



Kontakty z Mediami
i Informacja

Trybunał Sprawiedliwości Unii Europejskiej
KOMUNIKAT PRASOWY nr 58/22
Luksemburg, 5 kwietnia 2022 r.

Wyrok w sprawie C-140/20
Commissioner of the Garda Síochána i in.

Trybunał potwierdził, że prawo Unii stoi na przeszkodzie uogólnionemu i nieodróżnicowanemu zatrzymywaniu danych o ruchu i danych o lokalizacji dotyczących łączności elektronicznej do celów walki z poważnymi przestępstwami

Sąd krajowy nie może ograniczyć w czasie skutków stwierdzenia nieważności uregulowania krajowego przewidującego takie zatrzymywanie danych

W marcu 2015 r. G.D. został skazany na karę dożywotniego pozbawienia wolności za zabójstwo kobiety w Irlandii. W apelacji od wyroku skazującego wniesionej do sądu apelacyjnego w Irlandii zainteresowany zarzucił między innymi sądowi pierwszej instancji, że błędnie dopuścił jako dowody dane o ruchu i dane o lokalizacji dotyczące rozmów telefonicznych. W celu zakwestionowania w ramach postępowania karnego dopuszczalności owych dowodów, G.D. wszczął równolegle przed wysokim trybunałem Irlandii postępowanie cywilne mające na celu stwierdzenie nieważności niektórych przepisów ustawy irlandzkiej z 2011 r. regulującej zatrzymywanie tych danych i dostęp do nich, uzasadniając to tym, że ustawa ta narusza prawa, jakie przyznaje mu prawo Unii. Orzeczeniem z dnia 6 grudnia 2018 r. wysoki trybunał uwzględnił argumentację G.D. Irlandia wniosła apelację od tego orzeczenia do sądu najwyższego Irlandii, będącego sądem odsyłającym w omawianej sprawie.

W swoim odesłaniu prejudycjalnym sąd najwyższy zwrócił się o wyjaśnienia w przedmiocie wymogów prawa Unii w dziedzinie zatrzymywania wspomnianych danych do celów walki z poważnymi przestępstwami, jak również w przedmiocie gwarancji koniecznych w dziedzinie dostępu do tychże danych. Sąd ten zastanawia się również nad zakresem i skutkiem czasowym ewentualnego stwierdzenia niezgodności z prawem Unii, którego ma on dokonać, ponieważ ustawa irlandzka z 2011 r. została wydana w celu transponowania dyrektywy 2006/24/WE¹, której nieważność Trybunał stwierdził w wyroku z dnia 2014 r. w sprawie *Digital Rights Ireland i in.*²

W swoim wyroku Trybunał, w składzie wielkiej izby, w pierwszej kolejności potwierdził swoje utrwalone orzecznictwo³, zgodnie z którym prawo Unii⁴ **stoi na przeszkodzie krajowym środkom ustawodawczym przewidującym, do celów walki z poważnymi naruszeniami, prewencyjne uogólnione i nieodróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji dotyczących łączności elektronicznej.**

¹ Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. 2006 L 105, s. 54).

² Wyrok z dnia 8 kwietnia 2014 r., *Digital Rights Ireland*, [C-293/12](#) (zob. komunikat prasowy nr [54/14](#)).

³ Wyroki z dnia 8 kwietnia 2014 r., *Digital Rights Ireland*, [C-293/12](#); z dnia 21 grudnia 2016 r., *Tele2 Sverige i Watson i in.*, [C-203/15 i C-698/15](#) (zob. komunikat prasowy nr [145/16](#)); z dnia 6 października 2020 r., *Privacy International*, [C-623/17](#), i *La Quadrature du Net i in.*, [C-511/18](#), [C-512/18 i C-520/18](#) (zob. komunikat prasowy nr [123/20](#)); a także z dnia 2 marca 2021 r., *Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej)*, [C-746/18](#) (zob. komunikat prasowy nr [29/21](#)).

⁴ Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37), zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11) („dyrektywa o prywatności i łączności elektronicznej”), interpretowana w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej („karta”).

Dyrektywa o prywatności i łączności elektronicznej nie ogranicza się bowiem do określenia ram dostępu do takich danych za pomocą gwarancji mających na celu zapobieganie nadużyciom, ale także ustanawia w szczególności **zasadę zakazu przechowywania** danych o ruchu i danych o lokalizacji. Zatrzymywanie tych danych stanowi zatem z jednej strony odstępstwo od tego zakazu przechowywania, a z drugiej strony ingerencję w prawa podstawowe do poszanowania życia prywatnego i do ochrony danych osobowych, ustanowione w art. 7 i 8 karty.

Choć dyrektywa o prywatności i łączności elektronicznej pozwala państwom członkowskim na ograniczenie tych praw i obowiązków w szczególności do celów walki z przestępstwami, takie ograniczenia muszą jednak być zgodne między innymi z zasadą proporcjonalności. Zasada ta wymaga spełnienia nie tylko wymogów zdatności i konieczności, ale także wymogu odnoszącego się do **proporcjonalnego charakteru** tych środków w stosunku do zamierzonego celu. I tak Trybunał orzekł już, że cel w postaci walki z poważną przestępczością, pomimo że ma on fundamentalne znaczenie, nie może sam w sobie uzasadniać stwierdzenia, że środek polegający na uogólnionym i nieodróżnicowanym zatrzymywaniu danych o ruchu i danych o lokalizacji, taki jak ten ustanowiony w dyrektywie 2006/24, jest konieczny. W tym samym duchu nawet pozytywne obowiązki państw członkowskich dotyczące ustanowienia przepisów umożliwiających skuteczne zwalczanie przestępstw nie mogą uzasadniać tak poważnych ingerencji w prawa podstawowe prawie całej ludności, jak te wynikające z uregulowania krajowego przewidującego takie zatrzymywanie danych, gdy dane zainteresowanych osób nie wykazują związku, choćby pośredniego, z zamierzonym celem.

Trybunał przypomniał również, że różne pozytywne obowiązki ciążyą na organach publicznych na podstawie karty, polegające na przykład na przyjęciu środków prawnych mających na celu ochronę życia prywatnego i rodzinnego, ochronę domu i komunikowania się, ale także ochronę integralności fizycznej i psychicznej osób, jak również zakaz tortur i niehumanitarnego lub poniżającego traktowania. Ich zadaniem jest zatem **pogodzenie różnych wchodzących w rachubę uzasadnionych interesów i praw**. Nie można bowiem dążyć do celu interesu ogólnego bez uwzględnienia okoliczności, że należy pogodzić go z prawami podstawowymi, których dotyczy środek, dokonując **zbilansowanego wyważenia** między celem interesu ogólnego z jednej strony a rozpatrywanymi prawami z drugiej strony, przy czym należy sprawdzić, czy znaczenie owego celu pozostaje w relacji do wagi ingerencji, jaką stanowi ten środek.

Rozważania te skłoniły Trybunał do oddalenia między innymi argumentacji, zgodnie z którą szczególnie poważna przestępczość może być utożsamiana z zagrożeniem dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub przewidywalne oraz może, przez określony czas, uzasadniać środek polegający na uogólnionym i nieodróżnicowanym zatrzymywaniu danych o ruchu i danych o lokalizacji. Takie zagrożenie różni się bowiem – ze względu na swój charakter, wagę i szczególny charakter składających się na nie okoliczności – od ogólnego i stałego ryzyka, jakim jest ryzyko wystąpienia napięć lub zakłóceń, nawet poważnych, dla bezpieczeństwa publicznego lub ryzyko poważnych przestępstw.

Natomiast w drugiej kolejności Trybunał orzekł, potwierdzając swoje wcześniejsze orzecznictwo, że prawo Unii nie stoi na przeszkodzie przepisom ustawodawczym przewidującym, na warunkach określonych w jego wyroku, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego:

- **ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji** w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego;
- **uogólnione i nieodróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia**;
- **uogólnione i nieodróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej**, oraz
- szybkie **zatrzymywanie** (quick freeze) danych o ruchu i danych o lokalizacji, którymi dysponują dostawcy usług łączności elektronicznej.

Trybunał dokonał różnych uściśleń w odniesieniu do tych różnych kategorii środków.

Przede wszystkim właściwe organy krajowe mogą przyjąć środek polegający na ukierunkowanym zatrzymywaniu danych oparty na kryterium geograficznym, takim jak między innymi średni wskaźnik przestępczości w danej strefie geograficznej, przy czym nie muszą one koniecznie dysponować konkretnymi wskazówkami dotyczącymi przygotowywania lub popełniania w danych strefach poważnych przestępstw. Trybunał dodał, że taki środek polegający na zatrzymywaniu danych odnoszący się do miejsc lub infrastruktury, w których regularnie przebywa bardzo wiele osób, lub też do miejsc strategicznych, takich jak porty lotnicze, dworce, porty morskie lub strefy poboru opłat za przejazd, pozwala właściwym organom na uzyskanie informacji na temat obecności, w tych miejscach lub strefach geograficznych, osób korzystających tam ze środka łączności elektronicznej oraz na wyciągnięcie, do celów zwalczania poważnej przestępczości, wniosków co do obecności i działalności owych osób w tychże miejscach lub strefach geograficznych.

Następnie Trybunał wskazał, że ani dyrektywa o prywatności i łączności elektronicznej, ani żaden inny akt prawa Unii nie stoją na przeszkodzie uregulowaniu krajowemu, mającemu na celu zwalczanie poważnej przestępczości, na podstawie którego nabycie środka łączności elektronicznej, takiego jak opłaconej z góry karty SIM, jest uzależnione od sprawdzenia urzędowych dokumentów ustalających tożsamość nabywcy i od zarejestrowania przez sprzedawcę wynikających z nich informacji, gdyż sprzedawca jest w stosownym przypadku zobowiązany do udzielenia dostępu do tych informacji właściwym organom krajowym.

Wreszcie Trybunał zauważył, że dyrektywa o prywatności i łączności elektronicznej nie stoi na przeszkodzie temu, by właściwe organy krajowe zarządziły środek polegający na szybkim zatrzymywaniu danych już na pierwszym etapie dochodzenia dotyczącego poważnego zagrożenia dla bezpieczeństwa publicznego lub ewentualnego poważnego przestępstwa, czyli w chwili, w której zgodnie z właściwymi przepisami prawa krajowego organy te mogą wszcząć takie dochodzenie. Taki środek może zostać rozszerzony na dane o ruchu i dane o lokalizacji dotyczące osób innych niż te, które są podejrzewane o planowanie lub popełnienie poważnego przestępstwa lub naruszenie bezpieczeństwa narodowego, o ile dane te mogą, w oparciu o obiektywne i niedyskryminacyjne kryteria, przyczynić się do wyjaśnienia takiego przestępstwa lub takiego naruszenia bezpieczeństwa narodowego, takie jak dane ofiary tego przestępstwa lub naruszenia, jak również dane jej otoczenia społecznego lub zawodowego.

Te różne środki mogą – zgodnie z wyborem ustawodawcy krajowego i przy poszanowaniu granic tego, co ściśle niezbędne – znaleźć wspólnie zastosowanie.

Trybunał oddalił również argumentację, jakoby zgodnie z jego orzecnictwem właściwe organy krajowe powinny móc mieć dostęp, dla celów walki z poważną przestępczością, do danych o ruchu i danych o lokalizacji, które zostały zatrzymane w sposób uogólniony i nieodróżnicowany, aby stawić czoła poważnemu zagrożeniu dla bezpieczeństwa narodowego, które jest rzeczywiste i aktualne lub przewidywalne. Argumentacja ta spowodowałaby bowiem uzależnienie tego dostępu od okoliczności niezwiązanych z celem w postaci zwalczania poważnej przestępczości. Ponadto zgodnie ze wspomnianą argumentacją dostęp do danych mógłby być uzasadniony celem mającym mniejsze znaczenie niż cel, który uzasadniał zatrzymywanie danych, czyli ochrona bezpieczeństwa narodowego, co pozostawałoby w sprzeczności z hierarchią celów interesu ogólnego, w ramach której należy ocenić proporcjonalność środka polegającego na zatrzymywaniu danych. Ponadto zezwolenie na taki dostęp groziłoby pozbawieniem wszelkiej skuteczności (effet utile) zakazu uogólnionego i nieodróżnicowanego zatrzymywania danych do celów zwalczania poważnej przestępczości.

W trzeciej kolejności Trybunał potwierdził, że prawo Unii stoi na przeszkodzie uregulowaniu krajowemu, na podstawie którego scentralizowane rozpatrywanie pochodzących od policji wniosków o udzielenie dostępu do danych zatrzymanych przez dostawców usług łączności elektronicznej, w ramach wykrywania i ścigania poważnych przestępstw, należy do funkcjonariusza policji, nawet jeśli jest on wspierany przez jednostkę ustanowioną w obrębie policji, której przysługuje określony stopień autonomii w wykonywaniu powierzonego jej zadania i której

decyzje mogą być następnie przedmiotem kontroli sądowej. Trybunał potwierdził bowiem w tym względzie swoje orzecznictwo, zgodnie z którym w celu zapewnienia w praktyce pełnej zgodności ze ścisłymi warunkami dostępu do danych osobowych takich jak dane o ruchu i dane o lokalizacji, dostęp właściwych organów krajowych do zatrzymanych danych musi być uzależniony od uprzedniej kontroli sprawowanej przez sąd lub przez niezależny organ administracyjny, zaś decyzja tego sądu lub organu powinna być wydawana na uzasadniony wniosek owych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie przestępstwom, ich wykrywanie lub ściganie karne. Otóż funkcjonariusz policji nie stanowi sądu i nie zapewnia wszystkich gwarancji niezależności i bezstronności wymaganych po to, by mógł on zostać uznany za niezależny organ administracyjny.

Wreszcie, w czwartej kolejności, Trybunał potwierdził swoje orzecznictwo, zgodnie z którym prawo Unii stoi na przeszkodzie ograniczeniu przez sąd krajowy w czasie skutków stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, a to ze względu na niezgodność tego uregulowania z dyrektywą 2002/58/WE.

Niezależnie od powyższego Trybunał przypomniał, że kwestia dopuszczalności dowodów uzyskanych za pomocą takiego zatrzymywania danych należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równowagi i skuteczności.

UWAGA: Odesłanie prejudycjalne pozwala sądom państw członkowskich, w ramach rozpatrywanego przez nie sporu, zwrócić się do Trybunału z pytaniem o wykładnię prawa Unii lub o ocenę ważności aktu Unii. Trybunał nie rozpoznaje sporu krajowego. Do sądu krajowego należy rozstrzygnięcie sprawy zgodnie z orzeczeniem Trybunału. Orzeczenie to wiąże w ten sam sposób inne sądy krajowe, które spotkają się z podobnym problemem.

Dokument nieoficjalny, sporządzony na użytek mediów, który nie wiąże Trybunału Sprawiedliwości.

[Pełny tekst](#) wyroku jest publikowany na stronie internetowej CURIA w dniu ogłoszenia.

Osoba odpowiedzialna za kontakty z mediami: Ireneusz Kolowca ☎ (+352) 4303 2793

Nagranie wideo z ogłoszenia wyroku jest dostępne przez [„Europe by Satellite”](#) ☎ (+32) 22964106.