Сборник съдебна практика

ЗАКЛЮЧЕНИЕ НА ГЕНЕРАЛНИЯ АДВОКАТ
M. SZPUNAR
представено на 27 октомври 2022 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 (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. Въпросът за съхраняването на и достъпа до определени данни на интернет потребителите е с постоянна актуалност и е разглеждан в по-новата, но вече богата практика на Съда.

2. Настоящото дело предоставя възможност на Съда да разгледа отново този въпрос, в подновения контекст на борбата с престъпленията против интелектуалната собственост, извършени изключително в интернет.

[1] Език на оригиналния текст: френски.

II. Правна уредба

A. Правото на Съюза

3. Съображения 2, 6, 7, 11, 22, 26 и 30 от Директива 2002/58[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 прихващане 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,

[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, 8.6.2017 г., стр. 27 и в ОВ L 241, 10.9.2013 г., стр. 9).

[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).

строго пропорционални на предвидената цел 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 неговото/нейното 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. […]“.

4. 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 радио-разпръскване през електронни комуникационни мрежи с изключение на информацията, която може да бъде свързана с идентифицируем абонат или потребител, получаващ информацията;

[…]“.

5. 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“.

6. 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“.

7. 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.

[…]“.

8. Член 15 („Приложение на някои разпоредби от Директива [95/46]“), параграф 1 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

9. Член L. 331-12 от Code de la propriété intellectuelle (Кодекс за интелектуалната собственост, наричан по-нататък „CPI“) в редакцията си, 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“.

10. 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; […]“.

11. 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“.

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

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

13. 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“.

14. 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 действия, извършени преди повече от шест месеца".

15. 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 действия, 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 действия, 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 датата е връчена препоръката.

В препоръките, отправяни на основание на настоящия член, се посочват датата и часът, в които са установени действията, 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".

16. 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 […]“.

17. 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]] […] 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.

[…]“.

18. Член L. 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

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

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, 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“.

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

„Лицето с право на достъп до обществени съобщителни услуги в интернет е длъжно да следи за това 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.

20. Член 1 от Декрета от 5 март 2010 г. в редакцията си, 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 на [CPI] с ранг на закон (дял III, глава I, раздел 3, подраздел 3) и книга III от част на същия кодекс с ранг на нормативен административен акт (дял III, глава I, раздел 2, подраздел 2);

2° сезира прокурора на Републиката за действия, 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 органите за професионална защита и организациите за колективно управление за действията по това сезиране;

[…]“.

21. Член 4 от същия декрет гласи:

„I.- Упълномощените съгласно член L. 331-21 от [CPI] от председателя на [Hadopi] 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“.

22. 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 от прокурора на Републиката:

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

Дата и час на извършване на действията;

IP адрес на съответните абонати;

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

Псевдоним, използван от абоната;

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

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 IP техническото средство.

[…]

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 télécommunications (Кодекс за пощите и телекомуникациите)

23. Член L. 34-1, параграф II bis от Code des postes et des communications électroniques (Кодекс за пощите и електронните съобщения), изменен с член 17 от Закон № 2021-998 от 30 юли 2021 г.[5] (наричан по-нататък „CPCE“), предвижда, че „операторите на електронни съобщителни услуги са длъжни да съхраняват:

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;

[5] JORF от 31 юли 2021 г., текст № 1. Тази редакция на член L. 34-1 от CPCE, 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 CPCE противоречи на Конституцията, с основния мотив, че „като разрешават общо и неизбирателно 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 тяхното естество, тяхното 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).

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 закриването 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. Спорът в главното производство, преюдициалните въпроси и производството пред Съда

24. С жалба от 12 август 2019 г. и две допълнителни писмени становища от 12 ноември 2019 г. и 6 май 2021 г. La Quadrature du Net, Fédération des fournisseurs d’accès à Internet associatifs, Franciliens.net и French Data Network искат Conseil d’État (Държавен съвет, Франция) да отмени мълчаливото решение, с което Premier ministre (министър-председателят на Франция) отхвърля искането им за отмяна на Декрет от 5 март 2010 г., въпреки че този декрет и разпоредбите, които съставляват правното му основание, не само накърняват прекомерно правата, гарантирани от френската Конституция, но и противоречат на член 15 от Директива 2002/58 и на членове 7, 8, 11 и 52 от Хартата.

25. По-специално, жалбоподателите в главното производство твърдят, че Декретът от 5 март 2010 т. и разпоредбите, които съставляват неговото правно основание, допускат по непропорционален начин достъп до данни за свързване при извършвани в интернет леки престъпления, с които се засяга авторското право, без да се извършва предварителен съдебен или административен контрол, при който се осигурява изпълнение на изискванията за независимост и безпристрастност.

26. В това отношение запитващата юрисдикция посочва най-напред, че в последното си решение La Quadrature du Net и др.[6] Съдът постановява, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11, както и с член 52, параграф 1 от Хартата допуска законодателни мерки, предвиждащи за целите на опазването на националната сигурност, борбата с тежката престъпност и опазването на обществената сигурност общо и неизбирателно запазване на *данни относно самоличността* на ползвателите на електронни съобщителни средства. Това запазване на данните е възможно за неопределен период за целите най-общо на разследването, разкриването и преследването на престъпления.

27. Оттук запитващата юрисдикция прави извод, че не е налице изтъкнатото от жалбоподателите в главното производство основание относно законосъобразността на Декрета от 5 март 2010 г., доколкото той е приет по принцип в контекста на борбата с леките престъпления.

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

28. По-нататък тази юрисдикция припомня, че в решение Tele2 Sverige и Watson[7] Съдът приема, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, която регламентира защитата и сигурността на данни за трафик и на данни за местонахождение, и по-специално достъпа на компетентните национални органи до запазените данни, като не го подчинява на предварителен контрол от юрисдикция или от независима административна структура.

29. Тя отбелязва, че в решение Tele2[8] Съдът уточнява, че за да се гарантира на практика пълното спазване на тези условия, от съществено значение е достъпът на компетентните национални органи до запазените данни по принцип да се предоставя, освен в надлежно обосновани неотложни случаи, след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура, като решението на тази юрисдикция или на тази структура да се постановява след мотивирана молба от тези органи, подадена по-специално в рамките на наказателни производства за предотвратяване, разкриване или наказателно преследване на престъпления.

30. Запитващата юрисдикция отбелязва, че Съдът припомня това изискване по отношение на събирането в реално време на данните за свързване от разузнавателните служби в решение La Quadrature du Net и др.[9], както и в решение Prokuratuur (Условия зя достъп до данни за електронните съобщения)[10] — що се отнася до достъпа на националните органи до данните за свързване.

31. Накрая, тази юрисдикция отбелязва, че от създаването си през 2009 г. Hadopi е изпратил над 12,7 милиона препоръки до притежателите на абонаменти по процедурата за поетапен отговор, предвидена в член L. 331-25 от CPI, включително 827 791 само през 2019 г. В това отношение служителите на Комисията за защита на правата на Hadopi трябва да могат да събират всяка година значително количество данни, свързани със самоличността на съответните ползватели. Запитващата юрисдикция приема, че поради това обвързването на това събиране на данни с предварителен контрол създава опасност процедурата за отправяне на препоръки да не може да бъде приложена.

32. При тези обстоятелства Conseil d'État (Държавен съвет) решава да спре производството по делото и да постави на Съда следните преюдициални въпроси:

„1) Спадат ли данните за самоличност, съответстващи на IP адрес, към данните за трафик или данните за местонахождение, които по принцип подлежат на предварителен контрол от юрисдикция или от независима административна структура с правомощия да издава правнообвързващи актове?

2) При утвърдителен отговор на първия въпрос и с оглед на ниската чувствителност на данните за самоличността на ползвателите, включително на техните данни за контакт, трябва ли Директива [2002/58] във връзка с [Хартата] да се тълкува в смисъл, че не допуска национална правна уредба, която предвижда събиране на тези данни,

7 Вж. решение от 21 декември 2016 г. (C-203/15 и C-698/15 EU:C:2016:970, наричано по-нататък „решение Tele2“, диспозитив).

8 Точка 120 от това решение.

9 Точка 189 от това решение.

10 Решение от 2 март 2021 г. (C-746/18, EU:C:2021:152, наричано по-нататък „решение Prokuratuur“).

съответстващи на IP адреса на ползвателите, от административен орган без предварителен контрол от юрисдикция или независима административна структура с правомощия да издава правнообвързващи актове?

3) При утвърдителен отговор на втория въпрос и с оглед: на ниската чувствителност на данните за самоличността; на обстоятелството, че само тези данни могат да бъдат събирани, и то единствено за да се предотврати неизпълнението на точно, изчерпателно и ограничително определени от националното право задължения, и на обстоятелството, че достъпът до данните на всеки ползвател е обект на систематичен контрол от юрисдикция или от трета административна структура с правомощия да издава правнообвързващи актове, като този контрол би могъл да наруши задачата за изпълнение на публични функции, възложена на събиращия данните административен орган, който сам по себе си е независим, представлява ли Директива [2002/58] пречка този контрол да се осъществява по съответно приспособени правила, като например автоматизиран контрол, евентуално под надзора на вътрешно звено на органа, което отговаря на изискванията за независимост и безпристрастност по отношение на служителите, натоварени със събирането на данните?“.

33. Жалбоподателите в главното производство, френското, естонското, шведското и норвежкото правителство и Европейската комисия представят писмени становища. Посочените страни, с изключение на естонското, датското и финландското правителство, са представлявани в съдебното заседание, проведено на 5 юли 2022 г.

IV. Анализ

A. По първия и втория преюдициален въпрос

34. С първия и втория преюдициален въпрос, които според мен следва да се разгледат заедно, запитващата юрисдикция иска да се установи по същество дали член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и с член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска национална правна уредба, позволяваща достъпа на административен орган, на който е възложена защитата на авторските и сродните им права срещу посегателства върху тези права в интернет, до данни за самоличност, съответстващи на IP адреси, за да може този орган да идентифицира притежателите на тези адреси, заподозрени, че са отговорни за извършените посегателства, и евентуално да може да предприеме действия срещу тях, без този достъп да подлежи на предварителен съдебен контрол или на контрол от независима административна структура.

1. Определяне на границите на преюдициалните въпроси

а) Предварителното събиране на IP адресите от организациите на титулярите на права

35. От акта за преюдициално запитване е видно, че разглежданият в главното производство механизъм за поетапен отговор включва две последователни операции по обработване на данни, които се състоят, от една страна, в предварителното събиране от организациите на титулярите на права на IP адресите в peer-to-peer мрежите на нарушители на авторското

право и от друга страна, във възможността Hadopi да свърже тези IP адреси със самоличността на съответните лица след сезирането му с цел отправяне на препоръки до лицата, чийто достъп до обществени съобщителни услуги в интернет е използван в нарушение на правилата относно авторското право.

36. Първият и вторият преюдициален въпрос се отнасят само до втория вид обработване, извършвано от Hadopi.

37. Според жалбоподателите в главното производство обаче Съдът трябва да подложи на проверка първия вид обработване, тъй като, ако тези IP адреси са получени в нарушение на разпоредбите на Директива 2002/58, използването им при втория вид обработване непременно би било в противоречие с тези разпоредби.

38. Този довод не може да бъде приет. Член 3, параграф 1 от Директива 2002/58 ограничава приложното ѝ поле до „обработването на личните данни в контекста на предоставянето на електронни съобщителни услуги“. Както обаче уточнява френското правителство в съдебното заседание, организациите на титулярите на права получават въпросните IP адреси не чрез доставчиците на електронни съобщителни услуги, а директно онлайн, посредством справка с данни, достъпни в интернет за широката публика.

39. Следователно може само да се отбележи, че предварителното събиране на IP адреси от организациите на титулярите на права не попада в обхвата на разпоредбите на Директива 2002/58 и както отбелязва Комисията, при това положение може да се анализира с оглед на разпоредбите на Регламент (ЕС) 2016/679[11]. При това положение според мен подобен анализ излиза извън обхвата на отправените до Съда преюдициални въпроси, още повече че запитващата юрисдикция не е предоставила подробности относно предварителното събиране на данни, които биха позволили на Съда да даде полезен отговор.

40. При тези условия ще съсредоточа анализа си върху въпроса за достъпа на Hadopi до данните за самоличност, съответстващи на IP адрес.

б) Връзката на IP адресите с данните за самоличност

41. Първият и вторият преюдициален въпрос се отнасят до „данните за самоличност, съответстващи на IP адрес“, които според запитващата юрисдикция са с ниска чувствителност. В постановеното решение тази юрисдикция се позовава единствено на точките от решение La Quadrature du Net и др. относно запазването на данните за самоличност.

42. Вярно е, че в практиката на Съда се прави разграничение между режима за запазване на данни и достъпа до IP адреси и режима на запазване на данни и достъпа до данни за самоличността на ползвателите на електронни съобщителни средства, като вторият режим е по-малко строг от първия[12].

[11] Регламент на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 2016 г., стр. 1).

[12] Вж. решение La Quadrature du Net и др. (т. 155 и 159).

43. Според мен обаче в този случай, въпреки формулировката на тези два преюдициални въпроса, не се разглежда само достъпът до данните за самоличността на ползвателите на електронни съобщителни средства, а самата възможност да се направи връзка между тези данни и IP адресите, с които разполага Hadopi след събирането и предаването им от организациите на титулярите на права. Всъщност, както отбелязва Комисията, достъпът на Hadopi до данните за самоличност има за цел да разкрие по-широка съвкупност от данни, по-специално IP адресите и извадки от ползваните файлове, и да позволи тяхното използване, тъй като данните за самоличност и IP адресите, независимо едни от други, не представляват интерес за националните органи, тъй като нито самоличността, нито IP адресите могат сами по себе си да предоставят информация за дейността на физическите лица в интернет, когато не може да се направи връзка помежду им.

44. Според мен от това следва, че първият и вторият преюдициален въпрос трябва да се разбират като отнасящи се не само до данните за самоличност на ползвателите на електронно съобщително средство, но и до достъпа до IP адресите, които позволяват да се идентифицира източникът на връзката.

в) Съхраняването на IP адресите от доставчиците на електронни съобщителни услуги

45. Вярно е, както посочват френското правителство и Комисията, че отправените до Съда преюдициални въпроси формално не се отнасят до съхраняването на данни от доставчиците на електронни съобщителни услуги, а само до достъпа на Hadopi до данните за самоличност, съответстващи на IP адреси.

46. Въпросът за достъпа на Hadopi до тези данни обаче според мен е неразривно свързан с предходния въпрос за съхраняването им от доставчиците на съобщителни услуги. Както Съдът подчертава, съхраняването на данни е единствено за целите на предоставянето при необходимост на достъп до тях на компетентните национални органи[13]. С други думи, съхраняването на данни и достъпът до тях не могат да се разглеждат изолирано, въпреки че достъпът до тях зависи от съхраняването им.

47. Наистина Съдът вече е разгледал въпроса дали е съвместима с член 15, параграф 1 от Директива 2002/58 национална правна уредба с оглед на обстоятелството, че компетентните национални органи имат единствено достъп до определени лични данни независимо от отговора на въпроса дали съхраняването на разглежданите данни е съвместимо с тази разпоредба[14]. Следователно на конкретните преюдициални въпроси може да се отговори без оглед на това дали съответните данни са съхранявани в съответствие с разпоредбите на правото на Съюза.

48. На първо място обаче отбелязвам, че в решение Ministerio Fiscal[15] при преценката си, що се отнася до съвместимостта с правото на Съюза на достъпа на националните органи до определени лични данни, Съдът следва стриктно същите принципи, както и при преценката за съвместимостта с правото на Съюза на съхраняването на тези данни. Всъщност Съдът се позовава единствено на развитата във връзка с последния проблем практика, за да я приложи към достъпа до лични данни. С други думи, при липса на разглеждане на въпроса дали съхраняването на определени данни е съвместимо с правото

[13] Вж. решение Tele2 (т. 79).

[14] Вж. решение от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018:788, т. 49).

[15] Решение от 2 октомври 2018 г. (C-207/16, EU:C:2018:788).

на Съюза, тази преценка се отлага за етапа на разглеждането на достъпа до тези данни, така че съвместимостта на този достъп в крайна сметка зависи от съвместимостта на съхраняването на съответните данни.

49. По-нататък Съдът ясно посочва, че достъпът до лични данни може да се предоставя само ако данните са били съхранявани от доставчиците на електронни съобщителни услуги в съответствие с член 15, параграф 1 от Директива 2002/58[16], и че достъпът до лични данни от частноправни лица, за да могат те да предявят граждански искове срещу нарушенията на авторското право, е съвместим с правото на Съюза само при условие че тези данни са съхранявани в съответствие с тази разпоредба[17].

50. Накрая, съгласно постоянната практика на Съда достъпът до данни за трафик и до данни за местонахождение, запазени от доставчиците в приложение на мярка, приета на основание член 15, параграф 1 от Директива 2002/58 (като този достъп трябва да се осъществява при пълно спазване на условията, произтичащи от съдебната практика по тълкуването на Директива 2002/58), по принцип може да бъде обоснован само с целта от общ интерес, за която тези доставчици са длъжни да ги съхраняват[18]. С други думи, въпросът за съвместимостта с правото на Съюза на достъпа на националните органи до определени лични данни зависи изцяло от отговора на въпроса за съвместимостта с правото на Съюза на запазването на тези данни.

51. Според мен оттук следва, че анализът на съвместимостта с правото на Съюза на национална правна уредба, която предвижда достъп на национален орган до лични данни, предполага първо да е установена съвместимостта с правото на Съюза на съхраняването на същите тези данни.

52. При тези обстоятелства ще започна анализа си с преглед на практиката на Съда относно съхраняването на IP адреси, предоставени на източника на свързване, за да покажа границите му и да предложа съобразена аналитична рамка на разглежданата правна уредба.

2. Практиката на Съда относно тълкуването на член 15, параграф 1 от Директива 2002/58, що се отнася до мерки за съхраняване на IP адреси, предоставени на източника на свързване

53. Член 5, параграф 1 от Директива 2002/58 прогласява принципа на поверителност както на електронните съобщения, така и на свързаните с тях данни за трафика и въвежда по-специално принципна забрана за съхраняването им от лица, различни от потребителите, или без тяхното съгласие[19].

54. Що се отнася до обработването и съхранението от доставчиците на електронни съобщителни услуги на данни за трафик, отнасящи се до абонатите и ползвателите, член 6, параграф 1 от Директива 2002/58 предвижда, че тези данни трябва да бъдат изтрити или да се направят анонимни, когато не са необходими повече за целите на предаване на съобщение, а в параграф 2 от този член се уточнява, че данните за трафик, необходими за

[16] Вж. решение Prokuratuur (т. 29).

[17] Вж. решение от 17 юни 2021 г., M.I.C.M. (C-597/19, EU:C:2021:492, т. 127—130).

[18] Вж. решения La Quadrature du Net и др. (т. 166), от 5 април 2022 г., Commissioner of An Garda Síochána и др. (C-140/20, EU:C:2022:258, наричано по-нататък „решение Commissioner of An Garda Síochána и др.“, т. 98), и от 20 септември 2022 г., SpaceNet (C-793/19 и C-794/19, EU:C:2022:702, наричано по-нататък „решение SpaceNet“, т. 131).

[19] Вж. решения La Quadrature du Net и др. (т. 107), Commissioner of An Garda Síochána и др. (т. 35) и SpaceNet (т. 52).

целите на изготвяне на сметката на абоната и плащания при взаимна връзка, могат да бъдат обработвани само до края на периода, през който сметката може законно да бъде оспорена или плащането – търсено. Що се отнася до данните за местонахождение, различни от данните за трафик, член 9, параграф 1 от тази директива предвижда, че те могат да се обработват само при определени условия и след като бъдат направени анонимни или се получи съгласие от ползвателите или абонатите [20].

55. Следователно с приемането на Директива 2002/58 законодателят на Съюза конкретизира правата, признати в членове 7 и 8 от Хартата, така че ползвателите на електронни съобщителни средства по принцип имат право да очакват, че техните съобщения и свързаните с тях данни, без тяхно съгласие, остават анонимни и няма да могат да бъдат записвани [21]. Ето защо по отношение на достъпа до такива данни тази директива не само предвижда гаранции, целящи предотвратяване на злоупотреби, но и закрепва в частност принципа на забрана на съхранението им от трети лица.

56. Доколкото член 15, параграф 1 от Директива 2002/58 позволява на държавите членки да приемат законодателни мерки, „за да ограничат обхвата“ на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от тази директива, като например произтичащите от принципите на поверителност на съобщенията и на забраната на съхранението на свързаните с тях данни, тази разпоредба предвижда изключение от общото правило, предвидено по-специално в тези членове 5, 6 и 9, и поради това съгласно постоянната съдебна практика трябва да се тълкува стриктно. Ето защо такава разпоредба не би могла да послужи като основание допускането на изключение от принципното задължение да се гарантира поверителността на електронните съобщения и на свързаните с тях данни, и по-специално от предвидената в член 5 от посочената директива забрана за съхраняване на тези данни, да се превърне в правило, без при това да се обезсмисли до голяма степен последната разпоредба [22].

57. Що се отнася до целите, които могат да обосноват ограничаване на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от Директива 2002/58, Съдът вече е постановил, че тези цели са изчерпателно изброени в член 15, параграф 1, първо изречение от Директива 2002/58, поради което приетата въз основа на тази разпоредба законодателна мярка трябва действително и строго да преследва някоя от тях [23].

58. Освен това от член 15, параграф 1, трето изречение от Директива 2002/58 следва, че мерките, приети от държавите членки въз основа на тази разпоредба, трябва да са съобразени с общите принципи на правото на Съюза, сред които е принципът на пропорционалност, и да осигуряват спазването на основните права, гарантирани от Хартата. В това отношение Съдът вече е постановил, че наложеното с национална правна уредба от държава членка задължение на доставчиците на електронни съобщителни услуги за запазване на данни за трафик с цел да може, когато се налага, да се предоставя достъп до тях на компетентните национални органи, повдига въпроси относно зачитането не само на членове 7 и 8 от Хартата, отнасящи се съответно до защитата на личния живот и до защитата на личните данни, но и на член 11 от Хартата, отнасящ се до свободата на

[20] Вж. решения Tele2 (т. 86), La Quadrature du Net и др. (т. 108), Commissioner of An Garda Síochána и др. (т. 38) и SpaceNet (т. 55).

[21] Вж. решения La Quadrature du Net и др. (т. 109), Commissioner of An Garda Síochána и др. (т. 37) и SpaceNet (т. 54).

[22] Вж. решения La Quadrature du Net и др. (т. 110 и 111), Commissioner of An Garda Síochána и др. (т. 40) и SpaceNet (т. 57).

[23] Вж. решения La Quadrature du Net и др. (т. 112), Commissioner of An Garda Síochána и др. (т. 41) и SpaceNet (т. 58).

изразяване на мнение, която представлява един от основните стълбове на демократичното и плуралистичното общество, отразяващо ценностите, на които се основава Съюзът в съответствие с член 2 ДЕС [24].

59. Доколкото обаче член 15, параграф 1 от Директива 2002/58 позволява на държавите членки да ограничат правата и задълженията, предвидени в членове 5, 6 и 9 от тази директива, първата посочена разпоредба отразява обстоятелството, че признатите в членове 7, 8 и 11 от Хартата права не са абсолютни прерогативи, а трябва да се разглеждат във връзка със своята социална функция. Всъщност, както следва от член 52, параграф 1 от Хартата, тя допуска ограничения на упражняването на тези права, стига тези ограничения да са предвидени в закон, да зачитат основното съдържание на посочените права и при спазване на принципа на пропорционалност да са необходими и действително да отговарят на признати от Съюза цели от общ интерес или на необходимостта да защитят правата и свободите на други хора. Така тълкуването на член 15, параграф 1 от Директива 2002/58 в светлината на Хартата изисква да се отчитат и значението на целите за защита на националната сигурност и борбата с тежката престъпност и приноса им за защитата на правата и свободите на други хора, и значението на правата, закрепени в членове 3, 4, 6 и 7 от Хартата [25], от които могат да произтичат задължения за действие за публичните органи [26].

60. С оглед на тези различни задължения за действие обаче следва да се пристъпи към съвместяване на различните разглеждани законни интереси и права. При това положение от самия текст на член 15, параграф 1, първо изречение от Директива 2002/58 следва, че държавите членки могат да приемат мярка, с която да дерогират принципа на поверителност, когато това представлява „необходима, подходяща и пропорционална мярка в рамките на демократично общество“, като в съображение 11 от тази директива се уточнява, че такава мярка трябва да бъде „строго“ пропорционална на предвидената цел [27].

61. В това отношение от практиката на Съда следва, че възможността за държавите да обосноват ограничение на правата и задълженията, предвидени по-специално в членове 5, 6 и 9 от Директива 2002/58, трябва да се прецени, като се измери тежестта на намесата в съответните основни права, която включва подобно ограничение, и като се провери дали значението на преследваната с това ограничение цел от общ интерес е свързано с тази тежест [28].

62. Освен това следва да се отбележи, че в практиката си Съдът прави разграничение между, от една страна, намеса, произтичаща от достъп до данни, които сами по себе си предоставят точна информация за въпросните съобщения и следователно за личния живот на лицето и по отношение на които е установен строг режим за съхранение, и от друга страна, намеса, произтичаща от достъп до данни, които могат да предоставят такава информация само доколкото са свързани с други данни, като например IP адреси [29].

63. Така, що се отнася по-специално до IP адресите, Съдът отбелязва, че те се генерират, без да са свързани с определено съобщение, и служат главно за идентифициране, посредством доставчиците на електронни съобщителни услуги, на физическото лице,

[24] Вж. решения La Quadrature du Net и др. (т. 113 и 114), Commissioner of An Garda Síochána и др. (т. 42) и SpaceNet (т. 60).

[25] Вж. решения La Quadrature du Net и др. (т. 120—122), Commissioner of An Garda Síochána и др. (т. 48) и SpaceNet (т. 63).

[26] Вж. решения La Quadrature du Net и др. (т. 120—122), Commissioner of An Garda Síochána и др. (т. 49) и SpaceNet (т. 64).

[27] Вж. решения La Quadrature du Net и др. (т. 127—129), Commissioner of An Garda Síochána и др. (т. 50 и 51) и SpaceNet (т. 65 и 66).

[28] Вж. решения La Quadrature du Net и др. (т. 131), Commissioner of An Garda Síochána и др. (т. 53) и SpaceNet (т. 68).

[29] Вж. точка 41 и сл. от настоящото заключение.

собственик на крайно устройство, от което се осъществява комуникация чрез интернет. Следователно, доколкото са съхранявани само IP адресите на източника на съобщението, но не и тези на неговия адресат, тази категория данни е с по-ниска степен на чувствителност в сравнение с другите данни за трафика [30].

64. Същевременно Съдът подчертава, че тъй като IP адресите могат да се използват по-специално за да се извърши изчерпателно проследяване на пътя на потребителя в сайтовете и страниците в интернет („clickstream“) и следователно на неговата онлайн дейност, тези данни позволяват да се установи подробният му профил и да се направят точни изводи за личния живот на ползвателя. Следователно съхраняването и анализът на тези IP адреси представляват *сериозна* намеса в основните права, закрепени в членове 7 и 8 от Хартата, която може да окаже възпиращо действие върху упражняването на свободата на изразяване на мнение, гарантирана с член 11 от Хартата [31].

65. Съгласно постоянната съдебна практика обаче за целите на необходимото съвместяване на разглежданите права и обосновани интереси, което се изисква съгласно съдебната практика, следва да се вземе предвид фактът, че в случай на извършено в интернет престъпление IP адресът може да бъде единственото средство за разследване, позволяващо да се установи самоличността на лицето, на което този адрес е бил предоставен към момента на извършване на това престъпление [32].

66. Ето защо Съдът е постановил, че законодателна мярка, която предвижда общо и неизбирателно съхраняване единствено на IP адресите, предоставени на източника на свързване, по принцип не е в противоречие с член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и с член 52, параграф 1 от Хартата, като тази възможност следва да е поставена в зависимост от стриктното спазване на материалните и процесуалните условия, които трябва да регламентират използването на тези данни, и като се има предвид, че с оглед на сериозността на намесата, до която може да доведе това запазване, същата може да бъде обоснована единствено от борбата с *тежката престъпност* и предотвратяването на сериозни заплахи за обществената сигурност, подобно на опазването на националната сигурност [33].

67. Освен това Съдът уточнява, че продължителността на съхраняването не може да надхвърля периода, който е строго необходим с оглед на преследваната цел, и че мярка от такова естество трябва да предвижда строги правила и гаранции за използването на тези данни [34].

[30] Вж. решение La Quadrature du Net и др. (т. 152).

[31] Вж. решения La Quadrature du Net и др. (т. 153), Commissioner of An Garda Síochána и др. (т. 73) и SpaceNet (т. 103) (курсивът е мой).

[32] Вж. решения La Quadrature du Net и др. (т. 154), Commissioner of An Garda Síochána и др. (т. 73) и SpaceNet (т. 103).

[33] Вж. решения La Quadrature du Net и др. (т. 155 и 156), Commissioner of An Garda Síochána и др. (т. 74) и SpaceNet (т. 104 и 105) (курсивът е мой).

[34] Вж. решения La Quadrature du Net и др. (т. 156) и SpaceNet (т. 105).

3. Пределите на съдебната практика относно тълкуването на член 15, параграф 1 от Директива 2002/58, що се отнася до мерки за съхраняване на IP адреси, предоставени на източника на свързване

68. Смятам обаче, че разрешението, до което стига Съдът по отношение на национални мерки за съхраняване на IP адреси, предоставени на източника на свързване, тълкувани с оглед на член 15, параграф 1 от Директива 2002/58, е свързано с две основни затруднения.

а) Съвместяването със съдебната практика относно разкриването на IP адреси, предоставени на източника на свързване, в рамките на искове за защита на правата върху интелектуална собственост

69. На първо място, както вече отбелязах в заключението си по дело M.I.C.M.[35], налице е известно напрежение между течението в тази съдебна практика, и съдебната практика, която се отнася до разкриването на IP адресите в рамките на искове за защита на правата върху интелектуална собственост на титулярите на тези права, която акцентира върху задължението на държавите членки да осигурят на титулярите на правата върху интелектуална собственост реални възможности да получат обезщетение за вредите, произтичащи от нарушенията на тези права[36].

70. Всъщност, що се отнася до второто течение в съдебната практика, Съдът трайно приема, че правото на Съюза допуска държавите членки да установяват задължение за предаване на лични данни на частноправни лица, за да могат те да предявят граждански искове срещу нарушенията на авторското право[37].

71. В това отношение Съдът отбелязва, че възможността държавите членки да предвидят задължение за разкриване на лични данни в рамките на граждански производства, произтича преди всичко от възможността такова разкриване да бъде предвидено в контекста на преследването на престъпления[38], чийто обхват впоследствие е разширен и покрива и гражданските производства.

72. Същевременно, що се отнася до IP адресите, Съда обаче постановява, че тези данни могат да бъдат съхранявани само в рамките на борбата с тежката престъпност и предотвратяването на сериозни заплахи срещу обществената сигурност[39].

73. Смятам, че опитите за съгласуване на тези две течения в съдебната практика водят до неподходящи резултати и са неубедителни.

74. От една страна, противно на твърденията на френското правителство в съдебното заседание, борбата с нарушенията на права върху интелектуална собственост не може да е част от борбата с тежката престъпност. Според мен понятието „тежка престъпност“ трябва да получи самостоятелно тълкуване. Това понятие не може да зависи от критериите на всяка държава членка, тъй като противното би означавало да се заобикалят изискванията на член 15, параграф 1 от Директива 2002/58 в зависимост от това дали държавите членки

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

36 Вж. заключението ми по дело M.I.C.M. (C-597/19, EU:C:2020:1063, т. 97).

37 Вж. решения от 19 април 2012 г., Bonnier Audio и др. (C-461/10, EU:C:2012:219, т. 55), от 4 май 2017 г., Rīgas satiksme (C-13/16, EU:C:2017:336, т. 34), и от 17 юни 2021 г., M.I.C.M. (C-597/19, EU:C:2021:492, т. 47—54).

38 Вж. в този смисъл решение от 29 януари 2008 г., Promusicae (C-275/06, EU:C:2008:54, т. 50—52).

39 Вж. точка 65 от настоящото заключение.

възприемат широко разбиране на понятието за борба с тежката престъпност. Впрочем, както вече отбелязах, интересите, свързани със защитата на правата върху интелектуалната собственост, не следва да се смесват с интересите, които са в основата на борбата с тежката престъпност [40].

75. От друга страна, разрешаването на предаването на IP адреси на титулярите на права върху интелектуална собственост в рамките на производствата, отнасящи се до тази защита, дори когато тези адреси са съхранявани само в рамките на борбата с тежката престъпност, очевидно ще противоречи на практиката на Съда относно съхраняването на данни за свързване и ще лиши от полезен ефект условията за съхраняването на такива данни, тъй като във всеки случай те могат да бъдат достъпни по различни мотиви.

76. Според мен от това следва, че съхраняването на IP адресите за целите на защитата на правата върху интелектуалната собственост, както и разкриването им на титулярите на тези права в рамките на производствата, отнасящи се до тази защита, е възможно да противоречат на член 15, параграф 1 от Директива 2002/58, както той се тълкува в практиката на Съда. Следователно задължението за предаване на лични данни на частноправни лица, за да могат те да предявят граждански искове срещу нарушенията на авторското право, впрочем възможно благодарение на самия Съд, същевременно се неутрализира от собствената му практика относно съхраняването на IP адреси от доставчиците на електронни съобщителни услуги.

77. Подобно разрешение обаче е незадоволително, тъй като може да постави под въпрос равновесието между различните засегнати интереси, което Съдът е искал да установи, като лишава титулярите на правата върху интелектуална собственост от основното, ако не и единствено средство да идентифицират извършителите на нарушенията на посочените права в интернет. Това съображение ме кара да изложа второто затруднение, което според мен може да произтече от практиката на Съда, що се отнася до национални мерки за съхраняване на IP адресите, предоставени на източника на свързване, тълкувано с оглед на член 15, параграф 1 от Директива 2002/58.

б) Рискът от системна безнаказаност за престъпленията, извършени изцяло в интернет

78. Така, на второ място, считам, че това разрешение е източник на практически затруднения. Както подчертава самият Съд, при престъпление, извършено изцяло в интернет, IP адресът може да е единственото средство за разследване, позволяващо да се установи самоличността на лицето, на което е предоставен този адрес в момента на извършване на нарушението.

79. Все пак ми се струва, че при претеглянето на разглежданите интереси това обстоятелство не е взето изцяло предвид. Предвид обстоятелството, че Съдът ограничава възможността за съхраняване на IP адресите в контекста на борбата с тежката престъпност, той същевременно изключва възможността тези данни да бъдат съхранявани за целите на борбата с престъпленията по принцип, въпреки че някои от тези престъпления могат да бъдат предотвратени, разкрити или санкционирани само благодарение на тези данни.

[40] Вж. заключението ми по дело M.I.C.M. (C-597/19, EU:C:2020:1063, т. 103).

80. С други думи, възможно е практиката на Съда да доведе до лишаване на националните органи от единственото средство за установяване на самоличността на извършителите на престъпления в интернет, които обаче не могат да се квалифицират като тежки престъпления, каквито са престъпленията против интелектуалната собственост. Това фактически би довело до системна безнаказаност на престъпленията, извършени изцяло в интернет, част от които далеч не са единствено престъпленията против интелектуалната собственост. Имам по-специално предвид престъплението клевета, извършено онлайн. Действително правото на Съюза предвижда мярка, с която да се задължат посредниците, чиито услуги са използвани за извършването на такива престъпления[41], но от практиката на Съда е възможно да се окаже, че самите извършители на тези деяния изобщо не могат да бъдат преследвани.

81. Освен ако се приеме, че редица престъпления изобщо не могат да бъдат разследвани в рамките на наказателно производство, считам, че равновесието между различните засегнати интереси трябва да бъде предмет на ново разглеждане.

82. Изложените разнообразни съображения ме мотивират да предложа на Съда да преразгледа практиката си относно националните мерки за съхраняване на IP адреси, тълкувани в светлината на член 15, параграф 1 от Директива 2002/58.

4. Предложението за преразглеждане на практиката на Съда относно тълкуването на член 15, параграф 1 от Директива 2002/58, що се отнася до мерки за съхраняване на IP адреси, предоставени на източника на свързване

83. С оглед на изложените съображения считам, че член 15, параграф 1 от Директива 2002/58 би трябвало да се тълкува в смисъл, че допуска мерки, които предвиждат общо и неизбирателно съхраняване на IP адреси, предоставени на източника на свързване, за ограничена до строго необходимото времева продължителност, с цел да се гарантират предотвратяването, разследването, разкриването и преследването на престъпления, извършени в интернет, за които IP адресът е *единственото средство* за разследване, позволяващо да се установи самоличността на лицето, на което е предоставен този адрес в момента на извършване на престъплението.

84. В това отношение трябва да подчертая, че според мен с това предложение не се поставя под въпрос изискването за пропорционалност, наложено за съхраняването на данни предвид сериозността на намесата в основните права, закрепени в членове 7 и 8 от Хартата, което изискване се предполага при наличието на такава намеса[42]. Напротив, това предложение отговаря напълно на това изискване.

85. От една страна, с ограничаване на правата и задълженията по членове 5, 6 и 9 от Директива 2002/58, каквото представлява съхраняването на IP адреси, се преследва цел от общ интерес във връзка с тази сериозност на намесата, а именно предотвратяване, разследване, разкриване и наказателно преследване на престъпленията, обхванати от разпоредбите на Директивата, които в противен случай биха били лишени от действие.

[41] Вж. член 15, параграф 1 от Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 година за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия) (ОВ L 178, 2000 г., стр. 1; Специално издание на български език, 2007 г., глава 13, том 29, стр. 257).

[42] Вж. точки 60 и 61 от настоящото заключение.

86. От друга страна, това ограничаване се въвежда в границите на строго необходимото. Всъщност такова съхраняване е ограничено до конкретни хипотези, а именно за престъпления, извършени в интернет и при които самоличността на извършителя може да бъде установена единствено благодарение на предоставения му IP адрес. С други думи, не става въпрос за разрешаване на безусловно общо и неизбирателно съхраняване на данни, а само за да се позволи наказателно преследване само за конкретни престъпления, а не като общо правило.

87. Макар обаче член 15, параграф 1 от Директива 2002/58 да допуска общо и неизбирателно съхраняване на IP адресите, предоставени на източника на свързване, с цел да се осигурят предотвратяването, разследването, разкриването и преследването на престъпления, извършени в интернет, когато IP адресът е единственото средство за разследване, позволяващо да се установи самоличността на лицето, на което е предоставен този адрес в момента на извършване на нарушението, трябва да се уточни, че съгласно съдебната практика тази възможност следва да е поставена в зависимост „от стриктното спазване на материалните и процесуалните условия, *които трябва да регламентират използването на тези данни*“ [43]. Съдът уточнява и че такава мярка „трябва да предвижда строги правила и гаранции за *използването на тези данни*“ [44].

88. С други думи, както вече подчертах, съхраняването на данни и достъпът до тях не могат да се разглеждат изолирано. При тези условия, макар възможността за Hadopi до получи достъп до IP адресите, по принцип да не е в противоречие с член 15, параграф 1 от Директива 2002/58, доколкото тези данни са съхранявани съобразно предвидените с тази разпоредба изисквания, за да се отговори на отправените до Съда преюдициални въпроси, е необходимо също така да се разгледа обстоятелството дали условията за достъп до IP адресите, предоставени на източника на свързване от Hadopi, сами по себе си са в съответствие с посочената разпоредба, по-конкретно що се отнася до необходимостта от предварителен контрол върху такъв достъп от юрисдикция или от независим административен орган.

89. След като разгледах предварителния въпрос относно съхраняването на IP адреси, предоставени на източника на свързване, ще разгледам въпроса за достъпа на Hadopi до тези данни с оглед на член 15, параграф 1 от Директива 2002/58.

5. Достъпът на Hadopi до данните за самоличност, съответстващи на IP адресите

90. Съгласно практиката на Съда по отношение на целите, които могат да обосноват национална правна уредба, която дерогира принципа на поверителност на електронните съобщения, при достъпа до данните трябва строго и обективно да се преследва някоя от тези цели и преследваната с тази правна уредба цел трябва да е свързана с тежестта на намесата в съответните основни права, до която води този достъп [45].

[43] Вж. решение La Quadrature du Net и др. (т. 155) (курсивът е мой).

[44] Вж. решение La Quadrature du Net и др. (т. 156) (курсивът е мой).

[45] Вж. решения от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018:788, т. 55), и Prokuratuur (т. 32).

91. Освен това, както вече посочих [46], достъпът до съхранявани от доставчици данни в изпълнение на приета на основание член 15, параграф 1 от Директива 2002/58 мярка по принцип може да бъде обоснован само с целта от общ интерес, за която тези доставчици са длъжни да съхраняват тези данни [47].

92. Така Съдът е постановил, че съгласно принципа на пропорционалност, 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“ [48].

93. В това отношение следва да се отбележи, противно на твърденията на френското правителство и на Комисията, че достъпът на Hadopi до данните за самоличност, съответстващи на IP адрес, действително представлява тежка намеса в основните права. Това е така, защото не става дума само за достъп до данните за самоличност, които сами по себе си са с ниска чувствителност, но и за свързването на тези данни с по-широка съвкупност от данни, а именно IP адреса, а също така, както подчертават жалбоподателите в главното производство, и с извадка от изтегления в нарушение на авторското право файл. Следователно става въпрос за необходимостта да се свърже самоличността на дадено лице със съдържанието на ползвания файл и с IP адреса, от който е извършено това ползване.

94. Въпреки това, по същия начин, както приемам, че следва да се позволи и съхраняване на данни, което представлява сериозна намеса в основните права с цел да се осигурят предотвратяването, разследването, разкриването и преследването на престъпления, извършени в интернет, когато IP адресът е единственото средство за разследване, позволяващо да се установи самоличността на лицето, на което е предоставен този адрес в момента на извършване на нарушението [49], считам, че достъпът до тези данни трябва да бъде възможен, за да се преследва същата цел, тъй като в противен случай би се допуснала обща безнаказаност на престъпленията, извършени изцяло в интернет.

95. Ето защо считам, че достъпът на Hadopi до данните за самоличност, свързани с IP адрес, е обоснован с целта от общ интерес, с оглед на която това съхраняване е въздигнато в задължение за доставчиците на електронни съобщителни услуги.

96. Все пак в практиката на Съда се уточнява, че национална правна уредба, която урежда достъпа на компетентните органи до запазените данни за трафик и данни за местонахождение, не може да се ограничи до изискването достъпът на компетентните национални органи до съответните данни да отговаря на преследваната с тази правна уредба цел, а трябва да предвижда също материални и процесуални условия за това използване [50].

97. По-специално, Съдът постановява, че тъй като общ достъп до всички запазени данни, независимо дали те имат някаква, макар и непряка, връзка с преследваната цел, не може да се счита за ограничен до строго необходимото, съответната национална правна уредба трябва да се основава на обективни критерии за определяне на обстоятелствата и условията, при които на компетентните национални органи трябва да се предоставя

[46] Точка 47 от настоящото заключение.

[47] Вж. решения SpaceNet (т. 131), La Quadrature du Net и др. (т. 166) и Commissioner of An Garda Síochána и др. (т. 98).

[48] Виж. решения Tele2 (т. 115), от 2 октомври 2018 г., Ministerio Fiscal (C-207/16, EU:C:2018:788, т. 56), и Prokuratuur (т. 33).

[49] Вж. точка 65 и сл. от настоящото заключение.

[50] Вж. решения Tele2 (т. 118), Prokuratuur (т. 49) и Commissioner of An Garda Síochána и др. (т. 104).

достъп до въпросните данни, така че да се провери дали достъпът да се предостави само до данните на лица, които са заподозрени, че подготвят, извършват или са извършили тежко престъпление или още че по някакъв начин са участвали в такова престъпление [51].

98. Съгласно съдебната практика, за да се гарантира на практика пълното спазване на тези условия, от съществено значение е достъпът на компетентните национални органи до запазените данни да се предоставя след предварителен контрол, осъществяван или от юрисдикция, или от независима административна структура [52].

99. Следва да се отбележи обаче, че Съдът е установил необходимостта от предварителен контрол на достъпа до лични данни при особени обстоятелства, които са различни от обстоятелствата по настоящия случай, свързани с *особено сериозна* намеса в личния живот на ползвателите на електронни съобщителни услуги.

100. Това е така, защото във всяко от решенията, в които се подчертава това изискване, става дума за национални мерки, които разрешават достъп до съвкупността от данни за трафика и за местонахождението на ползватели на всички електронни съобщителни средства [53] или най-малкото, на стационарните и мобилните телефони [54]. По-конкретно, в тях се разглежда достъпът до „съвкупност от данни […], които могат да дадат информация за извършените комуникации от даден ползвател на средство за електронна комуникация или за местонахождението на използваните от него крайни устройства и позволяват да се направят точни изводи относно личния живот на засегнатите лица“ [55], така че според мен само при тези условия съществува изискване за предварителен контрол на достъпа до тези данни от юрисдикция или независима административна структура.

101. От една страна обаче, достъпът от Hadopi остава ограничен до възможността да се установи връзка между данните за самоличност и използвания IP адрес и файла, използван в конкретен момент, без това да води нито до възможност компетентните органи да проследят пътя на посочения потребител в интернет, нито следователно до възможност те да направят конкретни изводи за личния му живот, освен да разкрият кой е конкретният ползван файл в момента на извършване на нарушението. Следователно не става въпрос да се позволява проследяване на всички извършвани действия в интернет на въпросния потребител.

102. От друга страна, тази информация се отнася само до данните за лицата, които, както се установява от изготвените от организациите на титулярите на права протоколи, са извършили действия, които представляват неизпълнение на задължението по член L.336-3 от CPI. Следователно достъпът на Hadopi до данните за самоличност, свързани с IP адресите, е строго ограничен до необходимото за постигане на преследваната цел, а именно да се гарантират предотвратяването, разследването, разкриването и преследването на престъпления, извършени в интернет, когато IP адресът е единственото средство за разследване, позволяващо да се установи самоличността на лицето, на което е предоставен този адрес в момента на извършване на нарушението, в което се вписва механизмът за поетапен отговор.

[51] Вж. решения Tele2 (т. 119), Prokuratuur (т. 50) и от Commissioner of An Garda Síochána и др. (т. 105).

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

[53] Вж. решения Tele2 и Commissioner of An Garda Síochána и др.

[54] Вж. решение Prokuratuur.

[55] Вж. решение Prokuratuur (т. 45).

103. При тези обстоятелства считам, че член 15, параграф 1 от Директива 2002/58 не изисква наличие на предварителен контрол на достъпа от страна на Hadopi до данните за самоличност, свързани с IP адресите на ползвателите, от юрисдикция или от независима административна структура.

104. В допълнение следва да се отбележи, както подчертава френското правителство, че достъпът от страна на Hadopi до тези данни, макар да не подлежи на предварителен контрол, осъществяван от юрисдикция или от независима структура, все пак подлежи на контрол, тъй като файлът, изпращан от Hadopi на операторите на електронни съобщителни услуги, се изготвя всеки ден от заклето длъжностно лице въз основа на получените жалби или сигнали, валидирани на случаен принцип чрез примерна извадка, преди тези данни да бъдат добавени във файла [56]. Преди всичко трябва да се отбележи, че процедурата за поетапен отговор попада в приложното поле на разпоредбите на Директива (ЕС) 2016/680 [57]. На това основание физическите лица, към които насочва действията си Hadopi, се ползват от съвкупност от материални и процесуални гаранции, предвидени в тази директива. Те обхващат правото на достъп, на поправяне и заличаване на лични данни, обработвани от Hadopi, както и възможността за обжалване по административен ред пред независим надзорен орган, последвана, в зависимост от конкретния случай, от възможността да се потърси съдебна защита по общия ред [58].

105. Ето защо предлагам на първия и втория преюдициален въпрос да се отговори, че член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и с член 52, параграф 1 от Хартата 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 електронни съобщителни услуги и ограничения достъпа на административен орган, на който е възложена защитата на авторските и сродните им права срещу извършени в интернет нарушения, само до такива данни, за да може този орган да идентифицира притежателите 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 е предоставен този адрес в момента на извършване на нарушението.

[56] Като допълнение следва да се отбележи, че с доводи за практическата осъществимост се опровергава тезата за задължението за систематичен предварителен контрол. Наличието на организирана система за борба с извършените в интернет престъпления, засягащи авторското право, като разглежданото в главното производство, предполага необходимостта да се обработва значително количество лични данни съобразно броя на преследваните престъпления, а именно, например за 2019 г., съгласно писменото становище на френското правителство — 33 465 заявления за идентифициране на IP адрес, разглеждани от Hadopi всеки ден. В този контекст задължението за осъществяване на предварителен контрол за достъпа до данни на практика би застрашило функционирането на механизмите за борба с фалшифицирането в интернет, поставяйки под въпрос баланса между правата на ползвателите и правата на авторите.

[57] Директива на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 2016 г., стр. 89).

[58] Всички тези гаранции са предвидени в разпоредбите на дял III, глава III от Loi nº 78-17 relative à l'informatique, aux fichiers et aux libertés, du 6 janvier 1978 (Закон № 78-17 за информационните технологии, компютърните файлове и гражданските свободи от 6 януари 1978 г.) (JORF от 7 януари 1978 г.).

Б. По третия преюдициален въпрос

106. С третия преюдициален въпрос запитващата юрисдикция иска да се установи дали, в случай че отговорът на първия и втория въпрос е утвърдителен, и с оглед на ниската чувствителност на данните за самоличност, строгата рамка на достъпа до данните и изискването да не се нарушава задачата за изпълнение на публични функции, възложена на съответния административен орган, член 15, параграф 1 от Директива 2002/58 във връзка с членове 7, 8 и 11 и с член 52, параграф 1 от Хартата трябва да се тълкува в смисъл, че не допуска предварителният контрол за достъп да се осъществява по съответно приспособени правила, като например автоматизиран контрол, в зависимост от конкретния случай, под надзора на вътрешно звено на органа, което отговаря на изискванията за независимост и безпристрастност по отношение на служителите, натоварени със събирането на данните.

107. От текста на третия преюдициален въпрос и от писмения отговор на френското правителство на въпросите на Съда следва, че съответно приспособени правила, по които се осъществява контролът за достъп и които са упоменати в този въпрос, се отнасят не само до съществуващ в националното право механизъм за контрол, но и до възможните разрешения, които имат за цел да се приложи механизмът по френското право, който, в зависимост от конкретния случай, е в съответствие с правото на Съюза.

108. Съгласно постоянната съдебна практика обаче преюдициалното запитване няма за цел да се формулират консултативни становища по общи или хипотетични въпроси, а да се отговори на необходимост, продиктувана от това, че действително трябва да се реши спор, свързан с правото на Съюза[59].

109. Ето защо според мен, тъй като има хипотетичен характер, третият преюдициален въпрос следва да се приеме за недопустим.

110. При всички положения, предвид отговора, който предлагам да бъде даден на първия и втория преюдициален въпрос, не следва да се отговаря на третия въпрос.

V. Заключение

111. С оглед на всички изложени съображения предлагам на Съда да отговори на преюдициалните въпроси, поставени от Conseil d'État (Държавен съвет, Франция), както следва:

„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) 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

[59] Вж. решения от 26 октомври 2017 г., Българска енергийна борса (C-347/16, EU:C:2017:816, т. 31), от 31 май 2018 г., Confetra и др. (C-259/16 и C-260/16, EU:C:2018:370, т. 63), и от 17 октомври 2019 г., Електроразпределение Юг (C-31/18, EU:C:2019:868, т. 32).

допуска национална правна уредба, позволяваща съхраняването на данните за самоличност, съответстващи на IP адреси, от страна на доставчиците електронни съобщителни услуги и ограничения достъпа на административен орган, на който е възложена защитата на авторските и сродните им права срещу извършени в интернет нарушения, само до такива данни, за да може този орган да идентифицира притежателите 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 е предоставен този адрес в момента на извършване на нарушението“.