C/2024/3717

24.6.2024

Wyrok Trybunału (w pełnym składzie) z dnia 30 kwietnia 2024 r. (wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Conseil d'État – Francja) – La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network/Premier ministre, Ministère de la Culture

[Sprawa C-470/21 [1]**, La Quadrature du Net i in. (Dane osobowe i walka z naruszeniami praw własności intelektualnej)]**

(Odesłanie prejudycjalne – Przetwarzanie danych osobowych i ochrona prywatności w sektorze łączności elektronicznej – Dyrektywa 2002/58/WE – Poufność komunikacji elektronicznej – Ochrona – Artykuł 5 i art. 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 11 oraz art. 52 ust. 1 – Przepisy krajowe mające na celu zwalczanie, poprzez działania podejmowane przez organ publiczny, naruszeń praw własności intelektualnej, do których dochodzi w Internecie – Tak zwana procedura stopniowej odpowiedzi – Mające miejsce w pierwszej kolejności zbieranie, przez zrzeszające uprawnionych organizacje, adresów IP wykorzystywanych do aktywności naruszającej prawa autorskie lub prawa pokrewne – Mający miejsce w drugiej kolejności dostęp odpowiedzialnego za ochronę praw autorskich i praw pokrewnych organu publicznego do przechowywanych przez dostawców usług łączności elektronicznej danych dotyczących tożsamości cywilnej odpowiadających tym adresom IP – Przetwarzanie zautomatyzowane – Wymóg dokonania uprzedniej kontroli przez sąd lub niezależny organ administracyjny – Warunki materialne i proceduralne – Gwarancje chroniące przed ryzykiem nadużyć oraz przed wszelkim niezgodnym z prawem dostępem do tych danych i wszelkim niezgodnym z prawem ich wykorzystywaniem)

(C/2024/3717)

Język postępowania: francuski

Sąd odsyłający

Conseil d'État

Strony w postępowaniu głównym

Strona skarżąca: La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network

Strona przeciwna: Premier ministre, Ministère de la Culture

Sentencja

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 Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej

należy interpretować w ten sposób, że:

nie stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala organowi publicznemu odpowiedzialnemu za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw, do których dochodzi w Internecie, na dostęp do przechowywanych przez dostawców publicznie dostępnych usług łączności elektronicznej danych dotyczących tożsamości cywilnej odpowiadających adresom IP zbieranym wcześniej przez organizacje zrzeszające uprawnionych, aby ów organ mógł zidentyfikować posiadaczy tych adresów wykorzystywanych do aktywności mogącej stanowić takie naruszenia i aby mógł on w razie potrzeby zastosować wobec nich środki, pod warunkiem że na mocy tego uregulowania:

— dane te przechowywane są w warunkach i zgodnie z zasadami technicznymi, które gwarantują, że wykluczone jest, by ich przechowywanie mogło pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego tych posiadaczy, na przykład poprzez ustalenie ich szczegółowego profilu, co można osiągnąć w szczególności poprzez nałożenie na dostawców usług łączności elektronicznej obowiązku przechowywania poszczególnych kategorii danych osobowych, takich jak dane dotyczące tożsamości cywilnej, adresy IP oraz dane o ruchu i dane dotyczące lokalizacji, gwarantującego rzeczywiście szczelne odseparowanie tych poszczególnych kategorii danych, które uniemożliwia na etapie przechowywania wszelkie powiązanie tych poszczególnych kategorii danych, przez okres nieprzekraczający tego, co ściśle niezbędne;

[1] Dz.U. C 462 z 15.11.2021.

— dostęp tego organu publicznego do takich danych przechowywanych w sposób odseparowany i rzeczywiście szczelny służy wyłącznie zidentyfikowaniu osoby podejrzewanej o dopuszczenie się czynu zabronionego i towarzyszą mu gwarancje niezbędne do wykluczenia, by, poza sytuacjami nietypowymi, dostęp ten mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego posiadaczy adresów IP, na przykład poprzez ustalenie ich szczegółowego profilu, co wymaga w szczególności, by upoważnionych do posiadania takiego dostępu urzędników owego organu obowiązywał zakaz ujawniania w jakiejkolwiek formie informacji na temat zawartości plików przeglądanych przez tych posiadaczy, z jedynym wyjątkiem wiążącym się z ujawnieniem ich w celu zawiadomienia prokuratury, zakaz śledzenia historii treści przeglądanych przez owych posiadaczy oraz, ogólniej, zakaz wykorzystywania tych adresów IP do celów innych niż zidentyfikowanie ich posiadaczy, aby zastosować wobec nich ewentualne środki;

— możliwość powiązania przez osoby odpowiedzialne w ramach wspomnianego organu publicznego za analizę zdarzeń takich danych z plikami zawierającymi elementy umożliwiające poznanie tytułów utworów chronionych, których udostępnienie w Internecie uzasadniało zebranie adresów IP przez organizacje zrzeszające uprawnionych, jest uzależniona – w przypadkach kolejnego ponowienia aktywności naruszającej prawa autorskie lub prawa pokrewne przez tę samą osobę – od dokonania przez sąd lub niezależny organ administracyjny kontroli, która nie może być w pełni zautomatyzowana i powinna mieć miejsce przed dokonaniem takiego powiązania, ponieważ powiązanie to może w takich przypadkach pozwolić na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego wspomnianej osoby, której adres IP wykorzystano do aktywności mogącej naruszać prawa autorskie lub prawa pokrewne;

— system przetwarzania danych wykorzystywany przez organ publiczny podlega w regularnych odstępach czasu kontroli niezależnego organu mającego status strony trzeciej w stosunku do tego organu publicznego, mającej na celu weryfikację integralności systemu, w tym skutecznych gwarancji chroniących przed ryzykiem takiego dostępu do tych danych lub takiego ich wykorzystywania, które nosiłyby znamiona nadużycia lub byłyby niezgodne z prawem, oraz jego skuteczności i niezawodności w wykrywaniu ewentualnych uchybień.