Trybunał Sprawiedliwości Unii Europejskiej
KOMUNIKAT PRASOWY nr 54/14
Luksemburg, 8 kwietnia 2014 r.

Kontakty z Mediami
i Informacja

Wyrok w sprawach połączonych C-293/12 i C-594/12
Digital Rights Ireland i Seitlinger i in.

Trybunał Sprawiedliwości orzekł, że dyrektywa w sprawie zatrzymywania danych jest nieważna

Dyrektywa stanowi ingerencję o znacznym zakresie i szczególnej wadze w podstawowe prawa do poszanowania życia prywatnego i do ochrony danych osobowych, przy czym ingerencja ta nie ogranicza się do tego, co ściśle niezbędne

Zasadniczym celem dyrektywy w sprawie zatrzymywania danych[1] jest harmonizacja przepisów państw członkowskich w dziedzinie zatrzymywania danych generowanych lub przetwarzanych przez dostawców ogólnie dostępnych usług komunikacji elektronicznej lub publicznych sieci łączności. Dąży ona zatem do zapewnienia dostępności owych danych do celów zapobiegania poważnym przestępstwom, takim jak w szczególności przestępczość zorganizowana i terroryzm, oraz do celów dochodzenia, wykrywania i ścigania takich przestępstw. I tak, dyrektywa stanowi, że wspomniani dostawcy powinni zatrzymywać dane o ruchu i lokalizacji oraz powiązane dane niezbędne do identyfikacji abonenta lub użytkownika. Dyrektywa ta nie zezwala natomiast na zatrzymywanie treści komunikatów i uzyskiwanych informacji.

High Court (Irlandia) oraz Verfassungsgerichtshof (trybunał konstytucyjny, Austria) wniosły do Trybunału Sprawiedliwości o zbadanie ważności dyrektywy, w szczególności w świetle dwóch praw podstawowych gwarantowanych przez Kartę praw podstawowych Unii Europejskiej, mianowicie prawa podstawowego do poszanowania życia prywatnego i prawa podstawowego do ochrony danych osobowych.

High Court musi rozstrzygnąć spór pomiędzy spółką irlandzką Digital Rights a władzami irlandzkimi w przedmiocie zgodności z prawem przepisów krajowych dotyczących zatrzymywania danych związanych z komunikatami elektronicznymi. Verfassungsgerichtshof rozpatruje kilka dotyczących zagadnień konstytucyjnych skarg wniesionych przez Kärntner Landesregierung (rząd kraju związkowego Karyntii) oraz przez M. Seitlingera, C. Tschohla i 11 128 innych skarżących. Skargi te mają na celu stwierdzenie nieważności przepisów krajowych transponujących dyrektywę do prawa austriackiego.

Dzisiejszym wyrokiem Trybunał orzekł, że dyrektywa jest nieważna[2].

Trybunał stwierdził przede wszystkim, że dane przeznaczone do zatrzymania umożliwiają w szczególności: 1) dowiedzenie się, z jaką osobą i za pomocą jakiego środka komunikował się abonent lub zarejestrowany użytkownik, 2) określenie czasu łączności oraz miejsca, z którego łączność ta została nawiązana i 3) ustalenie częstości komunikowania się abonenta lub zarejestrowanego użytkownika z określonymi osobami w danym okresie. Dane te, rozpatrywane łącznie, mogą dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak nawyki życia codziennego, miejsca stałego lub

[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. L 105, s. 54).

[2] Zważywszy na to, że Trybunał nie ograniczył skutków wyroku w czasie, uznanie nieważności staje się skuteczne z dniem wejścia w życie dyrektywy.

czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają.

Trybunał uznał, że **nakładając obowiązek zatrzymywania danych i umożliwiając dostęp do nich właściwym organom krajowym, dyrektywa ingeruje w sposób szczególnie poważny w prawa podstawowe do poszanowania życia społecznego i do ochrony danych osobowych**. Ponadto okoliczność, że zatrzymywanie i późniejsze wykorzystywanie danych jest dokonywane bez poinformowania o tym abonenta i zarejestrowanego użytkownika, może wywołać u zainteresowanych osób poczucie, iż ich życie prywatne podlega stałemu nadzorowi.

Trybunał zbadał następnie, czy taka ingerencja w omawiane prawa podstawowe jest uzasadniona.

Trybunał stwierdził, że przewidziane dyrektywą **zatrzymywanie danych nie narusza zasadniczej treści praw podstawowych do poszanowania życia prywatnego i do ochrony danych osobowych**. Dyrektywa nie pozwala bowiem na zapoznawanie się z treścią komunikatów elektronicznych jako taką i stanowi, że dostawcy usług lub sieci powinni przestrzegać określonych zasad ochrony i bezpieczeństwa danych.

Co więcej, zatrzymanie danych w celu ich ewentualnego udostępnienia właściwym organom krajowym **rzeczywiście odpowiada celowi w postaci interesu ogólnego, jakim jest zwalczanie poważnej przestępczości oraz - ostatecznie - bezpieczeństwo publiczne**.

Jednakże, zdaniem Trybunału, przyjmując dyrektywę w sprawie zatrzymywania danych, prawodawca Unii przekroczył granice, które wyznacza poszanowanie zasady proporcjonalności.

W tym względzie Trybunał zauważył, że przy uwzględnieniu, po pierwsze, znaczącej roli, którą odgrywa ochrona danych osobowych w odniesieniu do prawa podstawowego do poszanowania życia prywatnego oraz, po drugie, zakresu i wagi ingerencji w to prawo, do której prowadzi dyrektywa, uprawnienia dyskrecjonalne prawodawcy Unii okazują się ograniczone, tak że należy przeprowadzić ścisłą kontrolę.

O ile można uważać, że wymagane dyrektywą zatrzymywanie danych jest w stanie realizować zakładany przez nią cel, o tyle **przewidziana tą dyrektywą znaczna i szczególnie poważna ingerencja w omawiane prawa podstawowe nie ma wystarczających ram, by zagwarantować, aby wspomniana ingerencja była ograniczona do tego, co ściśle niezbędne**.

Po pierwsze, dyrektywa obejmuje bowiem w sposób uogólniony wszystkie jednostki, środki łączności elektronicznej i dane o ruchu, przy czym nie przewidziano jakiegokolwiek **zróżnicowania, ograniczenia lub wyjątku** w zależności od celu dotyczącego zwalczania poważnych przestępstw.

Po drugie, dyrektywa nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby zagwarantować, by właściwe organy krajowe miały **dostęp do danych** i mogły je wykorzystywać wyłącznie do zapobiegania przestępstwom, które mogą być uważane w świetle zakresu i wagi ingerencji w omawiane prawa podstawowe za wystarczająco poważne, by uzasadnić taką ingerencję, oraz do wykrywania i ścigania karnego takich przestępstw. Przeciwnie, dyrektywa ogranicza się do odesłania w sposób ogólny do pojęcia „poważnych przestępstw" zdefiniowanych przez każde państwo członkowskie w jego prawie krajowym. Ponadto dyrektywa nie przewiduje materialnych i proceduralnych przesłanek dotyczących sytuacji, w których właściwe organy krajowe mogą uzyskać dostęp do danych i je później wykorzystywać. Dostęp do danych nie jest w szczególności podporządkowany uprzedniej kontroli sądu lub niezależnego organu administracyjnego.

Po trzecie, w odniesieniu do **okresu zatrzymania** danych, dyrektywa przewiduje okres co najmniej sześciu miesięcy, przy czym nie przeprowadza jakiegokolwiek rozróżnienia pomiędzy kategoriami danych w zależności od zainteresowanych osób lub ewentualnej użyteczności danych w stosunku

do zakładanego celu. Ponadto okres ten wynosi od co najmniej sześciu miesięcy do co najwyżej dwudziestu czterech miesięcy, przy czym dyrektywa nie precyzuje obiektywnych kryteriów, na podstawie których należy ustalić okres zatrzymywania, by zagwarantować jego ograniczenie do tego, co ściśle niezbędne.

Trybunał stwierdził poza tym, że dyrektywa nie przewiduje wystarczających gwarancji umożliwiających zapewnienie skutecznej ochrony danych przed **niebezpieczeństwem nadużycia** oraz przed jakimkolwiek dostępem do danych i ich wykorzystywaniem w sposób niedozwolony. Zauważył także między innymi, że dyrektywa upoważnia usługodawców do brania pod uwagę względów gospodarczych przy określaniu stosowanego przez nich poziomu bezpieczeństwa (w szczególności w odniesieniu do kosztów wprowadzenia środków bezpieczeństwa) i że nie gwarantuje ona nieodwracalnego zniszczenia danych po upływie ich okresu zatrzymania.

Trybunał krytycznie ocenił wreszcie to, że dyrektywa **nie** nakłada obowiązku, by dane były **zatrzymywane na obszarze Unii**. I tak, dyrektywa nie gwarantuje w pełni kontroli poszanowania wymogów ochrony i bezpieczeństwa przez niezależny organ, jak tego jednak wyraźnie wymaga Karta. Taka zaś kontrola, dokonywana na podstawie prawa Unii, stanowi zasadniczy element poszanowania ochrony osób w odniesieniu do przetwarzania danych osobowych.

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.

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