Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
MACIEJA SZPUNARA
przedstawiona w dniu 28 września 2023 r.[1]

Sprawa C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
przeciwko
Premier ministre,
Ministère de la Culture

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Conseil d'État (radę stanu, Francja)]

Odesłanie prejudycjalne – Przetwarzanie danych osobowych i ochrona prywatności w sektorze łączności elektronicznej – Dyrektywa 2002/58/WE – Artykuł 15 ust. 1 – Możliwość ograniczenia przez państwa członkowskie zakresu niektórych praw i obowiązków – Obowiązek uprzedniej kontroli przez sąd lub niezależny organ administracyjny posiadający uprawnienia władcze – Dane dotyczące tożsamości cywilnej odpowiadające adresowi IP

I. Wprowadzenie

1. Na wniosek wielkiej izby złożony na podstawie art. 60 § 3 regulaminu postępowania przed Trybunałem, w dniu 7 marca 2023 r. Trybunał postanowił przydzielić niniejszą sprawę pełnemu składowi.

2. Postanowieniem z dnia 23 marca 2023 r. Trybunał (w pełnym składzie) otworzył na nowo ustny etap postępowania oraz wezwał zainteresowane podmioty wskazane w art. 23 statutu Trybunału Sprawiedliwości Unii Europejskiej, a także Europejskiego Inspektora Ochrony Danych (EIOD, zwanego dalej „Inspektorem") oraz Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) do uczestnictwa w ponownej rozprawie.

3. W dniu 27 października 2022 r., przed zamknięciem ustnego etapu postępowania, przedstawiłem opinię w tej sprawie. Niniejsza nowa opinia daje mi zatem możliwość pogłębienia niektórych części rozumowania dotyczącego tej sprawy o doniosłym znaczeniu dla kwestii przechowywania i dostępu do danych osobowych.

[1] Język oryginału: francuski.

II. Ramy prawne

A. Prawo Unii

4. Motywy 2, 6, 7, 11, 22, 26 i 30 dyrektywy 2002/58/WE [2] mają następujące brzmienie:

„(2) Niniejsza dyrektywa dąży do poszanowania fundamentalnych praw i jest zgodna z zasadami uznanymi w szczególności przez Kartę praw podstawowych Unii Europejskiej [zwaną dalej »kartą«]. W szczególności niniejsza dyrektywa zmierza do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 tej [k]arty.

[…]

(6) Internet przekształca tradycyjne struktury rynkowe przez udostępnienie ogólnej, globalnej infrastruktury dostarczającej szerokiego spektrum usług łączności elektronicznej. Usługi łączności elektronicznej ogólnodostępne za pośrednictwem Internetu stwarzają nowe możliwości użytkownikom, ale również powodują powstanie nowych zagrożeń dotyczących ich danych osobowych i prywatności.

(7) W przypadku publicznych sieci łączności należy wprowadzić szczególne przepisy prawne, wykonawcze i techniczne w celu ochrony podstawowych praw i wolności osób fizycznych oraz uzasadnionego interesu osób prawnych, w szczególności w odniesieniu do zwiększonej pojemności automatycznego przechowywania i przetwarzania danych odnoszących się do abonentów i użytkowników.

[…]

(11) Niniejsza dyrektywa, podobnie jak dyrektywa [95/46/WE [3]], nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem wspólnotowym. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a możliwością państw członkowskich do podejmowania środków, określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego niniejsza dyrektywa nie wpływa na możliwości państw członkowskich do zgodnego z prawem przejmowania danych w łączności elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregokolwiek z tych celów i zgodne z europejską Konwencją o ochronie praw człowieka i podstawowych wolności [podpisaną w Rzymie w dniu 4 listopada 1950 r.], dla której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe, [ściśle] współmierne do zamierzonego celu i niezbędne w ramach społeczeństwa demokratycznego oraz powinny podlegać stosownym zabezpieczeniom zgodnie z europejską Konwencją o ochronie praw człowieka i podstawowych wolności.

[…]

[2] Dyrektywa 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), (zwana dalej „dyrektywą 2002/58”).

[3] Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. 1995, L 281, s. 31).

(22) Zakaz przechowywania komunikatów oraz związanych z nimi danych dotyczących ruchu w sieci przez osoby inne niż użytkownicy lub bez ich zgody nie ma na celu zakazu automatycznego, pośredniego i przejściowego przechowywania takiej informacji, wówczas gdy odbywa się to wyłącznie do celu przeprowadzenia transmisji w sieci łączności elektronicznej oraz pod warunkiem że informacja nie jest przechowywana przez okres dłuższy niż jest to konieczne w celu wykonania transmisji i zarządzania ruchem, oraz, że w okresie przechowywania zagwarantowana zostaje poufność. […]

[…]

(26) Dane dotyczące abonentów przetwarzane w ramach sieci łączności elektronicznej w celu ustanowienia połączenia i przenoszenia informacji zawierają informacje dotyczące prywatnego życia osób fizycznych i dotyczą prawa do poszanowania tajemnicy korespondencji lub dotyczą uzasadnionych interesów osób prawnych. Takie dane mogą być przechowywane tylko przez określony czas i wyłącznie w zakresie umożliwiającym świadczenie usług związanych z naliczaniem opłat i rozliczeń międzyoperatorskich. Wszelkie dalsze przetwarzanie tego rodzaju danych […] może być dozwolone tylko w przypadkach, gdy abonent wyraził na to zgodę na podstawie udzielonej mu przez dostawcę usług dokładnej i pełnej informacji o rodzajach zamierzonego dalszego przetwarzania oraz prawie abonenta do nieudzielenia zgody na przetwarzanie lub jej odwołania. […]

[…]

(30) Systemy dostarczania sieci i usług łączności elektronicznej powinny być zaprojektowane w taki sposób, aby ograniczać ilość niezbędnych danych osobowych do ścisłego minimum. […]”.

5. Zgodnie z art. 2 tej dyrektywy, zatytułowanym „Definicje”:

„[…]

Stosuje się również następujące definicje:

a) »użytkownik« oznacza każdą osobę fizyczną korzystającą z publicznie dostępnych usług łączności elektronicznej, do celów prywatnych lub handlowych, niekoniecznie na podstawie abonamentu za te usługi;

b) »dane o ruchu« oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi;

c) »dane dotyczące lokalizacji« oznaczają wszelkie dane przetwarzane w sieci łączności elektronicznej lub w ramach usług łączności elektronicznej, wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług łączności elektronicznej;

d) »komunikat« oznacza każdą informację wymienianą lub przekazaną między określoną liczbą stron za pośrednictwem usług publicznie dostępnej łączności elektronicznej. Nie obejmuje on informacji przekazanej jako część publicznych usług nadawczych przez sieć łączności elektronicznej, z wyjątkiem zakresu, w jakim informacja może się odnosić do możliwego do zidentyfikowania abonenta lub użytkownika otrzymującego informację;

[…]".

6. Artykuł 3 wspomnianej dyrektywy, zatytułowany „Usługi", stanowi:

„Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie, włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych".

7. Artykuł 5 tej dyrektywy, zatytułowany „Poufność komunikacji", stanowi:

„1. Państwa członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności.

[…]

3. Państwa członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem, że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą [95/46] po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla każdego technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika".

8. Zgodnie z art. 6 dyrektywy 2002/58, zatytułowanym „Dane o ruchu":

„1. Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, bez uszczerbku dla przepisów ust. 2, 3 i 5 niniejszego artykułu oraz art. 15 ust. 1.

2. Można przetwarzać dane o ruchu niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich. Przetwarzanie takie jest dozwolone tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym należy uiścić opłatę.

[…]”.

9. Artykuł 15 dyrektywy 2002/58, zatytułowany „Stosowanie niektórych przepisów dyrektywy [95/46]”, stanowi w ust. 1:

„Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy [95/46]. W tym celu państwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa [Unii], w tym zasadami określonymi w art. 6 ust. 1 i 2 [TUE]”.

B. Prawo francuskie

1. Code de la propriété intellectuelle (kodeks własności intelektualnej)

10. Artykuł L. 331-12 code de la propriété intellectuelle (kodeksu własności intelektualnej, zwanego dalej „CPI”), w wersji mającej zastosowanie do sporu w postępowaniu głównym, stanowi:

„La Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie) [zwany dalej »Hadopi«] jest niezależnym organem publicznym”.

11. Artykuł L. 331-13 CPI przewiduje:

„[Hadopi] wypełnia:

[…]

2) zadania w zakresie ochrony [utworów i przedmiotów, z którymi związane jest prawo autorskie lub prawo pokrewne w sieciach łączności elektronicznej] w odniesieniu do naruszeń tych praw w sieciach łączności elektronicznej wykorzystywanych w celu świadczenia usług internetowej komunikacji publicznej; […]”.

12. Zgodnie z art. L. 331-15 CPI:

„W skład [Hadopi] wchodzą kolegium i komisja ochrony praw. […].

[…]

Przy wykonywaniu swoich uprawnień członkowie kolegium i komisji ochrony praw nie otrzymują instrukcji od żadnego organu”.

13. Artykuł L. 331-17 CPI stanowi:

„Zadaniem komisji ochrony praw jest podejmowanie środków przewidzianych w art. L. 331-25".

14. Zgodnie z art. L. 331-21 CPI:

„Dla celów wykonywania zadań przez komisję ochrony praw [Hadopi] dysponuje zaprzysiężonymi urzędnikami, upoważnionymi przez [jego] prezesa na warunkach określonych dekretem wydanym po zasięgnięciu opinii Conseil d'État (rady stanu). […]

Członkowie komisji ochrony praw oraz urzędnicy wymienieni w akapicie pierwszym otrzymują wnioski skierowane do tej komisji na zasadach przewidzianych w art. L. 331-24. Następnie dokonują oni analizy faktów.

Na potrzeby postępowania mogą oni uzyskać wszelkie dokumenty, niezależnie od nośnika, w tym dane przechowywane i przetwarzane przez operatorów łączności elektronicznej na podstawie art. L. 34-1 code des postes et des communications électroniques (kodeksu poczty i łączności elektronicznej) i usługodawców wymienionych w art. 6 ust. I pkt 1 i 2 loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (ustawy nr 2004-575 z dnia 21 czerwca 2004 r. o zaufaniu do gospodarki cyfrowej).

Mogą oni również otrzymać kopię dokumentów, o których mowa w poprzednim akapicie.

Mogą oni w szczególności uzyskać od operatorów łączności elektronicznej dane dotyczące tożsamości, adres pocztowy, adres elektroniczny i numer telefonu abonenta, którego dostęp do usług internetowej komunikacji publicznej został wykorzystany do celów zwielokrotniania, rozpowszechniania, podawania do publicznej wiadomości lub publicznego udostępniania utworów lub przedmiotów objętych ochroną bez zgody właścicieli praw […], o ile jest ona wymagana".

15. Artykuł L. 331-24 CPI stanowi:

„Komisja ochrony praw podejmuje działania na wniosek zaprzysiężonych i zatwierdzonych urzędników […] wyznaczonych przez:

– utworzone zgodnie z prawem organizacje ochrony interesów zawodowych;

– organizacje zbiorowego zarządzania;

– Centre national du cinéma et de l'image animée (krajowe centrum kinematografii i animacji).

Komisja ochrony praw może również działać na podstawie informacji przekazanych jej przez procureur de la République (prokuratora).

Nie rozpatruje ona okoliczności faktycznych które zaszły ponad sześć miesięcy wcześniej".

16. Zgodnie z art. L. 331-25 CPI, który to przepis reguluje tzw. procedurę „stopniowej odpowiedzi”:

„Rozpatrując okoliczności faktyczne mogące stanowić uchybienie obowiązkowi określonemu w art. L. 336-3 [CPI], komisja ochrony praw może wysłać abonentowi […] zalecenie przypominające mu o przepisach art. L. 336-3, nakazujące mu przestrzeganie określonego w nich obowiązku i ostrzegające o grożących sankcjach wynikających z art. L. 335-7 i art. L. 335-7-1. Zalecenie obejmuje również poinformowanie abonenta o zgodnej z prawem ofercie treści kulturalnych w Internecie, o istnieniu środków bezpieczeństwa zapobiegających naruszeniom obowiązku określonego w art. L. 336-3, jak również o zagrożeniach dla rozwoju twórczości artystycznej i dla gospodarki sektora kultury, jakie niosą ze sobą praktyki, które nie respektują praw autorskich i pokrewnych.

W przypadku ponowienia w terminie sześciu miesięcy od daty wysłania zalecenia, o którym mowa w akapicie pierwszym, czynów mogących stanowić uchybienie obowiązkowi określonemu w art. L. 336-3, komisja może skierować nowe zalecenie zawierające takie same informacje jak poprzednie, drogą elektroniczną […]. Do zalecenia dołącza się pismo za potwierdzeniem odbioru lub inne środki pozwalające na wykazanie daty przedstawienia tego zalecenia.

Zalecenia skierowane na podstawie niniejszego artykułu wskazują datę i godzinę, w której zostały stwierdzone okoliczności mogące stanowić uchybienie obowiązkowi określonemu w art. L. 336-3. Natomiast nie ujawniają one treści utworów lub przedmiotów objętych ochroną, których dotyczy to uchybienie. Wskazują one numery telefonu oraz adresy pocztowe i elektroniczne, pod które adresat może, jeśli sobie tego życzy, skierować uwagi do komisji ochrony praw oraz uzyskać, jeśli złoży wyraźne żądanie, wyjaśnienia co do treści utworów lub przedmiotów objętych ochroną, których dotyczy zarzucane mu uchybienie”.

17. Artykuł L. 331-29 CPI stanowi:

„Dozwolone jest tworzenie przez [Hadopi] systemu zautomatyzowanego przetwarzania danych osobowych dotyczących osób, wobec których toczy się postępowanie na podstawie niniejszej podsekcji.

Celem przetwarzania danych jest wdrożenie, przez komisję ochrony praw, przewidzianych w niniejszej podsekcji środków, wszystkich czynności procesowych dotyczących tych środków oraz zasad informowania organizacji ochrony interesów zawodowych i organizacji zbiorowego zarządzania o ewentualnych postępowaniach sądowych i zawiadomieniach przewidzianych w art. L. 335-7 akapit piąty.

Zasady stosowania niniejszego artykułu ustala się w drodze dekretu […]. W szczególności dekretem ustala się:

– kategorie rejestrowanych danych i okres ich przechowywania;

– odbiorców upoważnionych do otrzymywania tych danych, w szczególności osoby, których działalność polega na zapewnianiu dostępu do usług internetowej komunikacji publicznej;

– warunki, na jakich zainteresowane osoby mogą wykonywać wobec [Hadopi] prawo dostępu do danych ich dotyczących […]”.

18. Artykuł R. 331-37 CPI stanowi:

„Operatorzy łączności elektronicznej […] i usługodawcy […] są zobowiązani do przekazywania, poprzez połączenie z zautomatyzowanym przetwarzaniem danych osobowych, o którym mowa w art. L. 331-29, lub za pomocą nośnika zapisu zapewniającego ich integralność i bezpieczeństwo, danych osobowych i informacji wymienionych w pkt 2 załącznika do décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du [CPI] dénommé »Système de gestion des mesures pour la protection des œuvres sur Internet«[4] [dekretu nr 2010-236 z dnia 5 marca 2010 r. w sprawie zautomatyzowanego przetwarzania danych osobowych dopuszczonego w art. L. 331-29 CPI, zwanego »systemem zarządzania środkami ochrony utworów w Internecie« (zwanego dalej »dekretem z dnia 5 marca 2010 r.«)] […] w terminie ośmiu dni od przekazania przez komisję ochrony praw danych technicznych niezbędnych do identyfikacji abonenta, którego dostęp do usług internetowej komunikacji publicznej został wykorzystany w celach zwielokrotniania, rozpowszechniania, udostępniania lub publicznego udostępniania utworów lub przedmiotów objętych ochroną bez zgody właścicieli praw […], jeżeli jest ona wymagana.

[…]".

19. Artykuł R. 335-5 CPI stanowi:

„I. Działanie bez uzasadnionego powodu przez osobę uprawnioną do dostępu do usług internetowej komunikacji publicznej stanowi rażące niedbalstwo zagrożone grzywną przewidzianą w odniesieniu do wykroczeń piątej klasy, gdy spełnione są przesłanki przewidziane w pkt II:

1) niezastosowanie środka zabezpieczającego ten dostęp; lub;

2) niedochowanie należytej staranności przy wdrażaniu tego środka.

II. Przepisy pkt I mają zastosowanie tylko wtedy, gdy spełnione są dwa następujące warunki:

1) na podstawie art. L. 331-25 i w formie przewidzianej w tym artykule komisja ochrony praw zaleciła osobie uprawnionej do dostępu zastosowanie środka zabezpieczającego jego dostęp, umożliwiającego zapobieżenie ponownemu korzystaniu z niego w celu zwielokrotniania, rozpowszechniania, podawania do publicznej wiadomości lub publicznego udostępniania utworów lub przedmiotów objętych ochroną na podstawie prawa autorskiego lub praw pokrewnych bez zgody właścicieli praw […], jeżeli jest ona wymagana;

2) w roku następującym po przedstawieniu tego zalecenia dostęp ten jest ponownie wykorzystywany do celów, o których mowa w ppkt 1 niniejszego pkt II".

20. Artykuł L. 336-3 CPI stanowi:

„Posiadacz dostępu do usług internetowej komunikacji publicznej ma obowiązek zapewnienia, aby dostęp ten nie był wykorzystywany w celach zwielokrotniania, rozpowszechniania, podawania do publicznej wiadomości lub publicznego udostępniania utworów lub przedmiotów objętych

[4] JORF z dnia 7 marca 2010 r., tekst nr 19.

ochroną na mocy prawa autorskiego lub praw pokrewnych bez zgody właścicieli tych praw […], jeżeli jest ona wymagana.

Uchybienie przez posiadacza dostępu obowiązkowi określonemu w akapicie pierwszym nie powoduje powstania odpowiedzialności karnej zainteresowanego […]".

2. Dekret z dnia 5 marca 2010 r.

21. Dekret z dnia 5 marca 2010 r., w brzmieniu mającym zastosowanie do okoliczności faktycznych sporu w postępowaniu głównym, przewiduje w art. 1:

„Przetwarzanie danych osobowych określane jako »system zarządzania środkami ochrony utworów w Internecie« ma na celu wdrożenie przez komisję ochrony praw [Hadopi]:

1) środków przewidzianych w księdze III części legislacyjnej [CPI] (tytuł III rozdział I sekcja 3 podsekcja 3) oraz w księdze III części normatywnej tego kodeksu (tytuł III rozdział I sekcja 2 podsekcja 2);

2) zgłoszeń do procureur de la République (prokuratora) czynów, które mogą stanowić przestępstwa określone w art. L. 335-2, L. 335-3, L. 335-4 i R. 335-5 tego kodeksu, jak również informowania organizacji ochrony interesów zawodowych i organizacji zbiorowego zarządzania o tych zgłoszeniach;

[…]".

22. Artykuł 4 tego dekretu stanowi:

„I.- Do danych osobowych i informacji wymienionych w załączniku do niniejszego dekretu bezpośredni dostęp mają zaprzysiężeni urzędnicy upoważnieni przez prezesa [Hadopi] na podstawie art. L. 331-21 [CPI] i członkowie komisji ochrony praw, o której mowa w art. 1.

II.- Operatorzy łączności elektronicznej i usługodawcy wymienieni w pkt 2 załącznika do niniejszego dekretu otrzymują:

– dane techniczne niezbędne do identyfikacji abonenta;

– zalecenia, o których mowa w art. L. 331-25 [CPI] w celu ich wysłania abonentom drogą elektroniczną;

– informacje niezbędne do wykonania dodatkowych kar zawieszenia dostępu do usług internetowej komunikacji publicznej podane do wiadomości komisji ochrony praw przez procureur de la République (prokuratora).

III.- Organizacje ochrony interesów zawodowych i organizacje zbiorowego zarządzania otrzymują informacje o zgłoszeniach do procureur de la République (prokuratora).

IV.- Organy sądowe otrzymują protokoły ustaleń dotyczących czynów, które mogą stanowić przestępstwa przewidziane w art. L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 i R. 335-5 [CPI].

Wykonanie kary zawieszenia zostaje zgłoszone do zautomatyzowanego rejestru karnego".

23. Załącznik do dekretu z dnia 5 marca 2010 r. przewiduje:

„W ramach przetwarzania określanego jako »system zarządzania środkami ochrony utworów w Internecie« rejestrowane są następujące dane osobowe i informacje:

1) Dane osobowe i informacje pochodzące od utworzonych zgodnie z prawem organizacji ochrony interesów zawodowych, organizacji zbiorowego zarządzania, Centre national du cinéma et de l'image animée (krajowego centrum kinematografii i animacji) oraz informacje pochodzące od procureur de la République (prokuratora):

W odniesieniu do czynów mogących stanowić uchybienie obowiązkowi określonemu w art. L. 336-3 [CPI]:

Data i godzina zdarzeń;

Adres IP zainteresowanych abonentów;

Używany protokół peer-to-peer;

Pseudonim używany przez abonenta;

Informacje dotyczące utworów lub przedmiotów objętych ochroną, których zdarzenia dotyczą;

Nazwa pliku obecnego na urządzeniu abonenta (w stosownych przypadkach);

Dostawca dostępu do Internetu, u którego abonowano dostęp lub który zapewnił zasoby techniczne IP.

[…]

2) Dane osobowe i informacje dotyczące abonenta zebrane od operatorów łączności elektronicznej […] i od usługodawców […]:

Nazwisko, imiona;

Adres pocztowy i adresy elektroniczne;

Dane telefoniczne;

Adres instalacji telefonicznej abonenta;

Dostawca dostępu do Internetu, wykorzystujący zasoby techniczne dostawcy dostępu, o którym mowa w pkt 1, z którym abonent zawarł umowę; numer abonencki;

Data zawieszenia dostępu do usługi internetowej komunikacji publicznej.

[…]".

3. Code des postes et des télécommunications (kodeks pocztowy i telekomunikacyjny)

24. Artykuł L. 34-1 code des postes et des communications électroniques (kodeksu poczty i łączności elektronicznej), zmieniony przez art. 17 loi nº 2021-998 du 30 juillet 2021 (ustawy nr 2021-998 z dnia 30 lipca 2021 r.)[5], stanowi w ust. II bis, że „operatorzy łączności elektronicznej są zobowiązani do przechowywania:

1) dla potrzeb postępowania karnego, zapobiegania zagrożeniom dla bezpieczeństwa publicznego i ochrony bezpieczeństwa narodowego – informacji dotyczących tożsamości cywilnej użytkownika, do upływu pięciu lat od wygaśnięcia jego umowy;

2) dla tych samych celów co wymienione w pkt 1 niniejszego ust. II bis – innych informacji dostarczonych przez użytkownika przy podpisaniu umowy lub utworzeniu konta, jak również informacji o płatności do końca rocznego terminu liczonego od wygaśnięcia umowy lub zamknięcia konta;

3) dla potrzeb zwalczania poważnej przestępczości i poważnych przestępstw, zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego i ochrony bezpieczeństwa narodowego – danych technicznych pozwalających na identyfikację źródła połączenia lub danych dotyczących używanego urządzenia końcowego do końca rocznego okresu liczonego od połączenia lub od użycia urządzenia końcowego”.

III. Postępowanie przed Trybunałem

25. W odpowiedzi na wezwanie skierowane do zainteresowanych stron, o których mowa w art. 23 statutu Trybunału Sprawiedliwości Unii Europejskiej, skarżące w postępowaniu głównym, rządy francuski, duński, estoński, irlandzki, niderlandzki, fiński, szwedzki, a także Komisja Europejska odpowiedziały na pytania pisemne Trybunału.

26. Ci sami uczestnicy, z wyjątkiem rządu fińskiego, oraz rządy czeski, hiszpański, cypryjski, łotewski i norweski, a także Inspektor i ENISA, wzięli udział w rozprawie, która odbyła się w dniu 15 maja 2023 r.

IV. Analiza

27. Na podstawie analizy pytań prejudycjalnych, którą przeprowadziłem w mojej pierwszej opinii, zaproponowałem, aby Trybunał orzekł, że art. 15 ust. 1 dyrektywy 2002/58 należy interpretować w ten sposób, iż nie stoi on na przeszkodzie uregulowaniu krajowemu pozwalającemu na przechowywanie danych przez dostawców usług łączności elektronicznej i na uzyskanie dostępu

[5] JORF z dnia 31 lipca 2021 r., tekst nr 1. Ta wersja art. L. 34-1 tego kodeksu, obowiązująca od dnia 31 lipca 2021 r., została przyjęta w następstwie orzeczenia Conseil d'État (rady stanu, Francja) z dnia 21 kwietnia 2021 r., nr 393099 (JORF z dnia 25 kwietnia 2021 r.), na mocy którego uchylono poprzednią wersję tego przepisu obejmującą obowiązek przechowywania danych osobowych „dla potrzeb badań, wykrywania i ścigania przestępstw lub uchybienia obowiązkowi określonemu w art. L. 336-3 [CPI]” wyłącznie w celu udostępnienia, w razie potrzeby, w szczególności Hadopi. Orzeczeniem nr 2021-976-977 QPC z dnia 25 lutego 2022 r. (A. Habib i in.) Conseil constitutionnel (rada konstytucyjna, Francja) uznała, że ta wcześniejsza wersja art. L. 34-1 tego kodeksu jest sprzeczna z konstytucją francuską głównie ze względu na to, że „zezwalając na ogólne i niezróżnicowane przechowywanie danych dotyczących połączeń, zaskarżone przepisy stanowią nieproporcjonalne naruszenie prawa do poszanowania życia prywatnego” (pkt 13). Sąd ten uznał bowiem, że dane dotyczące połączeń, które powinny być przechowywane na mocy tych przepisów, dotyczą nie tylko identyfikacji użytkowników usług łączności elektronicznej, lecz również innych danych, które „ze względu na ich charakter, ich różnorodność i przetwarzanie, któremu mogą one podlegać […] dostarczają na temat tych użytkowników, a także, w stosownych przypadkach, na temat osób trzecich, licznych i dokładnych informacji, stanowiących szczególne naruszenie ich życia prywatnego” (pkt 11).

do nich przez organ administracyjny taki jak Hadopi [6], ograniczonego do danych dotyczących tożsamości cywilnej odpowiadających adresom IP, tak aby organ ten mógł zidentyfikować posiadaczy tych adresów podejrzanych o popełnienie naruszeń prawa autorskiego i praw pokrewnych i aby mógł podjąć w razie potrzeby działania wobec nich, bez poddania tego dostępu uprzedniej kontroli sądu lub niezależnego organu administracyjnego, jeśli te dane stanowią jedyny środek dochodzenia pozwalający na identyfikację osoby, której adres ten był przypisany w chwili popełnienia przestępstwa.

28. W niniejszej opinii postaram się pogłębić pewne elementy mojej poprzedniej analizy oraz zagadnienia, które były dyskutowane podczas rozprawy przeprowadzonej w dniu 15 maja 2023 r., aby przedstawić przyczyny, dla których podtrzymuję zarówno moją propozycję odpowiedzi na pytania prejudycjalne, jak i rozumowanie, które mnie do niej doprowadziło [7].

29. Ściślej rzecz ujmując, wykażę, że przechowywanie danych dotyczących tożsamości cywilnej odpowiadających adresowi IP i dostęp do nich bez uprzedniej kontroli w celu identyfikacji sprawców przestępstw, jeśli te dane stanowią jedyny środek pozwalający na identyfikację tych sprawców, spełnia wypracowane przez Trybunał wymogi odnoszące się do badania środków przyjmowanych na podstawie art. 15 ust. 1 dyrektywy 2002/58 (zob. śródtytuł B poniżej).

30. Wykażę przy tym, że takie rozstrzygnięcie nie stanowi zwrotu w stawiającym wysokie wymogi i chroniącym prawa podstawowe orzecznictwie wypracowanym przez Trybunał od czasu wyroków Tele2 Sverige i Watson i in. [8] oraz La Quadrature du Net i in. [9], lecz konieczne rozwinięcie tego orzecznictwa, które według mnie wpisuje się w kontynuację wypracowanych przez Trybunał zasad. Nie jest to wyłącznie semantyczne rozróżnienie. Proponowane przeze mnie rozwiązanie nie ma bowiem na celu zakwestionowania istniejącego orzecznictwa, lecz umożliwienie, w imię pewnego pragmatyzmu, dostosowania go do szczególnych, bardzo ściśle oznaczonych okoliczności (zob. śródtytuł C poniżej).

31. W trosce o jasność oraz mając na uwadze, że z dyskusji podczas rozprawy wynikła potrzeba uściśleń w tym względzie, rozpocznę moją analizę od przypomnienia zasad funkcjonowania stosowanego przez Hadopi mechanizmu stopniowej odpowiedzi (zob. śródtytuł A poniżej).

6 W dniu 1 stycznia 2022 r. z Conseil supérieur de l'audiovisuel (CSA, wyższej rady ds. radiofonii i telewizji) i Hadopi powstał Autorité de régulation de la communication audiovisuelle et numérique (Arcom, organ ds. regulacji komunikacji radiowo-telewizyjnej i cyfrowej). Jednakże mając na uwadze okres, w którym miały miejsce okoliczności faktyczne sporu w postępowaniu głównym, w niniejszej opinii będę się odnosił do Hadopi.

7 Podtrzymuję w tym względzie również moją propozycję przeformułowania pytań prejudycjalnych oraz moje rozumienie przedmiotu tych pytań. Chociaż bowiem w pytaniu prejudycjalnym jest mowa wyłącznie o dostępie do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP, kwestia dostępu do tych danych jest nierozerwalnie związana z kwestią ich przechowywania przez dostawców usług łączności elektronicznej, w związku z czym analiza zgodności przechowywania z prawem Unii jest niezbędnym warunkiem wstępnym analizy zgodności dostępu. Jeśli chodzi o to zagadnienie, zob. pkt 45 i nast. mojej pierwszej opinii. Podobnie, mimo że pytania prejudycjalne odnoszą się do „danych dotyczących tożsamości cywilnej odpowiadających adresowi IP", należy rozumieć, że odnoszą się one również do adresów IP pozwalających na identyfikację źródła połączenia. Jeśli chodzi o to zagadnienie, zob. pkt 41 i nast. mojej pierwszej opinii.

8 Wyrok z dnia 21 grudnia 2016 r. (C-203/15 i C-698/15, zwany dalej „wyrokiem Tele2", EU:C:2016:970).

9 Wyrok z dnia 6 października 2020 r. (C-511/18, C-512/18 i C-520/18, zwany dalej wyrokiem „La Quadrature du Net i in.", EU:C:2020:791).

A. Mechanizm stopniowej odpowiedzi stosowany przez Hadopi

32. Hadopi jest niezależnym organem administracyjnym odpowiadającym za ochronę prawa autorskiego i praw pokrewnych przed naruszeniami tych praw popełnianymi w Internecie. W tym celu został stworzony tzw. mechanizm „stopniowej odpowiedzi", którego wdrożenie powierzono komisji ochrony praw przy Hadopi.

33. Komisja ta rozpoznaje wnioski składane przez organizacje zrzeszające uprawnionych, w ramach których niektórzy zaprzysiężeni i zatwierdzeni przez ministre de la Culture (ministra kultury) pełnomocnicy zbierają w sieciach peer-to-peer adresy IP internautów udostępniających publicznie utwory bez zgody właścicieli praw. Sporządzane są wówczas protokoły. Zawierają one między innymi adres IP dostępu do Internetu wykorzystanego do popełnienia tych naruszeń prawa autorskiego, datę i godzinę stwierdzonego naruszenia, a także tytuł utworu, którego dotyczy sprawa. Protokoły są przekazywane komisji ochrony praw przy Hadopi. Należy w tym względzie podkreślić, na co wskazał także Inspektor, że przetwarzanie danych osobowych przez pełnomocników w organizacjach zrzeszających uprawnionych odbywa się na podstawie upoważnienia Commission nationale de l'informatique et des libertés (krajowej komisji ds. informatyki i wolności, CNIL), francuskiego organu kontroli w dziedzinie ochrony danych [10].

34. Po otrzymaniu protokołów oraz po zautomatyzowanej kontroli mającej na celu zapewnienie, że zawierają one wszystkie wymagane dane, komisja ochrony praw przy Hadopi może uzyskać od dostawców usług łączności elektronicznej dane dotyczące tożsamości, adresu pocztowego, adresu elektronicznego i numeru telefonu posiadacza abonamentu, który został wykorzystany do popełnienia przestępstwa przeciwko prawu autorskiemu.

35. Hadopi może wówczas wysłać do takiej osoby „zalecenie", informując ją, że jej dostęp do Internetu został wykorzystany w sposób naruszający prawo autorskie, oraz nakazując, aby osoba podejrzewana o uchybienie obowiązkowi zachowania należytej staranności w zakresie poszanowania w Internecie zasad dotyczących utworów chronionych prawem autorskim lub prawem pokrewnym, podporządkowała się temu obowiązkowi. Innymi słowy, zalecenie jest skierowane do posiadacza dostępu do Internetu, którym w praktyce może być osoba inna niż ta, która udostępniła utwór z naruszeniem prawa autorskiego. W razie ponownego stwierdzenia naruszenia prawa autorskiego z wykorzystaniem tego samego dostępu do Internetu może zostać wydane ponowne zalecenie. W przypadku kolejnych naruszeń komisja ochrony praw przy Hadopi może postanowić o złożeniu zawiadomienia do procureur de la République (prokuratora) w celu wszczęcia postępowania karnego. W tym względzie, jak wskazał rząd francuski w swoich pierwszych uwagach, urzędnicy Hadopi odpowiedzialni za stosowanie mechanizmu stopniowej odpowiedzi są zaprzysiężeni i upoważnieni przez prezesa Hadopi, mają obowiązek zachowania tajemnicy zawodowej oraz jako jedyni w Hadopi są upoważnieni do uzyskania dostępu do danych osobowych przetwarzanych w ramach tego mechanizmu.

36. Muszę w tym względzie wyjaśnić, że zbieranie i przekazywanie do Hadopi nie dotyczy danych wszystkich użytkowników sieci peer-to-peer, gdy ci ostatni ograniczają się do pobierania takich treści [11], lecz wyłącznie danych osób, które udostępniły treści naruszające prawo autorskie, to znaczy *zamieściły* takie treści.

[10] Zobacz w tym względzie uchwałę CNIL nr 2010-225 z dnia 10 czerwca 2010 r., zmieniającą upoważnienie do wdrożenia przez Société des auteurs compositeurs et éditeurs de musique (SACEM, spółkę twórców, kompozytorów i wydawców muzycznych) przetwarzania danych osobowych w celu wykrywania i stwierdzania popełnienia przestępstw przeciwko prawom autorskim w sieciach wymiany plików tzw. peer-to-peer (upoważnienie nr 1425421).

[11] Jeśli chodzi o funkcjonowanie sieci peer-to-peer oraz różne profile internautów w tych sieciach, zob. moja opinia w sprawie M.I.C.M. (C-597/19, EU:C:2020:1063, pkt 37 i nast.).

37. Tytułem przykładu, w 2021 r. Hadopi otrzymał prawie cztery miliony protokołów od organizacji zrzeszających uprawnionych, przesłał 210 595 pierwszych zaleceń i 53 564 ponownych zaleceń, a w 1484 przypadkach złożył zawiadomienia do procureur de la République (prokuratora).

38. Po przypomnieniu tych okoliczności wykażę, w jaki sposób ten mechanizm, zakładający przechowywanie danych dotyczących tożsamości cywilnej odpowiadających adresom IP i dostęp do nich, moim zdaniem spełnia wymogi orzecznicze odnoszące się do środków krajowych przyjmowanych na podstawie art. 15 ust. 1 dyrektywy 2002/58.

B. Zgodność z wymogami wynikającymi z orzecznictwa Trybunału dotyczącego wykładni art. 15 ust. 1 dyrektywy 2002/58

39. Ponieważ już w mojej pierwszej opinii przypomniałem orzecznictwo Trybunału dotyczące przechowywania adresów IP przypisywanych do źródła połączenia i dostępu do nich [12], w niniejszej opinii skupię się na tym, co w mojej ocenie stanowi istotę tego orzecznictwa, a mianowicie, po pierwsze, na wymogu proporcjonalności, a po drugie, jeśli chodzi o dostęp do tych danych, na ewentualnej konieczności uprzedniej kontroli przez sąd lub niezależny organ administracyjny.

1. W przedmiocie proporcjonalności rozpatrywanego środka

40. Aby ustalić, czy dany środek obejmujący przechowywanie danych dotyczących tożsamości cywilnej odpowiadających adresowi IP i dostęp do nich jest zgodny z prawem Unii, należy, jak wielokrotnie podkreślał Trybunał, pogodzić ze sobą różne wchodzące w rachubę uzasadnione interesy i prawa, jakimi są, z jednej strony, prawo do ochrony życia prywatnego i ochrony danych osobowych [13] gwarantowane na mocy art. 7 i 8 karty, a z drugiej strony, ochrona praw i wolności innych osób oraz praw zapisanych w art. 3, 4, 6 i 7 karty [14]. Dodam, że w niniejszej sprawie prawo do ochrony życia prywatnego i prawo do ochrony danych osobowych należy również pogodzić z zapisanym w art. 17 karty prawem własności, ponieważ mechanizm stopniowej odpowiedzi służy in fine ochronie prawa autorskiego i praw pokrewnych.

41. Trybunał wyjaśnia w tej kwestii, że pogodzenie interesów w myśl art. 15 ust. 1 dyrektywy 2002/58 umożliwia państwom członkowskim przyjmowanie środków stanowiących odstępstwa od zasady poufności, w sytuacji gdy dany środek jest „*niezbędny, właściwy i proporcjonalny* w ramach społeczeństwa demokratycznego” (wyróżnienie własne). Motyw 11 tej dyrektywy wskazuje, iż środek tego rodzaju musi być „ściśle” *współmierny* do zamierzonego celu [15].

[12] Punkt 53 i nast. mojej pierwszej opinii.

[13] Wyrazem prawa do ochrony życia prywatnego i ochrony danych osobowych w kontekście dyrektywy 2002/58 jest ustanowiona w niej zasada poufności komunikacji i zakaz przechowywania związanych z tą sferą danych.

[14] Wyroki: La Quadrature du Net i in. (pkt 120–122, 127, 128); z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in. (C-140/20, zwany dalej „wyrokiem Commissioner of An Garda Síochána i in.”, EU:C:2022:258, pkt 48 i 50); z dnia 20 września 2022 r., SpaceNet i Telekom Deutschland (C-793/19 i C-794/19, zwany dalej wyrokiem „SpaceNet i Telekom Deutschland”, EU:C:2022:702, pkt 63, 65).;

[15] Wyroki: La Quadrature du Net i in. (pkt 129); Commissioner of An Garda Síochána i in. (pkt 51); SpaceNet i Telekom Deutschland (pkt 66).

42. Ponadto Trybunał odwołuje się do zasady proporcjonalności w całym toku swojego rozumowania odnoszącego się do wykładni art. 15 ust. 1 dyrektywy 2002/58, a zatem czyni z niej kluczowy element badania przyjętego na podstawie tego przepisu środka krajowego, dotyczącego przechowywania danych osobowych lub dostępu do nich.

43. Bardziej pogłębiona analiza tego rozumowania pozwala stwierdzić, że w kontekście art. 15 ust. 1 dyrektywy 2002/58 zasada proporcjonalności obejmuje różne aspekty dotyczące, po pierwsze, wagi ingerencji w prawa podstawowe, która wynika z przechowywania lub dostępu do danych o ruchu, a po drugie, konieczności rozpatrywanego środka.

44. Jeśli chodzi o przechowywanie przez Hadopi danych dotyczących tożsamości cywilnej odpowiadających adresom IP i dostęp do nich, jestem zdania, że zarówno waga ingerencji, jak i niezbędny charakter tych danych powinny skłonić Trybunał do zniuansowania jego analizy proporcjonalności środka krajowego przyjętego na podstawie art. 15 ust. 1 dyrektywy 2002/58.

a) Waga ingerencji w prawa podstawowe

45. Z utrwalonego orzecznictwa Trybunału wynika jasno, że zgodnie z zasadą proporcjonalności znaczenie celu przyświecającego środkowi przyjętemu na podstawie art. 15 ust. 1 dyrektywy 2002/58 musi pozostawać w związku z wagą ingerencji, która z niego wynika [16].

46. Ściślej rzecz ujmując, Trybunał orzekł, jak podkreśliłem w mojej pierwszej opinii, że w dziedzinie zapobiegania przestępstwom, ich dochodzenia, wykrywania i ścigania poważną ingerencję może uzasadniać jedynie cel w postaci zwalczania przestępczości, która również powinna być kwalifikowana jako poważna [17].

47. Jeśli chodzi o adresy IP, Trybunał uznaje, że chociaż wykazują one mniejszy stopień wrażliwości niż inne dane o ruchu, to ich przechowywanie i analizowanie poważnie ingeruje w prawa podstawowe, ponieważ dane te mogą być wykorzystywane do wyczerpującego prześledzenia poruszania się internauty w sieci, a tym samym pozwalają na ustalenie jego szczegółowego profilu oraz na wyciągnięcie dokładnych wniosków na temat jego życia prywatnego [18].

48. W sprawie w postępowaniu głównym przechowywanie danych dotyczących tożsamości cywilnej odpowiadających adresowi IP i dostęp do nich ma na celu zwalczanie naruszeń prawa autorskiego i praw pokrewnych. Według mnie jest zatem jasne, że zwalczanie tych zjawisk nie może być określone mianem walki z poważną przestępczością [19], nawet jeżeli skala tych naruszeń ma charakter masowy. Istnieje zatem rozdźwięk między wagą ingerencji w prawa podstawowe, wynikającą z rozpatrywanego środka, a celem, jakiemu on służy.

[16] Wyroki: Commissioner of An Garda Síochána i in. (pkt 56); SpaceNet i Telekom Deutschland (pkt 71).

[17] Wyroki: Tele2 (pkt 115); z dnia 2 października 2018 r., Ministerio Fiscal (C-207/16, EU:C:2018:788, pkt 56); z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, zwany dalej „wyrokiem Prokuratuur”, EU:C:2021:152, pkt 33). Zobacz również pkt 92 mojej pierwszej opinii.

[18] Zobacz wyroki: La Quadrature du Net i in. (pkt 152, 153); Commissioner of An Garda Síochána i in. (pkt 73); SpaceNet i Telekom Deutschland (pkt 103). Zobacz również pkt 63, 64 i 93 mojej pierwszej opinii.

[19] W mojej pierwszej opinii wskazałem, że pojęcie „poważnej przestępczości” powinno być interpretowane w sposób autonomiczny, aby uniemożliwić państwom członkowskim obchodzenie wymogów ustanowionych w art. 15 ust. 1 dyrektywy 2002/58. Podtrzymuję to stanowisko. Pragnę jednakże podkreślić, że nawet gdyby Trybunał miał orzec, iż zdefiniowanie pojęcia „poważnej przestępczości” pozostawiono państwom członkowskim, pojęcie to powinno w każdym razie być określone w granicach prawa Unii i nie może ulegać rozszerzeniu w stopniu powodującym pozbawienie treści tego przepisu.

49. W mojej pierwszej opinii uznałem, zgodnie z orzecznictwem Trybunału, że posiadanie przez Hadopi dostępu do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP niewątpliwie stanowi poważną ingerencję w prawa podstawowe. Chociaż uznałem również, że mimo to przechowywanie tych danych i dostęp do nich powinien być dopuszczalny, w następstwie rozprawy pragnę poczynić kilka uściśleń.

50. Mechanizm stopniowej odpowiedzi umożliwia Hadopi powiązanie zgłoszonego przez organizacje zrzeszające uprawnionych adresu IP osoby podejrzewanej o wykorzystanie dostępu do Internetu w celu popełnienia naruszenia prawa autorskiego w sieci peer-to-peer, z tożsamością cywilną tej osoby oraz z fragmentem pliku, który został zamieszczony z naruszeniem prawa autorskiego. Jak wskazali Komisja i Inspektor podczas rozprawy, takie elementy, mimo że z pewnością umożliwiają uzyskanie większego zakresu informacji niż sama tożsamość domniemanego sprawcy przestępstwa, nie prowadzą jednak do wyciągnięcia bardzo szczegółowych wniosków na temat życia prywatnego tej osoby. Jak bowiem wskazałem w mojej pierwszej opinii[20], chodzi wyłącznie o incydentalne ujawnienie przeglądanych treści, które ujmowane z osobna nie mogą umożliwić ustalenia szczegółowego profilu osoby, która dokonywała tych czynności.

51. Jest tak, tym bardziej że przede wszystkim przeważającą większość zgłaszanych do Hadopi adresów IP stanowią tak zwane „dynamiczne" adresy IP, które ze swej natury są zmienne i odpowiadają konkretnej tożsamości wyłącznie w jednym momencie, który pokrywa się z udostępnieniem rozpatrywanych treści. Adresy takie wykluczają zatem możliwość wyczerpującego śledzenia.

52. Następnie pragnę podkreślić, że nie wydaje mi się, aby ochrona praw podstawowych w Internecie mogła uzasadniać uniemożliwienie uzyskania samych danych dotyczących adresu IP, do treści utworu oraz do tożsamości osoby, która go udostępniła z naruszeniem prawa autorskiego, a gwarancje powinny dotyczyć wyłącznie przechowywania i dostępu do tych ostatnich. W mojej ocenie analogia ze światem rzeczywistym jest w tym względzie wymowna: osoba podejrzana o kradzież nie może powoływać się na przysługujące jej prawo do ochrony życia prywatnego, aby uniemożliwić osobom prowadzącym dochodzenie w sprawie tego przestępstwa zapoznanie się z przedmiotem kradzieży. Natomiast osoba ta może zasadnie powoływać się na swoje prawa podstawowe w celu uniemożliwienia, w toku postępowania, dostępu do większego zbioru danych niż dane niezbędne do dokonania kwalifikacji prawnej zarzucanego przestępstwa.

53. Pragnę wreszcie wskazać, że wbrew temu, co twierdzą skarżące, mechanizm stopniowej odpowiedzi nie wydaje się prowadzić do uogólnionego nadzoru nad użytkownikami sieci peer-to-peer. Nie chodzi bowiem o weryfikowanie całej ich aktywności w danej sieci w celu ustalenia, czy udostępnili utwór, naruszając prawo autorskie, lecz raczej o ustalenie, w związku z wykryciem pliku naruszającego prawa autorskie, kto jest posiadaczem dostępu do Internetu, który posłużył internaucie do dokonania udostępnienia utworu. Podobnie, jak wskazał Inspektor podczas rozprawy, nie chodzi o nadzór nad aktywnością wszystkich użytkowników sieci peer-to-peer, lecz jedynie nad aktywnością tych osób, które zamieszczają pliki naruszające prawo autorskie, z zastrzeżeniem że zamieszczanie tych plików o tyle mniej ujawnia okoliczności dotyczące życia prywatnego danej osoby, o ile może do niego dochodzić wyłącznie w celu umożliwienia następnie tym internautom pobierania innych plików.

[20] Punkt 101 mojej pierwszej opinii.

54. W tych okolicznościach nie wydaje mi się, aby powody, dla których Trybunał uznał przechowywanie adresów IP i dostęp do nich za poważną ingerencję w prawa podstawowe, były relewantne w przypadku mechanizmu stopniowej odpowiedzi, takiego jak ten stosowany przez Hadopi. Wynika z tego, że przy badaniu zasady proporcjonalności należy zniuansować wagę ingerencji wynikającej z tego przechowywania i tego dostępu.

55. Innymi słowy jestem zdania, że orzecznictwo Trybunału dotyczące wagi ingerencji w prawa podstawowe, spowodowanej przechowywaniem i dostępem do adresów IP, należy interpretować nie w sposób, który oznacza, że ingerencja ta zawsze ma poważny charakter, lecz w sposób wskazujący, że ma ona taki charakter wyłącznie w sytuacji, gdy na podstawie adresów IP można wyczerpująco prześledzić nawigację internauty i wyciągnąć bardzo szczegółowe wnioski co do jego życia prywatnego.

56. Ponieważ sytuacja taka nie zachodzi w postępowaniu głównym, ingerencja wynikająca z przechowywania i dostępu do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP wykorzystanemu do udostępniania treści z naruszeniem prawa autorskiego, powinna być uzasadniona względami zwalczania przestępczości w szerszym znaczeniu niż wyłącznie poważna przestępczość.

57. Pragnę ponadto wyjaśnić, że wagi ingerencji w prawa podstawowe, wynikającej z przechowywania danych dotyczących tożsamości cywilnej odpowiadających adresowi IP i dostępu do nich w sytuacji takiej jak rozpatrywana w postępowaniu głównym, nie zwiększa okoliczność, że posiadacz dostępu do Internetu wykorzystanego w celu udostępnienia treści naruszających prawo autorskie nie zawsze musi być sprawcą tego udostępnienia, przez co skierowane przez Hadopi zalecenie mogłoby skutkować ujawnieniem temu posiadaczowi treści, do której dostęp mogła mieć osoba trzecia. Po pierwsze, przypomnę, że Hadopi prowadzi dochodzenia w sprawie przestępstw polegających na uchybieniu obowiązkowi zapewnienia, aby dostęp do Internetu nie był wykorzystywany w celach udostępniania treści z naruszeniem prawa autorskiego. Niezbędne jest zatem, aby domniemany sprawca przestępstwa otrzymał informacje umożliwiające taką kwalifikację prawną. Po drugie, jak już wskazałem, jestem zdania, że informacje odnoszące się do danego utworu nie umożliwiają wyciągnięcia szczegółowych wniosków na temat życia prywatnego osoby, która udostępniła utwór. Ewentualne przekazanie tych informacji posiadaczowi łącza internetowego nie wykracza zatem poza to, co niezbędne dla umożliwienia prowadzenia dochodzenia w sprawie rozpatrywanego przestępstwa przeciwko prawu autorskiemu.

b) Niezbędność rozpatrywanych danych dla wykrywania i ścigania przestępstwa

58. Aby zapewnić proporcjonalność środka przyjętego na podstawie art. 15 ust. 1 dyrektywy 2002/58, obejmującego przechowywanie danych o ruchu, takich jak dane dotyczące tożsamości cywilnej odpowiadające adresowi IP i dostęp do nich, w myśl orzecznictwa Trybunału konieczne jest, aby wynikająca z niego ingerencja była ograniczona do tego, co ściśle niezbędne dla umożliwienia osiągnięcia zamierzonego celu[21]. Moim zdaniem tak właśnie jest w przypadku środka rozpatrywanego w postępowaniu głównym.

[21] Wyroki: La Quadrature du Net i in. (pkt 120–122, 132); Commissioner of An Garda Síochána i in. (pkt 48, 54); SpaceNet i Telekom Deutschland (pkt 63, 69).

59. Jak podkreśliłem w mojej pierwszej opinii [22], z samego orzecznictwa Trybunału wynika, że w przypadku przestępstwa popełnionego wyłącznie w Internecie, takiego jak naruszenie prawa autorskiego w sieci peer-to-peer, adres IP może stanowić jedyny środek dochodzenia pozwalający na identyfikację osoby, której adres ten był przypisany w chwili popełnienia tego przestępstwa [23]. Moim zdaniem wynika z tego, że przechowywanie danych dotyczących tożsamości cywilnej odpowiadających adresowi IP i dostęp do nich w celu wykrywania i ścigania przestępstw przeciwko prawu autorskiemu popełnionych w Internecie są, w myśl orzecznictwa, ściśle niezbędne do osiągnięcia zamierzonego celu.

60. Prawdą jest, że wszelkie wymogi ochrony danych osobowych zakładają ograniczenie uprawnień w zakresie dochodzenia. Wynika to z samej zasady godzenia sprzecznych interesów i taki rezultat sam w sobie nie może być kwestionowany. Jednakże sytuacja, gdy adres IP jest jedynym sposobem identyfikacji osoby podejrzewanej o popełnienie przestępstwa przeciwko prawu własności intelektualnej w Internecie, różni się od większości przypadków ścigania karnego, w odniesieniu do których Trybunał wskazał, że „skuteczność […] zależy zazwyczaj nie od jednego instrumentu dochodzeniowego, lecz od wszystkich instrumentów dochodzeniowych, jakimi dysponują właściwe organy krajowe w tym celu” [24]. Przyjęcie, że w sytuacji takiej jak rozpatrywana w postępowaniu głównym przechowywanie danych dotyczących tożsamości cywilnej odpowiadających adresom IP i dostęp do nich nie powinny być dopuszczalne, nie prowadziłoby, tak jak każdy środek zapewniający ochronę danych o ruchu, jedynie do ograniczenia uprawnień w zakresie dochodzenia, lecz do pozbawienia organów krajowych jedynego środka pozwalającego na wykrycie i ściganie niektórych przestępstw.

61. Innymi słowy, zgodnie z proponowaną przeze mnie wykładnią art. 15 ust. 1 dyrektywy 2002/58 nie chodzi o umożliwienie – w drodze badania niezbędności takiego środka – przechowywania i dostępu do danych, które jedynie *ułatwiają* wykrycie i ściganie przestępstw, w sytuacji gdy wykrywanie i ściganie tych przestępstw jest możliwe również z wykorzystaniem alternatywnych, choćby mniej skutecznych środków. Chodzi natomiast o umożliwienie przechowywania tych danych i dostępu do nich, gdy są one *niezbędne* w celu identyfikacji osoby podejrzewanej o popełnienie przestępstwa, której ściganie byłoby niemożliwe bez użycia tych środków, ponieważ rozpatrywane dane stanowią jedyny instrument umożliwiający identyfikację internauty w przypadku przestępstwa popełnionego wyłącznie w Internecie.

62. Moim zdaniem taką właśnie wykładnię należy przyjąć, gdyż w przeciwnym razie należałoby zaakceptować okoliczność, że wiele przestępstw nigdy nie będzie ściganych [25].

63. Moim zdaniem z powyższego wynika, że uregulowanie krajowe pozwalające na przechowywanie danych przez dostawców usług łączności elektronicznej i na dostęp do nich przez organ administracyjny, które to czynności są ograniczone do danych dotyczących tożsamości cywilnej odpowiadających adresom IP, jest w pełni proporcjonalne do zamierzonego celu, jakim jest ściganie naruszeń prawa autorskiego i praw pokrewnych w Internecie, o ile waga ingerencji w prawa podstawowe wynikającej z tych czynności jest ograniczona, a dane te stanowią jedyny środek dochodzenia pozwalający na identyfikację osoby, której adres ten był przypisany w chwili popełnienia przestępstwa.

22 Punkt 78 mojej pierwszej opinii.

23 Wyroki: La Quadrature du Net i in. (pkt 154); Commissioner of An Garda Síochána i in. (pkt 73); SpaceNet i Telekom Deutschland (pkt 100).

24 Wyrok Commissioner of An Garda Síochána i in. (pkt 69).

25 Punkt 81 mojej pierwszej opinii. Jeśli chodzi o tę kwestię, zob. również pkt 79 i nast. niniejszej opinii.

64. W związku z tym jestem zdania, że art. 15 ust. 1 dyrektywy 2002/58 należy interpretować w ten sposób, iż nie stoi on na przeszkodzie takiemu uregulowaniu.

2. W przedmiocie istnienia odpowiednich gwarancji materialnych i proceduralnych

65. Jeśli chodzi konkretnie o dostęp do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP, z orzecznictwa Trybunału wynika, że sama tylko proporcjonalność środka nie wystarcza, aby sprawić, iż jest on zgodny z art. 15 ust. 1 dyrektywy 2002/58.

66. Trybunał orzekł bowiem, że aby zapewnić, iż dostęp do danych o ruchu i lokalizacji jest ograniczony do tego, co ściśle niezbędne, istotne jest poddanie tego dostępu uprzedniej kontroli sądu lub niezależnego organu administracyjnego, dysponującego wszelkimi uprawnieniami i gwarancjami niezbędnymi do pogodzenia różnych wchodzących w grę uzasadnionych interesów i praw [26].

67. Dosłowne odczytywanie orzecznictwa prowadziłoby zatem do uznania, że posiadanie przez Hadopi dostępu do danych dotyczących tożsamości cywilnej odpowiadających adresom IP osób podejrzewanych o popełnienie w Internecie przestępstwa przeciwko prawu autorskiemu powinno być uzależnione od takiej uprzedniej kontroli, której brakuje w istniejącym mechanizmie stopniowej odpowiedzi.

68. Jednakże, jak wskazał rząd irlandzki podczas rozprawy i jak stwierdziłem w mojej pierwszej opinii, w mojej ocenie wymóg uprzedniej kontroli sądu lub niezależnego organu administracyjnego nie jest wymogiem stosowanym automatycznie, lecz zależy od bardziej ogólnej analizy rozpatrywanego środka uwzględniającej zarówno wagę wynikającej z niego ingerencji, jak i przewidziane w jego ramach gwarancje.

69. Pragnę bowiem podkreślić, że w każdym z wyroków formułujących ów wymóg uprzedniej kontroli sądu lub niezależnego organu administracyjnego chodziło o uregulowania krajowe umożliwiające dostęp do wszystkich danych o ruchu i danych o lokalizacji użytkowników w odniesieniu do wszystkich środków łączności elektronicznej [27] lub przynajmniej w odniesieniu do telefonów stacjonarnych i komórkowych [28] zidentyfikowanych użytkowników.

70. Wnioskuję z tego, że wymóg takiej uprzedniej kontroli jest uzasadniony wagą rozpatrywanej w tych sprawach ingerencji. Jak wskazał Trybunał, chodziło o dane, które mogą „rzeczywiście pozwolić na wyciągnięcie precyzyjnych, a nawet bardzo precyzyjnych wniosków dotyczących życia prywatnego osób […] takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje towarzyskie i środowiska społeczne, w których osoby te się obracają” [29]. Ponadto sprawa dotyczyła danych osób już zidentyfikowanych i podejrzewanych o popełnienie przestępstwa na podstawie innych poszlak, a zatem rozpatrywane dane umożliwiały wzmocnienie dowodów obciążających danego użytkownika poprzez rozszerzenie zakresu dotyczących go danych.

[26] Wyroki: Tele2 (pkt 120); Prokuratuur (pkt 51, 52); Commissioner of An Garda Síochána i in. (pkt 106, 107).

[27] Wyroki: Tele2; Commissioner of An Garda Síochána i in.

[28] Wyrok Prokuratuur.

[29] Wyrok Prokuratuur (pkt 36).

71. Jak już zauważyłem, jeśli chodzi o uregulowanie rozpatrywane w postępowaniu głównym, waga ingerencji wynikającej z powiązania danych dotyczących tożsamości cywilnej z adresem IP jest znacznie mniejsza niż waga ingerencji wynikającej z dostępu do wszystkich danych o ruchu i lokalizacji danej osoby, ponieważ powiązanie to nie dostarcza żadnych wskazówek umożliwiających wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osoby, której dane dotyczą.

72. Ponadto, jak zauważyłem w mojej pierwszej opinii [30], dane te dotyczą wyłącznie osób, które zgodnie z obiektywnym ustaleniem przez organizacje zrzeszające uprawnionych faktu wykorzystania adresu IP z naruszeniem prawa autorskiego popełniły czyny mogące stanowić uchybienie obowiązkowi zachowania należytej staranności przewidzianemu w art. L. 336-3 CPI. Nie są one uprzednio zidentyfikowane przy pomocy innych środków, ponieważ powiązanie adresu IP z danymi dotyczącymi tożsamości cywilnej jest jedynym środkiem umożliwiającym identyfikację danej osoby. Zatem inaczej niż w sprawach, w których wcześniej orzekał Trybunał, dostęp do tych danych umożliwia nie tyle uzyskanie dodatkowych i dokładnych informacji na temat działań osoby już podejrzewanej na podstawie innych informacji, lecz jedynie wykorzystanie adresu IP, który w przeciwnym wypadku byłby pozbawiony znaczenia. W tych okolicznościach dane, do których dostęp posiada Hadopi, są de facto ograniczone.

73. Według mnie istnieje zasadnicza różnica między dostępem do danych osobowych dotyczących osoby podejrzewanej o popełnienie przestępstwa w celu udowodnienia jej winy a takim dostępem w celu umożliwienia ustalenia tożsamości sprawcy przestępstwa, które zostało już stwierdzone.

74. W mojej ocenie jest tak, tym bardziej że zbieranie adresów IP w sieciach peer-to-peer odbywa się na podstawie uprzedniego upoważnienia, ograniczonego wyłącznie do tych danych, tak że Hadopi nigdy nie posiada nieograniczonego zbioru danych dotyczących internautów podejrzewanych o popełnienie przestępstw przeciwko prawu autorskiemu w Internecie [31].

75. W związku z tym logika leżąca u podstaw wymogu uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny nie znajduje zastosowania w przypadku mechanizmu stopniowej odpowiedzi, takiego jak rozpatrywany w postępowaniu głównym, w związku z czym wymóg taki nie wydaje mi się niezbędny dla zapewnienia, aby wynikająca z tego mechanizmu ingerencja w prawa podstawowe była ograniczona to tego, co ściśle niezbędne.

76. Z powyższego wynika, że uregulowanie krajowe pozwalające niezależnemu organowi administracyjnemu takiemu jak Hadopi na przechowywanie danych dotyczących tożsamości cywilnej odpowiadających adresowi IP i na dostęp do takich danych w celu identyfikacji posiadaczy tych adresów podejrzewanych o naruszenia prawa autorskiego, bez poddania tego dostępu uprzedniej kontroli sądu lub niezależnego organu administracyjnego nie narusza, in fine, zasad wypracowanych przez orzecznictwo Trybunału, jeśli dane te stanowią jedyny środek pozwalający na identyfikację osoby, której adres IP był przypisany w chwili popełnienia przestępstwa, wobec czego art. 15 ust. 1 dyrektywy 2002/58 należy interpretować w ten sposób, iż nie stoi on na przeszkodzie takiemu uregulowaniu.

77. Oprócz tych rozważań odnoszących się konkretnie do sprawy w postępowaniu głównym, chciałbym jeszcze sformułować bardziej ogólne uwagi dotyczące potrzeby wspomnianego rozwinięcia orzecznictwa Trybunału.

30 Punkt 102 mojej pierwszej opinii.

31 Punkt 33 niniejszej opinii.

C. Niezbędne i ograniczone rozwinięcie orzecznictwa

78. Szereg argumentów przemawia za uściśleniem orzecznictwa Trybunału odnoszącego się do przechowywania i dostępu do danych takich jak adresy IP, powiązanych z danymi dotyczącymi tożsamości cywilnej.

79. W pierwszej kolejności, jak już wskazałem [32], w sytuacji rozpatrywanej w postępowaniu głównym, uzyskanie danych odpowiadających adresowi IP jest jedynym środkiem dochodzenia pozwalającym na identyfikację osoby, której adres ten był przypisany w chwili popełnienia przestępstwa.

80. Wynika z tego niezbicie, że gdyby Trybunał miał uznać, iż art. 15 ust. 1 dyrektywy 2002/58 stoi jednak na przeszkodzie przechowywaniu tych danych i dostępowi do nich, organy krajowe zostałyby de facto pozbawione tego jedynego środka umożliwiającego identyfikację, a tym samym nie można byłoby w ogóle ścigać sprawców tych przestępstw [33]. To właśnie sprawiło, że w mojej pierwszej opinii wspomniałem o możliwości systemowej bezkarności w przypadku tych przestępstw [34].

81. Ryzyko systemowej bezkarności nie jest ograniczone do przestępstw przeciwko prawu autorskiemu popełnianych w sieciach peer-to-peer, lecz, jak zauważył rząd czeski podczas rozprawy, obejmuje wszystkie przestępstwa, do których dochodzi wyłącznie w Internecie.

82. Przestępstwa, których sprawcę można zidentyfikować wyłącznie poprzez jego adres IP, nie mogłyby bowiem nigdy być ścigane, a przepisy ustanawiające kary za ich popełnienie nie mogłyby nigdy być stosowane, gdyby zostało orzeczone, że zarówno przechowywanie danych, jak i dostęp do nich są sprzeczne z prawem Unii.

83. Pragnę w tym względzie zauważyć, że prawdą jest, jak wskazały skarżące w postępowaniu głównym, iż inne środki mogłyby teoretycznie umożliwić zidentyfikowanie sprawców niektórych przestępstw popełnianych wyłącznie w Internecie. Skarżące powołują się między innymi na identyfikatory używane w sieciach społecznościowych oraz na dane skojarzone z kontem użytkownika, jego adres poczty elektronicznej, jego numer telefonu lub na ujawnione przez daną osobę okoliczności dotyczące życia prywatnego. Jednakże powiązanie takich danych z tożsamością osoby wymaga pogłębionego dochodzenia, w ramach którego analizowana jest aktywność internauty w sieci. Moim zdaniem posłużenie się takimi środkami dochodzeniowymi, w odróżnieniu od samego adresu IP, może pozwolić na wyciągnięcie bardzo precyzyjnych wniosków na temat życia prywatnego osób, tak że przechowywanie tych danych oraz dostęp do nich byłyby z tego względu sprzeczne z art. 15 ust. 1 dyrektywy 2002/58.

84. W tych okolicznościach dostęp do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP internauty wprawdzie nie jest teoretycznie jedynym środkiem dochodzeniowym umożliwiającym identyfikację osoby będącej posiadaczem tego adresu w chwili popełnienia przestępstwa, lecz jest środkiem umożliwiającym ściganie tej osoby przy najmniejszej ingerencji w jej prawa podstawowe, a jednocześnie pozwalającym uniknąć całkowitej bezkarności.

[32] Punkt 59 niniejszej opinii.

[33] Punkt 62 niniejszej opinii.

[34] Punkt 78 i nast. mojej pierwszej opinii.

85. W drugiej kolejności pragnę ponownie podkreślić, że takie rozwiązanie pozwala moim zdaniem pogodzić dwie linie orzecznictwa Trybunału będące źródłem pewnej niespójności, na którą wskazałem w mojej pierwszej opinii [35] i w opinii w sprawie M.I.C.M. [36], a mianowicie, z jednej strony orzecznictwa odnoszącego się do przechowywania danych i dostępu do nich, a z drugiej strony, orzecznictwa odnoszącego się do udostępniania adresów IP przypisanych do źródła połączenia w ramach powództw o ochronę praw własności intelektualnej wytaczanych przez osoby prywatne.

86. W trzeciej kolejności, o ile orzecznictwo Trybunału od czasu wyroków Tele2 i La Quadrature du Net i in. zasługuje na aprobatę ze względu na to, że umożliwiło wdrożenie systemu chroniącego prawa podstawowe użytkowników usług komunikacji elektronicznej, o tyle jest ono nacechowane pewną kazuistyką. W miarę napływu spraw poddawanych Trybunałowi do rozstrzygnięcia, Trybunał uściślał bowiem stopniowo swoje orzecznictwo, co pozwalało mu analizować różne uregulowania krajowe w świetle art. 15 ust. 1 dyrektywy 2002/58. Jednakże Trybunał nie ma możliwości potencjalnie antycypować wszystkich środków, które mogłyby być przedmiotem analizy w świetle tego przepisu. Świadczy o tym zresztą liczba dotyczących tego przepisu odesłań prejudycjalnych [37] od czasu wyroku Tele2, która według mnie dowodzi trudności, z jakimi mogą mierzyć się sądy krajowe, stosując sformułowane w orzecznictwie Trybunału zasady do sytuacji różniących się od tych, na gruncie których zapadły tamte wyroki [38].

87. Moim zdaniem wynika z tego, że niezbędna jest pewna elastyczność, w sytuacji gdy analizie Trybunału poddawane są środki, które nie mogły być badane w poprzednich wyrokach, takie jak uregulowania odnoszące się do przestępstw, które można ścigać wyłącznie pod warunkiem przechowywania i udostępniania danych dotyczących tożsamości cywilnej odpowiadających adresowi IP, co do których to uregulowań Trybunał nie miał wcześniej sposobności orzekać.

88. Nie chodzi zatem o postulowany przez rząd duński zwrot w orzecznictwie, lecz o przyznanie, że w oparciu o zasady leżące u podstaw tego orzecznictwa, w bardzo ograniczonych okolicznościach, można wywieść bardziej zniuansowane rozstrzygnięcie.

89. Proponowana przeze mnie wykładnia art. 15 ust. 1 dyrektywy 2002/58 umożliwia w istocie przechowywanie danych dotyczących tożsamości cywilnej odpowiadającej adresowi IP oraz dostęp do nich wyłącznie w przypadku ścigania przestępstw, których sprawców nie można byłoby zidentyfikować bez tych danych. Wykładnia ta odnosi się zatem jedynie do przestępstw popełnianych wyłącznie w Internecie i nie podważa sformułowanych w orzecznictwie rozstrzygnięć dotyczących przechowywania danych i dostępu do nich w szerszym zakresie oraz w innych celach.

[35] Punkt 69 i nast. mojej pierwszej opinii.

[36] C-597/19, EU:C:2020:1063.

[37] Wyroki: z dnia 2 października 2018 r., Ministerio Fiscal (C-207/16, EU:C:2018:788); La Quadrature du Net i in.; Prokuratuur; Commissioner of An Garda Síochána i in.; SpaceNet i Telekom Deutschland.

[38] Wielość wniosków o wydanie orzeczeń w trybie prejudycjalnym dotyczących wykładni art. 15 ust. 1 dyrektywy 2002/58 może również wskazywać na swego rodzaju powściągliwość sądów krajowych, jeśli chodzi o stosowanie wypracowanych przez Trybunał zasad do nieco odmiennych sytuacji, z uwagi na specyfikę krajowych porządków prawnych. Jeśli chodzi o tę kwestię, zob. w szczególności I. Cameron, Metadata retention and national security: *Privacy international* and *La Quadrature du Net*, *Common Market Law Review*, 2021, vol. 58, nº 5, s. 1433–1471 ; a także B. Bertrand, L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin?, *Dalloz IP/IT*, 2021, nº 9, s. 468–472. W perspektywie utrzymania owocnego dialogu między Trybunałem a sądami państw członkowskich wydaje mi się zatem tym bardziej istotne, aby Trybunał umiał wykazać się elastycznością, gdy wymagają tego okoliczności. Jak zauważono w piśmiennictwie, wysoki standard ochrony ustanowiony w orzecznictwie Trybunału nie może być realnie skuteczny bez wsparcia ze strony sądów krajowych, które w pierwszej kolejności odpowiadają za jego wdrożenie. Jeśli chodzi o tę kwestię, zob. w szczególności J. Teyssedre, Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Siochana*, *Common Market Law Review*, vol. 60, nº 2, 2023, s. 569–588; J. Sirinelli, La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite, *Revue trimestrielle de droit européen*, vol. 57, nº 2, 2021, s. 313–329.

V. Wnioski

90. W świetle całości powyższych rozważań proponuję, aby na pytania prejudycjalne zadane przez Conseil d'État (radę stanu, Francja) Trybunał udzielił następującej odpowiedzi:

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 związku z 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 pozwalającemu na przechowywanie danych przez dostawców usług łączności elektronicznej i na uzyskanie dostępu do nich przez organ administracyjny, któremu powierzono ochronę prawa autorskiego i praw pokrewnych przed naruszeniami tych praw w Internecie, ograniczonego do danych dotyczących tożsamości cywilnej odpowiadających adresom IP, tak aby organ ten mógł zidentyfikować posiadaczy tych adresów podejrzanych o popełnienie tych naruszeń i aby mógł podjąć w razie potrzeby działania wobec nich, bez poddania tego dostępu uprzedniej kontroli sądu lub niezależnego organu administracyjnego, jeśli te dane stanowią jedyny środek dochodzenia pozwalający na identyfikację osób, którym adresy te były przypisane w chwili popełnienia przestępstwa.