

- 2) Artykuł 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 4 ust. 2 TUE, a także art. 7, 8 i 11 oraz 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu umożliwiającemu organowi państwa nałożenie na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego.

(<sup>1</sup>) Dz.U. C 22 z 22.1.2018

**Wyrok Trybunału (wielka izba) z dnia 6 października 2020 r. (wnioski o wydanie orzeczenia w trybie prejudycjalnym złożone przez Conseil d'État, Cour constitutionnelle – Belgia, Francja) – La Quadrature du Net (C-511/18 i C-512/18), French Data Network (C-511/18 i C-512/18), Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 i C-512/18), Igwan.net (C-511/18) / Premier ministre (C-511/18 i C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 i C-512/18), Ministre de l'Intérieur (C-511/18), Ministre des Armées (C-511/18), Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX / Conseil des ministres**

(Sprawy połączone C-511/18, C-512/18 i C-520/18) (<sup>1</sup>)

*(Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Dostawcy usług łączności elektronicznej – Dostawcy usług hostingowych i dostawcy dostępu do Internetu – Uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji – Zautomatyzowana analiza danych – Dostęp do danych w czasie rzeczywistym – Ochrona bezpieczeństwa narodowego i walka z terroryzmem – Zwalczanie przestępczości – Dyrektywa 2002/58/WE – Zakres stosowania – Artykuł 1 ust. 3 i art. 3 – Poufność łączności elektronicznej – Ochrona – Artykuł 5 i art. 15 ust. 1 – Dyrektywa 2000/31/WE – Zakres stosowania – Karta praw podstawowych Unii Europejskiej – Artykuły 4, 6 – 8 i 11 oraz art. 52 ust. 1 – Artykuł 4 ust. 2 TUE)*

(2020/C 433/03)

Język postępowania: francuski

#### Sąd odsyłający

Conseil d'État, Cour constitutionnelle

#### Strony w postępowaniu głównym

(Sprawy C-511/18 i C-512/18)

*Strona skarżąca:* La Quadrature du Net (C-511/18 i C-512/18), French Data Network (C-511/18 i C-512/18), Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 i C-512/18), Igwan.net (C-511/18)

*Strona pozwana:* Premier ministre (C-511/18 i C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 i C-512/18), Ministre de l'Intérieur (C-511/18), Ministre des Armées (C-511/18)

*przy udziale:* Privacy International (C-512/18), Center for Democracy and Technology (C-512/18),

(Sprawa C-520/18)

*Strona skarżąca:* Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX

*Strona pozwana:* Conseil des ministres

*przy udziale:* Child Focus (C-520/18)

## Sentencja

1) Artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r., w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że stoi on na przeszkodzie środkom ustawodawczym przewidującym, w celach, o których mowa w tym art. 15 ust. 1, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji. Natomiast wspomniany art. 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty praw podstawowych nie stoi na przeszkodzie przepisom ustawodawczym

- umożliwiającym, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji w sytuacjach, gdy dane państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia, przy czym decyzja o wydaniu takiego nakazu może być przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, mającej na celu weryfikację występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, które powinny zostać przewidziane, zaś wspomniany nakaz można wydać jedynie na określony czas ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia;
- przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego, na okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;
- przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne;
- przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania przestępczości i ochrony bezpieczeństwa publicznego, uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz
- umożliwiającym, w celu zwalczania poważnej przestępczości oraz, a fortiori, ochrony bezpieczeństwa narodowego, posłużenie się nakazem skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, szybkiego zatrzymywania przez określony czas danych o ruchu i danych o lokalizacji, którymi dysponują ci dostawcy usług,

jeśli środki te zawierają jasne i precyzyjne przepisy zapewniające, że rozpatrywane zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych warunków, oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.

- 2) Artykuł 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty praw podstawowych należy interpretować w ten sposób, że nie stoi on na przeszkodzie uregulowaniu krajowemu zobowiązującemu dostawców usług łączności elektronicznej, po pierwsze, do posłużenia się zautomatyzowaną analizą oraz do gromadzenia w czasie rzeczywistym w szczególności danych o ruchu i danych o lokalizacji, a po drugie do gromadzenia w czasie rzeczywistym danych technicznych o lokalizacji wykorzystywanych urządzeń końcowych, jeśli
- posłużenie się zautomatyzowaną analizą ogranicza się do sytuacji, w których państwo członkowskie napotyka na poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub przewidywalne, przy czym posłużenie się tą analizą może podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja ma wiążący skutek, mającej na celu sprawdzenie, czy wystąpiła sytuacja uzasadniająca wspomniany środek, jak również weryfikację poszanowania warunków i gwarancji, które powinny zostać przewidziane, oraz
  - korzystanie z gromadzenia w czasie rzeczywistym danych o ruchu i danych o lokalizacji jest ograniczone do osób, wobec których istnieje uzasadniony powód, by podejrzewać, że są one zaangażowane w taki lub inny sposób w działalność terrorystyczną, i podlega uprzedniej kontroli dokonywanej albo przez sąd, albo przez niezależny organ administracyjny, którego decyzja ma wiążący skutek, w celu zapewnienia, że takie gromadzenie w czasie rzeczywistym jest dozwolone jedynie w granicach tego, co jest ściśle niezbędne. W należycie uzasadnionych pilnych przypadkach kontrola powinna nastąpić w krótkim czasie.
- 3) Dyrektywę 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywę o handlu elektronicznym) należy interpretować w ten sposób, że nie ma ona zastosowania w dziedzinie ochrony poufności porozumiewania się i osób fizycznych w związku z przetwarzaniem danych osobowych w ramach usług społeczeństwa informacyjnego, ponieważ ochrona ta jest w zależności od przypadku regulowana przez dyrektywę 2002/58, zmienioną dyrektywą 2009/136, lub przez rozporządzenie 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. Artykuł 23 ust. 1 rozporządzenia 2016/679 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty praw podstawowych należy interpretować w ten sposób, że stoi on na przeszkodzie przepisom krajowym nakładającym na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych obowiązek uogólnionego i nieodróżnicowanego zatrzymywania między innymi danych osobowych dotyczących tych usług.
- 4) Sąd krajowy nie może zastosować przepisu prawa krajowego, który upoważnia go do ograniczenia w czasie skutków stwierdzenia niezgodności z prawem, którego ma on dokonać na mocy tego prawa w odniesieniu do ustawodawstwa krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek, w szczególności w celu ochrony bezpieczeństwa narodowego i zwalczania przestępczości, uogólnionego i nieodróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z art. 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty praw podstawowych. Ów art. 15 ust. 1, interpretowany w świetle zasady skuteczności, zobowiązuje krajowy sąd karny do nieuwzględnienia informacji i dowodów uzyskanych w wyniku uogólnionego i nieodróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstwa, jeżeli osoby te nie są w stanie skutecznie ustosunkować się do tych informacji i dowodów należących do dziedziny niepodlegającej rozpoznaniu przez sąd i mogących mieć decydujący wpływ na ocenę okoliczności faktycznych.

(<sup>1</sup>) Dz.U. C 392 z 29.10.2018.  
Dz.U. C 408 z 12.11. 2018.