

dr Zbigniew Okoń

Radca prawny (ORCID: <https://orcid.org/0000-0002-0999-780X>).

Koniec anonimowości w sieci? Glosa do wyroku Trybunału Sprawiedliwości z 30.04.2024 r., C-470/21, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network przeciwko Premier ministre, Ministre de la Culture

Słowa kluczowe: retencja danych telekomunikacyjnych, dane osobowe, ochrona prywatności, adresy IP, łączność elektroniczna, Karta praw podstawowych Unii Europejskiej, zwalczanie naruszeń praw autorskich online

Retencja danych telekomunikacyjnych jest od dekady przedmiotem licznych pytań kierowanych do Trybunału Sprawiedliwości Unii Europejskiej przez sądy krajowe. Kolejnym rozstrzygnięciem dotyczącym tej problematyki jest wyrok TS z 30.04.2024 r., C-470/21, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network przeciwko Premier ministre, Ministre de la Culture¹, dotyczący wykładni art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)² w kontekście francuskiego systemu zwalczania masowych naruszeń praw autorskich online (Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet, HADOPI). Trybunał, orzekając w pełnym składzie, uznał, że ogólna retencja adresów IP, przy zachowaniu szczelnej separacji od innych kategorii danych, nie stanowi poważnej ingerencji w prawa zagwarantowane w art. 7, 8 i 11 Karty praw podstawowych Unii Europejskiej³ i może być prowadzona w celu zwalczania każdej przestępczości, bez uprzedniej kontroli sądowej pod warunkiem spełnienia szczegółowych wymogów technicznych i proceduralnych mających zapobiec agregacji danych. Przyjęta interpretacja liberalizuje dotychczasowe zasady retencji, wychodząc naprzeciw oczekiwaniom części państw członkowskich, kosztem pewnego osłabienia ochrony praw podstawowych.

1. Prawo UE

Dyrektywa 2002/58/WE zapewnia ochronę poufności komunikacji elektronicznej i metadanych dotyczących tej komunikacji. Jej częścią jest ogólny zakaz przetwarzania danych

o ruchu (rozumianych jako informacje przetwarzane w celu przekazywania komunikatów lub naliczania opłat) oraz danych o lokalizacji (wskazujących położenie geograficzne terminala użytkownika), który obejmuje również zakaz przechowywania i udostępniania tych danych osobom trzecim przez operatorów usług łączności elektronicznej (zakaz tzw. retencji danych telekomunikacyjnych). Od tego zakazu dyrektywa 2002/58/WE przewiduje kilka wyjątków. Podstawowe znaczenie ma wyjątek przewidziany w art. 15 ust. 1, zgodnie z którym państwa członkowskie mogą w swoim ustawodawstwie ograniczyć ochronę

1 EU:C:2024:370 – wyrok C-470/21, La Quadrature du Net II.

2 Dz.Urz. WE L 201, s. 37, ze zm. – dalej dyrektywa 2002/58/WE.

3 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 389 – dalej KPP.

poufności komunikacji i metadanych, jeżeli ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw lub niedozwolonego używania systemów łączności elektronicznej. Zgodnie z motywem 11, środki te powinny być właściwe, współmierne i niezbędne do zamierzonego celu oraz powinny zapewniać odpowiednie zabezpieczenia zgodnie z Konwencją o ochronie praw człowieka i podstawowych wolności, sporządzoną w Rzymie 4.11.1950 r., zmienioną następnie Protokołami nr 3, 5 i 8 oraz uzupełnioną Protokołem nr 2⁴.

Mimo podejmowanych prób reform obowiązujący od 2002 r. art. 15 ust. 1 dyrektywy 2002/58/WE jest nadal jedynym przepisem prawa unijnego bezpośrednio regulującym retencję danych telekomunikacyjnych. Wprawdzie kilka lat po uchwaleniu dyrektywy 2002/58/WE zmiany w tej dziedzinie zostały wprowadzone dyrektywą 2006/24/WE Parlamentu Europejskiego i Rady z 15.03.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE⁵, jednak przyjęty w niej model retencji danych, kwestionowany już wcześniej przez sądy konstytucyjne kilku państw członkowskich⁶, został w 2014 r. uznany przez TS za niezgodny z art. 7, 8 i 52 ust. 1 KPP w wyroku z 8.04.2014 r., sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.*⁷ Trybunał orzekł, że prawodawca unijny przekroczył granice wyznaczone przez zasadę proporcjonalności, nakładając generalny obowiązek retencji bez ograniczenia do zwalczania poważnych przestępstw, przewidując retencję ogólną (tj. obejmującą dane wszystkich użytkowników, w tym korzystających z tajemnicy zawodowej), nie określając obiektywnych kryteriów dostępu organów krajowych do danych oraz nie zapewniając adekwatnych gwarancji bezpieczeństwa, w tym wymogu zatrzymywania danych na terytorium UE. W konsekwencji TS uznał dyrektywę 2006/24/WE za nieważną *ex tunc*, skutkiem czego regulacje krajowe dotyczące retencji danych telekomunikacyjnych państw członkowskich są nadal oceniane wyłącznie na podstawie art. 15 ust. 1 dyrektywy 2002/58/WE oraz wynikających z tego przepisu wymogów niezbędności, adekwatności, proporcjonalności i zgodności z prawami podstawowymi⁸.

2. Prawo krajowe

Do takich regulacji krajowych należy wprowadzony w 2009 r. francuski system stopniowanej reakcji⁹, realizowany przez utworzony w tym celu organ publiczny – HADOPI¹⁰. System polega na identyfikacji przypadków wykorzystania usług dostępu do Internetu do naruszeń praw autorskich, a następnie stosowaniu wobec ich użytkowników stopniowanego mechanizmu ostrzeżeń („zaleceń”), poprzedzających dalej idącą reakcję prawną. Ostrzeżenia kierowane są do użytkowników dostępu do Internetu, którzy niekoniecznie sami dopuszczają się naruszeń praw autorskich – faktycznymi naruszcicielami mogą być bowiem np. członkowie rodziny czy osoby trzecie korzystające bez wiedzy użytkownika z niezabezpieczonego dostępu.

Skuteczne funkcjonowanie tego systemu wymaga powiązania naruszeń popełnianych online z konkretnymi osobami. Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet musi więc ustalić tożsamość osób będących abonentami usług dostępu do Internetu, wykorzystywanych do nielegalnego udostępniania utworów. Proces identyfikacji abonentów przebiega dwuetapowo. W pierwszym etapie organizacje reprezentujące uprawnionych za pomocą programów monitorujących zbierają adresy IP wykorzystywane do nielegalnego udostępniania chronionych utworów. Przekazują je następnie do HADOPI w postaci protokołów zawierających: adres IP, datę i godzinę naruszenia, wykorzystywany protokół udostępniania (konkretną sieć *peer-to-peer*, w której doszło do udostępnienia pliku), pseudonim danej osoby (jeśli jest dostępny), informacje o utworze lub innym przedmiocie ochrony (tytuł i nazwę pliku) oraz dane dostawcy usług internetowych.

W drugim etapie HADOPI zwraca się do dostawców o identyfikację abonentów usług dostępu do Internetu, którym przypisany został dany adres IP. Dostawcy przyporządkowują adresy IP do danych klientów na podstawie przechowywanych danych osobowych (imię i nazwisko, adres, numer telefonu, adres e-mail) oraz rejestrów przydziału adresów IP – zarówno stałych, jak i dynamicznych. Następnie przekazują HADOPI: nazwisko, imię, adres korespondencyjny, adresy poczty elektronicznej i numer telefonu. Umożliwia to organowi wysłanie ostrzeżeń i przeprowadzenie dalszych etapów stopniowanej reakcji w stosunku do zidentyfikowanych w ten sposób użytkowników. Proces jest więc skonstruowany w ten sposób, że HADOPI jest jedynym podmiotem, który zna zarówno tożsamość abonenta połączenia internetowego wykorzystanego do naruszenia, jak i informacje dotyczące samego naruszenia, takie jak np. to, kiedy nastąpiło i jakiego utworu dotyczyło.

4 Dz.U. z 1993 r. Nr 61, poz. 284 ze zm. – dalej EKPC.

5 Dz.Urz. UE. L 105, s. 54, ze zm. – dalej dyrektywa 2006/24/WE.

6 Chodzi o wyrok Federalnego Trybunału Konstytucyjnego (BVerfG) z 2.03.2010 r., 1 BvR 256/08, 1 BvR 263/08 i 1 BvR 586/08 (Vorratsdatenspeicherung), ECLI:DE:BVerfG:2010:rs20100302.1bvr025608; opubl. w: BVerfGE 125, s. 260–385; wyrok czeskiego sądu konstytucyjnego (Ústavní soud České republiky) z 22.03.2011 r., sp. zn. Pl. ÚS 24/10, opubl. w: Sbirka zákonů č. 94/2011 Sb; wyrok rumuńskiego sądu konstytucyjnego (Curtea Constituțională a României) z 8.10.2009 r., nr 1258; wyrok Wysockiego Sądu Administracyjnego Bułgarii (Върховен административен съд) z 11.12.2008 r., nr 13627; wyrok Sądu Najwyższego Cypru z 1.02.2011 r. w sprawach 65/2009, 78/2009, 82/2009, 15/2010–22/201. Zob. szerzej E. Kosta, *The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, „SCRIPTed” 2013/3, s. 340.

7 EU:C:2014:238 – dalej wyrok sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland*.

8 Zob. M. Rojszczak, *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*, „European Constitutional Law Review” 2021/4, s. 611.

9 System został wprowadzony ustawą nr 2009-669 z 12.06.2009 r. (JORF nr 0135 z 13.06.2009 r., s. 9666, NOR: MCCX0811238L), która utworzyła HADOPI, i ustawą nr 2009-1311 z 28.10.2009 r. (JORF nr 0251 z 29.10.2009 r., s. 18290, NOR: JUSX0913484L), która ponownie uregulowała zasady odpowiedzialności użytkowników po wyroku Rady Konstytucyjnej (*Conseil constitutionnel*) nr 2009-580 DC z 10.06.2009 r., ECLI:FR:CC:2009:2009.580.DC, opubl. JORF z 13.06.2009 r., s. 9675, poz. 3, w którym uznano za niekonstytucyjne pierwotnie przyznane HADOPI uprawnienie do nakładania kar administracyjnych. Zob. szerzej N. Lucchi, *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, „Cardozo Journal of International and Comparative Law” 2011/3, s. 652.

10 Od 2022 r. HADOPI połączono z Conseil supérieur de l’audiovisuel (CSA, wyższą radą ds. radiofonii i telewizji), tworząc Autorité de régulation de la communication audiovisuelle et numérique (ARCOM, organ ds. regulacji komunikacji radiowo-telewizyjnej i cyfrowej). Procedura stopniowej odpowiedzi pozostała jednak zasadniczo niezmienną.

3. Postępowanie główne i pytania prejudycjalne

Szczegółowe zasady funkcjonowania systemu HADOPI, w tym procedury zautomatyzowanego przetwarzania danych dostosowane do masowej skali działań organu, określa dekret nr 2010-236 z 5.03.2010 r.¹¹ Z wnioskiem o uchylenie dekretu wystąpiły w 2019 r. organizacje działające na rzecz obrony praw cyfrowych i zraszające dostawców usług łączności elektronicznej – La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net oraz French Data Network, składając do premiera Francji wnioski o jego uchylenie. Wniosek pozostał bez odpowiedzi, co zgodnie z francuskim prawem administracyjnym oznaczało w tym przypadku dorozumianą decyzję o jego oddaleniu (*décision implicite de rejet*). Dnia 12.08.2019 r. wspomniane organizacje wniosły do Conseil d'État skargę o stwierdzenie nieważności tej decyzji.

W uzasadnieniu skarżący podnieśli, że dekret oraz stanowiące jego podstawę przepisy art. L. 331-21 akapity od trzeciego do piątego Code de la propriété intellectuelle¹² nadmiernie ingerują w konstytucyjne prawo do poszanowania życia prywatnego, a ponadto są sprzeczne z prawem UE, w szczególności art. 15 ust. 1 dyrektywy 2002/58/WE oraz art. 7, art. 8, art. 11 i art. 52 KPP. W zakresie prawa unijnego zasadniczy zarzut dotyczył naruszenia zasady proporcjonalności przez umożliwienie dostępu do danych o ruchu w sprawach o naruszenia prawa autorskiego niestanowiące „poważnej przestępczości”, a także braku obligatoryjnej kontroli sądu lub niezależnego organu administracyjnego poprzedzającej ten dostęp. Skarżący podnieśli zarówno zarzuty niekonstytucyjności przepisów krajowych, jak i ich sprzeczności z prawem UE.

Conseil d'État rozstrzygnął je etapami: najpierw skierował do Conseil constitutionnel pytanie priorytetowe o zgodność z konstytucją (*question prioritaire de constitutionnalité*, QPC). Conseil constitutionnel w orzeczeniu nr 2020-841 QPC z 20.05.2020 r. potwierdził część zarzutów, uznając za niekonstytucyjne akapity trzeci i czwarty art. L. 331-21 CPI, z pewnymi zastrzeżeniami utrzymując jednak w mocy akapit piąty tego artykułu¹³. Następnie Conseil d'État przystąpił do rozpoznania zarzutów naruszenia prawa unijnego, wychodząc od analizy dotychczasowego orzecznictwa TSUE. Zwrócił uwagę, że zgodnie z wyrokiem z 6.10.2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in. przeciwko Premier ministre i in. oraz Ordre des barreaux francophones et germanophone i in. przeciwko Conseil des ministres¹⁴, państwa członkowskie mogą przewidywać ogólną i nieodróżnicowaną retencję danych dotyczących „tożsamości cywilnej” użytkowników usług łączności (imię, adres,

e-mail, telefon) także dla zwalczania „zwykłej”, a nie tylko „poważnej” przestępczości. Zauważył też, że według wyroku z 21.12.2016 r., sprawy połączone C-203/15 i C-698/15, Tele2 Sverige AB przeciwko Post- och telestyrelsen oraz Secretary of State for the Home Department przeciwko Tom Watson, Peter Brice, Geoffrey Lewis¹⁵, oraz późniejszego orzecznictwa TSUE dostęp władz do danych o ruchu i lokalizacji musi co do zasady podlegać uprzedniej kontroli sądu albo niezależnego organu. Na tym tle Conseil d'État powziął wątpliwość, czy dane tożsamości przypisane do adresu IP podpadają pod kategorię danych, do których dostęp wymaga kontroli sądowej szczególnie, że ze względu na masową skalę procedury „stopniowanej reakcji” (miliony zawiadomień rocznie¹⁶) poddanie każdego żądania dostępu do danych uprzedniej kontroli prowadziłoby do faktycznego paraliżu systemu¹⁷.

Wobec tych wątpliwości Conseil d'État zawiesił postępowanie i skierował do Trybunału Sprawiedliwości UE trzy pytania prejudycjalne. Pierwsze dotyczyło tego, czy tożsamość cywilna powiązana z adresem IP stanowi dane o ruchu lub lokalizacji, które podlegają kontroli sądu lub niezależnego organu. Drugie, aktualne w razie odpowiedzi twierdzącej na pytanie pierwsze, zmierzało do ustalenia czy prawo unijne sprzeciwia się gromadzeniu takich danych przez organ administracyjny bez tej kontroli. Trzecie pytanie, warunkowane twierdzącą odpowiedzią na dwa poprzednie, dotyczyło dopuszczalności „kontroli dostosowanej”, tj. zautomatyzowanego mechanizmu, nadzorowanego przez wewnętrzną jednostkę takiego organu dysponującą gwarancjami niezależności jako spełniającej wymóg kontroli sądu lub niezależnego organu.

4. Postępowanie przed Trybunałem i wyrok

Sprawa C-470/21, La Quadrature du Net II, została pierwotnie przydzielona Wielkiej Izbie, jednak 7.03.2023 r. przekazano ją do rozpoznania przez pełny skład Trybunału na podstawie art. 60 § 2 zd. drugie Regulaminu postępowania przed Trybunałem Sprawiedliwości Unii Europejskiej¹⁸. Decyzję tę wiąże się z narastającym napięciem między TS niektórymi sądami państw członkowskich po wyroku C-511/18, La Quadrature du Net I, oraz utrzymującą się presją części państw członkowskich w kierunku złagodzenia restrykcyjnej linii orzeczniczej w sprawach retencji danych¹⁹.

11 JORF nr 0056 z 7.03.2010 r., poz. 19; NOR: MCCC1004830D.

12 JORF nr 0153 z 3.07.1992 r. – dalej CPI.

13 Wyrok Conseil constitutionnel nr 2020-841 QPC z 20.05.2020 r., ECLI:FR:CC:2020:2020.841.QPC (JORF nr 0124 z 21.05.2020 r., poz. 97; NOR: CSCX2012592S). Akapity trzeci i czwarty art. L. 331-21 CPI nadawały HADOPI ogólne prawo żądania „wszystkich dokumentów, niezależnie od nośnika”, w tym danych łączności, bez wystarczających ograniczeń co do zakresu i podmiotów oraz bez gwarancji powiązania z konkretnym naruszeniem, co z uwagi na szczególną wrażliwość danych łączności nadmiernie ingerowało w prywatność. Utrzymano (z wyłączeniem zwrotu „w szczególności”) możliwość uzyskania przez HADOPI od dostawców danych identyfikacyjnych abonenta (tożsamość, adres pocztowy, e-mail, telefon) potrzebnych do wysłania zaleceń.

14 EU:C:2020:791 – dalej wyrok C-511/18, La Quadrature du Net I.

15 EU:C:2016:970, pkt 120 – dalej wyrok sprawy połączone C-203/15 i C-698/15, Tele2 Sverige AB.

16 Szczytowy okres aktywności HADOPI przypadł na 2016 r., kiedy wysłano 2 083 082 pierwszych ostrzeżeń, 152 665 ponownych ostrzeżeń i w 688 przypadkach złożono zawiadomienia do prokuratury. Zob. *Rapport d'activité 2015–2016*, <https://www.vie-publique.fr/files/rapport/pdf/174000037.pdf> (dostęp: 20.08.2025 r.), s. 76. Od 2016 r. liczba zaleceń i ponownych ostrzeżeń wyraźnie spada, rośnie natomiast liczba zawiadomień. I tak przykładowo w 2021 r. przesłano 210 595 pierwszych zaleceń i 53 564 ponownych zaleceń, a w 1484 przypadkach złożono zawiadomienia. Zob. *Rapport annuel 2021 de l'Hadopi*, <https://www.arcom.fr/se-documenter/etudes-et-donnees/etudes-bilans-et-rapports-de-larcom/rapports-annuels-2021-du-csa-et-de-lhadopi> (dostęp: 20.08.2025 r.), s. 51.

17 Wyrok *Conseil d'État* nr 433539 z 5.07.2021 r., ECLI:FR:CECHR:2021:433539.20210705.

18 Dz.Urz. UE L 265 z 2012 r., s. 1, ze zm.

19 Po wyroku C-511/18, La Quadrature du Net I, francuski Conseil d'État (wyrok z 21.04.2021 r., nr 393099, ECLI:FR:CEASS:2021:393099.20210421) nie odmówił wprowadzić zastosowania prawa UE, ale zinterpretował je – powołując się na wyjątek dotyczący zagrożenia bezpieczeństwa narodowego – w sposób, który z niewielkimi korektami pozwolił zachować krajowe przepisy o powszechnej retencji danych. Zob. J. Ziller, *The Conseil d'Etat*

Rzecznik Generalny M. Szpunar przedstawił dwie opinie. W pierwszej wskazał na niespójność w orzecznictwie Trybunału dotyczącym adresów IP²⁰. Z jednej strony w wielu wyrokach TS uznał za dopuszczalne nałożenie przez prawo krajowe obowiązku ujawnienia adresów IP podmiotom praw autorskich przez dostawców usług w postępowaniach cywilnych o ochronę praw własności intelektualnej²¹. Z drugiej strony w sprawach dotyczących retencji danych przyjął wykładnię art. 15 ust. 1 dyrektywy 2002/58/WE, zgodnie z którą przechowywanie adresów IP jest dopuszczalne wyłącznie dla celów zwalczania „poważnych przestępstw”, do których naruszenia praw autorskich nie należą. Udostępnienie danych zakłada jednak ich wcześniejsze przechowywanie, na które orzecznictwo retencyjne dla tych celów nie pozwalało. Zwrócił też uwagę, że ograniczenie dopuszczalności retencji adresów IP do zwalczania poważnej przestępczości rodzi ryzyko systemowej bezkarności sprawców przestępstw popełnianych wyłącznie w Internecie – takich jak naruszenia praw autorskich czy zniesławienia – pozbawiając organy krajowe często jedynego środka identyfikacji sprawców. Dlatego zaproponował korektę dotychczasowego podejścia, polegającą na uznaniu dopuszczalności retencji adresów IP w celu zwalczania nie tylko „poważnej”, lecz także każdej przestępczości internetowej, o ile adres IP stanowi jedyny środek dochodzeniowy pozwalający na identyfikację sprawców²².

W drugiej opinii, wydanej już po przekazaniu sprawy do rozpoznania przez pełny skład Trybunału, Rzecznik rozwinął analizę testu proporcjonalności ograniczeń praw podstawowych. Celem było wykazanie, że ingerencja w prywatność związana z przechowywaniem i dostępem do adresów IP nie jest na tyle poważna, by wymagała uzasadnienia wyłącznie celem zwalczania „poważnej przestępczości”. Na mniejszą intensywność tej ingerencji wskazywać miał zdaniem rzecznika incydentalny charakter ujawnianych treści (np. tytułu utworu), który nie pozwala na wyciągnięcie szczegółowych wniosków co do życia prywatnego, oraz przechowywanie w zasadniczej większości dynamicznych adresów IP, zmieniających się w kolejnych połączeniach. Skoro adresy te odpowiadają konkretnej tożsamości tylko w momencie naruszenia, ich ujawnienie organowi publicznemu nie umożliwia „wyczerpującego śledzenia” aktywności

internauty w sieci²³, a to właśnie możliwość takiego śledzenia była w dotychczasowym orzecznictwie uznawana za cechę nadającą retencji i udostępnianiu adresu IP charakter „poważnej ingerencji” w prawa podstawowe²⁴.

Wyrok C-470/21, *La Quadrature du Net II*, który zapadł 30.04.2024 r., dopuścił retencję adresów IP dla celów zwalczania ogółu przestępstw popełnianych online, jednak Trybunał uzasadnił to inaczej niż Rzecznik Generalny. Nie podzielił argumentu jedynego środka identyfikacji, lecz na nowo przeprowadził test proporcjonalności. Punktem wyjścia było spostrzeżenie, że we wcześniejszych sprawach adresy IP były przechowywane łącznie z innymi danymi o ruchu i lokalizacji, co stwarzało możliwość ich agregacji i ustalenia szczegółowego profilu aktywności użytkownika²⁵. To właśnie ta możliwość nadawała retencji adresów IP charakter „poważnej ingerencji” w prawa podstawowe. Trybunał zauważył jednak, że ocena proporcjonalności zmienia się, gdy adresy IP są przechowywane w warunkach szczelnej separacji od danych o ruchu, lokalizacji i tożsamości cywilnej²⁶. Uznał więc, że w sytuacji, w której agregacja kategorii danych jest wykluczona, samo zestawienie adresu IP z tożsamością cywilną użytkownika nie umożliwia wyciągnięcia „precyzyjnych wniosków” dotyczących jego życia prywatnego, a tym samym nie stanowi poważnej ingerencji w prawa podstawowe.

W konsekwencji Trybunał orzekł, że retencja i udostępnianie adresów IP mogą być uzasadnione celem zwalczania ogółu czynów zabronionych, o ile spełnione są cztery warunki. Po pierwsze, dane muszą być przechowywane w warunkach szczelnej separacji adresów IP od danych o ruchu i lokalizacji oraz od danych o tożsamości cywilnej. Po drugie, dostęp organu publicznego do tych danych może służyć wyłącznie identyfikacji osoby podejrzewanej o popełnienie czynu zabronionego, a system przetwarzania musi wykluczać możliwość wyciągnięcia precyzyjnych wniosków na temat życia prywatnego użytkownika. Po trzecie, w przypadku ponownych naruszeń powiązanie adresów IP z informacjami o tytułach utworów uzasadniających ich zebranie może pozwolić na wyciągnięcie takich wniosków, dlatego wymaga uprzedniej kontroli sądu lub niezależnego organu administracyjnego. Po czwarte, system przetwarzania danych musi podlegać regularnej kontroli niezależnego organu zewnętrznego wobec organu ubiegającego się o dostęp²⁷.

5. Komentarz

W dotychczasowym orzecznictwie Trybunał wypracował różnicowany reżim prawny dla poszczególnych kategorii danych telekomunikacyjnych, wiążąc dopuszczalność retencji i udostępniania danej kategorii ze stopniem ingerencji w prawa podstawowe gwarantowane przez art. 7, art. 8 i art. 11 KPP. Retencję i udostępnianie danych o ruchu i lokalizacji Trybunał uznał za poważną ingerencję w prawa podstawowe, ponieważ – jak podkreślił – dane te mogą ujawnić informacje o wielu aspektach

refuses to follow the Pied Piper of Karlsruhe, <https://verfassungsblog.de/the-conseil-detat-refuses-to-follow-the-pied-piper-of-karlsruhe/> (dostęp: 8.02.2026 r.). Na znaczenie tego rozstrzygnięcia dla decyzji o przydzieleniu sprawy C-470/21 pełnemu składowi Trybunału wskazuje G. Robinson, *A 'necessary and limited development' of the data retention case law, or its death by a thousand cuts?*, „Computer Law & Security Review” 2025/58, s. 2.

20 Opinia Rzecznika Generalnego M. Szpunara z 27.10.2022 r., C-470/21, *La Quadrature du Net I* i in. przeciwko Premier ministre i Ministère de la Culture, EU:C:2022:838, pkt 69 – dalej opinia z 27.10.2022 r., C-470/21, *La Quadrature du Net II*. Podobne stanowisko zostało wyrażone już w opinii Rzecznika Generalnego M. Szpunara z 17.12.2020 r., C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) przeciwko Telenet BVBA*, EU:C:2020:1063, pkt 98 – dalej opinia C-597/19, M.I.C.M.

21 Opinia z 27.10.2022 r., C-470/21, *La Quadrature du Net II*, pkt 70. Rzecznik powołał wyroki TS: z 19.04.2012 r., C-461/10, *Bonnier Audio AB i in. przeciwko Perfect Communication Sweden AB*, EU:C:2012:219, pkt 55; z 4.05.2017 r., C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde przeciwko Rīgas pašvaldības SIA „Rīgas satiksme”*, EU:C:2017:336, pkt 34; i z 17.06.2021 r., C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited przeciwko Telenet BVBA*, EU:C:2021:492, pkt 47–54.

22 Opinia z 27.10.2022 r., C-470/21, *La Quadrature du Net II*, pkt 80, 82, 94.

23 Opinia Rzecznika Generalnego Macieja Szpunara z 28.09.2023 r., C-470/21, *La Quadrature du Net I* i in. przeciwko Premier ministre i Ministère de la Culture, EU:C:2023:711, pkt 50, 51 – dalej opinia z 28.09.2023 r., C-470/21, *La Quadrature du Net II*.

24 Opinia z 28.09.2023 r., C-470/21, *La Quadrature du Net II*, pkt 47, 55.

25 Zob. wyrok C-511/18, *La Quadrature du Net I*, pkt 117–118, 153.

26 Wyrok C-470/21, *La Quadrature du Net II*, pkt 78–79, 82, 86–93.

27 Wyrok C-470/21, *La Quadrature du Net II*, pkt 164.

życia prywatnego, w tym o orientacji seksualnej, poglądach politycznych, przekonaniach religijnych czy stanie zdrowia²⁸. W związku z tym, zgodnie z zasadą proporcjonalności, ogólna retencja tych danych może być uzasadniona jedynie względami bezpieczeństwa narodowego i poddana kontroli sądu lub niezależnego organu²⁹. W nieco szerszym zakresie dopuścił retencję ukierunkowaną, tj. dotyczącą nie ogółu użytkowników, a jedynie pewnych ich grup wyselekcjonowanych na podstawie obiektywnych kryteriów, która może być uzasadniona celem zwalczania „poważnej przestępczości” lub zapobiegania poważnym zagrożeniom bezpieczeństwa publicznego i tak samo poddana kontroli sądu lub niezależnego organu przy dostępie do danych³⁰. Najniższe wymogi sformułowane zostały w stosunku do danych o tożsamości cywilnej użytkowników usług łączności elektronicznej, tj. imienia, nazwiska, adresu, numeru telefonu i adresu poczty elektronicznej. W wyroku C-511/18, *La Quadrature du Net I*, Trybunał uznał za zgodną z prawem UE ogólną i niezróżnicowaną, tj. dotyczącą ogółu użytkowników, retencję tych danych dla celów zwalczania każdej, a nie tylko „poważnej” przestępczości³¹.

Początkowo adresy IP klasyfikowane były – zgodnie z art. 2 lit. b dyrektywy 2002/58/WE – jako dane o ruchu podlegające co do zasady temu samemu reżimowi co pozostałe dane tej kategorii³². Dopiero w wyroku C-511/18, *La Quadrature du Net I*, Trybunał przyznał, że wykazują one mniejszy stopień wrażliwości niż inne dane o ruchu i lokalizacji, ponieważ źródłowy adres IP wskazuje jedynie na fakt połączenia danego urządzenia z siecią, nie ujawniając sam w sobie adresata komunikacji³³.

(Spostrzeżenie to stało się podstawą dopuszczenia w wyroku sprawy połączone C-793/19 i C-794/19, *SpaceNet AG i Telekom*, ogólnej retencji adresów IP w odniesieniu do niektórych poważnych przestępstw, gdzie adres IP jest jedynym środkiem dowodowym³⁴. Towarzyszyło temu jednak kategoryczne stwierdzenie, że „jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego mogą, podobnie jak ochrona bezpieczeństwa narodowego, uzasadniać uogólnione zatrzymywanie adresów IP przypisanych do źródła połączenia”³⁵.

Dopuszczenie w głosowanym wyroku retencji adresów IP dla celów zwalczania ogółu czynów zabronionych popełnianych on-line, na pierwszy rzut oka może się wydawać sprzeczne z tym podejściem. W rzeczywistości w wyroku C-470/21, *La Quadrature du Net II*, TS raczej rozwinął tezę wcześniejszego orzecznictwa, niż je odrzucił³⁶. Dotychczas miał bowiem okazję wypowiadać się tylko w przypadkach, w których adresy IP były przechowywane łącznie z innymi danymi o ruchu lub lokalizacji. Istniała więc możliwość ich agregacji, która potencjalnie mogła prowadzić do wyciągnięcia daleko idących wniosków o życiu prywatnym użytkownika, a tym samym poważnej ingerencji w prawa podstawowe³⁷. Dopiero w sprawie zakończonej wyrokiem C-470/21, *La Quadrature du Net II*, pojawił się stan faktyczny, w którym przechowywane i udostępniane były wyłącznie adresy IP w celu powiązania ich z tożsamością cywilną użytkownika, a system skonstruowany był w sposób realnie ograniczający możliwości powiązania tych danych z innymi danymi. Zmienione warunki umożliwiły TS ponowne przeprowadzenie testu proporcjonalności, a jego wynik pozwolił na dalsze złagodzenie wymogów dotyczących retencji adresów IP i wyjście naprzeciw oczekiwaniom niektórych państw członkowskich bez odrzucania dotychczasowego dorobku orzeczniczego³⁸.

Obniżenie progu dopuszczalności retencji adresów IP pozwala na ograniczenie sygnalizowanego przez rzecznika generalnego problemu „systemowej bezkarności” sprawców przestępstw popełnianych w Internecie³⁹. Adresy IP i logi połączeń należą do najczęściej żądanych przez organy ścigania kategorii danych, a praktyka państw nieprzewidujących obowiązku ich retencji ujawniła, że ze względu na brak dostępu do tych danych identyfikacja sprawców przez organy ścigania często jest niemożliwa⁴⁰. Fragment wyroku, w którym TS formułuje

28 Zob. wyroki: sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland*, pkt 27; sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB*, pkt 99; wyrok C-511/18, *La Quadrature du Net I*, pkt 117. Por. A. Grzelak, *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności – glosa do wyroku TS z 21.12.2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB oraz C-698/15 Watson, Brice, Lewis*, „Europejski Przegląd Sądowy” 2017/3, s. 33; J. Wojnowska-Radzińska, *Implications of Pre-emptive Data Surveillance for Fundamental Rights in the European Union*, Leiden–Boston 2023, s. 31.

29 Zob. wyrok C-511/18, *La Quadrature du Net I*, pkt 134–139. Por. również wyroki TS: z 2.03.2021 r., C-746/18, *Prokuratuur*, EU:C:2021:152, pkt 33 – dalej wyrok C-746/18, *Prokuratuur*; z 5.04.2022 r., C-140/20, G.D. przeciwko *The Commissioner of the Garda Síochána i in.*, EU:C:2022:258, pkt 58 – dalej wyrok C-140/20, *Commissioner of An Garda Síochána*; z 20.09.2022 r., sprawy połączone C-793/19 i C-794/19, *Bundesrepublik Deutschland przeciwko SpaceNet AG (C793/19), Telekom Deutschland GmbH (C794/19)*, EU:C:2022:702, pkt 91–94 – dalej wyrok sprawy połączone C-793/19 i C-794/19, *SpaceNet AG i Telekom*.

30 Zob. sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland*, pkt 46–47, 60; sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB*, pkt 102, 118–120; wyrok C-511/18, *La Quadrature du Net I*, pkt 140. Stanowisko to potwierdzone zostało w wyrokach: C-746/18, *Prokuratuur*, pkt 35; C-140/20, *Commissioner of An Garda Síochána*, pkt 63–67.

31 Zob. wyrok C-511/18, *La Quadrature du Net I*, pkt 157–159, podobnie w wyroku z 2.10.2018 r., C-207/16, *Ministerio Fiscal*, EU:C:2018:788, pkt 62.

32 Zgodnie z art. 2 lit. b dyrektywy 2002/58/WE dane o ruchu oznaczają „wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi”. Zob. G. Robinson, *A ‘necessary and limited development’...*, s. 3.

33 Wyrok C-511/18, *La Quadrature du Net I*, pkt 152. Por. K.S. Zielińska, *Powracający problem retencji danych telekomunikacyjnych. Potrzeba zapewnienia bezpieczeństwa narodowego czy może chęć utrzymania niekontrolowanej inwigilacji? – glosa do wyroku Trybunału Sprawiedliwości z 5.04.2022 r., C-140/20, G.D. przeciwko The Commissioner of the Garda Síochána i in.*, „Europejski Przegląd Sądowy” 2022/11, s. 44; A. Grzelak, K.S. Zielińska, *Między prawem do prywatności i ochroną danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International*, „Europejski Przegląd Sądowy” 2021/8, s. 34.

34 Wyrok sprawy połączone C-793/19 i C-794/19, *SpaceNet AG i Telekom*, pkt 100–102.

35 Wyrok sprawy połączone C-793/19 i C-794/19, *SpaceNet AG i Telekom*, pkt 103.

36 Tak M. Rojszczak, *Data retention in the light of copyright infringements: Protecting the status quo or seeking a third way?*, „Maastricht Journal of European and Comparative Law” 2024/4, s. 522.

37 Zob. wyrok C-511/18, *La Quadrature du Net I*, pkt 117–118, 153.

38 Por. N. Bouché, S. Valk, *CJEU in second round of privacy dispute by La Quadrature du Net: national authorities get their cake but they have to eat it with cutlery*, *European Law Blog* 2024.

39 Uzupełniona opinia Rzecznika Generalnego M. Szpunara z 28.09.2023 r., C-470/21, *La Quadrature du Net II*, pkt 60, 85. Por. opinię C-597/19, *M.I.C.M.*, pkt 103.

40 Według raportu SIRIUS z 2024 r. 41% organów sądowych UE wskazało brak ram retencji jako jedną z trzech głównych przeszkód w dochodzeniach transgranicznych; *connection logs* (51%) i adresy IP (38%) to najczęściej wskazywane kategorie danych niezbędnych w dochodzeniach; wnioski o dane kierowane przez organy UE do ośmiu głównych dostawców usług wzrosły z 87 tys. w 2018 r. do 267 tys. w 2023 r. (Europol, Eurojust, SIRIUS *EU Electronic Evidence Situation Report 2024*, The Hague 2024, s. 19,

szczegółowe warunki, na jakich retencja adresów IP nie stanowi poważnej ingerencji w prawa podstawowe, wydaje się mieć na celu stworzenie wzorca, na którym ustawodawcy krajowi mogą oprzeć regulację retencji w prawie wewnętrznym⁴¹. Głosowany wyrok nie powinien być więc rozumiany wyłącznie jako wąskie ustępstwo Trybunału „legalizujące” system HADOPI, a raczej jako próba znalezienia szerszego kompromisu pomiędzy ochroną praw podstawowych a potrzebami związanymi ze zwalczaniem przestępczości. W ten sposób został zresztą odczytany w dokumentach instytucjonalnych związanych z prowadzonymi przez Komisję Europejską pracami nad zharmonizowanym reżimem retencji⁴², gdzie uznaje się go za potwierdzenie dopuszczalności ogólnej retencji adresów IP w celu zwalczania przestępczości w każdym przypadku, w którym nie prowadzi ona do poważnej ingerencji w prawa podstawowe⁴³.

Towarzyszy temu jednak dostrzegalne osłabienie ochrony praw podstawowych. Nie chodzi jedynie o erozję poufności metadanych pochodzących z łączności elektronicznej i rozszerzenie dopuszczalności retencji adresów IP z poważnej przestępczości na ogół czynów zabronionych popełnianych w Internecie⁴⁴. Obniżony został również standard gwarancji proceduralnych. We wcześniejszym orzecznictwie Trybunał wymagał, by dostępowi do danych o ruchu towarzyszyła uprzednia kontrola sądu lub niezależnego organu administracyjnego. W głosowanym wyroku C-470/21, *La Quadrature du Net II*, przyjął natomiast, że skoro retencja adresów IP w warunkach szczelnej separacji nie stanowi poważnej ingerencji w prawa podstawowe, dostęp do nich nie wymaga kontroli indywidualnej, a wystarczy okresowa weryfikacja całego systemu retencji przez niezależny organ⁴⁵. Gwarancja uprzedniej kontroli sądowej, traktowana dotychczas jako warunek dostępu do danych o ruchu, zostaje w ten sposób zastąpiona kontrolą o charakterze systemowym, niezwiązaną z indywidualnymi przypadkami dostępu do danych⁴⁶.

Trudno przy tym uzasadnić obniżenie gwarancji proceduralnych samą potrzebą zwalczania „systemowej bezkarności” sprawców przestępstw internetowych. Do ograniczenia tego problemu wystarczyłoby rozszerzenie dopuszczalności retencji, bez rezygnacji z uprzedniej kontroli sądowej przy dostępie do danych. Rezygnacja ta ma jednak inne uzasadnienie. Uprzednia kontrola indywidualna jest trudna do pogodzenia z masowym, zautomatyzowanym dostępem do danych, jak w systemie HADOPI, w ramach którego identyfikacja użytkowników na podstawie adresów IP następuje na skalę liczoną w milionach przypadków rocznie. Uznanie, że taki dostęp nie wymaga uprzedniej kontroli sądu, otwiera drogę do wprowadzenia analogicznych rozwiązań w przepisach krajowych – nie tylko w odniesieniu do naruszeń praw autorskich, lecz także potencjalnie do każdego rodzaju czynów zabronionych popełnianych w Internecie (np. zniesławień czy mowy nienawiści)⁴⁷. Dokumenty instytucjonalne potwierdzają ten kierunek. Kontrola sądowa traktowana jest w nich jako wymóg warunkowy, stosowany jedynie „o ile jest niezbędna”, a rekomendacje dotyczące przyszłego reżimu retencji nie wymieniają uprzedniej kontroli sądowej wśród warunków dostępu do danych⁴⁸.

Obniżenie progu dopuszczalności retencji adresów IP zmniejsza napięcie między orzecznictwem retencyjnym a orzecznictwem dotyczącym ujawniania danych na potrzeby dochodzenia cywilnoprawnych roszczeń z tytułu naruszenia praw autorskich, nie eliminuje go jednak⁴⁹. W tym drugim obszarze Trybunał konsekwentnie orzekał, że prawo unijne nie stoi na przeszkodzie ustanowieniu przez państwa członkowskie obowiązku ujawniania tożsamości abonenta na podstawie adresu IP na potrzeby takich postępowań, lecz nie nakłada takiego obowiązku⁵⁰. Podstawą tej linii orzecniczej było odesłanie zawarte w art. 15 ust. 1 dyrektywy 2002/58/WE do art. 13 ust. 1 dyrektywy 95/46/WE, który upoważniał państwa członkowskie do ograniczenia obowiązku zachowania poufności danych osobowych m.in. w celu ochrony praw i wolności osób trzecich⁵¹. Trybunał odczytywał to odesłanie jako podstawę

38, 53, https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf, dostęp: 30.03.2026 r.). W państwach bez obowiązku retencji identyfikacja sprawcy bywa niemożliwa: HLG, *Concluding Report*, 22.11.2024 r., s. 26, https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en (dostęp: 30.03.2026 r.).

41 Wyrok C-470/21, *La Quadrature du Net II*, pkt 83–89.

42 HLG on Access to Data for Effective Law Enforcement, *Recommendations*, 6.06.2024 r., Rekomendacja 27, https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en (dostęp: 30.03.2026 r.). Komisja Europejska, *Call for Evidence: Impact assessment on retention of data by service providers for criminal proceedings*, Ares(2025)4081079, 21.05.2025 r.; *Roadmap for Effective and Lawful Access to Data for Law Enforcement*, COM(2025) 349 final, 24.06.2025 r., <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0349> (dostęp: 30.03.2026 r.). Propozycja legislacyjna planowana na I połowę 2026 r.

43 Raport SIRIUS 2024 streszcza wyrok jako zezwolenie na nałożenie na dostawców obowiązku ogólnej retencji IP w celu zwalczania przestępstw (SIRIUS 2024, s. 43). Raport końcowy grupy Going Dark wywodzi z wyroku zasadę, że „prywatność można zapewnić poprzez połączenie zasad przechowywania danych i dostępu do nich: (HLG, *Concluding Report*..., s. 35, przyp. 76).

44 Por. G. Robinson, *A 'necessary and limited development'...*, s. 12; M. Rojszczak, *Data retention*..., s. 533–534.

45 Wyrok C-470/21, *La Quadrature du Net II*, pkt 93, 96–99. Por. wyrok sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB*, pkt 120; wyrok C-746/18, *Prokuratuur*, pkt 51–52 (odnośnie do wymogu uprzedniej kontroli).

46 Tak M. Rojszczak, *Data retention*..., s. 534; A. Dekhuijzen, *La Quadrature du Net II and Data Retention under Article 15(1) ePrivacy Directive*, „European Data Protection Law Review” 2025/2, s. 257; Ch. Berthélémy, J. Lund, B. Le Querrec, *A complete U-turn in jurisprudence: HADOPI and the future of the CJEU's authority*, European Law Blog 2023.

47 Por. G. Robinson, *A 'necessary and limited development'...*, s. 4.

48 HLG, *Concluding Report*..., s. 9; s. 25, przyp. 39. Recommendation Cluster 6 (s. 34) nie wymienia uprzedniej kontroli sądowej wśród warunków dostępu. *Roadmap for Effective and Lawful Access to Data for Law Enforcement*, COM(2025) 349 final w ogóle nie odnosi się do wymogu kontroli sądowej.

49 G. Robinson, *A 'necessary and limited development'...*, s. 2; D. Jongsma, *The thorny issue of IP address retention and online copyright infringement: The full Court shows the way in La Quadrature du Net and Others (Personal data and action to combat counterfeiting)*, Social Science Research Network 2024, <https://papers.ssrn.com/abstract=4977631> (dostęp: 18.08.2025 r.), s. 2.

50 Wyrok TS z 29.01.2008 r., C-275/06, *Productores de Música de España (Promusicae)* przeciwko *Telefónica de España SAU*, EU:C:2008:54, pkt 68–70 – dalej wyrok C-275/06, *Promusicae*; wyrok TS z 19.04.2012 r., C-461/10, *Bonnier Audio*, EU:C:2012:219, pkt 55; wyrok TS z 17.06.2021 r., C-597/19, *Mircom International Content Management & Consulting (M.I.C.M.) Limited* przeciwko *Telenet BVBA*, EU:C:2021:492, pkt 125 – dalej wyrok C-597/19, *M.I.C.M.*

51 Wyrok C-275/06, *Promusicae*, pkt 53. Art. 13 ust. 1 lit. g dyrektywy 95/46/WE dopuszczał ograniczenia konieczne dla „ochrony osoby, której dane dotyczą, lub praw i wolności osób trzecich”. Por. art. 23 ust. 1 lit. j rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1, ze zm.), który potwierdza tę linię, wymieniając wprost egzekwowanie roszczeń cywilnoprawnych (zob. wyrok C-597/19, *M.I.C.M.*, pkt 117).

dopuszczalności udostępniania danych w kontekście egzekwowania praw autorskich, równoważąc ochronę danych osobowych z prawem własności intelektualnej (art. 17 ust. 2 KPP) i prawem do skutecznego środka prawnego (art. 47 KPP)⁵².

Pierwszy raz do zbliżenia obu linii orzeczniczych doszło w sprawie zakończonej wyrokiem TS z 17.06.2021 r., C-597/19, Mircom International Content Management & Consulting (M.I.C.M.) Limited przeciwko Telenet BVBA. Trybunał przejął w niej z wydanego rok wcześniej wyroku C-511/18, La Quadrature du Net I, zarówno kwalifikację adresów IP jako danych o ruchu⁵³, jak i wymóg krajowego środka ustawodawczego z art. 15 ust. 1 dyrektywy 2002/58/WE jako podstawy ich retencji⁵⁴. Nie odniósł się natomiast do centralnej tezy wyroku C-511/18, La Quadrature du Net I, zgodnie z którą retencja adresów IP może być uzasadniona „jedynie walką z poważną przestępczością”⁵⁵, pozostawiając sądom krajowym ocenę, czy prawo krajowe przewiduje podstawę prawną retencji i dostępu spełniającą wymogi prawa unijnego. Z wyroku wynika jednak, że gdyby retencja adresów IP i dostęp do nich okazały się sprzeczne z wymogami sformułowanymi w wyroku C-511/18, La Quadrature du Net I, powinny być uznane za niezgodne z prawem Unii⁵⁶.

Głosowany wyrok, obniżając próg dopuszczalności retencji do „ogółu czynów zabronionych”, poszerza zakres przypadków, w których ogólna retencja adresów IP jest dopuszczalna, i w ten sposób łagodzi wskazaną niespójność. Nie przesądza jednak wprost o warunkach, na jakich uprawnieni z tytułu praw autorskich mogą uzyskiwać dostęp do danych retencyjnych w postępowaniu cywilnym. Ma to znaczenie o tyle, że gwarancje uznane przez Trybunał za łagodzące ryzyko dla prywatności zostały sformułowane w odniesieniu do organu publicznego i mogą być trudne do przeniesienia na podmioty prywatne. Jaki standard powinny stosować sądy krajowe, rozstrzygając o żądaniu ujawnienia tożsamości użytkownika w postępowaniu cywilnym wytoczonym przez uprawnionego z tytułu praw autorskich, pozostaje więc kwestią otwartą⁵⁷.

Wyrok w sprawie C-470/21, La Quadrature du Net II, porusza się w ramach pojęć i kategorii wypracowanych w dotychczasowym orzecznictwie, nie zawsze jednak stosuje je konsekwentnie. Najpoważniejsza niespójność dotyczy kwalifikacji adresów IP. Trybunał potwierdza, że stanowią one dane o ruchu w rozumieniu dyrektywy 2002/58/WE⁵⁸, jednocześnie jednak odróżnia je od pozostałych danych tej kategorii i od danych lokalizacyjnych⁵⁹, traktując je jako podgrupę w obrębie danych o ruchu. Wymienia więc: dane dotyczące tożsamości cywilnej, adresy IP, „dane o ruchu inne niż adresy IP” oraz dane dotyczące lokalizacji⁶⁰. W kontekście dostępu HADOPI idzie jednak dalej, stwierdzając, że adres IP stanowi „dane dotyczące tożsamości

cywilnej, a nie dane o ruchu”⁶¹, a sentencja posługuje się językiem sugerującym, że adresy IP tworzą kategorię odrębną zarówno od danych o tożsamości cywilnej, jak i od pozostałych danych o ruchu⁶². Adres IP – formalnie należący do kategorii danych o ruchu – jest więc w kolejnych fragmentach wyroku traktowany w sposób właściwy dla innej kategorii, bez wskazania kryteriów decydujących o jego przypisaniu do jednej lub drugiej z nich⁶³. Granice między kategoriami danych, na których opiera się cały reżim retencji, ulegają w ten sposób zatarciu, co utrudnia sądom krajowym prawidłowe stosowanie orzecznictwa Trybunału⁶⁴.

Wyrok C-470/21, La Quadrature du Net II, nie wpływa na ocenę polskich przepisów retencyjnych. Po wyroku sprawy połączone C-293/12 i C-594/12, Digital Rights Ireland, nie zostały one dostosowane do standardów wynikających z orzecznictwa Trybunału. Obowiązek przechowywania metadanych dotyczących połączeń realizowanych za pomocą publicznie dostępnych usług oraz lokalizacji telekomunikacyjnych urządzeń końcowych, zawarty pierwotnie w art. 180a ustawy z 16.04.2004 r. – Prawo telekomunikacyjne⁶⁵, został przeniesiony (10.11.2024 r.) – bez istotnych zmian merytorycznych – do art. 47 ust. 1 w zw. z art. 49 ust. 1 ustawy z 12.07.2024 r. – Prawo komunikacji elektronicznej⁶⁶. Przepisy te przewidują ogólną i nieodróżnioną retencję danych o ruchu i lokalizacji przez 12 miesięcy, obejmującą wszystkich użytkowników i wszystkie środki komunikacji elektronicznej⁶⁷. Żaden z wymogów sformułowanych w wyrokach sprawy połączone C-203/15 i C-698/15, Tele2 Sverige AB, C-511/18, La Quadrature du Net I, czy sprawy połączone C-793/19 i C-794/19, SpaceNet AG i Telekom, nie został uwzględniony. Retencja ma więc charakter prewencyjny i uogólniony, w wielu przypadkach możliwy jest dostęp organów bez uprzedniej kontroli sądowej, nie przewidziano również ograniczenia kręgu podmiotów uprawnionych do dostępu wyłącznie do organów zwalczających poważną przestępczość⁶⁸. Niezgodność polskiej regulacji z prawem unijnym ma więc charakter strukturalny i nie może zostać usunięta przez powołanie się na złagodzenie przez TSUE jednego z wielu wymogów. Pewne nadzieje na zmianę tego stanu rzeczy można natomiast wiązać z pytaniami prejudycjalnymi skierowanymi przez Sąd Okręgowy w Gdańsku, który zwrócił się do Trybunału o ocenę zgodności

52 Wyrok C-275/06, Promusicae, pkt 61–65; wyrok C-597/19, M.I.C.M., pkt 120, 123.

53 Wyrok C-597/19, M.I.C.M., pkt 113, z odwołaniem do wyroku C-511/18, La Quadrature du Net I, pkt 152.

54 Wyrok C-597/19, M.I.C.M., pkt 129, z odwołaniem do wyroku C-511/18, La Quadrature du Net I, pkt 154.

55 Wyrok C-511/18, La Quadrature du Net I, pkt 156.

56 Wyrok C-597/19, M.I.C.M., pkt 119, 128, 130.

57 D. Jongsma, *The thorny issue...*, s. 15–16.

58 Wyrok C-470/21, La Quadrature du Net II, pkt 60.

59 Wyrok C-470/21, La Quadrature du Net II, pkt 76.

60 Wyrok C-470/21, La Quadrature du Net II, pkt 87.

61 Wyrok C-470/21, La Quadrature du Net II, pkt 101.

62 Wyrok C-470/21, La Quadrature du Net II, pkt 164.

63 Tak G. Robinson, *A 'necessary and limited development'...*, s. 3. Podobnie G. Westkamp, *Data retention, information disclosure and intellectual property enforcement: a truly „high standard” of protection?*, „Intellectual Property Quarterly” 2025/1, s. 50.

64 Zob. M. Rojszczak, *Data retention in the light of copyright infringements...*, s. 529–530.

65 Dz.U. z 2024 r. poz. 34 ze zm.

66 Dz.U. z 2024 r. poz. 1221 ze zm.

67 S. Piątek, *Prawo komunikacji elektronicznej. Komentarz*, Warszawa 2025, art. 47, nb 2–5.

68 *Prawo komunikacji elektronicznej. Komentarz*, red. M. Rogalski, Warszawa 2025, art. 47, nb 8. Na niezgodność polskich przepisów retencyjnych z prawem UE wskazywano od dawna: zob. A. Grzelak, K.S. Zielińska, *Miedzy prawem do prywatności...*, s. 35; K.S. Zielińska, *Powracający problem retencji...*, s. 48. Zob. również M. Rojszczak, *Polskie przepisy inwigilacyjne na tle standardów europejskich – glosa do wyroku Europejskiego Trybunału Praw Człowieka z 28.05.2024 r., skargi nr 72038/17 i 25237/18, Pietrzak i Bychawska-Siniarska i in. przeciwko Polsce*, „Europejski Przegląd Sądowy” 2025/1, s. 38. Zob. również pismo Prezesa UODO z 11.07.2024 r. (DOL.0623.15.2021).

art. 47 ustawy – Prawo komunikacji elektronicznej z art. 15 ust. 1 dyrektywy 2002/58/WE⁶⁹.

6. Podsumowanie

Dyrektywa 2002/58/WE reguluje przetwarzanie danych przez dostawców usług łączności elektronicznej, nie działalność organów ścigania. Sformułowane w orzecznictwie Trybunału ograniczenia dotyczące przechowywanych i udostępnianych przez operatorów danych określają jednak, jakie dane i na jakich warunkach mogą być udostępnione organom ścigania i innym uprawnionym podmiotom⁷⁰. Dotychczasowe orzecznictwo dopuszczało retencję adresów IP jedynie dla celów zwalczania „poważnej przestępczości”, co uniemożliwiało identyfikację sprawców „mniej poważnych” przestępstw popełnianych wyłącznie w Internecie, dla których adres IP stanowi często jedyny środek dochodzeniowy. Trybunał obniżył ten próg, dopuszczając powiązanie adresu IP z tożsamością cywilną użytkownika na potrzeby zwalczania ogółu czynów zabronionych, pod warunkiem, że dane te nie są agregowane z innymi danymi o ruchu i lokalizacji. Ponieważ adres IP sam w sobie identyfikuje tylko urządzenie użytkownika, takie rozwiązanie jest proporcjonalne i zasługuje na aprobatę.

Zastrzeżenia budzi przede wszystkim towarzysząca mu rezygnacja z uprzedniej kontroli sądowej przy dostępie do danych. Trybunał zastąpił ją okresową weryfikacją systemu przez niezależny organ, dopasowując standard gwarancyjny do specyfiki francuskiego systemu HADOPI, w ramach którego identyfikacja użytkowników następuje na skalę milionów przypadków rocznie. W takim kontekście kontrola indywidualna jest rzeczywiście trudna do pogodzenia ze skalą działania systemu. Problem polega jednak na tym, że głosowany wyrok formułuje ten obniżony standard w odniesieniu do „ogółu czynów zabronionych popełnianych on-line”, a nie wyłącznie do naruszeń praw autorskich. W przypadku zniesławień, mowy nienawiści czy innych form wypowiedzi w Internecie masowa identyfikacja autorów wypowiedzi, prowadzona bez kontroli sądowej, rodzi ryzyko ingerencji nie tylko w prawo do prywatności (art. 7 i 8 KPP), lecz także w wolność wypowiedzi (art. 11 KPP). Tego czynnika test proporcjonalności przeprowadzony w głosowanym wyroku nie bierze pod uwagę.

Bibliografia/References

Berthélemy C., Lund J., Querrec B.L., *A complete U-turn in jurisprudence: HADOPI and the future of the CJEU's authority*, „European Law Blog” 2023.
Bouché G., Valk E., *CJEU in second round of privacy dispute by La Quadrature du Net: national authorities get their cake but they have to eat it with cutlery*, „European Law Blog” 2024.
Dekhuijzen A.E., *La Quadrature du Net II and Data Retention under Article 15(1) ePrivacy Directive: CJEU Walks a Tightrope on IP Addresses Retention and Access for Public Authorities in*

Non-Serious Crime, „European Data Protection Law Review” 2025/2.

Grzelak A., *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności – glosa do wyroku TS z 21.12.2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB oraz C-698/15 Watson, Brice, Lewis*, „Europejski Przegląd Sądowy” 2017/3.

Grzelak A., Zielińska K.S., *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International*, „Europejski Przegląd Sądowy” 2021/8.

Jongsma D., *The thorny issue of IP address retention and online copyright infringement: The full Court shows the way in La Quadrature du Net and Others (Personal data and action to combat counterfeiting)*, Social Science Research Network 2024, <https://papers.ssrn.com/abstract=4977631> (dostęp: 18.08.2025 r.).

Kosta E., *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, „SCRIPTed” 2013/3.

Lucchi N., *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, „Cardozo Journal of International and Comparative Law” 2011/3.

Piątek S., *Prawo komunikacji elektronicznej: komentarz*, Warszawa 2025.

Prawo komunikacji elektronicznej: komentarz, red. M. Rogalski, Warszawa 2025.

Robinson G., *A 'necessary and limited development' of the data retention case law, or its death by a thousand cuts?*, „Computer Law & Security Review” 2025/58.

Rojszczak M., *Data retention in the light of copyright infringements: Protecting the status quo or seeking a third way? (Case C-470/21 La Quadrature du Net II)*, „Maastricht Journal of European and Comparative Law” 2024/4.

Rojszczak M., *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*, „European Constitutional Law Review” 2021/4.

Rojszczak M., *Polskie przepisy inwigilacyjne na tle standardów europejskich – glosa do wyroku Europejskiego Trybunału Praw Człowieka z 28.05.2024 r., skargi nr 72038/17 i 25237/18, Pietrzak i Bychawska-Siniarska i in. przeciwko Polsce*, „Europejski Przegląd Sądowy” 2025/1.

Westkamp G., *Data retention, information disclosure and intellectual property enforcement: a truly „high standard” of protection?*, „Intellectual Property Quarterly” 2025/1.

Wojnowska-Radzińska J., *Implications of Pre-emptive Data Surveillance for Fundamental Rights in the European Union*, Leiden–Boston 2023.

Zielińska K.S., *Powracający problem retencji danych telekomunikacyjnych. Potrzeba zapewnienia bezpieczeństwa narodowego czy może chęć utrzymania niekontrolowanej inwigilacji? – glosa do wyroku Trybunału Sprawiedliwości z 5.04.2022 r., C-140/20, G.D. przeciwko The Commissioner of the Garda Síochána i in.*, „Europejski Przegląd Sądowy” 2022/11.

Ziller J., *The Conseil d'Etat refuses to follow the Pied Piper of Karlsruhe*, <https://verfassungsblog.de/the-conseil-detat-refuses-to-follow-the-pied-piper-of-karlsruhe/> (dostęp: 8.02.2026 r.).

69 Zob. postanowienie SO w Gdańsku z 13.11.2025 r., I C 1281/25; sprawa zarejestrowana w TSUE pod sygn. C-741/25, Ranerski, <https://infocuria.curia.europa.eu/tabs/document/C/2025/C-0741-25-000000000RP-01-P-01/DDP/313092-PL-1-pdf> (dostęp: 17.06.2026 r.).

70 Zob. wyrok sprawy połączone C-203/15 i C-698/15, Tele2 Sverige AB, pkt 75–81. Por. A. Grzelak, *Trybunał Sprawiedliwości ponownie...*, s. 35; K.S. Zielińska, A. Grzelak, *Między prawem do prywatności...*, s. 32.

Abstract

dr Zbigniew Okoń

Legal advisor

(ORCID: <https://orcid.org/0000-0002-0999-780X>).**Is It the End of Online Anonymity?****Commentary on Judgment of the Court of Justice**of 30 April 2024, C-470/21, *La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network v Premier ministre, Ministre de la Culture***Keywords:** telecommunications data retention, personal data, protection of privacy, IP addresses, electronic communications, Charter of Fundamental Rights of the European Union, combating infringements of copyright committed online

The retention of telecommunications data has been the subject of numerous questions referred to the Court of Justice of the European Union by national courts over the last ten years. The CJEU judgment of 30 April 2024, C-470/21, *La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network v Premier ministre, Ministre de la Culture*, regarding the interpretation of Article 15(1) of Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) in the context of the French system for combating infringements of copyrights committed online (*Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet, HADOPI*), is one of the judgments on this issue. The Court, adjudicating as the full Court, ruled that the general retention of IP addresses, while ensuring a watertight separation from other categories of data, does not constitute a serious interference with the rights guaranteed by Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union and is allowed for combating criminal offences in general, without prior court review, on condition that detailed technical and procedural requirements intended to prevent data aggregation are satisfied. The adopted interpretation liberalises the retention rules to date, addressing the expectations of some of the Member States at the expense of some weakening of the protection of fundamental rights.

REKLAMA



GDZIE KOŃCZY SIĘ INSPIRACJA, A ZACZYNA NADUŻYCIE?

Folklor coraz częściej trafia do świata mody, reklamy i popkultury. Publikacja odświeża skalę problemu niewłaściwej eksploatacji motywów ludowych, które coraz częściej funkcjonują w oderwaniu od swojego pochodzenia i kulturowego sensu.

Autor pokazuje, gdzie kończy się inspiracja, a zaczyna nadużycie. Przedstawia mechanizmy ochrony folkloru przed jego niekontrolowanym, komercyjnym wykorzystywaniem, udowadniając, że wiele form twórczości tradycyjnej może – i powinno – podlegać realnej ochronie prawnej.

Na podstawie szerokiej analizy prawa międzynarodowego i krajowego autor proponuje nowoczesny, spójny model ochrony folkloru.

**ZAMÓW KSIĄŻKĘ Z RABATEM 20% W KSIĘGARNI PROFINFO.PL
W FORMULARZU ZAMÓWIENIA WPISZ KOD: WKCZA20**

OCHRONA FOLKLORU W PRAWIE WŁASNOŚCI INTELEKTUALNEJ

Łukasz Maryniak