberprzestępczości jest wiążącym instrumentem międzynarodowym, który wymaga od Układających się Stron określenia w prawie krajowym konkretnych przestępstw popełnionych przeciwko sieciom elektronicznym lub z ich wykorzystaniem oraz nadania konkretnych uprawnień i stworzenia procedur umożliwiających organom krajowym prowadzenie śledztw, w tym gromadzenie dowodów w sprawie przestępstw w postaci elektronicznej. Promuje się w niej również współpracę międzynarodową między Układającymi się Stronami. Są to konkretne środki służące stawieniu czoła wyzwaniom wynikającym ze zmienności danych. W tym względzie Konwencja przewiduje przyspieszone zabezpieczenie przechowywanych danych komputerowych. Ponieważ przeniesienie zabezpieczonego materiału dowodowego do państwa wnioskującego jest zależne od ostatecznej decyzji wydanej w odpowiedzi na wniosek o wzajemną pomoc prawną, zabezpieczenie nie powinno być zależne od pełnego katalogu przesłanek odmowy; w szczególności podwójna karalność powinna być wymagana wyłącznie w wyjątkowych sytuacjach (art. 29).
- (¹⁴) Zob. opinia EIOD 2/2019 w sprawie mandatu negocjacyjnego na potrzeby zawieranej między Unią Europejską a Stanami Zjednoczonymi umowy w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego oraz opinia EIOD 3/2019 dotycząca uczestnictwa w negocjacjach dotyczących drugiego protokołu dodatkowego do budapesztańskiej konwencji o cyberprzestępczości.
- (¹⁵) Dostępne na stronie: <https://www.congress.gov/bill/115th-congress/house-bill/1625/text>.
- (¹⁶) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_fr
- (¹⁷) <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-counteracting-serious-crime-cs-usa-no62019>