



Kontakty z Mediami
i Informacja

Trybunał Sprawiedliwości Unii Europejskiej
KOMUNIKAT PRASOWY nr 145/16

Luksemburg, 21 grudnia 2016 r.

Wyrok w sprawach połączonych C-203/15 Tele2 Sverige AB / Post-och telestyrelsen i C-698/15 Secretary of State for the Home Department / Tom Watson i in.

Państwa członkowskie nie mogą nakładać na podmioty świadczące usługi elektroniczne ogólnego obowiązku zatrzymywania danych

Uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i tych dotyczących lokalizacji jest niezgodne z prawem Unii, ale państwu członkowskiemu przysługuje prawo przewidzenia indywidualnego zatrzymywania danych tytułem prewencji, mającego na celu jedynie zwalczanie poważnej przestępczości, pod warunkiem, że takie zatrzymywanie – w zakresie dotyczącym podlegających mu danych, stosowanych środków łączności, zaangażowanych w ten proces podmiotów oraz przyjętego okresu przechowywania danych – nie będzie wykraczać poza to, co jest absolutnie konieczne. Organy krajowe mogą mieć dostęp do tych zatrzymywanych danych pod określonymi warunkami, do których należy w szczególności podleganie uprzedniej kontroli niezależnego organu oraz przechowywanie tych danych na obszarze Unii

W wyroku w sprawie Digital Rights Ireland z 2014 r.¹ Trybunał Sprawiedliwości stwierdził nieważność dyrektywy w sprawie zatrzymywania danych² ze względu na to, że ta wiążąca się z nałożonym w tej dyrektywie ogólnym obowiązkiem zatrzymywania danych o ruchu oraz danych dotyczących lokalizacji ingerencja w prawa podstawowe do poszanowania życia prywatnego oraz ochrony danych osobowych wykracza poza to, co absolutnie konieczne.

W następstwie wydania tego wyroku do Trybunału wpłynęły dwie sprawy dotyczące nałożonego w Szwecji i w Zjednoczonym Królestwie na podmioty świadczące usługi telekomunikacyjne ogólnego obowiązku zatrzymywania danych dotyczących łączności elektronicznej, który to obowiązek został ustanowiony w unieważnionej dyrektywie.

W dzień po ogłoszeniu wyroku w sprawie Digital Rights Ireland przedsiębiorstwo telekomunikacyjne Tele2 Sverige powiadomiło szwedzki organ nadzorujący rynek pocztowy i telekomunikacyjny o swojej decyzji o zaprzestaniu zatrzymywania danych oraz o zamiarze usunięcia już utrwalonych danych (sprawa C-203/15). Na gruncie prawa szwedzkiego podmioty świadczące usługi łączności elektronicznej są bowiem zobowiązane do bezwarunkowego i systematycznego zatrzymywania w sposób ciągły wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich ich abonentów i zarejestrowanych użytkowników niezależnie od zastosowanych środków łączności elektronicznej.

W sprawie C-698/15 Tom Watson, Peter Brice i Geoffrey Lewis zaskarżyli brytyjskie przepisy prawa dotyczące zatrzymywania danych, na mocy których minister spraw wewnętrznych jest upoważniony do zobowiązania publicznych operatorów telekomunikacyjnych do zatrzymywania, przez okres nieprzekraczający dwunastu miesięcy, wszystkich danych dotyczących połączeń, z wyłączeniem przekazywanych za ich pomocą treści.

Kammarrätten i Stockholm (administracyjny sąd apelacyjny w Sztokholmie, Szwecja) oraz Court of Appeal (England and Wales) (Civil Division) (wydział cywilny sądu apelacyjnego dla Anglii i Walii,

¹ Wyrok Trybunału z dnia 8 kwietnia 2014 r. *Digital Rights Ireland i Seitlinger i in.* (sprawy połączone [C-293/12 i C-594/12](#), zob. [komunikat prasowy nr 54/14](#)).

² 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).

Zjednoczone Królestwo) zwróciły się do Trybunału Sprawiedliwości o wskazanie, czy przepisy prawa krajowego, które nakładają na podmioty świadczące usługi łączności elektronicznej ogólny obowiązek zatrzymywania danych oraz przyznają właściwym organom krajowym dostęp do przechowywanych danych, nie ograniczając tego dostępu jedynie do celów związanych ze zwalczaniem poważnej przestępczości i nie poddając go uprzedniej kontroli niezależnego organu sądowiczego lub administracyjnego, są zgodne z prawem Unii (zwłaszcza z dyrektywą „o prywatności i łączności elektronicznej”³ w kontekście Karty praw podstawowych⁴).

W ogłoszonym dzisiaj wyroku Trybunał odpowiedział, że **przepisy prawa krajowego przewidujące uogólnione i nieodróżnicowane zatrzymywanie danych są niezgodne z prawem Unii.**

Trybunał potwierdził w pierwszej kolejności, że rozpatrywane **środki krajowe wchodzą w zakres zastosowania dyrektywy**. Zagwarantowana przez dyrektywę ochrona poufności łączności elektronicznej i danych dotyczących ruchu znajduje bowiem zastosowanie do środków stosowanych przez podmioty inne niż użytkownicy, niezależnie od tego, czy są to podmioty prywatne czy też państwowe.

Trybunał stwierdził następnie, że choć ta dyrektywa daje państwom członkowskim możliwość ograniczenia tego mającego zasadnicze znaczenie obowiązku zapewnienia poufności łączności oraz związanych z nią danych o ruchu, to jednak na jej gruncie nie można uzasadnić tego, aby odstąpienie od tego mającego zasadnicze znaczenie obowiązku i, w szczególności, od zakazu przechowywania tych danych, stało się regułą.

Następnie Trybunał przypomniał swe utrwalone orzecznictwo, zgodnie z którym ochrona prawa podstawowego do poszanowania prywatności wymaga, aby **odstąpienia** od ochrony danych osobowych **pozostawały w granicach tego, co jest „absolutnie konieczne”**. Trybunał zastosował to orzecznictwo zarówno do norm rządzących zatrzymywaniem danych, jak i tych regulujących dostęp do przechowywanych danych.

W odniesieniu do zatrzymywanych danych Trybunał stwierdził, że w swym całościowym kształcie **umożliwiają one wyciągnięcie bardzo szczegółowych wniosków odnośnie do życia prywatnego osób**, których dane zostały zatrzymane.

Ingerencję będącą wynikiem stosowania przepisów krajowych przewidujących zatrzymywanie danych o ruchu i tych dotyczących lokalizacji należy więc uznać za **szczególnie poważną**. Okoliczność, że użytkownicy usług łączności elektronicznej nie wiedzą o tym, że dane te są zatrzymywane, może pociągnąć za sobą powstanie po ich stronie wrażenia, że ich prywatne życie podlega ciągłej obserwacji. Co za tym idzie, **tego rodzaju ingerencja może być uzasadniona jedynie walką z poważną przestępczością**.

Trybunał podniósł, że **przepisy przewidujące to uogólnione i nieodróżnicowane zatrzymywanie danych nie ustanawiają wymogu istnienia związku pomiędzy danymi, które mają być zatrzymywane, a zagrożeniem bezpieczeństwa publicznego** i, w szczególności, nie ustanawiają ograniczeń tego zatrzymywania danych w czasie lub przestrzeni czy nie ograniczają go do kręgu osób, które mogłyby być zaangażowane w poważne przestępstwo. **Takie przepisy krajowe wykraczają więc poza granice tego, co jest absolutnie konieczne i nie można ich uznać za uzasadnione w demokratycznym społeczeństwie, który to wymóg wynika również z dyrektywy czytanej w świetle Karty**.

Trybunał wyjaśnił natomiast, że **nie są sprzeczne z tą dyrektywą przepisy krajowe ustanawiające obowiązek indywidualnego zatrzymywania danych** w celu zwalczania poważnej przestępczości, pod warunkiem, że takie zatrzymywanie – w zakresie dotyczącym

³ 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. L 201, s. 37), zmieniona dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. (Dz.U. L 337, s. 11).

⁴ Artykuły 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej.

danych podlegających zatrzymywaniu, stosowanych środków łączności, zaangażowanych w ten proces podmiotów oraz przyjęty okres przechowywania danych – **nie będzie wykraczać poza to, co jest absolutnie konieczne**. Zdaniem Trybunału **wszystkie przyjęte w tym względzie przepisy muszą być jednoznaczne i szczegółowe oraz przewidywać gwarancje wystarczające do tego, aby chronić te dane przed ryzykiem ich nadużycia**. Przepisy te powinny wskazywać okoliczności i warunki, w których środek w zakresie zatrzymywania danych może zostać zastosowany tytułem prewencji w taki sposób, który gwarantuje, aby jego zakres w praktyce ograniczał się rzeczywiście do tego, co jest absolutnie konieczne. W szczególności takie przepisy powinny opierać się na **obiektywnych elementach** umożliwiających namierzenie osób, których dane mogą mieć związek z poważną przestępczością, przyczyniać się do walki z taką przestępczością czy też zapobiegać powstawaniu poważnych zagrożeń dla bezpieczeństwa publicznego.

W zakresie dotyczącym **dostępu odpowiednich organów krajowych do przechowywanych danych** Trybunał potwierdził, że rozpatrywane przepisy krajowe nie mogą ograniczać się do ustanowienia wymogu, by dostęp ten uwzględniał jeden z realizowanych przez dyrektywę celów, polegający na prowadzeniu walki z poważną przestępczością, lecz muszą one też ustanawiać materialne i proceduralne warunki regulujące dostęp odpowiednich organów krajowych do przechowywanych danych. Przepisy te powinny opierać się na **obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu do tych danych właściwym organom krajowym**. Uwzględniając cel polegający na zwalczaniu poważnej przestępczości, dostęp ten może co do zasady zostać przyznany jedynie odnośnie do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też dopuszczenie się już poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo. Niemniej jednak, w szczególnych sytuacjach, takich jak te, w których istotne interesy związane z bezpieczeństwem narodowym, obroną czy też bezpieczeństwem publicznym są zagrożone wskutek działań terrorystycznych, dostęp do danych dotyczących innych osób może zostać przyznany również wówczas, gdy istnieją obiektywne elementy pozwalające uznać, że dane te mogłyby w konkretnym przypadku rzeczywiście przyczynić się do zwalczania takich działań.

Trybunał uznał ponadto za istotne, aby **dostęp do przechowywanych danych podlegał, za wyjątkiem pilnych przypadków, uprzedniej kontroli** sprawowanej przez sąd lub inny niezależny organ. Ponadto właściwe organy władzy krajowej, którym przyznano dostęp do przechowywanych danych, powinny o tym poinformować zainteresowane osoby.

Uwzględniając ilość tych danych, ich znaczenie oraz niebezpieczeństwo związane z uzyskaniem bezprawnego do nich dostępu, **przepisy krajowe powinny ustanawiać obowiązek ich przechowywania na obszarze Unii**, a także – obowiązek ich nieodwracalnego niszczenia po upływie okresu ich przechowywania.

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 znajduje się 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) 2 2964106