Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
M. SZPUNAR
представено на 28 септември 2023 година [1]

**Дело C-470/21**

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

(Преюдициално запитване, отправено от Conseil d'État (Държавен съвет, Франция)

„Преюдициално запитване — Обработка на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации — Директива 2002/58/ЕО — Член 15, параграф 1 — Възможност за държавите членки да ограничават обхвата на някои права и задължения — Задължение за предварителен контрол от съд или от независима административна структура с правомощия да издава правнообвързващи актове — Данни за самоличност, съответстващи на IP адрес"

## I. Въведение

1. По искане на големия състав на основание член 60, параграф 3 от Процедурния правилник на Съда от 7 март 2023 г. Съдът решава да поиска делото да бъде преразпределено в пленум.

2. С определение от 23 март 2023 г. Съдът (пленум) постановява възобновяване на устната фаза на производството и приканва заинтересованите субекти по член 23 от Статута на Съда на Европейския съюз, както и Европейския надзорен орган по защита на данните (ЕНОЗД) и Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) да участват в ново съдебно заседание.

3. На 27 октомври 2022 г. представих първото си заключение по това дело преди приключване на устната фаза на производството. Ето защо според мен новото заключение е повод да задълбоча анализа на някои аспекти от съображенията си по това дело с основни предизвикателства, що се отнася до съхраняването и достъпа до лични данни.

[1] Език на оригиналния текст: френски.

## II. Правна уредба

### *A. Правото на Съюза*

4. Съображения 2, 6, 7, 11, 22, 26 и 30 от Директива 2002/58/ЕО [2] гласят:

„(2) Настоящата директива се стреми да зачита основните права и да спазва признатите принципи, по-специално от Хартата на основните права на Европейския съюз [(наричана по-нататък „Хартата“)]. По-специално[,] настоящата директива се стреми да осигури пълно зачитане на правата, предвидени в членове 7 и 8 от Хартата.

[…]

(6) Интернет преобръща традиционните пазарни структури, като осигурява обща глобална инфраструктура за доставка на широк обхват от електронни комуникационни услуги. Публично достъпните електронни комуникационни услуги чрез интернет разкриват нови възможности за потребителите, но също нови рискове за техните лични данни и неприкосновеност на личния им живот.

(7) В случая на публични комуникационни мрежи[…] трябва да се изготвят специфични законови, подзаконови и технически разпоредби, за да се защитят основните права и свободи на физическите лица и легитимните интереси на юридическите лица, по-специално по отношение на увеличаващата се способност за автоматизирано съхранение и обработка на данни за абонати и потребители.

[…]

(11) Както Директива [95/46/ЕО [3]], настоящата директива не се отнася до въпросите за защита на основните права и свободи[,] свързани с дейности, които не се управляват от законодателството на Общността. Затова тя не променя съществуващия баланс между правото на индивида на неприкосновеност на личния живот и възможността на държавите членки да предприемат мерки, съгласно член 15, параграф 1 от настоящата директива, необходими за защита на обществената сигурност, отбраната, сигурността на държавата (включително икономическото благополучие на държавата, когато дейностите се отнасят до въпроси по сигурността на държавата) и прилагане в изпълнение на наказателното право. Следователно настоящата директива не засяга възможността на държавите членки да провеждат законно пр[е]хващане на електронни комуникации или да предприемат други мерки, ако е необходимо за някои от тези цели и в съответствие с Европейската конвенция за защита на човешките права и основните свободи[, подписана в Рим на 4 ноември 1950 г.], съгласно тълкуването на решенията на Европейския съд за [правата на човека]. Такива мерки трябва да бъдат уместни, строго пропорционални на предвидената цел

[2] Директива на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63, и поправки в ОВ L 145, 2017 г., стр. 27 и в ОВ L 241, 2013 г., стр. 9), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година (ОВ L 337, 2009 г., стр. 11) (наричана по-нататък „Директива 2002/58“).

[3] Директива на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10).

и необходими в едно демократично общество[…] и следва да бъдат предмет на съответна защита в съответствие с Европейската конвенция за защита на човешките права и основните свободи.

[…]

(22) Забраната да се съхраняват съобщения и свързаните данни за трафик от лица, различни от потребителите, или без тяхното съгласие, не е насочен[а] да забрани автоматично, междинно и временно съхранение на тази информация, доколкото това се прави с единствената цел осъществяване на предаване в електронни комуникационни мрежи и при условие че тази информация не се съхранява за период, по-дълъг от необходимия за предаване и за целите на ръководене на трафика, и че през периода на съхранение[…] конфиденциалният характер остава гарантиран. […]

[…]

(26) Данните, отнасящи се до абонатите, обработвани в електронн[и] комуникационни мрежи за осъществяване на връзки и предаване на информация, съдържат информация за личния живот на физически лица и засягат правото да се зачита тяхната кореспонденция или засягат легитимни интереси на юридически лица. Такива данни могат да бъдат съхранени само до степен, която е необходима за осигуряване на услугата с цел изготвяне на сметка и за плащания при взаимна връзка и за ограничено време. Всякаква по-нататъшна обработка на такива данни […] може да бъде позволена[…] само ако абонатът е дал съгласието си за това, на базата на точна и пълна информация, дадена от доставчика на публично достъпни електронни комуникационни услуги, за типа на по-нататъшната обработка, предвидена да се извърши, и за правото на абоната да не даде или да оттегли [своето] съгласие за такава обработка. […]

[…]

(30) Системите за обезпечаване на електронни комуникационни мрежи и услуги трябва да бъдат направени[…] така[,] че да ограничават количеството на необходимите лични данни до точен минимум. […]“.

5. Съгласно член 2 („Дефиниции“) от тази директива:

„[…]

Прилагат се също следните дефиниции:

а) „потребител“ означава всяко физическо лице, използващо публично достъпни електронни комуникационни услуги за частни или бизнес цели, без да е необходимо да се е абонирал за тази услуга;

б) „данни за трафик“ означава всякакви данни, обработени с цел пренасяне на комуникация през електронни комуникационни мрежи или за изготвяне на сметка за това;

в) „данни за местонахождение“ означава всякакви данни, обработени в електронна съобщителна мрежа или чрез електронна съобщителна услуга, показващи географското местоположение на крайното оборудване на ползвателя на обществено достъпни електронни съобщителни услуги;

г) „комуникация“ означава всяка информация, обменена или пренесена между определен брой страни с помощта на публично достъпни електронни комуникационни услуги. Това не включва информация, пренасяна като част от услуга за публично радиоразпръскване през електронни комуникационни мрежи[,] с изключение на информацията, която може да бъде свързана с идентифицируем абонат или потребител, получаващ информацията;

[…]“.

6. Член 3 („Обхванати услуги“) от посочената директива предвижда:

„Настоящата директива се прилага при обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в Общността, включително обществени съобщителни мрежи, поддържащи събиране на данни и устройства за идентификация“.

7. Член 5 („Конфиденциалност на комуникациите“) от същата директива предвижда:

„1. Държавите членки гарантират конфиденциалност на съобщенията и свързани[те с тях данни за трафика] през публични комуникационни мрежи и публично достъпни електронни комуникационни услуги, чрез националното си законодателство. По-специално[,] те забраняват слушане, записване, съхранение и други видове подслушване или наблюдение на съобщения и свързаните данни за трафика от страна на лица, различни от потребители[,] без съгласието на заинтересованите потребители, с изключение на законно упълномощени да извършват това[,] в съответствие с член 15[,] параграф 1. Настоящият параграф не пречи на техническото съхранение, което е необходимо за пренасяне на комуникация, без да противоречи на принципа за конфиденциалност.

[…]

3. Държавите членки гарантират, че съхраняването на информация или получаването на достъп до информация, вече съхранявана в крайното оборудване на абоната или ползвателя, е позволено само при условие че съответният абонат или ползвател е дал своето съгласие след получаване на предоставена ясна и изчерпателна информация в съответствие с Директива [95/46], inter alia, относно целите на обработката. Това не пречи на всякакво техническо съхранение или достъп с единствена цел осъществяване на предаването на съобщение по електронна съобщителна мрежа или доколкото е строго необходимо, за да може доставчикът да предостави услуга на информационното общество, изрично поискана от абоната или ползвателя“.

8. Съгласно член 6 („Данни за трафик“) от Директива 2002/58:

„1. Данни за трафик, отнасящи се до абонати и потребители, обработени и съхранени от доставчика на публични комуникационни мрежи или публично достъпни електронни

комуникационни услуги, трябва да бъдат изтрити или да се направят анонимни, когато не са необходими повече за целите на предаване на комуникация, без да се накърнява[т] параграф[и] 2, 3 и 5 от настоящия член и член 15, параграф 1.

2. Могат да бъдат обработени данни за трафик, необходими за целите на изготвяне на сметката на абоната и плащания при взаимна връзка. Такава обработка е допустима само до края на периода, през който сметката може законно да бъде оспорена или плащането търсено.

[…]“.

9. Член 15, параграф 1 („Приложение на някои разпоредби от Директива [95/46]“) от Директива 2002/58 гласи:

„Държавите членки могат да приемат законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в член 5, член 6, член 8, параграф[и] 1, 2, 3[…] и 4 и член 9 от настоящата директива, когато такова ограничаване представлява необходима, подходяща и пропорционална мярка в рамките на демократично общество, за да гарантира национална сигурност (т.е. държавна сигурност), отбрана, обществена безопасност и превенцията, разследването, разкриването и преследването на [престъпления] или неразрешено използване на електронна комуникационна система, както е посочено в член 13, параграф 1 от Директива [95/46]. В тази връзка[…] държавите членки могат, inter alia, да одобрят законодателни мерки, предвиждащи съхранението на данни за ограничен период, оправдани на основанията, изложени в настоящия параграф. Всички мерки, упоменати в настоящия параграф, трябва да бъдат в съответствие с общите принципи на законодателството на [Съюза], включително онези, упоменати в член 6, параграф[и] 1 и 2 [ДЕС]“.

### *Б. Френското право*

#### *1. Кодексът за интелектуалната собственост*

10. Член L. 331-12 от Code de la propriété intellectuelle (Кодекс за интелектуалната собственост, наричан по-нататък „CPI“), в редакцията му, приложима към спора по главното производство, гласи:

„Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (Висшият орган за разпространение на произведенията и защитата на правата в интернет [наричан по-нататък „Hadopi“]) е независим публичен орган“.

11. Член L. 331-13 от CPI предвижда:

„[Hadopi] осигурява:

[…]

2° Изпълнението на функции по закрила [на произведения и обекти, по отношение на които са налице авторски или сродни права, когато тези произведения са предавани по електронни съобщителни мрежи] по отношение на нарушения на тези права, извършени в електронните съобщителни мрежи, използвани за предоставяне на публични съобщителни услуги в интернет; […]“.

12. Съгласно член L. 331-15 от този кодекс:

„[Hadopi] се състои от Колегия и Комисия за защита на правата. […]

[…]

При изпълнение на правомощията си членовете на Колегията и на Комисията за защита на правата не получават указания от други органи“.

13. Член L. 331-17 от посочения кодекс гласи:

„Комисията за защита на правата е компетентна да предприеме мерките по член L. 331-25“.

14. Съгласно член L. 331-21 от същия кодекс:

„За да може Комисията за защита на правата да упражнява своите правомощия, [Hadopi] има на разположение заклети длъжностни лица, назначени от [неговия] председател при условия, определени с декрет, съгласуван с Държавния съвет. […].

Жалбите и сигналите до Комисията за защита на правата се получават от членовете на тази комисия и от посочените в алинея първа длъжностни лица при условията, предвидени в член L. 331-24. Те извършват проверка на фактите.

За нуждите на производството те имат право да получат всички документи, независимо от информационния носител, включително данните, запазвани и обработвани от операторите на електронни съобщителни услуги по член L. 34-1 от Code des postes et des communications électroniques (Кодекс за пощите и електронните съобщения) и доставчиците по член 6, параграф I, точки 1 и 2 от Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique (Закон № 2004-575 от 21 юни 2004 г. за доверието в цифровата икономика).

Те могат да получават също копия от посочените в предходната алинея документи.

Те могат по-специално да получават от операторите на електронни съобщителни услуги данни за самоличността, пощенския адрес, адреса на електронна поща и телефонните номера на абоната, чийто достъп до обществени съобщителни услуги в интернет е бил използван за възпроизвеждане, представяне, предоставяне на публично разположение или публично разгласяване на произведения или други закриляни обекти без разрешението на титулярите на правата […], когато се изисква такова“.

15. Член L. 331-24 от CPI гласи:

„Когато е сезирана, Комисията за защита на правата упражнява своите правомощия чрез заклети и упълномощени длъжностни лица […], които са назначени от:

– законосъобразно конституирани органи за професионална защита,

– организации за колективно управление на авторски права,

– Centre national du cinéma et de l'image animée (Национален кинематографичен център).

Комисията за защита на правата може да предприема действия и въз основа на данни, които са ѝ предадени от прокурора на Републиката.

Тя не може да бъде сезирана за деяния, извършени преди повече от шест месеца".

16. Съгласно член L. 331-25 от този кодекс, който урежда процедурата, наречена „поетапен отговор":

„Когато Комисията за защита на правата е сезирана за извършването на деяния, които могат да съставляват неизпълнение на задължението по член L. 336-3 [от CPI], тя може да отправи препоръка до абоната […], с която да му припомни разпоредбата на член L. 336-3, който повелява да се спазва задължението по този член, и да му посочи санкциите, които могат да бъдат налагани съгласно членове L. 335-7 и L. 335-7-1. С тази препоръка абонатът се уведомява също за условията за законосъобразно предлагане на произведения с културно съдържание в интернет, за наличието на правни средства за защита, които позволяват да се избегне неизпълнение на задължението по член L. 336-3, както и за опасностите за обновяване на художественото творчество и за икономиката на културния сектор в резултат на практики, които са в нарушение на авторското право и сродните му права.

В случай че в срок от шест месеца след изпращането на препоръката по алинея първа бъдат повторно извършени деяния, които могат да съставляват неизпълнение на задължението по член L. 336-3, Комисията може да отправи по електронен път нова препоръка, съдържаща същата информация като предходната […]. Комисията прилага към препоръката обратна разписка, потвърждаваща получаването срещу насрещен подпис или друго подходящо средство, с което може да се докаже на коя дата е връчена препоръката.

В препоръките, отправяни на основание настоящия член, се посочват датата и часът, в които са установени извършените деяния, които могат да съставляват неизпълнение на задължението по член L. 336-3. В тези препоръки обаче не се разкрива съдържанието на закриляните произведения или обекти, засегнати от неизпълнението на задължението. В препоръките се посочват телефонни номера, пощенски адрес и адрес на електронна поща, на които получателят може да представи по желание становище до Комисията за защита на правата и да получи при изрично направено искане уточнения относно съдържанието на закриляните произведения или обекти, засегнати от неизпълнението, в което е упрекнат".

17. Член L. 331-29 от посочения кодекс гласи:

„[Hadopi] може да въведе система за автоматизирана обработка на лични данни на лицата, срещу които е образувано производство по настоящия раздел.

Целта на тази обработка е Комисията за защита на правата да може да прилага предвидените в настоящия подраздел мерки, да издава всички свързани с производството актове и да спазва реда и начина за уведомяване на органите за професионална защита и на организациите за колективно управление на авторски права за евентуални жалби до съдебния орган, както и за уведомленията, предвидени в член L. 335-7, пета алинея.

Редът и условията за прилагане на настоящия член се определят с декрет […]. С декрета по-специално се уточняват:

– категориите регистрирани данни и продължителността на тяхното съхраняване,

– лицата, които са упълномощени да получават тези данни, по-специално лицата, осъществяващи дейност по предоставяне на достъп до обществени съобщителни услуги в интернет,

– условията, при които заинтересованите лица могат да упражнят пред [Hadopi] правото си на достъп до свързаните с тях данни […]“.

18. Член R. 331-37 от същия кодекс предвижда:

„Операторите на електронни съобщителни услуги […] и доставчиците […] са длъжни чрез взаимна свързаност със системата за автоматична обработка на лични данни, посочена в член L. 331-29, или чрез записването им на информационен носител, осигуряващ тяхната цялост и сигурност, да предоставят личните данни и информацията, посочена в [точка] 2 от приложението към [Декрет № 2010-236 от 5 март 2010 г. относно автоматизираната обработка на лични данни, разрешена съгласно член L. 331-29 от [CPI], наречена „Система за управление на мерките за закрила на произведения в интернет“ [4] (наричан по-нататък „Декретът от 5 март 2010 г.)] […], в срок от осем дни, след като Комисията за защита на правата е получила техническите данни, необходими за установяването на самоличността на абоната, чийто достъп до обществени съобщителни услуги в интернет е използван за възпроизвеждане, представяне, предоставяне на публично разположение или публично разгласяване на закриляни произведения или обекти без разрешението на титулярите на правата […], когато се изисква такова.

[…]“.

[4] JORF от 7 март 2010 г., текст № 19.

19. Член R. 335-5 от CPI гласи:

„I.- Когато са налице условията по параграф II, лицето с право на достъп до обществени съобщителни услуги в интернет извършва деяние при условията на груба небрежност, което се наказва с глобата, предвидена за престъпления от пета категория, ако това лице без основателна причина:

1° не е предприело мерки за обезопасяване на достъпа или

2° не е положило дължимата грижа при прилагането на тези мерки.

II.- Разпоредбите на параграф I се прилагат само ако са изпълнени следните две условия:

1° Ако в съответствие с член L. 331-25 и в предвидените от този член форми Комисията за защита на правата е препоръчала на лицето с право на достъп да приведе в изпълнение мерки за обезопасяване на достъпа до обществени съобщителни услуги в интернет, с което да позволи да се избегне възможността този достъп да се използва отново за възпроизвеждане, представяне, предоставяне на публично разположение или публично разгласяване на произведения или обекти, закриляни от авторско или сродно право, без разрешението на титулярите на права […], когато се изисква такова;

2° Ако през годината, след като е направена тази препоръка, този достъп е използван повторно за целите по точка 1 от настоящия параграф II“.

20. Член L. 336-3 от този кодекс гласи:

„Лицето с право на достъп до обществени съобщителни услуги в интернет е длъжно да следи този достъп да не се използва за възпроизвеждане, представяне, предоставяне на публично разположение или публично разгласяване на произведения или обекти, закриляни от авторско или сродно право, без разрешението на титулярите […], когато се изисква такова.

Неизпълнението на задължението по алинея първа от лицето с право на достъп до интернет не води до ангажиране на наказателната отговорност на заинтересованото лице […]“.

*2. Декретът от 5 март 2010 г.*

21. Член 1 от Декрета от 5 март 2010 г., в редакцията му, приложима към фактите по спора в главното производство, гласи:

„Целта на обработването на лични данни, наречено „Система за управление на мерките за закрила на произведения в интернет“, е Комисията за защита на правата към [Hadopi] да може да:

1° прилага мерките, предвидени в книга III от част от [CPI] с ранг на закон (дял III, глава I, раздел 3, подраздел 3) и книга III от част от същия кодекс с ранг на нормативен административен акт (дял III, глава I, раздел 2, подраздел 2);

2° сезира прокурора на Републиката за деяния, които могат да са съставомерни по членове L. 335-2, L. 335-3, L. 335-4 и R. 335-5 от същия кодекс, както и да уведомява

организациите за професионална защита и организациите за колективно управление за действията по това сезиране;

[…]“.

22. Член 4 от същия декрет гласи:

„I.- Упълномощените съгласно член L. 331-21 от [CPI] от председателя на [Hadopi] заклети длъжностни лица и членовете на Комисията за защита на правата по член 1 имат пряк достъп до личните данни и до информацията, посочена в приложението към настоящия декрет.

II.- Операторите на електронни съобщителни услуги и доставчиците по точка 2 от приложението към настоящия декрет са получатели на:

– техническите данни, необходими за установяването на самоличността на абоната,

– препоръките по член L. 331-25 от [CPI] с оглед изпращането на същите по електронен път на абонатите,

– данните, необходими за изпълнение на допълващите наказания, изразяващи се в спиране на достъпа до обществена съобщителна услуга в интернет, за които прокурорът на Републиката е уведомил Комисията за защита на правата.

III.- Органите за професионална защита и организациите за колективно управление са получатели на информация относно действията по сезиране на прокурора на Републиката.

IV.- Съдебните органи са получатели на протоколите за установяване на извършените деяния, които могат да са съставомерни по членове L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 и R. 335-5 от [CPI].

Автоматизираният регистър за съдимост се уведомява за изпълнението на наказанието спиране на достъпа до услугата“.

23. Приложението към Декрета от 5 март 2010 г. предвижда:

„Лични данни и сведения, записани при обработката, наречена „Система за управление на мерките за закрила на произведения в интернет“, са следните:

1° Лични данни и сведения с източник от законосъобразно конституирани органи за професионална защита, организации за колективно управление на авторски права, Националния кинематографичен център и прокурора на Републиката:

По отношение на деянията, които могат да съставляват неизпълнение на задължението по член L. 336-3 от [CPI]:

Дата и час на извършване на деянията;

IP адрес на съответните абонати;

Използван протокол с равноправен достъп (peer-to-peer);

Псевдоним, използван от абоната;

Информация за защитените произведения и обекти, засегнати от извършените деяния;

Име на файла, както фигурира на компютърната работна станция на абоната (евентуално);

Доставчик на достъп до интернет, с който е сключен договор за достъп до интернет или който предоставя техническото средство IP.

[…]

2° Лични данни и информация за абоната, събрани от операторите на електронни съобщителни услуги […] и от доставчиците […]:

Име и фамилно име;

Пощенски адрес и адрес на електронна поща;

Телефонни номера;

Местонахождение на телефонната инсталация на абоната;

Доставчик на достъп до интернет, използващ техническите ресурси на доставчика на достъп, посочен в точка 1, с който абонатът е сключил договор; номер на преписка;

Начална дата на спиране на достъпа до обществена съобщителна услуга в интернет.

[…]“.

*3. Code des postes et des communications électroniques (Кодекс за пощите и електронните съобщения)*

24. Член L. 34-1, параграф II bis от Code des postes и des communications électroniques (Кодекс за пощите и електронните съобщения), изменен с член 17 от Закон № 2021-998 от 30 юли 2021 г.[5], гласи следното:

„[О]ператорите на електронни съобщителни услуги са длъжни да съхраняват:

[5] JORF от 31 юли 2021 г., текст № 1. Тази редакция на член L. 34-1 от този кодекс, която е в сила от 31 юли 2021 г., е приета след решение № 393099 на Conseil d'État (Държавен съвет, Франция) от 21 април 2021 г. (JORF от 25 април 2021 г.), с което се отменя предходна редакция на тази разпоредба, която включва задължение за запазване на личните данни „за целите на разследването, разкриването и наказателното преследване на престъпления или на неизпълнението на задължението по член L. 336-3 [от CPI]“, с единствената цел да се направи възможно евентуалното им предоставяне, по-специално на Hadopi. С решение № 2021-976-977 QPC от 25 февруари 2022 г. (Habib A. и др.) Conseil constitutionnel (Конституционен съвет, Франция) приема, че предходната редакция на член L. 34-1 от посочения кодекс противоречи на Френската конституция, с основния мотив, че „като разрешават общо и несистематизирано съхраняване на данните за свързване с интернет, оспорените разпоредби накърняват несъразмерно правото на зачитане на личния живот“ (т. 13). Всъщност тази юрисдикция приема, че данните за свързване, които трябва да се съхраняват по силата на тези разпоредби, не се отнасят само до идентифицирането на ползвателите на електронни съобщителни услуги, но и до други данни, които „предвид своето естество, своето разнообразие и обработването, на което могат да бъдат предмет, […] предоставят изобилна и конкретна информация за тези ползватели, както и евентуално за трети лица, която накърнява в значителна степен личния им живот“ (т. 11).

1° За целите на наказателното преследване, с оглед на предотвратяването на заплахи срещу обществената сигурност и с цел опазване на националната сигурност — информация относно самоличността на ползвателя до изтичането на срок от пет години, считано от датата на изтичане на срока на действие на неговия договор;

2° За същите цели като посочените в точка 1° от настоящия [параграф] II bis — другата информация, предоставяна от ползвателя при сключването на договор или създаването на профил, както и информация за плащането, до изтичането на срок от една година от датата на изтичане на срока на действие на неговия договор или на закриване на неговия профил;

3° За целите на борбата с тежката престъпност, с оглед предотвратяване на сериозни заплахи срещу обществената сигурност и с цел опазване на националната сигурност — техническите данни, позволяващи да се идентифицира източникът на връзката, или данните за използваните крайни устройства — до изтичането на срок от една година от установяването на връзката или от използването на крайните устройства“.

## III. Производството пред Съда

25. В отговор на поканата до заинтересованите страни по член 23 от Статута на Съда на Европейския съюз жалбоподателите в главното производство, френското, датското, естонското, ирландското, нидерландското, финландското и шведското правителство и Европейската комисия отговарят на поставените от Съда писмени въпроси.

26. Същите страни, с изключение на финландското правителство — чешкото, испанското, кипърското, латвийското и норвежкото правителство, както и ЕНОЗД и ENISA участват в съдебното заседание, проведено на 15 май 2023 г.

## IV. Анализ

27. Въз основа на моя анализ на преюдициалните въпроси в първото ми заключение предлагам на Съда да постанови, че член 15, параграф 1 от Директива 2002/58 трябва да се тълкува в смисъл, че допуска национална правна уредба, позволяваща съхраняването на данните за самоличност, съответстващи на IP адреси, от страна на доставчиците на електронни съобщителни услуги и ограничения достъп на административен орган като Hadopi [6] само до такива данни, за да може този орган да идентифицира титулярите на тези адреси, заподозрени, че носят отговорност за извършването на нарушения на авторските и сродните им права, и в зависимост от съответния случай да може да предприеме конкретни действия срещу тях, без този достъп да бъде подлаган на предварителен контрол от юрисдикция или от независима административна структура, когато тези данни са единственото средство за разследване, позволяващо да се идентифицира лицето, на което е предоставен този адрес в момента на извършване на деянието.

[6] На 1 януари 2022 г. Conseil supérieur de l’audiovisuel (Висш съвет за аудио-визуални медии, наричан накратко „CSA“) и Hadopi се преобразуват в Autorité de régulation de la communication audiovisuelle et numérique (Регулаторен орган в областта на аудио-визуалната и цифровата комуникация, наричан накратко „Arcom“). Въпреки това, предвид периода, през който настъпват фактите в главното производство, анализът ми в настоящото заключение е относно Hadopi.

28. В настоящото заключение ще се опитам да задълбоча анализа на някои аспекти от предходния си анализ и на въпросите, обсъдени в съдебното заседание, проведено на 15 май 2023 г., за да изложа причините, поради които поддържам както предложението си за отговор на преюдициалните въпроси, така и съображенията, довели до него[7].

29. По-конкретно, ще докажа, че разрешаването на възможност за съхраняване и достъп до данни за самоличност, съответстващи на IP адреси, без предварителна проверка, за да се идентифицират извършителите на нарушения, когато тези данни са единственото средство за идентифицирането им, отговаря на изискванията, изведени от Съда по отношение на разглеждането на мерките, приети на основание член 15, параграф 1 от Директива 2002/58 (раздел Б).

30. С оглед на това ще докажа, че такова разрешение не представлява преразглеждане на взискателната и защитаваща основните права практика на Съда след решения Tele2 Sverige и Watson и др.[8] и La Quadrature du Net и др.[9], а необходимо развитие на съдебната практика, което според мен е в съответствие с принципите, изведени от Съда. Това разграничение не е само смислово. Това е така, защото разрешението, което предлагам, няма за цел да постави под въпрос съществуващата съдебна практика, а да позволи, в името на известен прагматизъм, нейното адаптиране към конкретни и много тясно очертани обстоятелства (раздел В).

31. От съображения за яснота и доколкото устните състезания в съдебното заседание показват необходимост от уточнения в това отношение, ще започна анализа си с припомняне на начина, по който функционира механизмът за поетапен отговор, прилаган от Hadopi (раздел А).

### *А. Механизмът за поетапен отговор, прилаган от Hadopi*

32. Hadopi е независим административен орган, на който е възложена защитата на авторските и сродните им права срещу извършени в интернет нарушения на тези права. За целта е въведен т.нар. механизъм за „поетапен отговор“, чието прилагане е поверено на Комисията за защита на правата към Hadopi.

33. Тази комисия е сезирана от организации на титулярите на права, в които някои заклети и упълномощени от министъра на културата длъжностни лица събират в мрежите с равноправен достъп (мрежите peer-to-peer) IP адресите на потребителите, които предоставят на публично разположение произведения без разрешение на техните титуляри. След това се изготвят протоколи. Те съдържат по-специално IP адреса на достъпа до интернет, използван за извършване на тези нарушения на авторското право, датата и часа на установеното нарушение, както и заглавието на въпросното произведение

[7] В това отношение поддържам и предложението си за преформулиране на преюдициалните въпроси, както и начина, по който разбирам техния предмет. Всъщност, макар в текста на преюдициалните въпроси да се споменава само достъпът до данните за самоличност, съответстващи на IP адреси, въпросът за достъпа до тези данни е неразривно свързан с въпроса за съхраняването им от доставчиците на електронни съобщителни услуги, поради което анализът на съвместимостта на съхраняването с правото на Съюза е необходима предпоставка за съвместимостта на достъпа. По този въпрос вж. точка 45 и сл. от първото ми заключение. По същия начин, макар преюдициалните въпроси да се отнасят до „данните за самоличност, съответстващи на IP адрес“, те следва да се разбират в смисъл, че се отнасят и до достъпа до IP адресите, позволяващи да се идентифицира източникът на свързване. По този въпрос вж. точка 41 и сл. от първото ми заключение.

[8] Решение от 21 декември 2016 г. (C-203/15 и C-698/15, наричано по-нататък „решение Tele2“, EU:C:2016:970).

[9] Решение от 6 октомври 2020 г. (C-511/18, C-512/18 и C-520/18, наричано по-нататък „решение La Quadrature du Net и др.“, EU:C:2020:791).

и се предават на Комисията за защита на правата към Hadopi. В това отношение следва да се подчертае, както отбелязва и ЕНОЗД, че обработването на лични данни от длъжностните лица в организациите на титулярите на права е предмет на уреждане от страна на Commission nationale de l'informatique et des libertés (Национална комисия по информационните технологии и свободите, CNIL) — френския надзорен орган в областта на защитата на данните [10].

34. След получаването на протоколите и след автоматизирана проверка с цел да се гарантира, че съдържат всички необходими данни, Комисията за защита на правата към Hadopi може да получи от доставчиците на електронни съобщителни услуги самоличността, пощенския адрес, адреса на електронна поща и телефонните номера на титуляря на абонамента, използван за извършване на нарушение на авторското право.

35. След това Hadopi може да отправи до това лице „препоръка", с която го уведомява, че достъпът му до интернет е бил използван в нарушение на авторските права, като тази препоръка съдържа разпореждане до заподозряното лице, което не е изпълнило задължението си за бдителност по отношение на зачитането в интернет на произведенията, защитени с авторско или сродно право, да изпълни това задължение. С други думи, препоръката е отправена до титуляря на правото на достъп до интернет, който на практика може да бъде лице, различно от това, което е предоставило на разположение произведението в нарушение на авторското право. Втора препоръка може да бъде издадена в случай на втора констатация на нарушение чрез същия достъп до интернет. В случай на повторни нарушения Комисията за защита на правата към Hadopi може да реши да сезира прокурора на Републиката за целите на наказателно преследване. В това отношение, както уточнява френското правителство в първото си становище, длъжностните лица на Hadopi, на които е възложено прилагането на механизма за поетапен отговор, са заклети длъжностни лица, упълномощени от председателя на Hadopi, които са длъжни да спазват професионална тайна и са единствените в рамките на Hadopi, но които е разрешен достъп до личните данни, обработвани в рамките на този механизъм.

36. В това отношение следва да се уточни, че не се събират и предават на Hadopi данните на всички потребители на peer-to-peer мрежите, когато последните само изтеглят такова съдържание [11], а само данните на лица, които са предоставили на разположение съдържание, нарушаващо права, тоест които *са качили* такова съдържание.

37. Така например за 2021 г. Hadopi е получил от организациите на титулярите на права близо четири милиона протоколи, изпратил е 210 595 първи препоръки и 53 564 втори препоръки и е сезирал прокурора на Републиката в 1 484 случая.

38. След като припомних това, ще покажа по какъв начин такъв механизъм, който предполага съхраняването и достъпа до данни за самоличност, съответстващи на IP адреси, според мен отговаря на изискванията на съдебната практика относно националните мерки, приети на основание член 15, параграф 1 от Директива 2002/58.

[10] Вж. в това отношение Решение № 2010-225 на CNIL от 10 юни 2010 г. за изменение на разрешението за обработване на лични данни на Société des auteurs compositeurs et éditeurs de musique (SACEM) (Сдружение на авторите и композиторите, SACEM) за целите на разследването и установяването на нарушения на авторското право, извършени чрез мрежите за обмен на файлове, наричани „peer to peer" (разрешение № 1425421).

[11] Относно функционирането на peer-to-peer мрежите и различните профили на потребители в тези мрежи вж. заключението ми по дело M.I.C.M. (C-597/19, EU:C:2020:1063, т. 37 и сл.).

### *Б. Спазването на изискванията на практиката на Съда относно тълкуването на член 15, параграф 1 от Директива 2002/58*

39. След като в първото си заключение вече припомних практиката на Съда относно съхраняването и достъпа до IP адреси, предоставени на източника на свързване [12], в настоящото заключение ще се съсредоточа върху това, което според мен е в основата на тази съдебна практика, а именно, от една страна, изискването за пропорционалност и от друга страна, що се отнася до достъпа до тези данни, евентуалната необходимост от предварителен контрол от юрисдикция или от независим административен орган.

#### *1. По пропорционалността на разглежданата мярка*

40. За да се определи дали дадена мярка за съхраняване или достъп до данни за самоличност, съответстващи на IP адрес, е съвместима с правото на Съюза, както Съдът многократно подчертава, следва да се пристъпи към съвместяване на различните разглеждани законни интереси и права, които са, от една страна, правото на защита на личния живот и правото на защита на личните данни [13], гарантирани с членове 7 и 8 от Хартата, и от друга страна, защитата на правата и свободите на други хора и на правата, закрепени в членове 3, 4, 6 и 7 от Хартата [14]. Ще добавя, че по настоящото дело както правото на защита на личния живот, така и правото на защита на личните данни също трябва да бъдат в съответствие с правото на собственост, закрепено в член 17 от Хартата, доколкото механизмът за поетапен отговор има за цел in fine защитата на авторското право и сродните му права.

41. В това отношение Съдът уточнява, че съвместяването на основание член 15, параграф 1 от Директива 2002/58 позволява на държавите членки да приемат мярка, с която да дерогират принципа на поверителност, когато това представлява „*необходима, подходяща и пропорционална* мярка в рамките на демократично общество“ (курсивът е мой). В съображение 11 от тази директива се уточнява, че такава мярка трябва да бъде „строго“ *пропорционална* на предвидената цел [15].

42. Освен това в целия си анализ относно тълкуването на член 15, параграф 1 от Директива 2002/58 Съдът се позовава на принципа на пропорционалност и следователно го превръща в ключов елемент за разглеждане на национална мярка за съхраняване или достъп до лични данни, приета въз основа на тази разпоредба.

43. По-задълбоченият прочит на този анализ показва, че в контекста на член 15, параграф 1 от Директива 2002/58 принципът на пропорционалност включва различни аспекти, свързани, от една страна, с тежестта на намесата в основните права, която предполагат съхраняването или достъпът до данните за трафик, и от друга страна, с необходимостта от разглежданата мярка.

[12] Точка 53 и сл. от първото ми заключение.

[13] В контекста на Директива 2002/58 правото на защита на личния живот и правото на защита на личните данни се изразяват в установените в нея принципи на поверителност на съобщенията и на забрана на съхранението на свързаните с тях данни.

[14] Решения La Quadrature du Net и др. (т. 120—122, 127 и 128), от 5 април 2022 г., Commissioner of An Garda Síochána и др. (C-140/20, наричано по-нататък „решение Commissioner of An Garda Síochána и др.“, EU:C:2022:258, т. 48 и 50), и от 20 септември 2022 г., SpaceNet и Telekom Deutschland (C-793/19 и C-794/19, наричано по-нататък „решение SpaceNet и Telekom Deutschland“, EU:C:2022:702, т. 63 и 65).

[15] Решения La Quadrature du Net и др. (т. 129), Commissioner of An Garda Síochána и др. (т. 51) и SpaceNet Telekom Deutschland (т. 66).

44. Що се отнася до съхраняването и до достъпа на Hadopi до данните за самоличност, съответстващи на IP адреси, считам, че както тежестта на намесата, така и абсолютната необходимост на тези данни би трябвало да накарат Съда да нюансира проверката на пропорционалността на национална мярка, приета на основание член 15, параграф 1 от Директива 2002/58.

*а) Относителната тежест на намесата в основните права*

45. От постоянната практика на Съда ясно произтича, че съгласно принципа на пропорционалност значението на преследваната с приетата мярка по член 15, параграф 1 от Директива 2002/58 цел трябва да има връзка с тежестта на следващата от мярката намеса [16].

46. По-конкретно, Съдът е постановил, както подчертах в първото си заключение, че в областта на превенцията, разследването, разкриването и преследването на престъпления тежка намеса може да бъде обоснована само от цел за борба с престъпността, като последната също трябва да е квалифицирана като „тежка“ [17].

47. Що се отнася до IP адресите, Съдът отбелязва, че макар те да се отличават с по-малка степен на чувствителност в сравнение с другите данни за трафика, тяхното съхраняване и анализ все пак представляват сериозна намеса в основните права, тъй като те могат да се използват по-специално за да се извърши изчерпателно проследяване на пътя на потребителя в сайтовете и страниците в интернет, и следователно позволяват да се установи подробният му профил и да се направят конкретни изводи за личния живот на лицето или лицата, чиито данни са били съхранени [18].

48. В делото по главното производство съхраняването и достъпът до данни за самоличност, съответстващи на IP адреси, се отнасят до борбата с нарушенията на авторското право и сродните му права. Според мен обаче е ясно, че тази борба не може да е част от борбата с тежката престъпност [19] дори да става въпрос за масов характер на тези нарушения. Следователно налице е несъответствие между тежестта на намесата в основните права, която разглежданата мярка предполага, и преследваната с нея цел.

49. В първото ми заключение, в съответствие с практиката на Съда, стигам до извода, че достъпът на Hadopi до данните за самоличност, съответстващи на IP адрес, действително представлява сериозна намеса в основните права. Макар да приемам и че съхраняването и достъпът до тези данни все пак трябва да бъдат разрешени в случая, след съдебното заседание следва да се направят още няколко уточнения.

[16] Решения Commissioner of An Garda Síochána и др. (т. 56) и SpaceNet и Telekom Deutschland (т. 71).

[17] Решения Tele2 (т. 115), от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018:788, т. 56), и от 2 март 2021 г., Prokuratuur (Условия зя достъп до данни за електронните съобщения) (C-746/18, наричано по-нататък „решение Prokuratuur“, EU:C:2021:152, т. 33). Вж. също точка 92 от първото ми заключение.

[18] Вж. решения La Quadrature du Net и др. (т. 152 и 153), Commissioner of An Garda Síochána и др. (т. 73) и SpaceNet и Telekom Deutschland (т. 103). Вж. също точки 63, 64 и 93 от първото ми заключение.

[19] В първото ми заключение поддържам, че понятието „тежка престъпност“ трябва да получи самостоятелно тълкуване, за да се предотврати заобикалянето от държавите членки на изискванията, установени в член 15, параграф 1 от Директива 2002/58. Поддържам това становище. Следва обаче да се подчертае, че дори Съдът да постанови, че дефиницията на понятието „тежка престъпност“ е оставено на държавите членки, то при всички положения трябва да се установи в рамките на правото на Съюза и не може да се разпростре до степен да изпразни от съдържание тази разпоредба.

50. Механизмът за поетапен отговор дава възможност на Hadopi да свърже IP адреса — който е съобщен от организациите на титулярите на права, на лица, заподозрени в използването на достъп до интернет за извършване на нарушение на авторското право в peer-to-peer мрежа — със самоличността на това лице, както и с извлечение от файла, качен в нарушение на авторското право. Както отбелязват Комисията и ЕНОЗД в съдебното заседание, макар да дават възможност да се получат със сигурност повече сведения, отколкото само самоличността на предполагаемия извършител на нарушението, тези данни все пак не позволяват да се направят много точни изводи за личния живот на това лице. Всъщност, както посочих в първото ми заключение[20], в случая става дума само за разкриване на конкретно консултиране на определено съдържание, което, разгледано самостоятелно, не позволява да се установи подробният профил на лицето, получило достъп до това съдържание.

51. Това важи в още по-голяма степен, тъй като, най-напред, по-голямата част от съобщените на Hadopi IP адреси са т.нар. „динамични“ IP адреси, които по естеството си са променящи се и съответстват на точна самоличност само в един момент, който съвпада с предоставянето на разположение на въпросното съдържание. Следователно те изключват каквато и да било възможност за изчерпателно проследяване.

52. На следващо място, трябва да се подчертае, че защитата на основните права в интернет според мен не може да обоснове достъпа само до данните, свързани с IP адреса, до съдържанието на произведение и до самоличността на лицето, което е предоставило на разположение произведението в нарушение на авторските права, а само че съхраняването и достъпът до тези данни трябва да се съпътстват от гаранции. В това отношение ми изглежда красноречива аналогия с реалния свят: лице, заподозряно в извършването на кражба, не може да се позове на правото си на защита на личния живот, за да не могат лицата, на които е възложено преследването на престъплението, да се запознаят с откраднатото съдържание. За разлика от това, въпросното лице може с основание да се позове на основните си права, за да може в хода на производството да препятства достъпа до съвкупност от данни, които са по-всеобхватни, отколкото единствено данните, необходими за квалифицирането на твърдяното престъпление.

53. Накрая ще отбележа, че противно на твърденията на жалбоподателите, механизмът за поетапен отговор, изглежда, не предполага общ контрол на ползвателите на peer-to-peer мрежите. Това е така, защото не става дума за проверка на цялата им дейност в дадена мрежа, за да се определи дали те са предоставили на разположение произведение в нарушение на авторските права, а по-скоро въз основа на файл, идентифициран като имитация, да се определи кой е титулярят на достъпа до интернет, от който потребителят е предоставил на разположение произведението. Също така, както подчертава ЕНОЗД в съдебното заседание, не става дума за упражняване на надзор върху дейността на всички ползватели на peer-to-peer мрежите, а само върху тази на лицата, които качват файлове, нарушаващи правата, тъй като качването на тези файлове в още по-малка степен разкрива обстоятелства, свързани с личния живот на лицето, при положение че е възможно това да се осъществи единствено за да позволи на потребителите да качват впоследствие други файлове.

[20] Точка 101 от първото ми заключение.

54. При тези условия съображенията, поради които Съдът приема съхраняването и достъпа до IP адресите като тежка намеса в основните права, според мен не намират приложение по отношение на механизъм за поетапен отговор като прилагания от Hadopi. От това следва, че тежестта на намесата, която това съхраняване и този достъп предполагат, следва да се нюансира при разглеждането на принципа на пропорционалност.

55. С други думи, считам, че практиката на Съда относно тежестта на намесата в основните права, с която са свързани съхраняването и достъпът до IP адреси, не следва да се тълкува в смисъл, че тази намеса е винаги тежка, а че е налице такава намеса само когато IP адресите могат да доведат до изчерпателно проследяване на пътя на потребителя в сайтовете и страниците в интернет и до много точни изводи за личния му живот.

56. Тъй като случаят в главното производство не е такъв, намесата, която предполагат съхраняването и достъпът до данните за самоличност, съответстващи на IP адрес, използван за предоставяне на съдържание в нарушение на авторското право, би трябвало да може да бъде обоснована с цел за борба с престъпността, която е по-широка, отколкото единствено борбата с тежката престъпност.

57. Освен това уточнявам, че намесата в основните права, която предполагат съхраняването и достъпът до данни за самоличност, съответстващи на IP адрес, в положение като разглежданото в главното производство не се утежнява от обстоятелството, че титулярят на достъп до интернет, използван за предоставяне на съдържание, което нарушава права, не е непременно в основата на това предоставяне на разположение, поради което е възможно отправената от Hadopi препоръка да доведе до разкриване на притежателя на това съдържание, до което трето лице е имало достъп. От една страна, следва да се припомни, че разследваното от Hadopi нарушение е неизпълнение на задължението достъпът да не бъде използван за целите на предоставянето на разположение на съдържание в нарушение на авторското право. Поради това е необходимо информацията, позволяваща да се квалифицира нарушението, да бъде предадена на предполагаемия извършител. От друга страна, както вече посочих, считам, че информацията относно въпросното произведение не позволява да се направят конкретни изводи за личния живот на лицето, което е в основата на предоставянето на произведение на разположение в мрежата. Следователно евентуалното предаване на тази информация на титуляря на интернет връзката не надхвърля необходимото за преследването на въпросното нарушение на авторското право.

*б) Абсолютната необходимост от разглежданите данни за разкриването и преследването на престъпление*

58. Съгласно практиката на Съда, за да се гарантира пропорционалността на мярка за съхраняване и за достъп до данни за трафик като данните за самоличност, съответстващи на IP адрес, приета на основание член 15, параграф 1 от Директива 2002/58, следва намесата, която те предполагат, да бъде ограничена до строго необходимото, за да се постигне преследваната цел [21]. Струва ми се, че точно такъв е случаят, когато става въпрос за мярката, разглеждана в главното производство.

[21] Решения La Quadrature du Net и др. (т. 120—122 и 132), Commissioner of An Garda Síochána и др. (т. 48 и 54) и SpaceNet и Telekom Deutschland (т. 63 и 69).

59. Както подчертах в първото ми заключение [22], от самата практика на Съда следва, че при престъпление, извършено изцяло в интернет, като нарушение на авторското право в peer-to-peer мрежа, IP адресът може да е единственото средство за разследване, чрез което да се идентифицира лицето, на което е предоставен този адрес в момента на извършване на нарушението [23]. Според мен от това следва, че съхраняването и достъпът до данни за самоличност, съответстващи на IP адреси, с цел разкриване и преследване на извършени в интернет нарушения на авторските права, в съответствие със съдебната практика, е строго необходимо за постигането на преследваната цел.

60. Вярно е, че всяко изискване за защита на личните данни предполага ограничаване на правомощията за разследване. Това следва от самия принцип на съвместяване на противоположни интереси и сам по себе си такъв резултат не може да бъде оспорен. В случая обаче, в който IP адресът е единственото средство за идентифициране на лицето, заподозряно в извършване на нарушение на право върху интелектуална собственост в интернет, такова положение се различава от по-голямата част от случаите на наказателно преследване, по повод на които Съдът отбелязва, че „ефективността […] по принцип зависи не от едно-единствено средство за разследване, а от всички средства за разследване, с които разполагат компетентните национални органи за тази цел“ [24]. Да се приеме, че данните за самоличност, съответстващи на IP адреси, не следва да бъдат предмет на съхраняване и достъп в положение като разглежданото в главното производство, подобно на всяка мярка, гарантираща защитата на данните за трафик, не води до просто ограничаване на правомощията за разследване, а по-скоро до лишаване на националните органи от единственото средство за разкриване и преследване на определени престъпления.

61. С други думи, съгласно тълкуването, което предлагам на член 15, параграф 1 от Директива 2002/58, не става дума чрез разглеждането на необходимостта от такава мярка да се разрешат съхраняването и достъпът до данни, които само *улесняват* разкриването и преследването на престъпления, когато тези престъпления могат да бъдат разкрити и преследвани и с конкурентни, макар по-малко ефективни средства. За сметка на това става дума да се разрешат съхраняването и достъпът до тези данни, когато те са *абсолютно необходими* за идентифицирането на лицето, заподозряно в извършване на престъпление, което не би могло да бъде преследвано без тези средства, при положение че въпросните данни са единственото средство за идентифициране на потребителя, доколкото престъплението е извършено изцяло онлайн.

62. Такова тълкуване според мен се налага, освен ако не се приеме, че срещу цяла поредица от престъпления никога няма да е възможно да се води наказателно преследване [25].

63. Според мен от всички изложени по-горе съображения следва, че национална правна уредба, която разрешава съхраняването от доставчиците на електронни съобщителни услуги и достъпа от административен орган само на данни за самоличност, съответстващи на IP адреси, е напълно пропорционална на преследваната цел, а именно преследването на посегателства върху авторски права и сродните им права в интернет, доколкото намесата в

[22] Точка 78 от първото ми заключение.

[23] Решения La Quadrature du Net и др. (т. 154), Commissioner of An Garda Síochána и др. (т. 73) и SpaceNet и Telekom Deutschland (т. 100).

[24] Решение Commissioner of An Garda Síochána и др. (т. 69).

[25] Точка 81 от първото ми заключение. Вж. също по този въпрос точка 79 и сл. от настоящото заключение.

основните права, която те предполагат, е с ограничена тежест и тези данни са единственото средство за разследване, позволяващо идентифицирането на лицето, на което този адрес е бил предоставен към момента на извършване на деянието.

64. Ето защо считам, че член 15, параграф 1 от Директива 2002/58 трябва да се тълкува в смисъл, че допуска такава правна уредба.

*2. По наличието на подходящи материални и процесуални гаранции*

65. Що се отнася по-специално до достъпа до данни за самоличност, съответстващи на IP адреси, от практиката на Съда следва, че само строгата пропорционалност на мярката не е достатъчна да я направи съвместима с член 15, параграф 1 от Директива 2002/58.

66. Всъщност, за да се гарантира, че достъпът до данни за трафик и местонахождение е ограничен до строго необходимото, Съдът е приел, че е от съществено значение този достъп да се предоставя след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура, която разполага с всички правомощия и представя всички необходими гаранции, за да осигури съвместяване на различните разглеждани законни интереси и права [26].

67. При това положение стриктното тълкуване на съдебната практика би довело до извода, че достъпът на Hadopi до данните за самоличност, съответстващи на IP адресите на лицата, заподозрени в извършването на нарушение на авторското право в интернет, би трябвало да бъде подчинен на такъв предварителен контрол, какъвто липсва в съществуващия механизъм за поетапен отговор.

68. Както обаче изтъква ирландското правителство в съдебното заседание и както поддържам в първото ми заключение, считам, че изискването за предварителен контрол от юрисдикция или от независима административна структура не е систематично изискване, а зависи от по-цялостен анализ на разглежданата мярка, при който се взема предвид както тежестта на намесата, която тя предполага, така и гаранциите, които тя предвижда.

69. Всъщност нека подчертая, че във всяко от решенията, с които се установява това изискване за предварителен контрол от юрисдикция или от независима административна структура, се разглеждат национални правни уредби, които разрешават достъп до всички данни за трафик и местонахождение на потребителите относно всички електронни съобщителни средства на потребители [27], или поне относно фиксирана и мобилна телефония [28] на идентифицирани потребители.

70. Оттук правя извода, че от съществено значение за изискването за такъв предварителен контрол е тежестта на съответната намеса по въпросните дела. Както Съдът подчертава, става дума за данни, които „действително мо[гат] да позвол[ят] да се направят точни и дори много точни изводи относно личния живот на лицата […], като навиците им в ежедневния живот, местата на постоянно или временно пребиваване, ежедневните им или други пътувания, упражняваните дейности, социалните връзки на тези лица и социалните

[26] Решения Tele2 (т. 120), Prokuratuur (т. 51 и 52) и Commissioner of An Garda Síochána и др. (т. 106 и 107).

[27] Решения Tele2 и Commissioner of An Garda Síochána и др.

[28] Решение Prokuratuur.

кръгове, в които се движат“ [29]. Освен това въпросните данни включвали данни на лица, които вече били идентифицирани и заподозрени в извършването на престъпление въз основа на други улики, като въпросните данни следователно позволявали да се допълнят уличаващите доказателства срещу въпросния потребител, като се разшири обхватът на данните, отнасящи се до него.

71. Що се отнася обаче до разглежданата в главното производство правна уредба, както посочих, тежестта на намесата, която свързването на данни за самоличност и IP адрес предполага, е с по-малка тежест, отколкото произтичащата от достъпа до всички данни за трафик и местонахождение на дадено лице, доколкото това свързване не дава повод да се направят конкретни изводи за личния живот на съответното лице.

72. Освен това, както отбелязах в първото ми заключение [30], тези данни се отнасят само до лица, които след обективна констатация за използването на IP адрес в нарушение на авторско право, направена от организациите на титулярите на права, са извършили деянията, представляващи неизпълнение на задължението за бдителност, предвидено в член L.336-3 от CPI. Те не са предварително идентифицирани с помощта на други средства, тъй като свързването на IP адреса с данните за самоличност е единственото средство за идентифициране на съответното лице. Следователно достъпът до тези данни не позволява, както е в случая по делата, по които Съдът вече се е произнесъл, да се получи допълнителна и конкретна информация за дейността на лица, които вече са заподозрени въз основа на други доказателства, а само да се направи използваем IP адресът, иначе лишен от интерес. При тези условия данните, до които Hadopi има достъп, са фактически ограничени.

73. Според мен съществува основна разлика между достъпа до лични данни на заподозряно в извършване на престъпление лице, за да се докаже неговата вина, и факта, че може да се разкрие самоличността на извършителя на вече установено престъпление.

74. Според мен това важи в още по-голяма степен, тъй като събирането на IP адреси в peer-to-peer мрежите е предмет на предварително разрешение, ограничено само до тези данни, поради което Hadopi никога не разполага с неограничена съвкупност от данни, що се отнася до потребителите, заподозрени в извършване на нарушение на авторски права в интернет [31].

75. Следователно логиката, която стои в основата на изискването за предварителен контрол, осъществяван от юрисдикция или независима административна структура, не се прилага по отношение на механизъм за поетапен отговор като разглеждания в главното производство, поради което подобно изискване не ми се струва необходимо, за да се гарантира, че намесата в основните права, която този механизъм предполага, е ограничена до строго необходимото.

76. От всички изложени съображения следва, че национална правна уредба, която разрешава съхраняването и достъпа от независим административен орган като Hadopi до данни за самоличност, съответстващи на IP адреси, за да се идентифицират титулярите на тези адреси, заподозрени, че са отговорни за извършени посегателства върху авторски права, без този достъп да подлежи на предварителен съдебен контрол или на контрол от независима административна структура, в крайна сметка е в съответствие с принципите,

[29] Решение Prokuratuur (т. 36).

[30] Точка 102 от първото ми заключение.

[31] Точка 33 от настоящото заключение.

прогласени в практиката на Съда, когато тези данни са единственото средство за идентифициране на лицето, на което IP адресът е бил предоставен към момента на извършване на нарушението, поради което член 15, параграф 1 от Директива 2002/58 би трябвало да се тълкува в смисъл, че допуска такава правна уредба.

77. Освен тези съображения, които се отнасят до разглеждания в главното дело случай, трябва да изложа и по-общи бележки относно необходимостта от развитие на практиката на Съда.

### *B. Необходимо и ограничено развитие на съдебната практика*

78. Няколко са аргументите в подкрепа на прецизиране на практиката на Съда относно съхраняването и достъпа до данни като IP адресите, свързани с данни за самоличност.

79. На първо място, както вече подчертах [32], в разглежданото в главното производство положение получаването на данни за самоличност, съответстващи на IP адрес, е единственото средство за разследване, позволяващо да се идентифицира лицето, на което този адрес е бил предоставен към момента на извършване на това деяние.

80. От това неизбежно следва, че ако Съдът трябва да приеме, че член 15, параграф 1 от Директива 2002/58 все пак не допуска съхраняването и достъпа до данните, националните органи действително биха били лишени от това единствено средство за идентифициране, а оттам и извършителите на въпросното престъпление никога не биха могли да бъдат преследвани [33]. В първото ми заключение стигнах до извода за възможността за системна безнаказаност за това престъпление [34].

81. Рискът от системна безнаказаност не се ограничава до извършените в peer-to-peer мрежите нарушения на авторското право, а обхваща, както изтъква чешкото правителство в съдебното заседание, всички престъпления, извършени изключително в интернет.

82. Всъщност престъпленията, чийто извършител може да бъде идентифициран само чрез IP адреса, никога не биха могли да бъдат преследвани, а текстовете, които ги санкционират, никога не биха могли да бъдат прилагани, ако се приеме, че както съхраняването на данните, така и достъпът до тях са в противоречие с правото на Съюза.

83. В това отношение отбелязвам, че действително, както изтъкват жалбоподателите в главното производство, на теория други средства биха могли да позволят идентифицирането на извършителите на някои престъпления, извършени изключително в интернет. Така те се позовават по-специално на идентификатора, използван в социалните мрежи, и на данните, свързани с профила на потребителя, адреса на електронна поща, телефонния номер или аспект на личния му живот, които лицето е разкрило. За да бъдат свързани със самоличността на лицето обаче, такива данни изискват задълбочено разследване, в хода на което се разглежда онлайн дейността на потребителя. Ето защо ми се струва, че прибягването до такива средства за разследване, за разлика само от IP адреса,

[32] Точка 59 от настоящото заключение.

[33] Точка 62 от настоящото заключение.

[34] Точка 78 и сл. от първото ми заключение.

може да позволи да се направят много точни изводи за личния живот на лицата, поради което съхраняването и достъпът до посочените данни в този смисъл са в противоречие с член 15, параграф 1 от Директива 2002/58.

84. При тези условия достъпът до данни за самоличност, съответстващи на IP адреса на потребител, несъмнено не е единственото теоретично средство за разследване, позволяващо идентифицирането на лицето, което е титуляр на този адрес към момента на извършване на деянието, а това, което позволява преследването му, като същевременно включва най-малката намеса в основните му права, а следователно и възможността да се предотврати обща безнаказаност.

85. На второ място, подчертавам отново, че такова разрешение би позволило според мен да се съвместят две насоки в практиката на Съда, които са източник на известно напрежение, което съм установил в първото ми заключение [35] и в заключението по дело M.I.C.M. [36], а именно, от една страна, съдебната практика относно съхраняването и достъпа до данни и от друга страна, съдебната практика относно разкриването на IP адресите, предоставени на източника на свързване, предявени от частноправни лица.

86. На трето място, макар практиката на Съда след решения Tele2 и La Quadrature du Net и др. да трябва да бъде приветствана, тъй като позволява въвеждането на рамка, която защитава основните права на потребителите на електронни съобщителни услуги, тя все пак е заимствана от определена казуистика. Всъщност при решаването на поставените му за разглеждане дела Съдът постепенно е прецизирал практиката си, което му позволява да разглежда различни национални правни уредби в светлината на член 15, параграф 1 от Директива 2002/58. Съдът обаче не може да предвиди всички вероятни мерки, които биха могли да бъдат анализирани в светлината на тази разпоредба. За това впрочем свидетелства броят на преюдициалните запитвания [37], отправени след решение Tele2, което според мен е индикатор за затрудненията, които могат да имат националните юрисдикции при прилагането на принципите, установени в практиката на Съда, към положения, различни от тези, по които са постановени въпросните решения [38].

87. Следователно според мен е необходима известна гъвкавост, когато Съдът трябва да разглежда мерки, които не са могли да бъдат разгледани в предходни съдебни решения, които Съдът досега не е имал повод да разглежда, каквито са правилата за престъпления, които могат да бъдат преследвани само доколкото данните за самоличност, съответстващи на IP адреси, се съхраняват и са достъпни.

[35] Точка 69 и сл. от първото ми заключение.

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

[37] Решения от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018:788), La Quadrature du Net и др., Prokuratuur, Commissioner of An Garda Síochána и др. и SpaceNet и Telekom Deutschland.

[38] В това отношение множеството преюдициални запитвания, които имат за предмет тълкуването на член 15, параграф 1 от Директива 2002/58, може също да е израз на определена форма на нежелание от страна на националните юрисдикции да прилагат изведените от Съда принципи към малко по-различни положения поради особеностите на националните правни системи. По този въпрос вж. по-специално *Cameron*, I. Metadata retention and national security: Privacy international and *La Quadrature du Net*. — Common Market Law Review, 2021, vol. 58, nº 5, 1433—1471 или *Bertrand*, B. L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin? — Dalloz IP/IT, 2021, nº 9, 468—472. Ето защо ми се струва още по-важно, за да се поддържа ползотворен диалог между Съда и юрисдикциите на държавите членки, да се позволи Съдът да докаже, че е адаптивен, когато обстоятелствата го изискват. Както отбелязват авторите в правната доктрина, високият стандарт за закрила, установен в практиката на Съда, не може да бъде действително ефективен, без националните юрисдикции да го приемат, като, на първо място, им е възложено да го прилагат. По този въпрос вж. по-специално *Teyssedre*, J. Strictly regulated retention and access regimes for metadata: Commissioner of An Garda Siochana. — Common Market Law Review, vol. 60, nº 2, 2023, 569—588, и *Sirinelli*, J. La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite. — Revue trimestrielle de droit européen, vol. 57, nº 2, 2021, 313—329.

88. Следователно не става въпрос, както твърди датското правителство, да се преразгледа практиката на Съда, а да се приеме, че въз основа на принципите в основата ѝ, в силно ограничени хипотези може да бъде изведено по-нюансирано разрешение.

89. Всъщност предложеното от мен тълкуване на член 15, параграф 1 от Директива 2002/58 позволява съхраняването и достъпа до данни за самоличност, съответстващи на IP адреси, само що се отнася до преследването на престъпления, чиито извършители не биха могли да бъдат идентифицирани при липсата на тези данни. Следователно това тълкуване се отнася само до престъпленията, извършени изключително в интернет, и не поставя под въпрос разрешенията, изложени в съдебната практика относно съхраняването и достъпа до по-всеобхватни данни, които преследват други цели.

## V. Заключение

90. С оглед на всички изложени съображения предлагам на Съда да отговори на преюдициалните въпроси, поставени от Conseil d'État (Държавен съвет, Франция), по следния начин:

„Член 15, параграф 1 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година, във връзка с членове 7, 8, 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз

трябва да се тълкува в смисъл, че

допуска национална правна уредба, позволяваща съхраняването на данните за самоличност, съответстващи на IP адреси, от страна на доставчиците на електронни съобщителни услуги и ограничения достъп на административен орган, на който е възложена защитата на авторските и сродните им права срещу извършени в интернет нарушения, само до такива данни, че да може този орган да идентифицира титулярите на тези адреси, заподозрени, че носят отговорност за извършването на посочените нарушения, и в зависимост от съответния случай да може да предприеме конкретни действия срещу тях, без този достъп да подлежи на предварителен контрол от юрисдикция или от независима административна структура, когато тези данни са единственото средство за разследване, позволяващо да се установи самоличността на лицето, на което са предоставени тези адреси в момента на извършване на нарушението“.