Opinia Rady (art. 70 ust. 1 lit. b))

Opinia 23/2018 w sprawie wniosków Komisji dotyczących europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów w sprawach karnych (art. 70 ust. 1 lit. b)

Przyjęta dnia 26 września 2018 r.

Spis treści

Europejska Rada Ochrony Danych

Uwzględniając art. 70 ust. 1 lit. b) rozporządzenia 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,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

Wprowadzenie

W kwietniu 2018 r. Komisja przedstawiła wniosek dotyczący rozporządzenia w sprawie europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów w sprawach karnych oraz wniosek dotyczący dyrektywy ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych. Te dwa wnioski COM (2018) 225 final i COM (2018) 226 final uzupełniają się. Ogólnym celem Komisji jest poprawa współpracy między organami państw członkowskich a dostawcami usług, w tym dostawcami usług spoza UE, a także zaproponowanie rozwiązań problemu określania i egzekwowania jurysdykcji w cyberprzestrzeni.

W projekcie rozporządzenia ustanowiono zasady i procedury mające zastosowanie do wydawania, doręczania i egzekwowania wobec podmiotów świadczących usługi łączności elektronicznej nakazów wydania dowodów i nakazów zabezpieczenia dowodów. W projekcie dyrektywy natomiast przewidziano minimalne zasady dotyczące mianowania przedstawiciela prawnego dla dostawców usług niemających siedziby w UE.

W listopadzie 2017 r.[1], zanim Komisja przedłożyła projekt wniosku, Grupa Robocza Art. 29 przypomniała o konieczności zapewnienia, aby wszelkie wnioski legislacyjne były w pełni zgodne z obowiązującym dorobkiem prawnym UE w dziedzinie ochrony danych, jak również ogólnie z unijnym prawem i orzecznictwem.

W szczególności Grupa Robocza Art. 29 ostrzegła przed ograniczeniami praw do ochrony danych i prywatności w odniesieniu do danych przetwarzanych przez dostawców usług telekomunikacyjnych i usług społeczeństwa informacyjnego, zwłaszcza gdy dane te są dalej przetwarzane przez organy ścigania, przypomniała o konieczności zapewnienia spójności wszelkich instrumentów UE z obowiązującą konwencją budapeszteńską Rady Europy o cyberprzestępczości oraz z dyrektywą UE w sprawie europejskiego nakazu dochodzeniowego (END), a także zaleciła doprecyzowanie odpowiednich przepisów proceduralnych regulujących dostęp do dowodów elektronicznych na szczeblu krajowym i unijnym w celu zapewnienia, aby nowy instrument nie przyznawał organom nowych uprawnień, których nie miałyby one wewnętrznie. Oprócz tych ogólnych uwag Grupa Robocza Art. 29 przedstawiła uwagi na temat wariantów ustawodawczych rozpatrywanych wówczas przez Komisję w odniesieniu do kategorii tych danych oraz odpowiadających im zabezpieczeń dostępu do nich, na temat możliwości kierowania nakazów wydania dowodów/wniosków o wydanie dowodów w celu nakłonienia dostawców usług spoza UE do udostępnienia danych, a także na temat

[1] Zob. oświadczenie Grupy Roboczej Art. 29 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

materialnych i proceduralnych warunków niezbędnych zabezpieczeń związanych z bezpośrednim dostępem do danych.

Teraz, gdy przedstawiono już gotowe wnioski dotyczące dostępu do dowodów elektronicznych, EROD pragnie w sposób bardziej szczegółowy przeanalizować zaproponowane instrumenty prawne pod kątem ochrony danych.

1. Podstawa prawna wniosku dotyczącego rozporządzenia (art. 82 TFUE)

Podstawę prawną zaproponowaną w projekcie rozporządzenia w sprawie dowodów elektronicznych stanowi art. 82 ust. 1 TFUE dotyczący współpracy sądowej w sprawach karnych, który stanowi, że:

> *1. Współpraca wymiarów sprawiedliwości w sprawach karnych w Unii opiera się na zasadzie wzajemnego uznawania wyroków i orzeczeń sądowych oraz obejmuje zbliżanie przepisów ustawowych i wykonawczych Państw Członkowskich w dziedzinach, o których mowa w ustępie 2 i w artykule 83.*
>
> *Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, przyjmują środki mające na celu:*
>
> *a) ustanowienie zasad i procedur zapewniających uznawanie w całej Unii wszystkich form wyroków i orzeczeń sądowych;*
>
> *b) zapobieganie sporom o jurysdykcję między Państwami Członkowskimi i ich rozstrzyganie;*
>
> *c) wspieranie szkolenia sędziów i innych pracowników wymiaru sprawiedliwości;*
>
> *d) ułatwianie współpracy między organami sądowymi lub równoważnymi organami Państw Członkowskich w ramach ścigania karnego i wykonywania orzeczeń.*

Jak podkreśliła Komisja w ocenie skutków towarzyszącej wnioskom, „art. 82 ust. 1 stanowi, że współpraca wymiarów sprawiedliwości w sprawach karnych opiera się na zasadzie wzajemnego uznawania. Wskazana podstawa prawna obejmowałaby ewentualne uregulowanie w sprawie bezpośredniej współpracy z usługodawcami, w ramach której organ wydającego państwa członkowskiego występowałyby bezpośrednio do danego podmiotu (dostawcy usług) w państwie wykonującym, a nawet nakładałby na niego obowiązki. Tym samym mechanizm wzajemnego uznawania nabrałby nowego wymiaru wykraczającego poza tradycyjną unijną współpracę sądową, która opierała się dotychczas na procedurach angażujących dwa organy sądowe – jeden w państwie wydającym i drugi w państwie wykonującym.”(podkreślenie dodane)

Biorąc pod uwagę nowatorskie zastosowanie wskazanej podstawy prawnej, które polega na możliwości bezpośredniego występowania organów publicznych do podmiotów prywatnych, Europejska Rada Ochrony Danych wyraża ubolewanie, że Komisja nie przedstawiła ani pogłębionej analizy, ani oceny tego podejścia.

Co więcej, jak już podkreśliła to grupa robocza w swoim poprzednim oświadczeniu, tak i obecnie zdaniem EROD zachodzą wątpliwości co do prawidłowego zastosowania tej podstawy prawnej. Wątpliwości te wzmacnia wywód Trybunału Sprawiedliwości Unii Europejskiej i jego rzecznika generalnego zawarty w opinii 1/15. Wśród uwag Trybunału odnoszących się do kwestii prawidłowości zastosowania art. 82 jako podstawy prawnej dla przewidywanej umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych PNR, Trybunał podkreślił, że kanadyjski właściwy

organ *„nie jest [..] ani organem sądowym, ani organem mu równoważnym”*[2]. W kontekście przedstawionych wniosków dotyczących dowodów elektronicznych jednym z głównych celów proponowanych regulacji wydaje się być, jak stwierdziła Komisja, uniknięcie „zbyt uciążliwej” współpracy sądowej. W związku z tym wniosek oparto na zasadzie, zgodnie z którą współpraca powinna odbywać się pomiędzy organem a usługodawcą, a nie pomiędzy dwoma organami. Zgodnie z przewidywaną procedurą to przede wszystkim podmioty prywatne mają być odbiorcami wniosków pochodzących od organów sądowych oraz do nich należałoby udzielanie odpowiedzi na te wnioski.

EROD zauważa, że wykonanie nakazu wydania dowodów lub nakazu zabezpieczenia dowodów mogłoby pociągać za sobą konieczność zaangażowania organu otrzymującego w sytuacji, gdy usługodawca, który otrzymał wniosek, nie wykonuje nałożonego na niego obowiązku, co wywołuje konieczność zwrócenia się o wykonanie nakazu ex post. Jako że głównym celem ustanowionej procedury jest jednak, by nie angażować organu otrzymującego, zdaniem EROD wątpliwości budzi kwestia, czy omawiana procedura pomocnicza mogłaby uzasadniać stosowanie art. 82 jako jedynej podstawy prawnej dla tego instrumentu.

Dlatego też EROD uważa, że współpraca taka wymagałaby stosowania innej podstawy prawnej, natomiast art. 82 należy stosować wówczas, gdy na głównych etapach procedury odbywa się współpraca pomiędzy dwoma organami sądowymi.

2. Niezbędność wprowadzenia dowodów elektronicznych a traktaty o pomocy prawnej i europejski nakaz dochodzeniowy

EROD zauważa, że Komisja zobowiązuje się przeprowadzić przegląd przeszkód w prowadzeniu dochodzeń w sprawach karnych, w szczególności co do kwestii dostępu do dowodów elektronicznych. W uzasadnieniu Komisja przedstawiła kontekst wniosku oraz podkreśliła ulotność dowodów elektronicznych, ich znaczenie międzynarodowe, jak również konieczność dostosowania mechanizmu współpracy do warunków ery cyfrowej. Wnioski dotyczące rozporządzenia i dyrektywy w sprawie przekazywania i dostępu do dowodów elektronicznych nie zmierzają do zastąpienia wcześniejszych instrumentów współpracy w sprawach karnych, takich jak konwencja budapeszteńska, traktat o pomocy prawnej oraz europejski nakaz dochodzeniowy (dyrektywa END). Według Komisji wnioski dotyczące dowodów elektronicznych mają na celu usprawnienie współpracy sądowej w sprawach karnych pomiędzy organami i usługodawcami w Unii Europejskiej, jak również z państwami trzecimi, w szczególności ze Stanami Zjednoczonymi.

Ponieważ te nowe narzędzia będą specjalnie służyć przekazywaniu dowodów elektronicznych i uzyskiwaniu do nich dostępu, EROD oceni wartość dodaną instrumentów w porównaniu z dyrektywą END oraz traktatem o pomocy prawnej.

a) Niezbędność wprowadzenia dowodów elektronicznych a zabezpieczenia przewidziane w europejskim nakazie dochodzeniowym i traktatach o pomocy prawnej

[2] Zob. pkt 103 opinii 1/15 i pkt 108 opinii rzecznika generalnego w tej sprawie.

Główny argument Komisji na poparcie wniosków dotyczących dowodów elektronicznych to przyspieszenie procesu zabezpieczania i uzyskiwania dowodów elektronicznych przechowywanych przez lub będących w posiadaniu dostawców usług prowadzących działalność w innej jurysdykcji.

EROD ubolewa jednak, że w ocenie skutków nie wskazano na konieczność stworzenia nowego instrumentu służącego udostępnianiu dowodów elektronicznych. Co więcej, we wnioskach tych nie wykazano, że można było wykorzystać inne mniej ingerujące w prywatność środki, aby osiągnąć cel wniosku. Jednocześnie można było rozważyć rozwiązania alternatywne. Przykładowo można było rozważyć możliwość wprowadzenia zmian i ulepszeń w dyrektywie END, co tym samym pozwoliłoby spełnić szczególny wymóg wynikający z przepisów tej dyrektywy, a wiążący się z oceną potrzeb wprowadzenia w niej zmian do dnia 21 maja 2019 r[3]. Innym rozwiązaniem mogłoby być takie uregulowanie nakazów zabezpieczenia, aby można je było wykorzystywać w celu zamrożenia danych tak długo, na jak długo dany wniosek na podstawie traktatu o pomocy prawnej formalnie wydano. Warianty te umożliwiłyby utrzymanie zabezpieczeń przewidzianych w tych instrumentach przy jednoczesnym zagwarantowaniu, że poszukiwane dane osobowe nie zostaną usunięte.

EROD zauważa, że terminy ustanowione w dyrektywie END są dłuższe niż te określone we wniosku dotyczącym dowodów elektronicznych. I tak, organ wykonujący ma 30 dni na podjęcie decyzji w sprawie uznania wniosku[4], a następnie powinien wykonać nakaz w terminie 90 dni[5]. Zdaniem EROD przyznanie organom wykonującym END 30-dniowego terminu do namysłu stanowi kluczowe zabezpieczenie pozwalające tym organom ocenić, czy dany wniosek o wykonanie jest właściwie uzasadniony oraz czy spełnione zostały wszystkie warunki wydania i przekazania END[6].

EROD wyraża obawę, że 10-dniowy termin do wykonania zaświadczenia europejskiego nakazu wydania dowodów (EPOC), który zaproponowano we wnioskach dotyczących dowodów elektronicznych, nie daje organowi czasu do namysłu, uniemożliwiając dokonanie właściwej oceny tego, czy EPOC spełnia wszystkie kryteria oraz czy jest poprawnie wypełniony.

Dlatego też EROD zaleca, aby ustanowić termin dłuższy, który umożliwi odbiorcy EPOC rozważenie, czy wykonanie nakazu jest zasadne.

EROD zauważa, że w przypadku zaświadczenia europejskiego nakazu zabezpieczenia dowodów nie ma gwarancji, że zabezpieczenie danych będzie ograniczone do tego, co jest niezbędne do ich wydania. Okres zabezpieczenia danych może być bowiem dłuższy niż 60 dni, ponieważ organ wydający nie jest związany terminem co do powiadomienia adresata o odstąpieniu od wydania nakazu wydania dowodów lub jego wycofaniu. W związku z powyższym EROD zaleca, aby ustanowić co najmniej termin do odstąpienia przez organ wydający od wydania nakazu wydania dowodów lub jego wycofania w celu zachowania zgodności z ustanowioną w RODO zasadą minimalizacji danych[7].

Wreszcie EROD zauważa, że w dyrektywie END ustanowiono zwrot dowodów przez państwo wydające organowi wykonującemu[8]. Wniosek dotyczący rozporządzenia w sprawie dowodów elektronicznych jednak na temat takiej możliwości milczy. Co stanie się z dowodami elektronicznymi po ich przekazaniu organowi wydającemu, tego nie wiadomo.

[3] Zob. art. 37 dyrektywy.
[4] Art. 12 ust. 3 dyrektywy END
[5] Art. 12 ust. 4 dyrektywy END
[6] Art. 6 dyrektywy END
[7] Art. 5 ust. 1 lit. c) RODO.
[8] Art. 13 ust. 3 i 4 dyrektywy END.

Dlatego też EROD zaleca, aby wniosek dotyczący rozporządzenia zawierał więcej informacji na temat wykorzystywania dowodów elektronicznych po ich przekazaniu organowi wydającemu w celu zapewnienia zgodności z RODO oraz z zasadą przejrzystości[9], jak również z zasadą ograniczonego celu ustanowioną w traktatach o pomocy prawnej.

b) Rezygnacja z zasady podwójnej karalności

EROD uznaje, że wzajemne uznawanie jest uzależnione od stosowania podwójnej karalności, która dla państw członkowskich jest jednym z przejawów ich suwerenności. Podwójna karalność jest jednak postrzegana w coraz większym stopniu jako przeszkoda dla sprawnej współpracy sądowej. Państwa członkowskie UE są coraz bardziej skłonne do współpracy nawet wówczas, gdy środki dochodzeniowe dotyczą czynów, które nie stanowią przestępstwa według ich prawa krajowego. EROD przypomina jednak, że zasada podwójnej karalności służy dodatkowemu zabezpieczeniu tego, aby dane państwo nie mogło zdać się na pomoc innego państwa w zastosowaniu sankcji karnej, której prawo tego innego państwa nie przewiduje. Mogłoby to przykładowo zapobiec sytuacji, w której dane państwo zwraca się o pomoc do innego państwa w celu pozbawienia kogoś wolności za głoszenie określonych poglądów politycznych w sytuacji, gdy ich głoszenie w państwie, do którego się zwrócono o pomoc, nie podlega odpowiedzialności karnej albo w celu ścigania kogoś za dokonanie aborcji w sytuacji, jeżeli osoba ta zamieszkuje w innym państwie, w którym dokonanie aborcji nie jest przestępstwem. Stosowanie zasady podwójnej karalności wiąże się często także z dodatkowymi ograniczeniami lub zabezpieczeniami dotyczącymi sankcji, jeżeli pomiędzy państwem występującym a państwem wykonującym występują bardzo znaczne różnice w ich uregulowaniu. Sztandarowym przykładem jest zobowiązanie się w niektórych traktatach o pomocy prawnej do niestosowania kary śmierci, gdy prawo jednego z państw-stron jej nie przewiduje.

EROD zauważa, że zasada podwójnej karalności nie znalazła się we wniosku dotyczącym rozporządzenia w sprawie dowodów elektronicznych. Oznacza to jednak wyeliminowanie nie tylko zwykłych formalności towarzyszących wzajemnemu uznawaniu, lecz również zabezpieczeń związanych z samą zasadą podwójnej karalności.

EROD zauważa w tym kontekście, że brakuje odesłania do prawa państwa, w którym usługodawca będący adresatem wniosku ma siedzibę, oraz że zabezpieczenie wszelkich danych, jak również wydanie danych abonenta lub danych dostępu, może być przedmiotem nakazu w odniesieniu do wszystkich przestępstw[10], niezależnie od tego, czy inne państwa członkowskie znają podobne rodzaje przestępstw.

Tymczasem nakazy wydania można wydawać i wykonywać jedynie wtedy, gdy podobny środek jest dostępny co do tego samego przestępstwa w porównywalnej sytuacji krajowej w państwie wydającym[11]. Ponadto, jak wyjaśniła Komisja w uzasadnieniu wniosku dotyczącego rozporządzenia, dane dotyczące transakcji i treści mają charakter szczególny, ponieważ uznaje się je za wrażliwsze. Co więcej, nakazy obejmujące dane dotyczące transakcji lub treści wydaje się w oparciu o próg dla przestępstw zagrożonych karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat w celu zapewnienia poszanowania zasady proporcjonalności oraz praw osób, których te dane te dotyczą[12]. EROD podkreśla jednak, że nie przeprowadzono jak dotąd na poziomie UE harmonizacji przestępstw zagrożonych karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat.

[9] Art. 5 ust. 1 lit. a) RODO.
[10] Art. 5 ust. 3 i art. 6 ust. 2 wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych.
[11] Art. 5 ust. 2 wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych
[12] Art. 5 ust. 4 lit. a) wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych

EROD z dezaprobatą odnosi się do rezygnacji z zasady podwójnej karalności, która ma na celu zapewnienie, aby dane państwo nie mogło zdać się na pomoc innych państw w zastosowaniu jego prawa karnego poza jego terytorium przez państwo, które nie przyjęło takiego samego podejścia, szczególnie biorąc pod uwagę, że nie ma już innych tradycyjnie stosowanych kluczowych zabezpieczeń w dziedzinie prawa karnego (zob. pkt 3 poniżej dotyczący kryteriów terytorialnych oraz pkt 7 lit. g) dotyczący potencjalnych konfliktów z regulacjami prawnymi państw trzecich).

c) Konsekwencje zwracania się bezpośrednio do przedsiębiorstw

EROD dostrzega, że dowody elektroniczne w coraz większym stopniu znajdują się w infrastrukturze prywatnej należącej do dostawców usług oraz że mogą one być dostępne poza granicami państwa prowadzącego dochodzenie lub śledztwo.

EROD zwraca uwagę, że w związku z rozstrzygnięciami w sprawach *Yahoo!*[13] i *Skype*[14] w Belgii oraz w kontekście ataków terrorystycznych zaistniała potrzeba sprawniejszej i szybszej współpracy pomiędzy podmiotami publicznymi a prywatnymi. W ocenie skutków Komisja odnosi się do trzech rodzajów instrumentów proceduralnych angażujących zarówno organy publiczne, jak i dostawców usług. Są to: współpraca sądowa, współpraca bezpośrednia oraz dostęp bezpośredni. O ile ta pierwsza forma nakłada obowiązek wykonania END nie na dostawcę usług, lecz na organ wykonujący[15], druga, tj. współpraca bezpośrednia, opiera się na współdziałaniu dostawcy usług. Z punktu widzenia dostawcy usług najbardziej ingerujący w prywatność jest dostęp bezpośredni, ponieważ organy publiczne mogą uzyskać dostęp do danych bez pomocy podmiotu pośredniczącego.

W związku z powyższym EROD obawia się, że w przypadku kontaktu bezpośredniego dostawcy usług nie zapewnią tak skutecznej ochrony danych osobowych, jaką mogą i są obowiązane zapewnić organy publiczne. EROD podkreśla, że w konsekwencji nie będzie możliwe zastosowanie niektórych gwarancji proceduralnych przewidzianych w ramach współpracy sądowej w odniesieniu do osób fizycznych, jak również do samych przedsiębiorstw[16]. Przykładowo dostawca usług, do którego zwrócono się z wnioskiem, musiałby zaskarżyć nakaz przed sądem innego państwa (członkowskiego), podczas gdy w ramach współpracy sądowej miałby on do czynienia z organami krajowymi. EROD zaleca, aby we wniosku dotyczącym rozporządzenia określone zostały dalsze gwarancje ochrony indywidualnych praw podstawowych, której udzielać będą dostawcy usług. Chodzi tu o ochronę danych osobowych oraz poszanowanie życia prywatnego i rodzinnego. Zalecane jest również informowanie właściwego organu ochrony danych w celu zapewnienia możliwości przeprowadzenia kontroli.

3. Nowa podstawa jurysdykcji oraz tzw. pominięcie kryteriów terytorialnych

EROD zauważa podkreślenie przez Komisję, że jedną z głównych zmian wprowadzonych w przedmiotowych wnioskach jest pominięcie kryteriów terytorialnych i umożliwienie właściwym

[13] Sąd Kasacyjny Belgii, YAHOO! Inc., Nr. P.13.2082.N z dnia 1 grudnia 2015 r.
[14] Sąd karny w Antwerpii, wydział zamiejscowy w Mechelen, Belgia, Nr. ME20.F1.105151-12 z dnia 27 października 2016 r. (Skype odwołał się od tego orzeczenia).
[15] Art. 10–16.
[16] Zob. też w perspektywie międzynarodowej ochrony danych dokument roboczy w sprawie standardów ochrony danych osobowych i prywatności dla transgranicznych wniosków o udostępnienie danych do celów egzekwowania prawa karnego, przyjęty na 63. posiedzeniu Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji, jakie odbyło się w dniach 9–10 kwietnia 2018 r. w Budapeszcie (Węgry).

organom zwracania się o zabezpieczenie i wydanie danych niezależnie od miejsca ich faktycznego przechowywania.

Z punktu widzenia ochrony danych to żadna nowość, że prawo UE o ochronie danych ma zastosowanie niezależnie od tego, gdzie dane określonych osób są przechowywane. RODO stosuje się bowiem wówczas, gdy administrator lub podmiot przetwarzający mają siedzibę w UE lub gdy przetwarza się dane osobowe osób, których dane dotyczą, przebywających w UE, nawet jeżeli administrator lub podmiot przetwarzający nie mają siedziby w UE[17], w którym to przypadku mają oni obowiązek wyznaczyć przedstawiciela prawnego w UE[18]. Z punktu widzenia ochrony danych należy zauważyć, że ów rozszerzony zakres terytorialny ma na celu zapewnienie pełniejszej ochrony osobom, których dane dotyczą, przebywających w UE, bez względu na to, gdzie przedsiębiorstwo przetwarzające ich dane ma siedzibę.

Dlatego też, mimo że pominięcie kryteriów terytorialnych można potraktować jako nowatorskie w dziedzinie prawa karnego, nie wydaje się, aby stanowiło ono kluczową zmianę z punktu widzenia ochrony danych. Ponadto EROD zauważa również, że powiązanie z terytorium UE występuje nadal, ponieważ wyłącznie dostawcy oferujący usługi w Unii objęci są zakresem omawianych wniosków, a fakt, że wnioski o dane można kierować wyłącznie w ramach postępowania przygotowawczego, oznacza powiązanie z UE (ponieważ przestępstwo popełniono na terytorium państwa członkowskiego albo ofiara przestępstwa lub przestępca był obywatelem państwa członkowskiego).

Skoro kryteria terytorialne nie powinny być już w prawie karnym stosowane, najistotniejsze zdaniem EROD jest to, jak zapewnić, aby niestosowanie tych kryteriów nie wpływało niekorzystnie na ochronę danych, na prawa procesowe osób, których dane dotyczą, i dostawców usług, do których o dane się zwrócono. Z tej perspektywy EROD uznaje, że gwarancje proceduralne w UE zostały, przynajmniej częściowo, zharmonizowane oraz że muszą być one zapewnione zgodnie z europejską konwencją praw człowieka. W związku z tym można stwierdzić, że pominięcie kryteriów terytorialnych miałoby prawdopodobnie bardziej ograniczone skutki, gdyby o dowody zwracano się na terytorium UE w porównaniu z sytuacją odwrotną, w której organy państw trzecich zwracają się o dane do przedsiębiorstw mających siedzibę w UE na tych samych warunkach określonych we wniosku dotyczącym rozporządzenia w sprawie dowodów elektronicznych. W szczególności EROD wyraża obawę, że pominięcie kryteriów terytorialnych może wywołać większą liczbę przypadków problematycznych. W ten sposób bowiem organy państw trzecich, w których w prawie karnym stosuje się różne i potencjalnie słabsze zabezpieczenia proceduralne, mogą mieć dostęp do danych, które w UE byłyby chronione dzięki dodatkowym zabezpieczeniom. Mając to na uwadze, EROD ponownie wyraża obawy co do stosowania podwójnego standardu i osłabiania praw podstawowych w sytuacji, gdy dostawcy usług i osoby, których te dane dotyczą, nie korzystają z zabezpieczeń proceduralnych przewidzianych w prawie UE, jeżeli o dane wystąpił organ państwa trzeciego.

Ponadto, jako że ta nowa podstawa jurysdykcji „niezależna od miejsca, w którym znajdują się dane", powiązana jest z procedurą opartą przede wszystkim na zwracaniu się właściwych organów o dane bezpośrednio do dostawców usług, EROD wyraża obawę, że przedsiębiorstwa prywatne otrzymujące wnioski, które nie są związane instrumentem prawnym, takim jak traktat o pomocy prawnej (tradycyjnie regulujący wymianę danych między organami sądowymi i przewidujący odpowiednie zabezpieczenia służące ochronie danych), tych zabezpieczeń mogą nie stosować. W szczególności w odniesieniu do traktatów o pomocy prawnej stosowanie minimalnych zabezpieczeń ochrony danych

[17] Zob. art. 3, w szczególności ust. 2.
[18] Zob. art. 27

wiąże się np. z obowiązkami zachowania poufności oraz respektowaniem zasady ograniczonego celu, która stanowi, że dane nie będą przetwarzane w innym celu.

EROD przypomina w związku z tym, że należy zapewnić stosowanie zabezpieczeń przewidzianych w dyrektywie 2016/680, w tym tych dotyczących przekazywania danych, a w szczególności przepisów art. 39, w sytuacjach, w których dostawca usług ma siedzibę w państwie trzecim, bez konieczności przyjmowania decyzji stwierdzającej odpowiedni stopień ochrony w tej dziedzinie. EROD podkreśla w szczególności, że przepis ten wymaga między innymi poinformowania właściwego organu ochrony danych w państwie członkowskim organu wydającego nakaz (y) oraz udokumentowania przekazania danych, w tym uzasadnienia bezskuteczności lub nieodpowiedniości przekazania danych do właściwego organu państwa trzeciego.

4. Pojęcie „dostawca usług" należy ograniczyć lub uzupełnić dodatkowymi zabezpieczeniami praw osób, których te dane dotyczą

Jeżeli chodzi o dostawców usług, EROD z zadowoleniem przyjmuje szeroką definicję, która pozwala uwzględnić zarówno usługi komunikacyjne, jak i usługi OTT, ponieważ wszystkie te usługi są funkcjonalnie równoważne, a zatem przewidywane środki mogłyby mieć podobny wpływ na prawo do prywatności i prawo do zachowania tajemnicy komunikowania się, jak podkreślono w oświadczeniu Grupy Roboczej Art. 29 i uprzednio już w opinii 01/2017 w sprawie wniosku dotyczącego rozporządzenia w sprawie prywatności i łączności elektronicznej. I tak, wniosek dotyczący rozporządzenia w sprawie dowodów elektronicznych obejmuje dostawców usług świadczących usługi łączności elektronicznej zdefiniowane w art. 2 ust. 4 dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej, usługi społeczeństwa informacyjnego zgodnie z definicją zawartą w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535, w przypadku których przechowywanie danych jest elementem definiującym usługę świadczoną na rzecz użytkownika, w tym portale społecznościowe, rynki internetowe ułatwiające transakcje pomiędzy użytkownikami oraz inni dostawcy usług hostingowych lub usługi dotyczące nazw domen internetowych i numeracji IP, takie jak dostawcy adresów IP, rejestry nazw domen, podmioty rejestrujące nazwy domen i powiązane usługi prywatności i usługi proxy[19].

Dostawca usług w rozumieniu projektu rozporządzenia to jednak każda osoba fizyczna lub prawna, która świadczy przynajmniej jedną z następujących kategorii usług. EROD wyraża zaniepokojenie tym, że instrument ten mógłby obejmować zarówno administratorów, jak i podmioty przetwarzające dane w rozumieniu RODO. Ponieważ „oferowanie usług", zdefiniowane w art. 2 ust. 4 projektu rozporządzenia, obejmuje zarówno umożliwianie osobom prawnym lub fizycznym w co najmniej jednym państwie członkowskim korzystania z wymienionych usług, jak i posiadanie istotnego powiązania z danym państwem członkowskim lub danymi państwami członkowskimi, czynności te obejmują m.in. czynności wykonywane przez podmiot przetwarzający dane na rzecz administratora danych, takie jak np. przechowywanie danych.

EROD wyraża zatem obawę, że bez nałożenia na dostawców usług działających w charakterze administratorów danych w rozumieniu RODO ograniczeń oraz bez nałożenia szczególnego obowiązku powiadamiania przez podmiot przetwarzający administratora danych o otrzymaniu nakazu wydania lub nakazu zabezpieczenia danych, prawa osób, których te dane dotyczą, mogą nie być respektowane.

[19] Art. 2 ust. 3 lit. c) wniosku dotyczącego rozporządzenia w sprawie dowodów elektronicznych

Właśnie taka sytuacja zachodzi, ponieważ w przypadku ewentualnych sprzecznych zobowiązań uniemożliwiających adresatowi zastosowanie się do otrzymanych nakazów, projekt rozporządzenia zachęca organy sądowe, by kierować nakazy do najbardziej właściwego podmiotu, niezależnie od obowiązujących przepisów dotyczących ochrony danych, w szczególności ze względu na fakt, że zwracać się mogą o wszelkie dane, a nie tylko dane osobowe objęte RODO[20].

Zgodnie z RODO podmiot przetwarzający podejmuje czynności wyłącznie na polecenie administratora. Dlatego obowiązkiem administratora jest zapewnienie przestrzegania praw osób, których dane dotyczą, oraz przekazywanie im odpowiednich informacji, w tym o odbiorcach ich danych, np. w kontekście korzystania z przysługującego im prawa dostępu. Podmiot przetwarzający nie będzie otrzymywał tych wniosków od osób, których dane dotyczą, i nie będzie mógł udzielać odpowiedzi, chyba że administrator wyraźnie się o to zwróci.

W związku z tym, chyba że ich prawo do bycia objętym RODO zostało ograniczone na mocy RODO, EROD podkreśla, że osoby, których dane dotyczą, objęte RODO mogą nie mieć możliwości skutecznego korzystania z przysługujących im praw, jeżeli administrator nie jest w stanie przekazać pełnych informacji. EROD zauważa również, że ryzyko braku informacji jest nawet wyższe, skoro podmiotów przetwarzających nie zobligowano do informowania administratora danych w sytuacjach, w których dane, o które się zwrócono, odnoszą się do osób, których te dane dotyczą, niekorzystających z ochrony przyznanej przez RODO. W tej sytuacji organy sądowe występujące o dane niekoniecznie będą zobligowane do informowania osób, których dane dotyczą, o ich dalszym przetwarzaniu. EROD wzywa zatem do ograniczenia zakresu do administratorów danych w rozumieniu RODO lub do wprowadzenia przepisu precyzującego, że w przypadku gdy dostawca usług, do którego się zwrócono, nie jest administratorem danych, informuje o tym administratora danych.

5. Pojęcia „siedziba” i „przedstawiciel prawny” w kontekście przedmiotowych wniosków powinny być wyraźnie rozróżnione od tych pojęć w ujęciu RODO

Ze względu na niestosowanie kryteriów terytorialnych w odniesieniu do danych adresatami nakazów wydania i nakazów zabezpieczenia są zgodnie z projektem rozporządzenia wyłącznie dostawcy usług oferujący usługi w Unii, niezależnie od tego, czy mają oni siedzibę na terytorium UE. Zgodnie z zasadami określonymi w projekcie dyrektywy dostawcy ci mają obowiązek wyznaczenia przedstawiciela prawnego. Pojęcia „siedziba” i „przedstawiciel prawny” zdefiniowano w związku z tym w projektowanych instrumentach.

EROD zwraca uwagę, że pojęcia te pojawiają się również w kontekście innych instrumentów UE, w szczególności w kontekście RODO. Należy zatem doprecyzować definicje oraz przeprowadzić rozróżnienie tych pojęć w kontekście projektowanych wniosków i w kontekście RODO.

a) Zakład

EROD przypomina również, że pojęcie „zakład” stosowane w kontekście projektu rozporządzenia nie powinno być mylone z tym stosowanym w kontekście RODO. Na potrzeby projektu rozporządzenia pojęcie zakładu zdefiniowane w art. 2 ust. 5 jest szersze niż to w RODO, ponieważ obejmuje ono albo rzeczywiste prowadzenie działalności gospodarczej przez nieokreślony czas za pośrednictwem stabilnej

[20] Zob. art. 7 ust. 3 i 4.

infrastruktury, z której świadczy się usługi, albo stabilną infrastrukturę, z której działalność ta jest zarządzana, niezależnie od tego, czy przetwarzanie danych osobowych odbywa się w kontekście działalności tego zakładu. Jeżeli zatem „zakład" w rozumieniu RODO miał bez wątpienia zawierać się w zakresie tego pojęcia, jak zdefiniowano je w projekcie rozporządzenia, to odwrotność w tym względzie raczej nie zachodzi.

Dlatego też EROD przestrzega, że zakłady dostawców usług w rozumieniu projektu rozporządzenia niekoniecznie oznaczają, że warunki stosowania RODO zgodnie z art. 3 ust. 1 są spełnione. W tym kontekście EROD zachęca administratorów i podmioty przetwarzające, aby sprawdzili, czy stosowanie RODO nie wynika z art. 3 ust. 2, co oznaczałoby konieczność wyznaczenia przedstawiciela prawnego w UE oraz brak mechanizmu kompleksowej obsługi.

b) Przedstawiciel prawny

W swoim oświadczeniu Grupa Robocza Art. 29 podkreśliła, że należy unikać wszelkich niejasności pomiędzy obowiązkiem wyznaczenia przedstawiciela prawnego zgodnie z art. 27 RODO a obowiązkiem wyznaczenia przedstawiciela prawnego zgodnie z projektem rozporządzenia w sprawie dowodów elektronicznych.

Na podstawie gotowego już wniosku EROD pragnie o tych zaleceniach przypomnieć, a w szczególności podkreślić, że w jego rozumieniu przedstawiciel prawny, o którym mowa w projekcie dyrektywy w sprawie mianowania przedstawicieli prawnych w kontekście wniosków dotyczących dowodów elektronicznych, powinien być wyznaczany w każdym przypadku. Należy wyposażyć go w określone funkcje, status niezależny od dostawcy usług, który mu udzielił mandatu, uprawnienie do udzielania odpowiedzi na wnioski i dokonywania czynności w imieniu dostawcy usług, a także określić jego odpowiedzialność w sposób surowszy od odpowiedzialności przedstawiciela prawnego, działającego w reżimie RODO.

Ponadto EROD podkreśla, że pomiędzy RODO a projektowanymi przepisami dotyczącymi dowodów elektronicznych występują różnice, jeśli chodzi o obowiązek wyznaczenia przedstawiciela prawnego, którego zgodnie z projektowanymi przepisami wyznacza się w każdym przypadku niezależnie od tego, czy usługodawca ma siedzibę w UE czy nie, możliwość wyznaczenia nawet kilku przedstawicieli prawnych tego samego dostawcy usług, która to możliwość wynika z projektu dyrektywy dotyczącej dowodów elektronicznych oraz o obowiązek powiadamiania organów państw członkowskich o wyznaczeniu przedstawiciela prawnego, którego to obowiązku RODO nie przewiduje, podobnie jak wyjątków dotyczących wyznaczania i ograniczeń odpowiedzialności przedstawiciela prawnego.

Biorąc zatem pod uwagę istotne różnice pod względem roli, zakresu odpowiedzialności i relacji z innymi zakładami dostawcy usług z jednej strony, a administratora lub podmiotu przetwarzającego z drugiej, EROD zaleca, aby w przypadku gdy dostawca usług nie posiada siedziby na terytorium UE, ale podlega zarówno RODO zgodnie z art. 3 ust. 2, jak i rozporządzeniu w sprawie dowodów elektronicznych, wyznaczonych było dwóch odrębnych przedstawicieli prawnych. Każdy z nich powinien posiadać wyraźnie odrębne funkcje, wynikające z odpowiedniego instrumentu prawnego, na podstawie którego został wyznaczony.

6. Nowe kategorie danych

W projektowanym rozporządzeniu w art. 2 określono różne kategorie danych: dane abonenta, dane dostępu, dane dotyczące transakcji oraz dane dotyczące treści. W motywie 20 wniosku Komisji

stwierdza się, że *kategorie danych objęte zakresem niniejszego rozporządzenia obejmują dane abonenta, dane dostępu, dane dotyczące transakcji (te trzy kategorie danych nazywane są dalej „danymi niedotyczącymi treści") oraz dane dotyczące treści. Powyższe rozróżnienie, nie licząc danych dostępu, istnieje w przepisach prawnych wielu państw członkowskich, a także w obecnym ramach prawnych Stanów Zjednoczonych, umożliwiających usługodawcom dobrowolne udostępnianie danych niedotyczących treści zagranicznym organom ścigania.*

W tym kontekście EROD podkreśla przede wszystkim, że wszystkie cztery kategorie danych, o których mowa powyżej, należy zgodnie z przepisami UE o ochronie danych uznać za dane osobowe, ponieważ zawierają one informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, niezależnie od tego, czy w proponowanym rozporządzeniu osobę, której dane dotyczą, określa się jako „abonenta", czy „użytkownika". Należy również zauważyć, że „dowód elektroniczny" zdefiniowany w art. 2 ust. 6 wniosku Komisji obejmuje wszystkie cztery kategorie danych i w związku z tym odnosi się do danych osobowych. Zamiast zatem ustanawiać zasady dotyczące dostępu do dowodów, definiowanych oraz kwalifikowanych zgodnie z prawem krajowym i procedurami sądowymi, w proponowanym rozporządzeniu przewiduje się nowe materialne i proceduralne warunki dostępu do danych osobowych.

Choć proponowane rozporządzenie ustanawia nowe podkategorie danych osobowych, w odniesieniu do których mają zastosowanie różne proceduralne warunki dostępu, EROD przypomina, że – zgodnie z odpowiednim orzecznictwem Trybunału Sprawiedliwości – dla stwierdzenia sprzeczności z podstawowym prawem do poszanowania życia prywatnego nie ma znaczenia, czy informacja dotycząca życia prywatnego jest wrażliwa lub czy dane osoby doświadczyły jakichkolwiek niedogodności.

Ponadto EROD przypomina, że w odniesieniu do „danych niedotyczących treści" obejmujących dane abonenta, dane dostępu i dane dotyczące transakcji, jak przewiduje wniosek Komisji, Trybunał Sprawiedliwości Unii Europejskiej orzekł w wyroku w sprawach połączonych C-203/15 i C-698/15 Tele *2 Sverige AB*, że metadane, takie jak dane o ruchu i dane dotyczące lokalizacji dają możność ustalenia profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów[21].

Jak już stwierdzono w oświadczeniu Grupy Roboczej Art. 29 w sprawie aspektów ochrony danych i prywatności związanych z transgranicznym dostępem do dowodów elektronicznych z dnia 29 listopada 2017 r., EROD ponownie przedstawia swoje wątpliwości i obawy dotyczące przyjętego rozgraniczenia pomiędzy danymi „niedotyczącymi treści" a danymi dotyczącymi treści oraz czterech kategorii danych osobowych przewidzianych w proponowanym rozporządzeniu. Te cztery proponowane kategorie nie wydają się być jasno wyodrębnione, a definicja „danych dostępu" w porównaniu z innymi kategoriami pozostaje niejasna. EROD wyraża zatem ubolewanie, że ani w ocenie skutków, ani we wniosku Komisja nie przedstawiła szerszego uzasadnienia dla stworzenia tych nowych podkategorii danych osobowych. EROD wyraża również zaniepokojenie ustanowieniem odmiennego poziomu gwarancji związanych z materialnymi i proceduralnymi warunkami dostępu do kategorii danych osobowych, w szczególności uwzględniwszy praktyczne trudności w ocenie, do której kategorii należy zaklasyfikować żądane dane w niektórych przypadkach. Przykładowo adresy IP można przyporządkować zarówno do danych dotyczących transakcji, jak i do danych abonenta.

W tym kontekście EROD przypomina również, że w motywie 14 wniosku dotyczącego rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności

[21] Wyrok TSUE z dnia 21 grudnia 2016 r., pkt 99.

elektronicznej Komisja stwierdza, że „dane pochodzące z łączności elektronicznej należy zdefiniować w dostatecznie szeroki i neutralny technologicznie sposób, aby ich definicja obejmowała wszelkie informacje dotyczące przesyłanych lub przekazywanych treści (treści łączności elektronicznej) oraz informacje dotyczące użytkowników końcowych usług łączności elektronicznej przetwarzane w celu przesyłania, dystrybuowania lub umożliwienia wymiany treści łączności elektronicznej; w tym dane służące do śledzenia i zidentyfikowania źródła i miejsca docelowego przypadku łączności, lokalizacji geograficznej oraz daty, godziny, czasu trwania oraz rodzaju łączności". Ponieważ obecne i przyszłe ramy dotyczące prywatności i łączności elektronicznej, jak również związane z nimi ograniczenia prawa do prywatności, będą miały zastosowanie do przepisów regulujących dostęp organów ścigania do dowodów elektronicznych, EROD zaleca, aby w proponowanym rozporządzeniu rozszerzyć definicję danych pochodzących z łączności elektronicznej w celu zapewnienia odpowiednich zabezpieczeń i warunków dostępu, które spójnie obejmą zarówno „dane niedotyczące treści", jak i „dane dotyczące treści".

7. Analiza procedur europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów

Ogólnie rzecz biorąc, wydaje się, że procedura przesyłania nakazów wydania lub zabezpieczenia dowodów wygląda następująco:

- Właściwy organ sądowy – organ wydający – w zależności od rodzaju żądanych danych i od rodzaju nakazu wydaje nakaz zgodnie z (nielicznymi) warunkami wymienionymi w art. 5 i 6, przekazuje nakaz za pośrednictwem zharmonizowanego zaświadczenia do adresata, tj. przedstawiciela prawnego dostawcy usług lub do któregokolwiek z jego zakładów w UE.
- Po otrzymaniu zaświadczenia adresat wykonuje nakaz to znaczy przekazuje dane w terminie 10 dni lub – w sytuacjach wyjątkowych – w terminie 6 godzin lub zabezpiecza je przez okres maksymalnie 60 dni chyba że jest to niemożliwe, ponieważ zaświadczenie jest niekompletne lub zaistniała siła wyższa lub faktyczna niemożliwość dla adresata, lub ponieważ adresat odmawia wykonania nakazu, powołując się na konflikt obowiązków w zakresie praw podstawowych lub podstawowych interesów państwa trzeciego lub na podstawie innych przesłanek.
- Jeżeli adresat nie zastosował się do otrzymanego nakazu bez podania powodów akceptowanych przez organ wydający, przewidziane jest zastosowanie przez właściwy organ przymuszający do wykonania nakazu w państwie członkowskim, w którym dostawca ma swoje przedstawicielstwo lub siedzibę, procedur służących wykonaniu nakazu, chyba że zastosowanie mają ściśle określone przesłanki odmowy, a organ przymuszający sprzeciwił się uznaniu lub wykonaniu nakazu.
- Jeżeli adresat zgłosił uzasadniony sprzeciw wobec nakazu ze względu na konflikt obowiązków, organ wydający kieruje sprawę do właściwego sądu w swoim państwie członkowskim, do którego następnie należy dokonanie oceny potencjalnego konfliktu i utrzymanie nakazu w mocy, o ile stwierdzono brak konfliktu. W razie stwierdzenia konfliktu właściwy sąd albo zwraca się do organów centralnych państwa trzeciego, za pośrednictwem organów centralnych swojego państwa, wyznaczając 15-dniowy termin na odpowiedź (na podstawie uzasadnionego wniosku termin ten może zostać przedłużony do 30 dni) w razie konfliktu obowiązków dotyczącego praw podstawowych lub podstawowych interesów państwa

trzeciego, albo sam rozstrzyga, czy podtrzymać lub wycofać nakaz na podstawie innych przesłanek, na które powołał się adresat.

- Bez uszczerbku dla środków ochrony prawnej na mocy RODO i dyrektywy 2016/680, osoby, których dane uzyskano za pośrednictwem nakazu wydania, mają również prawo do skutecznych środków odwoławczych od tego nakazu.

EROD dokonał oceny procedur i zabezpieczeń przewidzianych w projekcie rozporządzenia, aby oznaczyć poszczególne etapy i po przeanalizowaniu wszystkich aspektów tu przedstawionych zaleca wprowadzenie następujących zabezpieczeń i zmian.

a) Należy podnieść progi powodujące wydanie nakazu, a na wydanie nakazu powinny wydawać zezwolenia sądy

Jeżeli chodzi o warunki wydawania nakazów, EROD z zadowoleniem przyjmuje zasadę stosowania wyższych zabezpieczeń dostępu do danych dotyczących transakcji lub danych dotyczących treści. EROD zauważa jednak, że biorąc pod uwagę brak pełnej harmonizacji sankcji karnych między państwami członkowskimi, odniesienie do przestępstw zagrożonych w państwie wydającym karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech 3 lat[22] nadal oznacza zróżnicowanie progów i powoduje rozbieżności w zakresie ochrony w UE danych osób, których dane dotyczą.

Ponadto EROD podkreśla, że, w szczególności ze względu na szeroką definicję danych abonenta, podany próg wydaje się raczej niski dla nakazów zabezpieczenia i dla nakazów wydania dotyczących danych abonenta lub danych dostępu, ponieważ wszystkie przestępstwa mogą co do zasady uzasadniać wydawanie takich nakazów. Podobnie organy, którym zezwolono na wydawanie takich nakazów, są bardziej ograniczone w kontekście nakazów wydania danych dotyczących transakcji lub danych dotyczących treści, niż w przypadku wydawania nakazów zabezpieczenia lub nakazów wydania dotyczących danych abonenta lub danych dostępu, ponieważ prokuratorzy mogą wystawiać lub zatwierdzać wyłącznie te ostatnie nakazy, podczas gdy każdy sędzia, sąd lub sędzia śledczy może wydać każdy nakaz lub zezwolić na wydanie każdego nakazu.

W szczególności EROD wyraża ubolewanie wobec tego, że najniższy próg umożliwiający organom ścigania wystąpienie o dostęp do danych abonenta i danych dostępu w przypadku każdego przestępstwa opiera się na wykładni *a contrario* orzecznictwa TSUE (który zajmował się innymi danymi) w celu rozróżnienia zabezpieczeń, które mają być ustanowione. Trybunał podkreślił w szczególności, że w przypadku danych o ruchu i danych o lokalizacji, dostęp właściwych organów powinien być ograniczony do celów walki z poważną przestępczością[23]. EROD mógłby uznać to za uzasadnione, jeżeli wniosek przewidywałby możliwość zwrócenia się o dostęp do bardzo podstawowych informacji, które pozwoliłyby tylko na zidentyfikowanie danej osoby bez ujawniania jakichkolwiek danych dotyczących łączności, bez uprzedniej zgody sądu. EROD wyraża jednak dezaprobatę wobec szerokiej wykładni *a contrario* tego orzeczenia przyjętej przez Komisję i wzywa do ustanowienia silniejszych zabezpieczeń w celu ograniczenia podstaw dostępu do innych danych abonenta i danych dostępu. EROD zaleca, aby ograniczyć dostęp do tych danych albo dla przestępstw wymienionych w wykazie zawartym

[22] Zob. art. 5 ust. 3 lit. a)
[23] Zob. sprawa 203/15 – pkt (125)

w projekcie rozporządzenia, albo przynajmniej dla „poważnych przestępstw", w szczególności biorąc pod uwagę niższy próg uprzedniego zezwolenia przewidziany w odniesieniu do tych danych.

Ponadto EROD podkreśla, że taka wykładnia *a contrario* prowadzi również do tego, że wniosek przyznaje prokuratorom możliwość wydawania nakazów lub zezwalania na ich wydawanie. EROD jest zdania, że – z wyjątkiem wniosków o bardzo podstawowe informacje, które pozwoliłyby tylko na zidentyfikowanie danej osoby bez ujawniania jakichkolwiek danych dotyczących łączności – podejście to stanowi krok wstecz w stosunku do orzecznictwa TSUE w zakresie dostępu do danych pochodzących z łączności elektronicznej. W swoim orzecznictwie dotyczącym dostępu do danych pochodzących z łączności elektronicznej do celów egzekwowania prawa TSUE ograniczył możliwość takiego dostępu poprzez uzależnienie go, *z wyjątkiem należycie uzasadnionych pilnych przypadków*[24], między innymi od *uprzedniej kontroli sądu lub niezależnego organu administracyjnego*, *uzasadnionego wniosku właściwych organów krajowych, złożonego w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub ściganie przestępstw*. [25]

EROD przypomina, że pojęcie „sąd" jest autonomicznym pojęciem prawa UE, oraz że TSUE stale podkreślał i przypominał kryteria, które należy spełnić, aby dany organ zakwalifikować jako sąd, w tym kryterium niezależności,[26] które nie jest spełnione w odniesieniu do prokuratorów, na co wskazał również w swoim orzecznictwie ETPCz[27].

Zatem art. 4 ust. 1) lit. a) i b) oraz art. 3 lit. a) i b) skutkują zastosowaniem procedur zawierających znacząco mniej zabezpieczeń w odniesieniu do danych abonenta i danych dostępu, ponieważ prokurator sam będzie mógł zażądać danych bez dodatkowej kontroli organu państwa, w którym te żądane dane się znajdują lub organu właściwego dla miejsca, w którym będzie znajdował się przedstawiciel prawny przedsiębiorstwa, do którego zwrócono się o dane, ani jakiejkolwiek kontroli niezależnego organu administracyjnego.

Ponadto EROD zwraca uwagę na tzw. dodatkowe zabezpieczenie przewidziane w art. 5 ust. 2, które ogranicza możliwość wydania nakazu wydania danych w przypadku, gdy podobny środek był dostępny w odniesieniu do tego samego przestępstwa w porównywalnej sytuacji krajowej. EROD pragnie jednak ostrzec przed odwrotnymi do zamierzonych skutkami zastosowania takiego przepisu: zamiast wprowadzania dodatkowych zabezpieczeń należy, jak się wydaje, zachęcać państwa członkowskie, aby rozszerzały swoje krajowe opcje zwracania się o wydanie danych abonenta lub danych dostępu i tym samym zapewniały możliwość wydawania nakazów wydania dowodów na podstawie tego rozporządzenia.

b) Terminy udostępniania danych powinny być uzasadnione

EROD zauważa, że na europejski nakaz wydania dowodów należy odpowiedzieć w ciągu 10 dni od daty otrzymania zaświadczenia, chyba że organ wydający wskaże przyczyny uzasadniające wcześniejsze wydanie, zaś w przypadkach nadzwyczajnych, najpóźniej w terminie 6 godzin od daty otrzymania zaświadczenia, zgodnie z art. 9 ust. 1 i 2.

EROD nie doszukał się jednak żadnych kryteriów dotyczących obowiązku wykazywania przez organy, nawet *ex post*, nadzwyczajnego charakteru danej sytuacji wymagającego wydania dowodów, które to kryteria umożliwiłyby kontrolę korzystania z tej bardzo szybkiej procedury ze względu na fakt, że termin sześciogodzinny najprawdopodobniej będzie wiązał się z przeprowadzeniem bardzo

[24] Zob. sprawa 203/15 – pkt (120)
[25] Zob. połączone sprawy C 293/12 i C 594/12 – pkt (62)
[26] Zob. np. sprawa C 203/14
[27] Zob. np. sprawa Moulin przeciwko Francji 23/11/2010

powierzchownej kontroli przed przekazaniem danych, jeżeli nie z brakiem jakiejkolwiek kontroli po stronie dostawcy usług. W ocenie skutków podkreśla się konieczność uzyskiwania przez właściwe organy dostępu do danych w odpowiednim czasie. Wszystkie jednak przytoczone w ocenie skutków przykłady dotyczą dowodów niezbędnych w przypadkach poważnych przestępstw (takich jak ataki terrorystyczne z wzięciem zakładników, trwające wykorzystywanie seksualne dzieci). Uzasadnienie oparte na ulotności dowodów nie wydaje się natomiast być dobrym rozwiązaniem, jeżeli nie mamy do czynienia ze szczególną, pilną koniecznością pozyskania danych, która opiera się na innych podstawach niż ich ulotność. Ponadto ulotność danych nie dostarcza dodatkowej argumentacji, jeżeli chodzi o kryterium proporcjonalności dostępu do danych obwarowanego słabszymi zabezpieczeniami. Dotyczy to sytuacji, w których pozyskanie danych nie jest pilne, a ich zażądanie nie opiera się na innej podstawie niż ich ulotność.

Ponadto EROD wyraża wątpliwość co do konieczności wprowadzenia sześciogodzinnego terminu, przy jednoczesnym założeniu, że nie będzie miał on zastosowania, dopóki organ wydający nie przedstawi dodatkowych wyjaśnień „w terminie pięciu dni" w sytuacji, gdy dostawca usług nie jest w stanie wywiązać się z tego obowiązku.

W związku z tym EROD wzywa do zawarcia w ocenie skutków dodatkowych elementów, które uzasadniałyby niezbędność stosowania tych terminów w przypadkach, gdy popełnione lub ścigane przestępstwo nie jest przestępstwem poważnym oraz- o ile takie szczegółowe elementy nie zostaną przedstawione - do ustanowienia jasnych kryteriów służących uzasadnianiu nadzwyczajnego charakteru sytuacji wtedy, gdy wydawane są zaświadczenia europejskiego nakazu wydania dowodów. Można by przykładowo przedstawić taki sam model, jak zastosowano w dyrektywie END. W dyrektywie END przewidziano krótszy termin, o ile jest to uzasadnione „terminami proceduralnymi, ciężarem przestępstwa lub innymi szczególnie pilnymi okolicznościami (zob. art. 12 ust. 2) lub termin 24-godzinny do podjęcia decyzji co do zastosowania środka tymczasowego (zob. art. 32 ust. 2). Ocena skutków projektu rozporządzenia nie zawiera szczegółowych elementów uzasadniających, dlaczego te terminy nie są efektywne. Jedyne na co wskazano, to znaczna liczba przesyłanych wniosków, których organy sądowe przyjmujące nie są w stanie rozpatrywać w przepisanych terminach.

c) Europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów można stosować do żądania danych osoby, której te dane dotyczą, z innego państwa członkowskiego jedynie po poinformowaniu właściwych organów tego państwa członkowskiego, w szczególności w odniesieniu do danych dotyczących treści

EROD przypomina, że w ramach obowiązujących instrumentów zapewnia się współpracę sądową i tym samym dodatkowe gwarancje, w szczególności te służące kontroli niezbędności i proporcjonalności wniosków. Należy podkreślić, że stosowanie tych zabezpieczeń jest bardziej uzasadnione wówczas, gdy występuje się o udostępnienie danych dotyczących treści, co wiąże się z większą liczbą ograniczeń praw osób, których dane dotyczą, do ochrony ich danych osobowych i prywatności. W tym względzie EROD przypomina, że w dyrektywie END przewidziano również możliwość przechwytywania przekazów telekomunikacyjnych z pomocą techniczną innego państwa członkowskiego (zob. art. 30), a także obowiązek powiadamiania właściwego organu innego państwa członkowskiego o każdym przechwytywaniu danych, w przypadkach gdy pomoc techniczna nie jest potrzebna do dokonania przechwycenia, a osoba, której dane dotyczą, przebywa lub będzie przebywała na terytorium tego państwa członkowskiego (zob. art. 31).

EROD nie widzi uzasadnienia dla ustanowienia procedury przewidzianej w projekcie rozporządzenia w sprawie dowodów elektronicznych, zakładającej udostępnianie danych dotyczących treści bez

udziału przynajmniej właściwych organów państwa członkowskiego, w którym osoba, której dane dotyczą, przebywa.

d) Europejskie nakazy zabezpieczenia nie mogą być wykorzystywane do obchodzenia obowiązków dostawców usług w zakresie zatrzymywania danych

EROD zauważa, że głównym celem europejskiego nakazu zabezpieczenia jest uniemożliwienie usuwania danych.

Mimo że EROD uznaje, że w niektórych przypadkach wydanie nakazu może być konieczne i proporcjonalne, to wyraża dezaprobatę z powodu braku towarzyszących temu związanych z wydawaniem takich nakazów. W szczególności EROD zaleca, by zagwarantować, że nakaz nigdy nie będzie służył dostawcy danych za podstawę do przetwarzania danych po pierwotnym terminie usunięcia w przypadkach, gdy nakazy zabezpieczenia ograniczają się do danych szczególnych, podczas gdy projekt umożliwia stosowanie nakazów w szerokim zakresie oraz gdy nakazy wydawane są w odniesieniu do danych przeznaczonych do usunięcia zgodnie z zasadą zatrzymywania danych. Innymi słowy, dane powinny być „zamrażane".

Ponadto powiązanie między nakazem zabezpieczenia a późniejszym wnioskiem o wydanie danych, czy to poprzez europejski nakaz wydania, END lub wniosek o wzajemną pomoc prawną, powinno zostać wzmocnione, aby zapewnić wydawanie europejskich nakazów zabezpieczenia tylko wtedy, gdy późniejszy wniosek jest pewny (nie zaś tylko rozważany). Należałoby również zapewnić, aby w przypadku oddalenia tego późniejszego wniosku, upadał również europejski nakaz zabezpieczenia, bez konieczności oczekiwania przez okres 60 dni,[28] jeżeli wniosek oddalono uprzednio.

e) Poufność i informowanie użytkowników

EROD zauważa, że w projekcie rozporządzenia został wprowadzony szczególny artykuł[29] dotyczący poufności przesyłanych nakazów. Aby uniknąć wszelkich niejasności i nieporozumień dotyczących prawa do ochrony danych, EROD przypomina, że choć RODO stanowi, iż ograniczenia praw osób, których dane dotyczą, służące zabezpieczeniu zapobiegania, wykrywania lub ścigania przestępstw, powinny być przewidziane w przepisach prawa, a zatem powinny być publicznie dostępne[30]. Przepisy te powinny wyraźnie wskazywać, że osoby, których dane dotyczą, mają prawo do bycia informowanym o tych ograniczeniach, chyba że może to naruszać cel danego ograniczenia[31]. RODO nie przewiduje jednak obowiązku informowania indywidualnie osób, których dane dotyczą, o każdym wniosku organu ścigania o dostęp do danych.

Tymczasem EROD przypomina jednak, że dyrektywa o ochronie danych nadaje prawo osobie, której dane dotyczą, do bycia informowanym przez same właściwe organy wszystkim osobom, których dane dotyczą, bez ograniczania go tylko do osób mających miejsce zamieszkania na terytorium UE, chyba że prawo to zostało ograniczone.

f) Procedura przymusowego wykonania nakazu w przypadku, gdy dostawca usług odmówił jego wykonania

[28] Zob. art. 10 ust. 1
[29] Zob. art. 11
[30] Zob. art. 23 ust. 1 lit. d)
[31] Zob. art. 23 ust. 2. lit. h)

EROD zauważa, że w art. 14 projektu rozporządzenia przewidziano procedurę mającą na celu zapewnienie przymusowego wykonania nakazu, jeżeli adresat nie zastosował się do niego. Procedura ta opiera się na współpracy sądowej pomiędzy organem wydającym a właściwym organem w państwie wykonującym nakaz.

Wydaje się jednak, że procedura ta nie pozwala organom przymuszającym na odmowę przymusowego wykonania przekazanego nakazu z przyczyn innych niż czysto proceduralne (takie jak przysługujące adresatowi, związane głównie z brakiem wystarczających informacji lub faktyczną niemożnością wydania danych), ponieważ dane te są chronione immunitetem lub przywilejem na podstawie przepisów jego prawa krajowego lub ich ujawnienie może mieć wpływ na podstawowe interesy tego państwa takie jak bezpieczeństwo narodowe i obrona[32].

W związku z tym EROD ponownie wyraża swoje obawy co do niezastosowania, w porównaniu z innymi instrumentami, jakiejkolwiek podwójnej weryfikacji przekazywanego nakazu przez właściwy organ otrzymujący. Nawet odmowa przymusowego wykonania nakazu ze względu na to, że naruszyłoby ono postanowienia Karty wydaje się być mocniejsza aniżeli klasyczne progi związane z naruszeniem praw podstawowych danej osoby. W związku z powyższym, na wzór europejskiego nakazu aresztowania, który przewiduje zarówno obligatoryjne, jak i fakultatywne podstawy odmowy, lub przynajmniej za przykładem dyrektywy END, która ogólnie stanowi, że można obalić domniemanie, zgodnie z którym utworzenie przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii opiera się na wzajemnym zaufaniu i domniemaniu przestrzegania przez inne państwa członkowskie prawa Unii, a zwłaszcza praw podstawowych,[33] w projekcie rozporządzenia należy przynajmniej przewidzieć minimalną klasyczną klauzulę derogacyjną, zgodnie z którą, jeżeli zachodzą istotne podstawy do uznania, że przymusowe wykonanie nakazu spowodowałoby naruszenie prawa podstawowego danej osoby, a państwo wykonujące wykazałoby się brakiem poszanowania dla swoich obowiązków związanych z ochroną praw podstawowych zagwarantowanych w Karcie, należy odmówić przymusowego wykonania nakazu.

g) Przymusowe wykonywanie a konflikt obowiązków wynikający z przepisów prawa państwa trzeciego (art. 15–16)

EROD z zadowoleniem przyjmuje przewidzianą w projekcie rozporządzenia możliwość odmowy wykonania nakazu na podstawie tego, że byłoby to sprzeczne z prawami podstawowymi, ponieważ ma ono na celu zapewnienie zabezpieczeń w razie zaistnienia konfliktu obowiązków prawnych. EROD uznaje również za szczególnie ważne, że wniosek przewiduje konsultacje z władzami krajów trzecich, przynajmniej w razie wystąpienia konfliktu, jak również obowiązek uchylenia nakazu, jeżeli organ państwa trzeciego zgłosił sprzeciw.

Należy zatem znacznie ulepszyć procedurę odmowy wykonania nakazu ze względu na konflikt obowiązków wynikający z przepisów prawa państwa trzeciego.

Po pierwsze, EROD zauważa, że w projekcie rozporządzenia powierza się prywatnemu przedsiębiorstwu, jako adresatowi nakazu wydania danych, przeprowadzenie oceny, czy nakaz ten byłby sprzeczny z odnośnymi przepisami prawa państwa trzeciego zakazującymi ujawnienia żądanych danych. Przedsiębiorstwo musi zgłosić uzasadniony sprzeciw, który powinien zawierać wszelkie właściwe informacje na temat przepisów prawa państwa trzeciego, ich stosowalności do danej sprawy oraz charakteru sprzecznych obowiązków.

[32] Zob. art. 14 ust. 2
[33] Zob. motyw 19 dyrektywy END

Co najważniejsze, EROD wyraża zaniepokojenie, że w razie zgłoszenia takiego sprzeciwu właściwy sąd państwa członkowskiego, w którym znajduje się organ wydający, samodzielnie dokona oceny, czy konflikt zachodzi, ponieważ zawiadomi on władze państwa trzeciego dopiero po stwierdzeniu, że konflikt występuje. Dlatego też uprawnienie do ostatecznej wykładni prawa państwa trzeciego w tym względzie należy do właściwego sądu unijnego, który nie do końca jest do rozstrzygania w tej materii powołany. EROD uważa, że obowiązek przeprowadzenia konsultacji z właściwymi organami państwa trzeciego jest zatem w analizowanym wniosku zbyt ograniczony. Jeżeli chodzi o dziedzinę ochrony danych, EROD pragnie zwrócić uwagę prawodawcy na fakt, że w razie dokonania przez właściwy sąd państwa trzeciego wykładni RODO w celu ustalenia, czy jest ono sprzeczne z wymogami tego państwa, unijne organy ochrony danych i właściwe sądy nadal byłyby właściwe w zakresie oceny zgodności z prawem przekazania danych na podstawie orzeczenia sądu lub trybunału lub na podstawie decyzji organu administracyjnego państwa trzeciego nakazującego przekazanie lub ujawnienie danych osobowych w ramach RODO[34].

Ponadto EROD podkreśla, że ocena prawa państwa trzeciego dokonana przez właściwy sąd wnioskującego państwa członkowskiego UE powinna opierać się na przesłankach obiektywnych oraz wiąże się z zastosowaniem kryteriów, które właściwy sąd bierze pod uwagę przy ocenie prawa państwa trzeciego na podstawie art. 15 ust. 4 i art. 16 ust. 5 lit. a) projektu rozporządzenia. Trybunał musiałby ocenić okoliczność, że zamiast mieć na celu ochronę praw podstawowych lub podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym lub obroną, przepisy prawa państwa trzeciego w oczywisty sposób mają na celu ochronę nielegalnych działań przed wnioskami organów ścigania dotyczącymi postępowania przygotowawczego lub interesów chronionych przez właściwe przepisy prawa państwa trzeciego, w tym interesu państwa trzeciego związanego z zapobieżeniem ujawnieniu odnośnych danych. Przykładowo, choć ta ocena w zasadzie powinna wymagać oparcia w dowodach w świetle wszelkich dostępnych informacji, biorąc pod uwagę potencjalny wpływ takiej decyzji, co najmniej sformułowanie w języku angielskim („is being aimed to") wydaje się niejasne i powinno zostać dostosowane („has the aim/objective to").

EROD wyraża ubolewanie, że organy państwa trzeciego byłyby konsultowane i mogłyby wnieść sprzeciw wobec wykonania nakazu wydania wyłącznie wówczas, gdyby ten właściwy sąd unijny uznał, że zachodzi konflikt. Wówczas przekazałby on wszelkie informacje do organów centralnych w zainteresowanym państwie trzecim, a organ centralny tego państwa trzeciego zgłosiłby sprzeciw w maksymalnym ścisłym terminie 50 dni (15 dni, z możliwością przedłużenia o 30 dni, a po upływie ostatniego możliwego ponaglenia – 5 dodatkowych dni). We wszystkich pozostałych przypadkach właściwy sąd mógłby utrzymać w mocy nakaz wydania i nałożyć sankcję pieniężną w przypadku odmowy wykonania nakazu przez dostawcę usług. EROD wyraża w związku z tym obawę, że właściwe sądy unijne nie będą miały szeroko ujętego obowiązku konsultowania się z właściwymi organami zainteresowanych państw trzecich w celu zapewnienia w większym zakresie systematycznego uwzględniania argumentów obu stron oraz uwzględniania i wykazywania jeszcze większego poszanowania dla przepisów prawa państw trzecich.

Zgodnie z powyższym oraz tym, co podkreślono w oświadczeniu Grupy Roboczej Art. 29, EROD przypomina, że szczególną uwagę należy zwrócić na przyjmowanie przez państwa trzecie podobnych instrumentów, które potencjalnie mogą oddziaływać na prawa osób, których dane dotyczą, oraz ich prawo do prywatności w UE, a w szczególności na ryzyko związane z przyjmowaniem instrumentów bezpośrednio kolidujących z unijnym prawem o ochronie danych.

[34] Zob. art. 48 RODO

Ponadto EROD podkreśla, że właściwy sąd państwa członkowskiego organu wydającego może nie być nawet właściwym sądem w zakresie wykonania nakazu na podstawie art. 14 projektu rozporządzenia, co może spowodować wzrost ryzyka wystąpienia kolizji procedur przy braku wzajemnej kontroli sprzecznych ze sobą regulacji prawnych. Wynika to z faktu, że w niektórych przypadkach zaangażowane mogłyby być trzy państwa: państwo organu wydającego nakaz, państwo trzecie dostawcy usług oraz państwo członkowskie, w którym znajduje się przedstawiciel prawny dostawcy usług w UE i w którym nakaz musiałby zostać wykonany. Zgodnie zatem z obecnie przewidzianą procedurą, sąd organu wnioskującego w państwie członkowskim A mógłby dokonać własnej wykładni prawa państwa trzeciego B dostawcy usług, nie zwracając się do organów tego państwa trzeciego o zajęcie stanowiska (które zgłosiłyby sprzeciw wobec tego nakazu) oraz wystąpiłby do sądu innego państwa członkowskiego UE C o wykonanie jego rozstrzygnięcia zupełnie bez możliwości zgłoszenia sprzeciwu.

Ponadto EROD z zadowoleniem przyjmuje wprowadzenie szczególnych środków ochrony prawnej dotyczących nakazów wydania, obok środków przewidzianych w RODO i w dyrektywie 2016/680. Grupa Robocza Art. 29 wezwała do wprowadzenia takich zabezpieczeń w swoim poprzednim oświadczeniu. EROD wyraża jednak ubolewanie z powodu tego, że takie środki ochrony prawnej nie są przewidziane również co do nakazów zabezpieczenia, ponieważ nakazy te mogą również pociągać za sobą ograniczenia praw podstawowych osób fizycznych, których dane zostały zatrzymane. Nakazy zabezpieczenia mogą wywoływać skutek zatrzymania danych przez czas dłuższy aniżeli wystąpiłoby to zgodnie z regulacjami o ochronie danych. W związku z tym nakaz zabezpieczenia danych ze swej istoty powoduje ograniczenie praw podstawowych osoby, której dane dotyczą. Uzasadnienie dla jego wydania podlega kontroli i zastosowaniu szczególnych środków ochrony prawnej, zwłaszcza wówczas, gdy nakaz zabezpieczenia zostanie wydany wraz z nakazem wydania w celu pozyskania danych. Jak zaleciła Grupa Robocza Art. 29 w swoim oświadczeniu, należy przewidzieć środki prawne, co najmniej równoważne środkom dostępnym w sprawie krajowej.

h) Bezpieczne przekazywanie danych w ramach wykonania nakazu

EROD zauważa, że projekt rozporządzenia przewiduje jedynie wydawanie nakazów kierowanych do adresatów w Unii Europejskiej i w związku z tym nie przewiduje szczególnego kanału przekazywania danych pomiędzy adresatami a dostawcami usług zlokalizowanymi poza Unią Europejską.

Choć EROD z zadowoleniem przyjmuje brak dalszych odstępstw od ogólnych ram UE w zakresie ochrony danych, przypomina, że każdy nakaz przesłany do adresata, z którym wiązałoby się przekazanie danych poza UE, musiałby być zgodny z ramami prawnymi ustanowionymi w RODO. Poruszanie się poza ramami prawnymi współpracy sądowej, w których przewidziano obowiązkowe zabezpieczenia ochrony danych, nie powinno jednak prowadzić do obchodzenia przez adresatów nakazów wydania lub nakazów zabezpieczenia wymogów dotyczących przekazywania danych w celu wykonania takich nakazów.

Ponadto, o ile EROD z zadowoleniem przyjmuje brak regulacji zobowiązującej do odszyfrowywania zaszyfrowanych danych[35], to wyraża obawy, że omawiane wnioski nie przewidują szczególnego wymogu dokonywania przez adresatów oceny autentyczności wydawanych danych. EROD podkreśla też, że taka ocena stanowi również wartość dodaną względem tradycyjnych instrumentów opartych na współpracy sądowej i pragnie ostrzec przed zwiększonym ryzykiem dla osób, których dane dotyczą, wynikającym z braku takiej oceny.

[35] Zob. motyw 19 i s. 240 oceny skutków

Podsumowanie

Na podstawie niniejszej analizy EROD pragnie skierować do współprawodawców następujące zalecenia:

1) Podstawą prawną rozporządzenia nie powinien być art. 82 ust. 1 TFUE.
2) Należałoby w większym stopniu uzasadnić niezbędność ustanowienia nowego instrumentu w kontekście obowiązującej dyrektywy END lub traktatów o pomocy prawnej, w tym poprzez dokonanie szczegółowej analizy mniej ingerujących w prawa podstawowe środków, takich jak wprowadzenie zmian w obowiązujących instrumentach lub ograniczenie zakresu tego instrumentu do nakazów zabezpieczenia w połączeniu z innymi dostępnymi obecnie procedurami służącymi występowaniu o dostęp do danych.
3) Rozporządzenie powinno przewidywać dłuższe terminy, aby umożliwić dostawcy usług wykonującemu nakaz przestrzeganie zabezpieczeń służących ochronie praw podstawowych.
4) Należałoby utrzymać zasadę podwójnej karalności, zwłaszcza w związku z rezygnacją ze stosowania kryteriów terytorialnych dotyczących danych w celu utrzymania obowiązku respektowania zabezpieczeń przewidzianych w obu zainteresowanych państwach (tj. w państwie organu wnioskującego i w państwie, w którym dostawca usług się znajduje).
5) Zakres podmiotowy rozporządzenia powinien być ograniczony do administratorów danych w rozumieniu RODO lub należałoby wprowadzić regulację, zgodnie z którą w sytuacji, gdy dostawca usług, do którego się zwrócono, nie jest administratorem danych, lecz podmiotem przetwarzającym, ten ostatni ma obowiązek poinformować administratora danych o wniosku.
6) Rozporządzenie powinno zawierać zabezpieczenia dotyczące przekazywania danych w przypadku, gdyby dostawca usług miał siedzibę w państwie trzecim, dla którego nie wydano decyzji stwierdzającej odpowiedni stopień ochrony w tej dziedzinie, lub odesłanie do dyrektywy 2016/680, ponieważ zabezpieczenia te będą miały zastosowanie.
7) Ponieważ obligatoryjne wyznaczenie przedstawiciela prawnego wykazuje różnice względem rozwiązania przyjętego w RODO, w rozporządzeniu należy sprecyzować, że przedstawiciel prawny wyznaczony na podstawie rozporządzenia w sprawie dowodów elektronicznych nie powinien być utożsamiany z przedstawicielem prawnym wyznaczonym na podstawie art. 3 ust. 2 RODO.
8) Rozporządzenie powinno zawierać szerszą definicję danych pochodzących z komunikacji elektronicznej, aby zapewnić ustanowienie odpowiednich zabezpieczeń i warunków dostępu obejmujących zarówno dane niedotyczące treści, jak i dane dotyczące treści.
9) Rozporządzenie powinno podnieść progi dotyczące wydawania nakazów, które powinny być wydawane lub zatwierdzane przez sądy, z wyjątkiem nakazów dotyczących danych abonenta, pod warunkiem że definicja tej kategorii danych zostanie zasadniczo zawężona do informacji bardzo podstawowych, umożliwiających jedynie identyfikację osoby bez dostępu do jakichkolwiek danych dotyczących łączności.
10) Rozporządzenie powinno ograniczyć dostęp do danych abonenta i danych dostępu dla wniosków dotyczących przestępstw ściśle określonych w odpowiednim wykazie lub co najmniej dotyczących „poważnych przestępstw".
11) W rozporządzeniu należy lepiej uzasadnić termin do wydania danych, zwłaszcza w przypadku sytuacji nadzwyczajnych. Natomiast możliwość stosowania szybkiej sześciogodzinnej procedury powinna wiązać się z obowiązkiem wykazania przez organy wnioskujące, nawet po fakcie, nadzwyczajnego charakteru danej sytuacji powodującego uruchomienie tej procedury w celu umożliwienia kontroli skorzystania z takich wyjątkowych uprawnień.

12) Należy zrezygnować z procedury umożliwiającej wydawanie danych dotyczących treści bez udziału właściwych organów państwa członkowskiego, w którym osoba, której dane dotyczą, się znajduje.
13) W rozporządzeniu należy zawrzeć lepsze zabezpieczenia związane z wydawaniem europejskich nakazów zabezpieczenia.
14) W rozporządzeniu powinna znaleźć się co najmniej minimalna klasyczna klauzula derogacyjna, zgodnie z którą w przypadku, gdy zachodzą istotne podstawy do uznania, że wykonanie nakazu spowodowałoby naruszenie prawa podstawowego danej osoby, wskutek którego państwo wykonujące wykazałoby się brakiem poszanowania dla swoich obowiązków związanych z ochroną praw podstawowych zagwarantowanych w Karcie, należy odmówić przymusowego wykonania nakazu.
15) W rozporządzeniu należy przewidzieć szerszy obowiązek konsultowania się z właściwymi organami państwa trzeciego w przypadku, gdy dostawca usług, do którego zwrócono się o przekazanie danych, znajduje się w sytuacji konfliktu przepisów prawa. Dzięki temu uniknąć można subiektywnej wykładni pochodzącej od pojedynczego sądu.
16) Ważność i termin obowiązywania nakazów zabezpieczenia powinny być w większym stopniu powiązane z towarzyszącymi im nakazami wydania.
17) Należy zapewnić większe bezpieczeństwo przekazywania danych.
18) Należy wprowadzić weryfikację autentyczności danych, w szczególności tam, gdzie mogłyby być dostarczane dane zaszyfrowane.

W imieniu Europejskiej Rady Ochrony Danych

Przewodniczący

(Andrea Jelinek)