Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
MACIEJA SZPUNARA
przedstawiona w dniu 27 października 2022 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. Kwestia przechowywania i dostępu do niektórych danych użytkowników Internetu nie traci na aktualności i jest przedmiotem wydanych stosunkowo niedawno, lecz licznych już orzeczeń Trybunału.

2. Niniejsza sprawa daje Trybunałowi możliwość ponownego rozważenia tej kwestii w jawiącym się w nowym świetle kontekście walki z naruszeniami praw własności intelektualnej popełnianymi wyłącznie w Internecie.

[1] Język oryginału: francuski.

## II. Ramy prawne

### *A. Prawo Unii*

3. Motywy 2, 6, 7, 11, 22, 26 i 30 dyrektywy 2002/58/WE [2] stanowią:

„(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, 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).

[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. […]”.

4. 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;

[…]".

5. 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".

6. 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".

7. 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.

[…]”.

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

„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. Kodeks własności intelektualnej*

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

„Wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie [zwany dalej »Hadopi«] jest niezależnym organem publicznym”.

10. Artykuł L. 331-13 CPI przewiduje:

„[Hadopi] zapewnia:

[…]

2) Zadania ochronne [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; […]”.

11. Zgodnie z art. L. 331-15 tego kodeksu:

„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”.

12. Artykuł L. 331-17 wspomnianego kodeksu stanowi:

„Zadaniem komisji ochrony praw jest podjęcie środków przewidzianych w art. L. 331-25”.

13. Na podstawie art. L. 331-21 tego kodeksu:

„Dla celów wykonywania zadań przez komisję ochrony praw [»Hadopi«] dysponuje zaprzysiężonymi urzędnikami, upoważnionymi przez [jego] przewodniczącego 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 kodeksu pocztowego oraz łączności elektronicznej i usługodawców wymienionych w art. 6 ust. I pkt 1 i 2 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 odtwarzania, przedstawiania, udostępniania lub publicznego komunikowania utworów lub przedmiotów objętych ochroną bez zgody właścicieli praw […], o ile jest ona wymagana”.

14. Artykuł L. 331-24 CPI stanowi:

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

– instytucje obrony zawodowej utworzone zgodnie z prawem;

– 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 prokuratora republiki.

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

15. Zgodnie z art. L. 331-25 tego kodeksu, to jest przepisem regulującym 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”.

16. Artykuł L. 331-29 wspomnianego kodeksu stanowi:

„Dozwolone jest tworzenie przez [Hadopi] 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 aktów postępowania dotyczących tych środków oraz ustaleń dotyczących informowania organizacji oferujących profesjonalną obronę i organizacji upoważnionych do pobierania i dystrybucji opłat o ewentualnych postępowaniach sądowych oraz zawiadomieniach przewidzianych w art. L. 335-7 akapit piąty.

Dekret […] ustala warunki stosowania niniejszego artykułu. W szczególności dekret ustala:

– 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 korzystać w [Hadopi] z prawa dostępu do danych ich dotyczących […]”

17. Artykuł R. 331-37 tego kodeksu przewiduje:

„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 [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«[4]] […] 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 odtwarzania, przedstawiania, udostępniania lub publicznego komunikowania utworów lub przedmiotów objętych ochroną bez zgody właścicieli praw […], jeżeli jest ona wymagana.

[…]".

18. 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 odtwarzania, przedstawiania, udostępniania lub publicznego komunikowania 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 pkt 1 niniejszego pkt II".

19. Artykuł L. 336-3 tego kodeksu stanowi:

„Posiadacz dostępu do usług internetowej komunikacji publicznej ma obowiązek zapewnienia, aby dostęp ten nie był wykorzystywany w celach odtwarzania, przedstawiania, udostępniania lub publicznego komunikowania utworów lub przedmiotów objętych 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.*

20. 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 o nazwie »System zarządzania środkami ochrony utworów w Internecie« ma na celu wdrożenie przez komisję ochrony praw [Hadopi]:

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

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 prokuratora republiki czynów, które mogą stanowić naruszenia przewidziane w art. L. 335-2, L. 335-3, L. 335-4 i R. 335-5 tego kodeksu, jak również informowania organizacji obrony zawodowej i organizacji zbiorowego zarządzania o tych zgłoszeniach;

[…]".

21. 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 prokuratora republiki.

III. Organizacje obrony zawodowej i organizacje zbiorowego zarządzania otrzymują informacje o zgłoszeniach do prokuratora republiki.

IV. Organy sądowe otrzymują protokoły ustaleń dotyczących czynów, które mogą stanowić naruszenia 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".

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

„Dane osobowe i informacje zarejestrowane w operacjach przetwarzania zwanych »systemem zarządzania środkami ochrony utworów w Internecie« są następujące:

1. Dane osobowe i informacje pochodzące od utworzonych zgodnie z prawem organizacji obrony zawodowej, organizacji zbiorowego zarządzania, krajowego centrum kinematografii i animacji oraz informacje pochodzące od prokuratora republiki:

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. Kodeks pocztowy i telekomunikacyjny*

23. Artykuł L. 34-1 code des postes et des communications électroniques (kodeksu pocztowego oraz łączności elektronicznej), zmienionego poprzez art. 17 ustawy nr 2021-998 z dnia 30 lipca 2021 r.[5], zwanego dalej „CPCE"), 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 walki z przestępczością i poważnymi wykroczeniami, 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 główne, pytania prejudycjalne oraz postępowanie przed Trybunałem

24. Pismem z dnia 12 sierpnia 2019 r. oraz dwoma pismami uzupełniającymi z dnia 12 listopada 2019 r. i z dnia 6 maja 2021 r. La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net i French Data Network wniosły do Conseil d'État (rady stanu, Francja) skargę o stwierdzenie nieważności dorozumianej decyzji, na mocy której premier oddalił ich wniosek o uchylenie dekretu z dnia 5 marca 2010 r., podczas gdy – zdaniem skarżących w postępowaniu głównym – dekret ten i przepisy stanowiące jego podstawę prawną nie tylko nadmiernie naruszają prawa zagwarantowane w konstytucji francuskiej, ale są również sprzeczne z art. 15 dyrektywy 2002/58 oraz z art. 7, 8, 11 i 52 karty.

25. W szczególności skarżący w postępowaniu głównym podnoszą, że dekret z dnia 5 marca 2010 r. i przepisy stanowiące jego podstawę prawną zezwalają na dostęp do danych dotyczących połączeń w sposób nieproporcjonalny do naruszeń prawa autorskiego popełnionych w Internecie i pozbawionych poważnego charakteru, bez uprzedniej kontroli sądu lub organu gwarantującego niezależność i bezstronność.

[5] JORF z dnia 31 lipca 2021 r., tekst nr 1. Ta wersja art. L. 34-1 CPCE, obowiązująca od dnia 31 lipca 2021 r., została przyjęta w następstwie decyzji Conseil d'État (rady stanu, Francja) z dnia 21 kwietnia 2021 r., nr 393099 (JORF z dnia 25 kwietnia 2021 r.), na mocy której odrzucono 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. (M. Habib A. i in.) Conseil constitutionnel (rada konstytucyjna, Francja) uznała, że ta wcześniejsza wersja art. L. 34-1 CPCE jest sprzeczna z konstytucją 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, liczne i dokładne informacje, szczególnie naruszające ich życie prywatne" (pkt 11).

26. W tym względzie sąd odsyłający podkreśla przede wszystkim, że Trybunał w ostatnim wyroku La Quadrature du Net i in.[6] orzekł, iż art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 i art. 52 ust. 1 karty nie stoi na przeszkodzie przepisom ustawodawczym przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania przestępczości i ochrony bezpieczeństwa publicznego uogólnione i niezróżnicowane przechowywanie *danych dotyczących tożsamości cywilnej* użytkowników środków łączności elektronicznej. Takie przechowywanie tych danych jest zatem możliwe bez szczególnego terminu w celu dochodzenia, wykrywania i karania przestępstw w ogóle.

27. Sąd odsyłający wnioskuje z tego, że podniesiony przez skarżących w postępowaniu głównym zarzut dotyczący niezgodności z prawem dekretu z dnia 5 marca 2010 r. w zakresie, w jakim został przyjęty w ramach zwalczania naruszeń pozbawionych poważnego charakteru, musi zostać oddalony.

28. Sąd ten przypomina następnie, że Trybunał w wyroku Tele2 Sverige i Watson[7] orzekł, iż art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 i art. 52 ust. 1 karty należy interpretować w ten sposób, że stoi on na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a w szczególności dostępu właściwych organów krajowych do przechowywanych danych, które to przepisy nie uzależniają przyznania wspomnianego dostępu od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny.

29. Sąd odsyłający wskazuje, że w wyroku Tele2[8] Trybunał wyjaśnił, iż w celu zapewnienia w praktyce pełnej zgodności z tymi warunkami ważne jest, aby dostęp właściwych organów krajowych do zatrzymanych danych był co do zasady, z wyjątkiem należycie uzasadnionych pilnych przypadków, uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, a decyzja tego sądu lub organu była wydawana na uzasadniony wniosek owych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie przestępstwom, ich wykrywanie lub ściganie.

30. Sąd odsyłający podkreśla, że Trybunał przypomniał ten wymóg w wyroku La Quadrature du Net i in.[9] w odniesieniu do zbierania w czasie rzeczywistym danych dotyczących połączeń przez służby wywiadowcze, a także w wyroku Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej)[10], w odniesieniu do dostępu organów krajowych do danych dotyczących połączeń.

31. Sąd ten zauważa wreszcie, że od momentu utworzenia w 2009 r. Hadopi skierował do posiadaczy abonamentów ponad 12,7 mln zaleceń w ramach procedury stopniowej odpowiedzi przewidzianej w art. L. 331-25 CPI, z czego 827 791 w trakcie jednego roku 2019. W tym celu pracownicy komisji ochrony praw Hadopi muszą mieć możliwość zebrania co roku znacznej liczby danych dotyczących tożsamości cywilnej zainteresowanych użytkowników. Uważa on, że biorąc pod uwagę liczbę tych zaleceń, poddanie zbierania tych danych uprzedniej kontroli może uniemożliwiać wdrożenie zaleceń.

6 Zobacz 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, sentencja.

7 Zobacz wyrok z dnia 21 grudnia 2016 r., C-203/15 i C-698/15, zwany dalej „wyrokiem Tele2”, EU:C:2016:970, sentencja.

8 Punkt 120 tego wyroku.

9 Punkt 189 tego wyroku.

10 Wyrok z dnia 2 marca 2021 r., C-746/18, zwany dalej „wyrokiem Prokuratuur”, EU:C:2021:152.

32. W tych okolicznościach Conseil d'État (rada stanu) postanowiła zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) Czy dane dotyczące tożsamości cywilnej odpowiadające adresowi IP należą do danych o ruchu lub lokalizacji podlegających, co do zasady, obowiązkowi uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny posiadający uprawnienia władcze?

2) W razie udzielenia odpowiedzi twierdzącej na pytanie pierwsze i przy uwzględnieniu niskiej wrażliwości danych dotyczących tożsamości cywilnej użytkowników, w tym ich danych kontaktowych – czy dyrektywę [2002/58] [odczytywaną] w świetle [karty] należy interpretować w ten sposób, że stoi ona na przeszkodzie uregulowaniu krajowemu przewidującemu gromadzenie przez organ administracyjny tych danych odpowiadających adresowi IP użytkowników bez uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny posiadający uprawnienia władcze?

3) W razie udzielenia odpowiedzi twierdzącej na pytanie drugie i przy uwzględnieniu niskiej wrażliwości danych dotyczących tożsamości cywilnej, okoliczności, że tylko te dane mogą być gromadzone, wyłącznie w celu zapobiegania naruszeniu obowiązków określonych w sposób precyzyjny, wyczerpujący i restrykcyjny w prawie krajowym, oraz faktu, że systematyczna kontrola dostępu do danych każdego użytkownika sprawowana przez sąd lub osobny organ administracyjny posiadający uprawnienia władcze mogłaby stanowić przeszkodę w realizacji [zadań publicznych] powierzonych niezależnemu organowi administracyjnemu, który sam jest niezależny i który gromadzi dane – czy dyrektywa [2002/58] stoi na przeszkodzie temu, by kontrola była dokonywana zgodnie z dostosowanymi procedurami, takimi jak przeprowadzanie zautomatyzowanej kontroli, w razie potrzeby pod nadzorem służby wewnętrznej organu dającego gwarancje niezależności i bezstronności w stosunku do urzędników odpowiedzialnych za gromadzenie danych?".

33. Skarżący w postępowaniu głównym, rządy francuski, estoński, szwedzki i norweski oraz Komisja Europejska przedstawiły uwagi na piśmie. Owi uczestnicy, z wyjątkiem rządów estońskiego oraz duńskiego i fińskiego, byli reprezentowani na rozprawie, która odbyła się w dniu 5 lipca 2022 r.

## IV. Analiza

### *A. W przedmiocie pytań prejudycjalnych pierwszego i drugiego*

34. Poprzez pytania prejudycjalne pierwsze i drugie, które moim zdaniem należy zbadać łącznie, sąd odsyłający dąży w istocie do ustalenia, czy art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty należy interpretować w ten sposób, że sprzeciwia się on uregulowaniu krajowemu pozwalającemu na uzyskanie – przez organ administracyjny odpowiedzialny za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw popełnionymi w Internecie – dostępu do danych dotyczących tożsamości cywilnej odpowiadających adresom IP, tak aby organ ten mógł zidentyfikować posiadaczy tych adresów podejrzewanych o odpowiedzialność za te naruszenia i mógł w stosownych przypadkach podjąć przeciwko nim działania, przy czym dostęp ten nie podlega uprzedniej kontroli sądu lub niezależnego organu administracyjnego.

## *1. Omówienie zakresu pytań prejudycjalnych*

### *a) Uprzednie zbieranie przez uprawnione podmioty adresów IP*

35. Z postanowienia odsyłającego wynika, że rozpatrywany w postępowaniu głównym mechanizm stopniowej odpowiedzi obejmuje dwie kolejne operacje przetwarzania danych polegające, po pierwsze, na uprzednim zbieraniu przez uprawnione podmioty w sieciach peer-to-peer adresów IP podmiotów naruszających prawo autorskie, a po drugie – na powiązaniu tych adresów IP z tożsamością cywilną osób przez Hadopi po wniesieniu do niego sprawy w celu wysłania zalecenia osobom, których dostęp do usług internetowej komunikacji publicznej został wykorzystany z naruszeniem przepisów prawa autorskiego.

36. Pytania prejudycjalne pierwsze i drugie dotyczą wyłącznie drugiej operacji przetwarzania przeprowadzanej przez Hadopi.

37. Skarżący w postępowaniu głównym utrzymują jednak, że Trybunał powinien zbadać pierwszą operację przetwarzania, ponieważ jeśli te adresy IP zostały uzyskane z naruszeniem przepisów dyrektywy 2002/58, ich wykorzystywanie w ramach drugiej operacji przetwarzania byłoby siłą rzeczy sprzeczne z tymi przepisami.

38. Takie rozumowanie nie jest przekonujące. Artykuł 3 ust. 1 dyrektywy 2002/58 ogranicza swój zakres stosowania do „przetwarzania danych osobowych w związku z dostarczaniem […] usług łączności elektronicznej”. Tymczasem, jak wyjaśnił rząd francuski na rozprawie, uprawnione podmioty uzyskują rozpatrywane adresy IP nie za pośrednictwem dostawców usług łączności elektronicznej, lecz bezpośrednio w Internecie, poprzez zapoznanie się z danymi dostępnymi publicznie.

39. Można zatem jedynie stwierdzić, że uprzednie zbieranie adresów IP przez uprawnione podmioty nie podlega przepisom dyrektywy 2002/58 i, jak podnosi Komisja, może być zatem analizowane w świetle przepisów rozporządzenia (UE) 2016/679[11]. Taka analiza wydaje się zatem moim zdaniem wykraczać poza ramy pytań prejudycjalnych skierowanych do Trybunału, tym bardziej że sąd odsyłający nie przedstawił wyjaśnień dotyczących uprzedniego zbierania, co umożliwiłoby Trybunałowi udzielenie mu użytecznej odpowiedzi.

40. W tych okolicznościach skoncentruję moją analizę na kwestii dostępu Hadopi do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP.

### *b) Powiązanie adresów IP z danymi dotyczącymi tożsamości cywilnej*

41. Pytania prejudycjalne pierwsze i drugie odnoszą się do „danych dotyczących tożsamości cywilnej odpowiadających adresowi IP”, które zdaniem sądu odsyłającego są wrażliwe w niewielkim stopniu. Sąd ten odnosi się w swoim postanowieniu wyłącznie do punktów wyroku Quadrature du Net i in. odnoszących się do przechowywania danych dotyczących tożsamości cywilnej.

[11] Rozporządzenie Parlamentu Europejskiego i Rady 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/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1).

42. Prawdą jest, że w orzecznictwie Trybunału dokonano rozróżnienia między regulacją prawną mającą zastosowanie do przechowywania i dostępu do adresów IP a regulacją prawną mającą zastosowanie do przechowywania i dostępu do danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej, przy czym ta druga jest mniej restrykcyjna niż ta pierwsza [12].

43. Jednakże wydaje mi się, że w niniejszej sprawie, pomimo sformułowania tych dwóch pytań prejudycjalnych, nie chodzi o sam dostęp do danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej, lecz o powiązanie tych danych z adresami IP, którymi dysponuje Hadopi w następstwie ich zebrania i przekazania przez uprawnione podmioty. Jak bowiem podnosi Komisja, dostęp Hadopi do danych dotyczących tożsamości cywilnej ma na celu odblokowanie dostępu do szerszego zbioru danych, w szczególności adresów IP i fragmentów przeglądanych plików, oraz umożliwienie ich wykorzystania. Dane dotyczące tożsamości cywilnej i adresy IP, ujmowane w oderwaniu od siebie, są pozbawione znaczenia dla organów krajowych, ponieważ ani sama tożsamość cywilna, ani sam adres IP nie mogą udzielić informacji na temat działalności osób fizycznych w Internecie, jeżeli nie są one powiązane.

44. Wynika z tego moim zdaniem, że pytania prejudycjalne pierwsze i drugie należy rozumieć jako odnoszące się nie tylko do danych dotyczących tożsamości cywilnej użytkowników środka komunikacji elektronicznej, lecz również do dostępu do adresów IP pozwalającego na identyfikację źródła połączenia.

*c) Przechowywanie adresów IP przez dostawców usług łączności*

45. Prawdą jest, jak podnoszą rząd francuski i Komisja, że pytania prejudycjalne skierowane do Trybunału nie dotyczą formalnie przechowywania danych przez dostawców usług łączności elektronicznej, lecz jedynie dostępu Hadopi do danych dotyczących tożsamości cywilnej odpowiadających adresom IP.

46. Jednakże kwestia dostępu Hadopi do tych danych wydaje mi się w rzeczywistości nierozerwalnie związana z wyprzedzającą ją kwestią przechowywania owych danych przez dostawców usług łączności. Jak podkreślił Trybunał, dane są przechowywane wyłącznie w celu zapewnienia, w stosownych przypadkach, dostępności danych dla właściwych organów krajowych [13]. Innymi słowy, przechowywanie i dostęp do danych nie mogą być postrzegane odrębnie, ponieważ drugie jest zależne od pierwszego.

47. Prawdą jest, że Trybunał zbadał już zgodność z art. 15 ust. 1 dyrektywy 2002/58 uregulowania krajowego dotyczącego samego dostępu przez właściwe organy krajowe do niektórych danych osobowych niezależnie od kwestii zgodności z tym przepisem przechowywania rozpatrywanych danych [14]. Na niniejsze pytania prejudycjalne można byłoby zatem udzielić odpowiedzi abstrahując od kwestii, czy rozpatrywane dane były przechowywane zgodnie z przepisami prawa Unii.

[12] Zobacz wyrok La Quadrature du Net i in., pkt 155, 159.

[13] Zobacz wyrok Tele2, pkt 79.

[14] Zobacz wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 49.

48. Pragnę jednak zauważyć przede wszystkim, że w wyroku Ministerio Fiscal [15] badanie przeprowadzone przez Trybunał w odniesieniu do zgodności z prawem Unii dostępu organów krajowych do pewnych danych osobowych odpowiada ściśle tym samym zasadom, co badanie, które Trybunał przeprowadza w odniesieniu do oceny zgodności z prawem Unii przechowywania tych danych. Trybunał odnosi się bowiem wyłącznie do orzecznictwa wypracowanego w tym ostatnim względzie w celu transponowania go do kwestii dostępu do danych osobowych. Innymi słowy, w braku badania zgodności z prawem Unii przechowywania niektórych danych badanie to zostaje przeniesione na etap badania kwestii dostępu do tych danych, tak że zgodność z prawem tego dostępu zależy in fine od zgodności z prawem przechowywania.

49. Następnie Trybunał wyraźnie wskazał, że dostęp do danych osobowych może zostać przyznany tylko wtedy, gdy dane te są przechowywane przez dostawców usług łączności elektronicznej w sposób zgodny z art. 15 ust. 1 dyrektywy 2002/58 [16] oraz że dostęp do danych osobowych przez osoby prywatne w celu umożliwienia wszczęcia przed sądami cywilnymi postępowania przeciwko naruszeniom prawa autorskiego jest zgodny z prawem Unii jedynie pod warunkiem, że dane te są przechowywane w sposób zgodny z tym przepisem [17].

50. Wreszcie Trybunał orzeka niezmiennie, że dostęp do danych o ruchu i do danych o lokalizacji przechowywanych przez dostawców w zastosowaniu środka przyjętego na podstawie art. 15 ust. 1 dyrektywy 2002/58, co musi mieć miejsce w pełnym poszanowaniu warunków wynikających z orzecznictwa, w którym dokonano wykładni dyrektywy 2002/58, może co do zasady być uzasadniony jedynie celem interesu ogólnego, dla którego dostawcy ci zostali zobowiązani do takiego przechowywania [18]. Innymi słowy, zgodność z prawem Unii dostępu organów krajowych do określonych danych osobowych jest całkowicie zależna od zgodności z prawem Unii przechowywania tych danych.

51. Wynika z tego moim zdaniem, że analiza zgodności z prawem Unii uregulowania krajowego przewidującego dostęp przez organ krajowy do danych osobowych wymaga uprzedniego ustalenia zgodności z prawem Unii przechowywania tych danych.

52. W tych okolicznościach rozpocznę moją analizę od przypomnienia orzecznictwa Trybunału dotyczącego kwestii przechowywania adresów IP przypisywanych do źródła połączenia w celu wykazania jego ograniczeń i zaproponowania dostosowanego schematu rozumienia rozpatrywanego uregulowania.

### *2. Orzecznictwo Trybunału dotyczące wykładni art. 15 ust. 1 dyrektywy 2002/58 w odniesieniu do środków mających na celu przechowywanie adresów IP przypisanych do źródła połączenia*

53. W art. 5 ust. 1 dyrektywy 2002/58 ustanowiono zasadę poufności zarówno łączności elektronicznej („komunikacji [elektronicznej]" jako takiej i „komunikatów"), jak i związanych z nią danych o ruchu, co oznacza w szczególności zakaz – nałożony co do zasady na każdą osobę inną niż użytkownicy – przechowywania tych komunikatów i tych danych bez ich zgody [19].

15 Wyrok z dnia 2 października 2018 r., C-207/16, EU:C:2018:788.

16 Zobacz wyrok Prokuratuur, pkt 29.

17 Zobacz wyrok z dnia 17 czerwca 2021 r., M.I.C.M., C-597/19, EU:C:2021:492, pkt 127–130.

18 Zobacz wyroki: La Quadrature du Net i in., pkt 166; 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 98; z dnia 20 września 2022 r., SpaceNet, C-793/19 i C-794/19, zwany dalej „wyrokiem SpaceNet", EU:C:2022:702, pkt 131.

19 Zobacz wyroki: La Quadrature du Net i in., pkt 107; Commissioner of An Garda Síochána i in., pkt 35; SpaceNet, pkt 52.

54. Jeśli chodzi o przetwarzanie i przechowywanie przez dostawców usług łączności elektronicznej danych o ruchu dotyczących abonentów i użytkowników, art. 6 dyrektywy 2002/58 przewiduje w ust. 1, że dane te muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, zaś w ust. 2 uściśla, że dane o ruchu, które są niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich, można przetwarzać tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym można dochodzić zapłaty. W odniesieniu do danych dotyczących lokalizacji innych niż dane o ruchu art. 9 ust. 1 rzeczonej dyrektywy przewiduje, że dane te mogą być przetwarzane wyłącznie po spełnieniu pewnych warunków i po ich anonimizacji lub za zgodą użytkowników lub abonentów [20].

55. Tak więc, przyjmując dyrektywę 2002/58, prawodawca Unii skonkretyzował prawa określone w art. 7 i 8 karty w taki sposób, że użytkownicy środków łączności elektronicznej mają prawo co do zasady oczekiwać, że ich łączność elektroniczna („komunikacja [elektroniczna]" jako taka i „komunikaty") i związane z nią dane pozostaną anonimowe i nie będą mogły być rejestrowane bez ich zgody [21]. Wobec tego dyrektywa ta nie ogranicza się do określenia ram dostępu do takich danych za pomocą gwarancji mających na celu zapobieganie nadużyciom, ale także ustanawia w szczególności zasadę zakazu ich przechowywania przez osoby trzecie.

56. W tych okolicznościach, w zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim przyjmować środki ustawodawcze mające na celu „ograniczenie zakresu" praw i obowiązków przewidzianych w szczególności w jej art. 5, 6 i 9, wynikających z zasad poufności komunikacji i zakazu przechowywania związanych z nią danych, przepis ten ustanawia wyjątek od ogólnej reguły przewidzianej w szczególności w tych art. 5, 6 i 9 i powinien zatem – zgodnie z utrwalonym orzecznictwem – być ściśle interpretowany. Taki przepis nie może zatem uzasadniać tego, że odstępstwo od zasadniczego obowiązku zapewnienia poufności łączności elektronicznej i danych z nią związanych, a w szczególności od zakazu przechowywania tych danych, przewidzianego w art. 5 wspomnianej dyrektywy, stanie się regułą, gdyż pozbawiłoby to ten przepis jego znaczenia [22].

57. Jeśli chodzi o cele, które mogą uzasadniać ograniczenie praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58, Trybunał orzekł już, że wyliczenie celów dokonane w art. 15 ust. 1 zdanie pierwsze tej dyrektywy ma charakter wyczerpujący, wobec czego środek ustawodawczy przyjęty na podstawie tego przepisu powinien odpowiadać rzeczywiście i ściśle jednemu z tych celów [23].

58. Ponadto z art. 15 ust. 1 zdanie trzecie dyrektywy 2002/58 wynika, że środki przyjmowane przez państwa członkowskie na podstawie tego przepisu muszą przestrzegać zasad ogólnych prawa Unii, do których należy zasada proporcjonalności, i zapewniać poszanowanie praw podstawowych gwarantowanych w karcie. W tym względzie Trybunał orzekł już, że nałożony przez państwo członkowskie na dostawców usług łączności elektronicznej w przepisach krajowych obowiązek przechowywania danych o ruchu w celu udzielenia właściwym organom krajowym dostępu do nich w razie potrzeby budzi wątpliwości co do zgodności nie tylko z art. 7 i 8 karty, dotyczącymi, odpowiednio, ochrony życia prywatnego oraz ochrony danych

[20] Zobacz wyroki: Tele2, pkt 86; La Quadrature du Net i in., pkt 108; Commissioner of An Garda Síochána i in., pkt 38; SpaceNet, pkt 55.

[21] Zobacz wyroki: La Quadrature du Net i in., pkt 109; Commissioner of An Garda Síochána i in., pkt 37; SpaceNet, pkt 54.

[22] Zobacz wyroki: La Quadrature du Net i in., pkt 110, 111; Commissioner of An Garda Síochána i in., pkt 40; SpaceNet, pkt 57.

[23] Zobacz wyroki: La Quadrature du Net i in., pkt 112; Commissioner of An Garda Síochána i in., pkt 41; SpaceNet, pkt 58.

osobowych, lecz również z art. 11 karty, dotyczącym wolności wypowiedzi, ponieważ ta wolność stanowi jeden z istotnych fundamentów pluralistycznego i demokratycznego społeczeństwa, zaliczając się do wartości, na jakich zgodnie z art. 2 TUE opiera się Unia [24].

59. Niemniej jednak w zakresie, w jakim art. 15 ust. 1 dyrektywy 2002/58 pozwala państwom członkowskim na ograniczenie praw i obowiązków przewidzianych w art. 5, 6 i 9 tej dyrektywy, przepis ten odzwierciedla okoliczność, że prawa ustanowione w art. 7, 8 i 11 karty nie wydają się stanowić prerogatyw o charakterze absolutnym, lecz należy je rozważać z uwzględnieniem ich funkcji społecznej. Jak bowiem wynika z art. 52 ust. 1 karty, dopuszcza ona ograniczenia wykonywania tych praw, o ile ograniczenia te są przewidziane ustawą, szanują istotę omawianych praw oraz – z zastrzeżeniem zasady proporcjonalności – są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. A zatem wykładnia art. 15 ust. 1 dyrektywy 2002/58 w świetle karty wymaga uwzględnienia również znaczenia praw ustanowionych w art. 3, 4, 6 i 7 karty oraz znaczenia, jakie mają cele ochrony bezpieczeństwa narodowego i walki z poważną przestępczością, przyczyniające się do ochrony praw i wolności innych osób [25], z których mogą wynikać pozytywne obowiązki ciążące na organach publicznych [26].

60. W obliczu tych różnych obowiązków do podjęcia określonych działań należy zatem pogodzić ze sobą różne wchodzące w rachubę uzasadnione interesy i prawa. W tych ramach z samego brzmienia art. 15 ust. 1 zdanie pierwsze dyrektywy 2002/58 wynika, że państwa członkowskie mogą uchwalić środek stanowiący odstępstwo od zasady poufności komunikacji, gdy taki środek jest „niezbędny, właściwy i proporcjonalny w ramach społeczeństwa demokratycznego", gdyż motyw 11 tej dyrektywy wskazuje w tym celu, iż środek tego rodzaju musi być „ściśle" proporcjonalny do zamierzonego celu [27].

61. W tym względzie z orzecznictwa Trybunału wynika, że możliwość uzasadnienia przez państwa członkowskie ograniczenia praw i obowiązków przewidzianych w szczególności w art. 5, 6 i 9 dyrektywy 2002/58 należy oceniać poprzez przeprowadzenie badania wagi ingerencji, jaką stanowi takie ograniczenie, oraz sprawdzenie, czy znaczenie celu interesu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi [28].

62. Pragnę ponadto zauważyć, że Trybunał rozróżnia w swoim orzecznictwie z jednej strony ingerencje wynikające z dostępu do danych, które jako takie dostarczają dokładnych informacji o rozpatrywanych przypadkach komunikacji elektronicznej, a zatem na temat życia prywatnego osoby, i w odniesieniu do których system przechowywania danych jest rygorystyczny, a z drugiej strony ingerencje wynikające z dostępu do danych, które mogą dostarczać takich informacji tylko wtedy, gdy zostaną powiązane z innymi danymi, takimi jak adresy IP [29].

63. W odniesieniu w szczególności do adresów IP Trybunał wskazał zatem, że są one generowane bez związku z określonym przypadkiem komunikacji elektronicznej i służą przede wszystkim identyfikowaniu przez dostawców usług łączności elektronicznej osoby fizycznej będącej właścicielem urządzenia końcowego, poprzez które odbywa się komunikacja za pośrednictwem

[24] Zobacz wyroki:La Quadrature du Net i in., pkt 113, 114; Commissioner of An Garda Síochána i in., pkt 42; SpaceNet, pkt 60.

[25] Zobacz wyroki: La Quadrature du Net i in., pkt 120–122; Commissioner of An Garda Síochána i in., pkt 48; SpaceNet, pkt 63.

[26] Zobacz wyroki: La Quadrature du Net i in., pkt 120–122; Commissioner of An Garda Síochána i in., pkt 49; SpaceNet, pkt 64.

[27] Zobacz wyroki: La Quadrature du Net i in., pkt 127–129; Commissioner of An Garda Síochána i in., pkt 50, 51; SpaceNet, pkt 65, 66.

[28] Zobacz wyroki: La Quadrature du Net i in., pkt 131; Commissioner of An Garda Síochána i in., pkt 53; SpaceNet, pkt 68.

[29] Zobacz pkt 41 i nast. niniejszej opinii.

Internetu. I tak, skoro przechowywane są jedynie adresy IP źródła danego przypadku komunikacji elektronicznej, a nie adresy jej odbiorcy, ta kategoria danych wykazuje mniejszy stopień wrażliwości niż inne dane o ruchu [30].

64. Trybunał podkreśla jednocześnie, że skoro adresy IP mogą być wykorzystywane w szczególności do wyczerpującego prześledzenia poruszania się internauty w sieci, a w konsekwencji jego działalności w Internecie, dane te pozwalają na ustalenie jego szczegółowego profilu oraz na wyciągnięcie dokładnych wniosków na temat życia prywatnego użytkownika. Tak więc przechowywanie i analizowanie wspomnianych adresów IP stanowi *poważną* ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty i może mieć zniechęcające skutki dla wykonywania wolności wypowiedzi zagwarantowanej w art. 11 karty [31].

65. Jednakże zgodnie z utrwalonym orzecznictwem do celów koniecznego pogodzenia rozpatrywanych praw i uzasadnionych interesów, wymaganego przez orzecznictwo, należy uwzględnić okoliczność, że w przypadku przestępstwa popełnionego w Internecie adres IP może stanowić jedyny środek pozyskiwania dowodów umożliwiający ustalenie tożsamości osoby, której adres ten był przypisany w chwili popełnienia tego przestępstwa [32].

66. Wobec tego Trybunał orzekł, że środek ustawodawczy przewidujący uogólnione i niezróżnicowane przechowywanie jedynie adresów IP przypisanych do źródła połączenia nie wydaje się co do zasady sprzeczny z art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 karty, oraz z art. 52 ust. 1 karty, ponieważ możliwość ta musi być uzależniona od ścisłego spełnienia przesłanek materialnych i proceduralnych, które winny regulować wykorzystywanie tych danych, i mając na uwadze, że ze względu na poważny charakter ingerencji, jaką pociąga za sobą to przechowywanie, jedynie walka z *poważną przestępczością* i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego mogą, podobnie jak ochrona bezpieczeństwa narodowego, uzasadniać tę ingerencję [33].

67. Trybunał uściśla ponadto, że okres przechowywania nie może przekraczać okresu ściśle niezbędnego w świetle zamierzonego celu, a środek tego rodzaju powinien przewidywać ścisłe warunki i gwarancje dotyczące wykorzystywania tych danych [34].

### *3. Ograniczenia orzecznictwa dotyczącego wykładni art. 15 ust. 1 dyrektywy 2002/58 w odniesieniu do przepisów mających na celu przechowywanie adresów IP przypisanych do źródła połączenia*

68. Rozwiązanie wypracowane przez Trybunał w odniesieniu do przepisów krajowych mających na celu przechowywanie adresów IP przypisanych do źródła połączenia, interpretowanych w świetle art. 15 ust. 1 dyrektywy 2002/58, wydaje się jednak wiązać z dwojakiego rodzaju zasadniczymi trudnościami.

30 Zobacz wyrok La Quadrature du Net i in., pkt 152.

31 Zobacz wyroki: La Quadrature du Net i in., pkt 153; Commissioner of An Garda Síochána i in., pkt 73; SpaceNet, pkt 103 (wyróżnienie moje).

32 Zobacz wyroki: La Quadrature du Net i in., pkt 154; Commissioner of An Garda Síochána i in., pkt 73; SpaceNet, pkt 103.

33 Zobacz wyroki: La Quadrature du Net i in., pkt 155, 156; Commissioner of An Garda Síochána i in., pkt 74; SpaceNet, pkt 104, 105 (wyróżnienie moje).

34 Zobacz wyroki: La Quadrature du Net i in., pkt 156; SpaceNet, pkt 105.

*a) Kwestia zgodności z orzecznictwem dotyczącym udostępniania adresów IP przypisanych do źródła połączenia w ramach powództw o ochronę praw własności intelektualnej*

69. W pierwszej kolejności, jak już wskazałem w mojej opinii w sprawie M.I.C.M. [35], istnieje pewne napięcie między tą linią orzeczniczą a linią dotyczącą udostępniania adresów IP w ramach powództw o ochronę praw własności intelektualnej podmiotom tych praw, która akcentuje obowiązek zapewnienia przez państwa członkowskie podmiotom praw autorskich rzeczywistych możliwości dochodzenia roszczeń odszkodowawczych wynikających z naruszenia tych praw [36].

70. Jeśli chodzi bowiem o tę drugą linię orzeczniczą, Trybunał orzeka w sposób utrwalony, że prawo Unii nie stoi na przeszkodzie ustanowieniu przez państwa członkowskie obowiązku przekazania prywatnym osobom danych osobowych w celu umożliwienia wszczęcia przed sądami cywilnymi postępowania przeciwko naruszeniom prawa autorskiego [37].

71. Trybunał wskazuje w tym względzie, że możliwość ustanowienia przez państwa członkowskie obowiązku ujawnienia w ramach postępowań cywilnych danych osobowych wynika przede wszystkim z możliwości takiego ujawnienia w kontekście ścigania przestępstw [38], która została następnie rozszerzona na postępowania cywilne.

72. Jednocześnie, jeśli chodzi o adresy IP, Trybunał wymaga jednak, aby dane te mogły być przechowywane jedynie w ramach walki z poważną przestępczością i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego [39].

73. Próby pogodzenia tych dwóch linii orzeczniczych prowadzą moim zdaniem do nieodpowiednich rezultatów i nie są przekonujące.

74. Z jednej strony, wbrew temu, co twierdził rząd francuski na rozprawie, zwalczanie naruszeń praw własności intelektualnej nie może być objęte zakresem walki z poważną przestępczością. Pojęcie „poważnej przestępczości" należy moim zdaniem interpretować w sposób autonomiczny. Nie może ono zależeć od koncepcji każdego państwa członkowskiego, gdyż w przeciwnym razie umożliwiłoby to obejście wymogów określonych w art. 15 ust. 1 dyrektywy 2002/58 w zależności od tego, czy państwa członkowskie przyjmują mniej lub bardziej szeroką koncepcję walki z poważną przestępczością. Tymczasem, jak już wskazałem, interesów związanych z ochroną praw własności intelektualnej nie można mylić z interesami leżącymi u podstaw walki z poważną przestępczością [40].

75. Z drugiej strony, dopuszczenie przekazania adresów IP podmiotom praw własności intelektualnej w ramach postępowań mających za przedmiot ich ochronę, podczas gdy ich przechowywanie jest możliwe jedynie w ramach walki z poważną przestępczością, byłoby wyraźnie sprzeczne z orzecznictwem Trybunału dotyczącym przechowywania danych dotyczących połączeń i sprowadzałoby się do pozbawienia skuteczności (effet utile) warunków wymaganych do przechowywania takich danych, ponieważ w każdym razie można byłoby uzyskać do nich dostęp z innych powodów.

35 C-597/19, EU:C:2020:1063, pkt 98.

36 Zobacz moja opinia w sprawie M.I.C.M., C-597/19, EU:C:2020:1063, pkt 97.

37 Zobacz wyroki: z dnia 19 kwietnia 2012 r., Bonnier Audio i in., C-461/10, EU:C:2012:219, pkt 55; z dnia 4 maja 2017 r., Rīgas satiksme, C-13/16, EU:C:2017:336, pkt 34; z dnia 17 czerwca 2021 r., M.I.C.M., C-597/19, EU:C:2021:492, pkt 47–54.

38 Zobacz podobnie wyrok z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 50–52.

39 Zobacz pkt 65 niniejszej opinii.

40 Zobacz moja opinia w sprawie M.I.C.M., C-597/19, EU:C:2020:1063, pkt 103.

76. Wynika z tego moim zdaniem, że przechowywanie adresów IP w celu ochrony praw własności intelektualnej oraz ich udostępnianie podmiotom tych praw w ramach postępowań mających za przedmiot tę ochronę może być sprzeczne z art. 15 ust. 1 dyrektywy 2002/58, zgodnie z jego wykładnią dokonaną w orzecznictwie Trybunału. Obowiązek przekazywania osobom prywatnym danych osobowych w celu umożliwienia wszczęcia przed sądami cywilnymi postępowania przeciwko naruszeniom prawa autorskiego, choć umożliwiony przez sam Trybunał, jest więc w tym samym czasie neutralizowany przez jego własne orzecznictwo dotyczące przechowywania adresów IP przez dostawców usług łączności elektronicznej.

77. Takie rozwiązanie nie jest jednak satysfakcjonujące, ponieważ podważałoby równowagę różnych wchodzących w grę interesów, którą Trybunał starał się zachować, pozbawiając właścicieli praw własności intelektualnej głównego, jeśli nie jedynego sposobu zidentyfikowania sprawców naruszeń tych praw w Internecie. Stwierdzenie to prowadzi mnie do wyjaśnienia drugiej trudności, która może moim zdaniem wynikać z orzecznictwa Trybunału w odniesieniu do przepisów krajowych mających na celu przechowywanie adresów IP przypisanych do źródła połączenia, interpretowanych w świetle art. 15 ust. 1 dyrektywy 2002/58.

*b) Kwestia ryzyka systemowej bezkarności w odniesieniu do przestępstw popełnianych wyłącznie w Internecie*

78. Tak więc, w drugiej kolejności, jestem zdania, że rozwiązanie to jest źródłem praktycznych trudności. Jak podkreśla sam Trybunał, w przypadku przestępstwa popełnionego wyłącznie w Internecie adres IP może stanowić jedyny środek dochodzenia pozwalający na identyfikację osoby, której adres ten był przypisany w chwili popełnienia tego przestępstwa.

79. Niemniej jednak wydaje mi się, że element ten nie jest w pełni brany pod uwagę przy wyważaniu wchodzących w grę interesów. Skoro Trybunał ogranicza jednak możliwość przechowywania adresów IP do ram walki z poważną przestępczością, jednocześnie wyklucza on możliwość przechowywania tych danych w celu zwalczania przestępstw w ogólności, chociaż niektórym z tych przestępstw można zapobiec lub je wykryć czy ukarać ich sprawców jedynie dzięki wspomnianym danym.

80. Innymi słowy, orzecznictwo Trybunału mogłoby prowadzić do pozbawienia organów krajowych jedynego środka identyfikującego sprawców przestępstw popełnionych w Internecie, nienależących jednak do poważnej przestępczości, takich jak naruszenia praw własności intelektualnej. Wynikałaby z tego de facto systemowa bezkarność w przypadku przestępstw popełnionych wyłącznie w Internecie, nie tylko zresztą samych naruszeń praw własności intelektualnej. Myślę w szczególności o aktach zniesławienia popełnionych w Internecie. Prawo Unii przewiduje wprawdzie nakazy przeciwko pośrednikom, których usługi są używane do popełniania takich przestępstw[41], jednak z orzecznictwa Trybunału wydaje się wynikać, że sami autorzy tych aktów mogliby nigdy nie być ścigani.

81. Jestem zdania, że równowaga między różnymi wchodzącymi w grę interesami powinna być przedmiotem ponownej analizy, w przeciwnym razie należałoby zaakceptować okoliczność, że wiele przestępstw nigdy nie będzie ściganych.

[41] Zobacz art. 15 ust. 1 dyrektywy 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 (dyrektywy o handlu elektronicznym) (Dz.U. 2000, L 178, s. 1).

82. Te różne rozważania prowadzą mnie do zaproponowania Trybunałowi pewnego zniuansowania orzecznictwa dotyczącego przepisów krajowych mających na celu przechowywanie adresów IP, interpretowanych w świetle art. 15 ust. 1 dyrektywy 2002/58.

*4. Propozycja zniuansowania orzecznictwa Trybunału dotyczącego wykładni art. 15 ust. 1 dyrektywy 2002/58 w odniesieniu do przepisów mających na celu przechowywanie adresów IP przypisanych do źródła połączenia*

83. Biorąc pod uwagę powyższe rozważania, jestem zdania, że art. 15 ust. 1 dyrektywy 2002/58 należy interpretować w ten sposób, iż nie stoi on na przeszkodzie przepisom przewidującym uogólnione i niezróżnicowane przechowywanie adresów IP przypisanych do źródła połączenia przez okres ograniczony czasowo do tego, co ściśle konieczne, w celu zapobiegania przestępstwom popełnionym w Internecie, ich dochodzenia, wykrywania i ścigania – w odniesieniu do których adres IP stanowi *jedyny środek* dochodzeniowy pozwalający na identyfikację osoby, której adres ten był przypisany w chwili popełnienia naruszenia.

84. W tym względzie pragnę podkreślić, że propozycja taka nie podważa moim zdaniem wymogu proporcjonalności nałożonego wobec przechowywania danych, zważywszy na poważny charakter ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, która wiąże się z tym przechowywaniem [42]. Przeciwnie, propozycja ta czyni w pełni zadość temu wymogowi.

85. Po pierwsze, ograniczenie praw i obowiązków przewidzianych w art. 5, 6 i 9 dyrektywy 2002/58, jakim jest przechowywanie adresów IP, służy realizacji celu leżącego w interesie ogólnym, pozostającego w związku z tym poważnym charakterem, a mianowicie zapobiegania, a także dochodzenia, wykrywania i ścigania przestępstw, o których mowa w przepisach, które w przeciwnym razie zostałyby pozbawione skuteczności.

86. Po drugie, ograniczenie to odbywa się w granicach tego, co jest absolutnie konieczne. Takie przechowywanie jest bowiem ograniczone do konkretnych sytuacji, a mianowicie do przestępstw popełnionych w Internecie, w odniesieniu do których identyfikacja sprawcy może nastąpić jedynie za pomocą przypisanego mu adresu IP. Innymi słowy, nie chodzi o zezwolenie na uogólnione i niezróżnicowane przechowywanie danych bez dodatkowych warunków, lecz jedynie o umożliwienie ścigania nie przestępstw w ogóle, lecz przestępstw ściśle określonych.

87. Jednakże, choć art. 15 ust. 1 dyrektywy 2002/58 nie stoi na przeszkodzie uogólnionemu i niezróżnicowanemu przechowywaniu adresów IP przypisanych do źródła połączenia w celu zapewnienia zapobiegania, dochodzenia, wykrywania i ścigania przestępstw popełnionych w Internecie, w odniesieniu do których adres IP stanowi jedyny środek dochodzenia pozwalający na identyfikację osoby, której ten adres był przypisany w chwili popełnienia przestępstwa, to jednak należy jeszcze wyjaśnić, że zgodnie z orzecznictwem możliwość ta powinna być uzależniona od „drobiazgowego spełnienia warunków materialnych i proceduralnych, *które winny regulować wykorzystywanie tych danych*” [43]. Trybunał precyzuje również, że taki przepis „powinien przewidywać ścisłe warunki i gwarancje dotyczące *wykorzystywania tych danych*” [44].

[42] Zobacz pkt 60 i 61 niniejszej opinii.

[43] Zobacz wyrok La Quadrature du Net i in., pkt 155 (wyróżnienie moje).

[44] Zobacz wyrok La Quadrature du Net i in., pkt 156 (wyróżnienie moje).

88. Innymi słowy, jak już podkreśliłem, przechowywanie danych i dostęp do nich nie mogą być postrzegane odrębnie. W tych okolicznościach, o ile możliwość udzielenia Hadopi dostępu do adresów IP nie jest z założenia sprzeczna z art. 15 ust. 1 dyrektywy 2002/58 w zakresie, w jakim dane te były przechowywane zgodnie z wymogami przewidzianymi w tym przepisie, o tyle w celu udzielenia odpowiedzi na pytania prejudycjalne przedłożone Trybunałowi konieczne jest jeszcze zbadanie, czy warunki uzyskania przez Hadopi dostępu do adresów IP przypisanych do źródła połączenia są same w sobie zgodne ze wspomnianym przepisem, w szczególności w odniesieniu do konieczności uprzedniej kontroli takiego dostępu przez sąd lub niezależny organ administracyjny.

89. Zbadawszy wstępną kwestię przechowywania adresów IP przypisanych do źródła połączenia, przeprowadzę analizę dostępu do tych danych przez Hadopi w świetle art. 15 ust. 1 dyrektywy 2002/58.

### *5. Dostęp Hadopi do danych dotyczących tożsamości cywilnej odpowiadających adresom IP*

90. Z orzecznictwa Trybunału wynika, że jeśli chodzi o cele mogące uzasadniać przepis krajowy stanowiący odstępstwo od zasady poufności łączności elektronicznej, dostęp do danych musi odpowiadać ściśle i obiektywnie jednemu z tych celów, a cel realizowany przez te przepisy musi pozostawać w związku z wagą ingerencji w prawa podstawowe, jaką pociąga za sobą ten dostęp [45].

91. Ponadto, jak już wskazałem [46], dostęp do danych przechowywanych przez dostawców w zastosowaniu przepisów przyjętych na podstawie art. 15 ust. 1 dyrektywy 2002/58 może co do zasady być uzasadniony jedynie celem interesu ogólnego, dla którego owi dostawcy zostali zobowiązani do tego przechowywania [47].

92. Trybunał orzekł zatem, zgodnie z zasadą proporcjonalności, że poważna ingerencja może być uzasadniona w zakresie zapobiegania przestępstwom, ich dochodzenia, wykrywania i ścigania jedynie przez cel polegający na zwalczaniu przestępczości, którą również można uznać za poważną [48].

93. W tym względzie pragnę zauważyć, wbrew twierdzeniom rządu francuskiego i Komisji, że dostęp Hadopi do danych dotyczących tożsamości cywilnej odpowiadających adresowi IP stanowi poważną ingerencję w prawa podstawowe. Chodzi tu bowiem nie tylko o dostęp do danych dotyczących tożsamości cywilnej, które same w sobie są wrażliwe w niewielkim stopniu, lecz o powiązanie tych danych z szerszym zbiorem danych, a mianowicie adresem IP, i również, jak podkreślają skarżący w postępowaniu głównym, z fragmentem pliku pobranego z naruszeniem prawa autorskiego. Chodzi zatem o powiązanie tożsamości cywilnej danej osoby z treścią przeglądanego pliku i z adresem IP, za pomocą którego uzyskano do niego dostęp.

94. Jednakże, podobnie jak jestem zdania, że należy dozwolić również na przechowywanie danych stanowiące poważną ingerencję w prawa podstawowe w celu zapewnienia zapobiegania, a także dochodzenia, wykrywania i ścigania przestępstw popełnionych w Internecie, w odniesieniu do których adres IP stanowi jedyny środek dochodzenia pozwalający na identyfikację osoby, której

45 Zobacz wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 55; wyrok Prokuratuur, pkt 32.

46 Punkt 47 niniejszej opinii.

47 Zobacz wyroki: SpaceNet, pkt 131; La Quadrature du Net i in., pkt 166; Commissioner of An Garda Síochána i in., pkt 98.

48 Zobacz wyrok Tele2, pkt 115; wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 56; wyrok Prokuratuur, pkt 33.

adres ten był przypisany w chwili popełnienia przestępstwa [49], uważam, że dostęp do tych danych powinien zostać umożliwiony w celu realizacji tego samego celu, gdyż w przeciwnym razie trzeba byłoby zgodzić się na ogólną bezkarność przestępstw popełnianych wyłącznie w Internecie.

95. Dostęp Hadopi do danych dotyczących tożsamości cywilnej związanych z adresem IP wydaje mi się zatem uzasadniony celem interesu ogólnego, dla którego dostawcy usług łączności elektronicznej zostali zobowiązani do tego przechowywania.

96. W orzecznictwie Trybunału uściślono jednak, że przepisy krajowe regulujące dostęp właściwych organów do zatrzymanych danych o ruchu i danych o lokalizacji nie mogą ograniczać się do wymagania, aby dostęp organów do danych odpowiadał celowi, do którego zmierza to uregulowanie, ale muszą również przewidywać warunki materialne i proceduralne regulujące dostęp organów krajowych do rozpatrywanych danych [50].

97. W szczególności Trybunał orzekł, że skoro powszechnego dostępu do wszelkich przechowywanych danych, niezależnie od jakiegokolwiek związku z realizowanym celem, nie można uważać za ograniczony do tego, co absolutnie konieczne, przepisy krajowe winny opierać się na obiektywnych kryteriach umożliwiających określenie okoliczności i warunków przyznania dostępu właściwym organom krajowym do danych użytkowników, tak aby zweryfikować, że dostęp zostanie przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo [51].

98. I tak zgodnie z orzecznictwem w celu zagwarantowania w praktyce pełnego przestrzegania tych warunków konieczne jest, aby dostęp właściwych organów krajowych do przechowywanych danych był co do zasady uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego [52].

99. Pragnę jednak zauważyć, że Trybunał ustanowił tę konieczność uprzedniej kontroli dostępu do danych osobowych w szczególnych okolicznościach, które różnią się od niniejszej sprawy, obejmujących *szczególnie poważne* ingerencje w życie prywatne użytkowników usług łączności elektronicznej.

100. W każdym z wyroków, w których podkreślono ten wymóg, chodziło bowiem o przepisy krajowe umożliwiające dostęp do wszystkich danych o ruchu i danych o lokalizacji użytkowników w odniesieniu do wszystkich środków łączności elektronicznej [53] lub przynajmniej w odniesieniu do telefonii stacjonarnej i komórkowej [54]. Dokładniej rzecz ujmując, chodziło o dostęp do „zbioru danych […], które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego” [55], a więc wymóg uprzedniej kontroli dostępu do tych danych przez sąd lub niezależny organ administracyjny istnieje moim zdaniem wyłącznie w tych okolicznościach.

[49] Zobacz pkt 65 i nast. niniejszej opinii.

[50] Zobacz wyroki: Tele2, pkt 118; Prokuratuur, pkt 49; Commissioner of An Garda Síochána i in., pkt 104.

[51] Zobacz wyroki: Tele2, pkt 119; Prokuratuur, pkt 50; Commissioner of An Garda Síochána i in., pkt 105.

[52] Zobacz wyroki: Tele2, pkt 120; Prokuratuur, pkt 51; Commissioner of An Garda Síochána i in., pkt 106.

[53] Zobacz wyrok Tele2 i wyrok Commissioner of An Garda Síochána i in.

[54] Zobacz wyrok Prokuratuur.

[55] Zobacz wyrok Prokuratuur, pkt 45.

101. Tymczasem, po pierwsze, dostęp Hadopi ogranicza się do powiązania danych dotyczących tożsamości cywilnej z używanym adresem IP i do przeglądanego w konkretnym momencie pliku, przy czym nie prowadzi to do umożliwienia właściwym organom prześledzenia ścieżki działań danego użytkownika w Internecie ani, co za tym idzie, wyciągnięcia precyzyjnych wniosków co do jego życia prywatnego poza znajomością konkretnych plików przeglądanych w momencie popełnienia naruszenia. Nie chodzi zatem o umożliwienie śledzenia wszystkich czynności danego użytkownika w Internecie.

102. Po drugie, dane te dotyczą wyłącznie osób, które – jak stwierdzono w protokołach sporządzonych przez uprawnione podmioty – popełniły czyny mogące stanowić uchybienie obowiązkowi przewidzianemu w art. L. 336-3 CPI. Dostęp Hadopi do danych dotyczących tożsamości cywilnej powiązanych z adresami IP jest zatem ściśle ograniczony do tego, co jest konieczne do osiągnięcia zamierzonego celu, a mianowicie umożliwienia zapobiegania przestępstwom, ich dochodzenia, wykrywania i ścigania –popełnionych w Internecie, w odniesieniu do których adres IP stanowi jedyny środek dochodzeniowy pozwalający na identyfikację osoby, której adres ten był przypisany w chwili popełnienia przestępstwa, w który wpisuje się mechanizm stopniowej odpowiedzi.

103. W tych okolicznościach jestem zdania, że art. 15 ust. 1 dyrektywy 2002/58 nie wymaga uprzedniej kontroli dostępu Hadopi do danych dotyczących tożsamości cywilnej powiązanych z adresami IP użytkowników przez sąd lub niezależny organ administracyjny.

104. Co więcej, pragnę zauważyć, jak podkreśla rząd francuski, że dostęp Hadopi do tych danych, choć nie podlega uprzedniej kontroli sądu lub niezależnego podmiotu, nie jest jednak zwolniony z wszelkiej kontroli, ponieważ plik przesłany przez Hadopi operatorom łączności elektronicznej jest tworzony codziennie przez zaprzysiężonego urzędnika z uzyskanego materiału, zweryfikowanego w sposób losowy za pomocą próbek przed włączeniem go do pliku [56]. W szczególności należy zauważyć, że procedura stopniowej odpowiedzi podlega przepisom dyrektywy (UE) 2016/680 [57]. W związku z tym osobom fizycznym, do których odnosi się działanie Hadopi, przysługuje szereg gwarancji materialnych i proceduralnych przewidzianych w tej dyrektywie. Obejmują one prawo dostępu, sprostowania i usunięcia danych osobowych przetwarzanych przez Hadopi, a także możliwość wniesienia odwołania do niezależnego organu sprawującego kontrolę, a następnie, w razie potrzeby, zaskarżenia do sądu na zasadach ogólnych [58].

105. W związku z tym proponuję, aby na pytania prejudycjalne pierwsze i drugie odpowiedzieć, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty 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 praw

[56] Pragnę zauważyć pomocniczo, że argumenty dotyczące wykonalności przemawiają również przeciwko obowiązkowi uprzedniej systematycznej kontroli. Istnienie zorganizowanego systemu zwalczania popełnianych w Internecie naruszeń prawa autorskiego, takiego jak rozpatrywany w postępowaniu głównym, zakłada konieczność zbadania znacznych ilości danych osobowych, odpowiednich do liczby ściganych naruszeń, a mianowicie, tytułem przykładu w roku 2019, zgodnie z uwagami rządu francuskiego, 33 465 wniosków o identyfikację adresu IP składanych dziennie przez Hadopi. W tym kontekście obowiązek kontroli poprzedzającej dostęp do tych danych mógłby w praktyce zagrozić funkcjonowaniu mechanizmów zorganizowanej walki z naruszaniem praw własności intelektualnej w Internecie, podważając równowagę między prawami użytkowników i autorów.

[57] Dyrektywa Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. 2016, L 119, s. 89).

[58] Wszystkie te gwarancje zostały przewidziane w przepisach rozdziału III tytuł III ustawy nr 78-17 w sprawie informatyki, plików i wolności z dnia 6 stycznia 1978 r. (JORF z dnia 7 stycznia 1978 r.).

autorskich 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 osoby, której adres ten był przypisany w chwili popełnienia naruszenia.

### *B. W przedmiocie pytania prejudycjalnego trzeciego*

106. Poprzez pytanie prejudycjalne trzecie sąd odsyłający zmierza do ustalenia, czy w przypadku udzielenia odpowiedzi twierdzącej na pytania pierwsze i drugie oraz z uwagi na niewielki stopień wrażliwości danych dotyczących tożsamości cywilnej ścisłe ramy dostępu do danych oraz wymóg, aby nie zagrażać realizacji zadań publicznych powierzonych danemu organowi administracyjnemu, art. 15 ust. 1 dyrektywy 2002/58, w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty, należy interpretować w ten sposób, że stoi on na przeszkodzie temu, by uprzednia kontrola dostępu była przeprowadzana zgodnie z dostosowanymi procedurami, takimi jak przeprowadzanie zautomatyzowanej kontroli, w razie potrzeby pod nadzorem służby wewnętrznej organu dającego gwarancje niezależności i bezstronności w stosunku do urzędników odpowiedzialnych za to zbieranie.

107. Z brzmienia pytania prejudycjalnego trzeciego oraz z odpowiedzi pisemnej rządu francuskiego na pytania zadane przez Trybunał wynika, że dostosowane procedury kontroli, o których mowa w tym pytaniu, dotyczą nie mechanizmu kontroli istniejącego w prawie krajowym, lecz możliwych do obrania dróg, zmierzających do dostosowania w razie potrzeby francuskiego mechanizmu do wymogów stawianych przez prawo Unii.

108. Tymczasem zgodnie z utrwalonym orzecznictwem wniosek o wydanie orzeczenia w trybie prejudycjalnym nie ma na celu formułowania opinii o charakterze doradczym w odpowiedzi na ogólne lub hipotetyczne pytania, ale faktyczne zaspokojenie potrzeby nierozerwalnie związanej z rzeczywistym rozstrzygnięciem sporu dotyczącego prawa Unii [59].

109. Skoro pytanie prejudycjalne trzecie ma zatem moim zdaniem charakter hipotetyczny, należy je uznać za niedopuszczalne.

110. W każdym razie, w świetle odpowiedzi, jakiej proponuję udzielić na pytania prejudycjalne pierwsze i drugie, nie ma potrzeby udzielenia odpowiedzi na pytanie trzecie.

[59] Zobacz wyroki: z dnia 26 października 2017 r., Balgarska energiyna borsa, C-347/16, EU:C:2017:816, pkt 31; z dnia 31 maja 2018 r., Confetra i in., C-259/16 i C-260/16, EU:C:2018:370, pkt 63; z dnia 17 października 2019 r., Elektrorazpredelenie Yug, C-31/18, EU:C:2019:868, pkt 32.

## V. Wnioski

111. 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) 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 praw autorskich 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 osoby, której adres ten był przypisany w chwili popełnienia naruszenia.