CONCLUZIILE AVOCATULUI GENERAL
DOMNUL MACIEJ SZPUNAR
prezentate la 28 septembrie 2023[1]

Cauza C-470/21

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

[cerere de decizie preliminară formulată de Conseil d'État (Consiliul de Stat, Franța)]

„Trimitere preliminară – Prelucrarea datelor cu caracter personal și protejarea confidențialității în sectorul comunicațiilor electronice – Directiva 2002/58/CE – Articolul 15 alineatul (1) – Posibilitatea statelor membre de a restrânge sfera de aplicare a anumitor drepturi și obligații – Obligația efectuării unui control prealabil de către o instanță sau o entitate administrativă independentă care dispune de putere de constrângere – Date de identitate civilă corespunzătoare unei adrese IP"

I. Introducere

1. La data de 7 martie 2023, Curtea a decis, la solicitarea Marii Camere întemeiată pe articolul 60 alineatul (3) din Regulamentul de procedură al Curții, să trimită prezenta cauză spre soluționare Plenului.

2. Prin Ordonanța din 23 martie 2023, Curtea (Plenul) a decis redeschiderea fazei orale a procedurii și a invitat persoanele interesate menționate la articolul 23 din Statutul Curții de Justiție a Uniunii Europene, Autoritatea Europeană pentru Protecția Datelor (AEPD) și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) să participe la o nouă ședință.

3. La 27 octombrie 2022, am prezentat primele noastre concluzii în această cauză înainte de închiderea fazei orale a procedurii. Prin urmare, aceste noi concluzii reprezintă pentru noi ocazia de a aprofunda anumite elemente ale raționamentului nostru în această cauză cu mize esențiale în ceea ce privește păstrarea și accesul la date cu caracter personal.

[1] Limba originală: franceza.

II. Cadrul juridic

A. Dreptul Uniunii

4. Considerentele (2), (6), (7), (11), (22), (26) și (30) ale Directivei 2002/58/CE[2] au următorul cuprins:

„(2) Prezenta directivă dorește respectarea drepturilor fundamentale și a principiilor recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene [(denumită în continuare «carta»)]. Directiva caută să asigure în special respectarea deplină a drepturilor menționate la articolele 7 și 8 ale cartei.

[…]

(6) Internetul a răsturnat structurile de piață tradiționale furnizând o infrastructură comună la nivel global pentru o gamă foarte largă de servicii de comunicare electronică. Serviciile de comunicare electronică publice prin internet deschid noi posibilități pentru utilizatori, dar reprezintă și noi riscuri pentru datele lor personale și pentru confidențialitatea comunicațiilor lor.

(7) În cazul rețelelor de comunicații publice, ar trebui adoptate acte cu putere de lege, norme administrative și norme tehnice pentru protejarea drepturilor și libertăților fundamentale ale persoanelor fizice și a intereselor legitime ale persoanelor juridice, mai cu seamă în privința capacităților în creștere de stocare automată și de prelucrarea a datelor referitoare la abonați și utilizatori.

[…]

(11) La fel ca Directiva [95/46/CE[3]], prezenta directivă nu se referă la chestiuni de protecție a drepturilor și libertăților fundamentale legate de activități care nu sunt reglementate de legile comunitare. Prin urmare, aceasta nu aduce atingere echilibrului existent între dreptul indivizilor la confidențialitate și posibilitatea ca statele membre să ia măsurile stipulate la articolul 15 alineatul (1) din prezenta directivă, posibilitate necesară în vederea protejării siguranței publice, apărării și siguranței statului (inclusiv bunăstării economice a acestuia, în cazul în care activitățile respective sunt legate de chestiuni de siguranța statului) și întăririi legii penale. În consecință, prezenta directivă nu interzice statelor membre să efectueze interceptări legale ale comunicațiilor electronice sau să ia alte măsuri pentru atingerea scopurilor menționate anterior, dacă acest lucru este necesar și în conformitate cu Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale, [semnată la Roma la 4 noiembrie 1950,] așa cum este aceasta interpretată de Curtea Europeană a Drepturilor Omului. Aceste măsuri trebuie să fie corespunzătoare, strict proporționale cu scopul urmărit și necesare în cadrul unei societăți democratice și trebuie însoțite de precauțiile corespunzătoare în conformitate cu Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale.

[2] Directiva Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO 2002, L 201, p. 37, Ediție specială, 13/vol. 36, p. 63), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO 2009, L 337, p. 11) (denumită în continuare „Directiva 2002/58”).

[3] Directiva Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10).

[…]

(22) Interdicția stocării comunicațiilor și a datelor de transfer aferente de către alte persoane decât utilizatorul sau fără acordul acestuia nu înseamnă interzicerea oricărei stocări automate, intermediare sau tranzitorii a acestor informații, în cazul în care acest lucru se întâmplă cu unicul scop al efectuării transmisiei prin rețeaua de comunicații electronice și cu condiția ca informațiile să nu fie stocate pentru o perioadă mai lungă decât este necesar în vederea transmiterii sau în scopuri legate de gestionarea traficului și ca în timpul perioadei de stocare să fie garantată confidențialitatea datelor. […]

[…]

(26) Datele referitoare la abonați prelucrate în cadrul rețelei de comunicații electronice pentru a stabili conexiuni sau pentru a transmite informații conțin informații despre viața personală a persoanelor fizice și intră sub incidența dreptului la respectarea confidențialității corespondenței sau a dreptului la protejarea intereselor legitime ale persoanelor juridice. Aceste date pot fi stocate doar pe timpul necesar furnizării serviciului sau facturării și pentru plăți online și numai pentru o perioadă limitată de timp. Orice altă prelucrare a acestor date […] este permisă numai în cazul în care abonatul își dă acordul la aceasta după o informare corectă și completă din partea prestatorului de servicii publice de comunicații electronice cu privire la modul de prelucrare ulterioară a datelor pe care intenționează să o efectueze și la dreptul abonatului de a nu acorda sau de a-și retrage acordul pentru această prelucrare. […]

[…]

(30) Sistemele de furnizare de servicii și rețele de comunicații electronice trebuie astfel construite încât să limiteze cantitatea de date personale necesare la un minimum strict. […]”

5. Potrivit articolului 2 din această directivă, intitulat „Definiții”:

„[…]

Se aplică de asemenea următoarele definiții:

(a) «utilizator» înseamnă orice persoană fizică ce folosește un serviciu public de comunicații electronice, în scopuri profesionale sau personale, fără a fi în mod necesar abonat la serviciul respectiv;

(b) «date de transfer» înseamnă orice date prelucrate în scopul transmiterii comunicației printr-o rețea de comunicații electronice sau în vederea facturării;

(c) «date de localizare» înseamnă orice date prelucrate într-o rețea de comunicații electronice sau prin intermediul unui serviciu de comunicații electronice, care indică poziția geografică a echipamentului terminal al unui utilizator al unui serviciu de comunicații electronice destinat publicului;

(d) «comunicație» înseamnă orice informație trimisă sau transmisă între un număr finit de părți prin intermediul unui serviciu public de comunicații electronice. Această categorie nu include informațiile transmise în cadrul unui serviciu de radiodifuziune pentru public prin intermediul unei rețele de comunicații electronice, în măsura în care aceste informații nu pot fi relaționate cu un abonat sau cu un utilizator identificabil care primește informația;

[…]”

6. Articolul 3 din directiva menționată, intitulat „Serviciile vizate”, prevede:

„Prezenta directivă se aplică prelucrării de date cu caracter personal legate de furnizarea de servicii de comunicații electronice destinate publicului prin intermediul rețelelor publice de comunicații din cadrul Comunității, inclusiv al rețelelor publice de comunicații care presupun colectarea de date și dispozitive de identificare.”

7. Articolul 5 din aceeași directivă, intitulat „Confidențialitatea comunicațiilor”, prevede:

„(1) Statele membre trebuie să asigure confidențialitatea comunicațiilor și a datelor de transfer aferente transmise prin intermediul unei rețele de comunicații publice sau unor servicii publice de comunicații electronice, prin legislația internă. Acestea interzic astfel în special ascultarea, înregistrarea, stocarea sau alte tipuri de interceptare sau supraveghere a comunicațiilor și a datelor de transfer aferente de către persoane altele decât utilizatorul, fără acordul utilizatorului în cauză, cu excepția cazurilor în care acest lucru este permis în temeiul articolului 15 alineatul (1). Prezentul alineat nu interzice stocarea tehnică necesară pentru transmisia comunicației care nu aduce atingere principiului confidențialității.

[…]

(3) Statele membre se asigură că stocarea de informații sau dobândirea accesului la informațiile deja stocate în echipamentul terminal al unui abonat sau utilizator este permisă doar cu condiția ca abonatul sau utilizatorul în cauză să își fi dat acordul, după ce a primit informații clare și complete, în conformitate cu Directiva [95/46], *inter alia*, cu privire la scopurile prelucrării. Aceasta nu împiedică stocarea sau accesul tehnic cu unicul scop de a efectua transmisia comunicării printr-o rețea de comunicații electronice sau în cazul în care acest lucru este strict necesar în vederea furnizării de către furnizor a unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator.”

8. Potrivit articolului 6 din Directiva 2002/58, intitulat „Datele de transfer”:

„(1) Datele de transfer referitoare la abonați și utilizatori prelucrate și stocate de către furnizorul rețelei de comunicații publice sau al serviciilor publice de comunicații electronice trebuie șterse sau trecute în anonimat de îndată ce nu mai sunt necesare în scopul transmiterii comunicației, fără a aduce atingere alineatelor (2), (3) și (5) din prezentul articol sau articolului 15 alineatul (1).

(2) Datele de transfer necesare în vederea facturării serviciilor oferite abonatului sau plății conexiunii pot să fie prelucrate. Prelucrarea lor este permisă doar până la sfârșitul perioadei în care factura poate fi contestată prin lege sau plata poate fi urmărită.

[…]”

9. Articolul 15 din această directivă, intitulat „Aplicarea anumitor dispoziții ale Directivei [95/46]”, prevede la alineatul (1):

„Statele membre pot adopta măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolul 5, articolul 6, articolul 8 alineatele (1), (2), (3) și (4) și articolul 9 ale prezentei directive, în cazul în care restrângerea lor constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională (de exemplu siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei [95/46]. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat. Toate măsurile menționate în acest alineat trebuie să fie conforme cu principiile generale ale legislației [Uniunii], inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) [TUE].”

B. Dreptul francez

1. Code de la propriété intellectuelle (Codul proprietății intelectuale)

10. Articolul L. 331-12 din Codul proprietății intelectuale, în versiunea aplicabilă litigiului principal (denumit în continuare „CPI”), prevede:

„Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet [Înalta autoritate pentru difuzarea operelor și protecția drepturilor pe internet (denumită în continuare «Hadopi»)] este o autoritate publică independentă.”

11. Articolul L. 331-13 din CPI prevede:

„[Hadopi] asigură:

[…]

2° O misiune de protecție [a operelor și obiectelor protejate de un drept de autor sau de un drept conex pe rețelele de comunicații electronice] împotriva încălcărilor acestor drepturi săvârșite pe rețelele de comunicații electronice utilizate pentru furnizarea serviciilor de comunicații publice online; […]”

12. Potrivit articolului L. 331-15 din acest cod:

„[Hadopi] este compusă dintr-un colegiu și o comisie pentru protecția drepturilor. […]

[…]

În exercitarea atribuțiilor lor, membrii colegiului și ai comisiei pentru protecția drepturilor nu primesc instrucțiuni de la nicio autoritate.”

13. Articolul L. 331-17 din codul menționat prevede:

„Comisia pentru protecția drepturilor este responsabilă de luarea măsurilor prevăzute la articolul L. 331-25.”

14. Potrivit articolului L. 331-21 din același cod:

„Pentru exercitarea de către comisia pentru protecția drepturilor a atribuțiilor sale, [Hadopi] dispune de agenți publici autorizați împuterniciți de președintele [acesteia] în condițiile stabilite printr-un decret adoptat pe baza avizului Conseil d'État (Consiliul de Stat). […]

Membrii comisiei pentru protecția drepturilor și agenții menționați la primul paragraf primesc sesizările adresate comisiei menționate în condițiile prevăzute la articolul L. 331-24. Aceștia efectuează o examinare a faptelor.

Ei pot obține, în măsura în care este necesar pentru desfășurarea procedurii, toate documentele, indiferent de suportul lor, inclusiv datele păstrate și prelucrate de operatorii de comunicații electronice în temeiul articolului L. 34-1 din code des postes et des communications électroniques (Codul poștal și al comunicațiilor electronice) și de prestatorii de servicii menționați la punctele 1 și 2 ale alineatului I al articolului 6 din loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Legea nr. 2004-575 din 21 iunie 2004 privind încrederea în economia digitală).

De asemenea, pot obține copii ale documentelor menționate la paragraful precedent.

În special, pot obține din partea operatorilor de comunicații electronice identitatea, adresa poștală, adresa electronică și datele de contact telefonic ale abonatului al cărui acces la servicii de comunicații publice online a fost utilizat în scopul reproducerii, al reprezentării, al punerii la dispoziție sau al comunicării publice de opere sau de obiecte protejate fără autorizarea titularilor drepturilor […] în cazul în care aceasta este necesară.”

15. Articolul L. 331-24 din CPI prevede:

„Comisia pentru protecția drepturilor acționează la sesizarea agenților autorizați și acreditați […] care sunt desemnați de:

– organismele de apărare a intereselor profesionale constituite periodic;

– organismele de gestiune colectivă;

– Centrul național al cinematografiei și al imaginii animate.

Comisia pentru protecția drepturilor poate acționa și pe baza informațiilor care îi sunt transmise de procurorul Republicii.

Aceasta nu poate fi sesizată cu privire la fapte care datează de mai mult de șase luni.”

16. Potrivit articolului L. 331-25 din acest cod, dispoziție care reglementează așa-numita procedură de „răspuns gradual”:

„Atunci când este sesizată cu privire la fapte care pot constitui o neîndeplinire a obligației definite la articolul L. 336-3 [din CPI], comisia pentru protecția drepturilor poate trimite abonatului […] o recomandare prin care îi amintește dispozițiile articolului L. 336-3, îi solicită să respecte obligația pe care acestea o definesc și îl avertizează cu privire la sancțiunile aplicabile în temeiul articolelor L. 335-7 și L. 335-7-1. Această recomandare conține de asemenea o informare a abonatului cu privire la oferta legală de conținuturi culturale online, cu privire la existența unor mijloace de securizare care permit prevenirea încălcării obligației definite la articolul L. 336-3, precum și cu privire la pericolele pentru reînnoirea creației artistice și pentru economia sectorului cultural pe care le prezintă practicile care nu respectă dreptul de autor și drepturile conexe.

În cazul repetării unor fapte care pot constitui o neîndeplinire a obligației definite la articolul L. 336-3, comisia poate adresa, în termen de șase luni de la trimiterea recomandării menționate la primul paragraf, o nouă recomandare care conține aceleași informații ca precedenta trimisă pe cale electronică […] Această recomandare trebuie trimisă printr-o scrisoare predată sub semnătură sau prin orice alt mijloc de natură să facă dovada datei aducerii la cunoștință a acestei recomandări.

Recomandările adresate în temeiul prezentului articol menționează data și ora la care au fost constatate faptele care pot constitui o neîndeplinire a obligației definite la articolul L. 336-3. În schimb, ele nu divulgă conținutul operelor sau al obiectelor protejate care fac obiectul acestei neîndepliniri a obligațiilor. Ele precizează coordonatele telefonice, poștale și electronice la care destinatarul lor poate, dacă dorește, să adreseze observații comisiei pentru protecția drepturilor și să obțină, dacă formulează o cerere expresă, precizări cu privire la conținutul operelor sau al obiectelor protejate care fac obiectul neîndeplinirii obligațiilor care îi este imputată.”

17. Articolul L. 331-29 din codul menționat prevede:

„Este autorizată crearea de către [Hadopi] a unei prelucrări automatizate a datelor cu caracter personal referitoare la persoanele care fac obiectul unei proceduri în cadrul prezentei subsecțiuni.

Această prelucrare are drept scop punerea în aplicare de către comisia pentru protecția drepturilor a măsurilor prevăzute în prezenta subsecțiune, a tuturor actelor de procedură aferente și a modalităților de informare a organismelor de apărare a intereselor profesionale și a organismelor de gestiune colectivă cu privire la eventualele sesizări ale autorității judiciare, precum și a notificărilor prevăzute la al cincilea paragraf al articolului L. 335-7.

Un decret […] stabilește normele de aplicare a prezentului articol. El precizează în special:

– categoriile de date înregistrate și perioada de păstrare a acestora;

– destinatarii abilitați să obțină comunicarea datelor respective, în special persoanele a căror activitate este aceea de a oferi acces la servicii de comunicații publice online;

– condițiile în care persoanele interesate își pot exercita, la [Hadopi], dreptul de acces la datele care le vizează […]”

18. Articolul R. 331-37 din același cod prevede:

„Operatorii de comunicații electronice […] și prestatorii de servicii […] sunt obligați să comunice, printr-o interconectare la prelucrarea automatizată a datelor cu caracter personal menționată la articolul L. 331-29 sau prin utilizarea unui suport de înregistrare care asigură integritatea și securitatea lor, datele cu caracter personal și informațiile menționate la punctul 2 din anexa la [décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du [CPI] dénommé «Système de gestion des mesures pour la protection des œuvres sur Internet» (Decretul nr. 2010-236 din 5 martie 2010 privind prelucrarea automatizată a datelor cu caracter personal autorizată prin articolul L. 331-29 din [CPI], denumită «Sistemul de gestionare a măsurilor pentru protecția operelor pe internet»)[4] (denumit în continuare «Decretul din 5 martie 2010»)] […] în termen de opt zile de la transmiterea de către comisia pentru protecția drepturilor a datelor tehnice necesare pentru identificarea abonatului al cărui acces la serviciile de comunicații publice online a fost utilizat în scopul reproducerii, al reprezentării, al punerii la dispoziție sau al comunicării publice de opere sau de obiecte protejate fără autorizarea titularilor drepturilor […] în cazul în care aceasta este necesară.

[…]”

19. Articolul R. 335-5 din CPI prevede:

„I.– Constituie o neglijență gravă, care se pedepsește cu amenda prevăzută pentru contravențiile din clasa a cincea, atunci când sunt îndeplinite condițiile prevăzute la alineatul II, faptul că, fără un motiv legitim, persoana titulară a unui acces la servicii de comunicații publice online:

1° Fie nu a implementat un mijloc de securizare a acestui acces;

2° Fie nu a exercitat diligența necesară în punerea în aplicare a acestui mijloc.

II.– Dispozițiile alineatului I sunt aplicabile numai atunci când sunt îndeplinite următoarele două condiții:

1° În temeiul articolului L. 331-25 și în formele prevăzute la acest articol, titularului accesului i s-a recomandat de către comisia pentru protecția drepturilor să pună în aplicare un mijloc de securizare a accesului său care să permită prevenirea repetării unei utilizări a acestuia în scopul reproducerii, al reprezentării sau al punerii la dispoziție sau al comunicării publice de opere sau de obiecte protejate de un drept de autor sau de un drept conex fără autorizarea titularilor drepturilor […] în cazul în care aceasta este necesară;

2° În anul următor aducerii la cunoștință a acestei recomandări, acest acces este din nou utilizat în scopurile menționate la punctul 1 al prezentului alineat II.”

20. Articolul L. 336-3 din acest cod prevede:

„Persoana titulară a accesului la servicii de comunicații publice online are obligația de a se asigura că acest acces nu face obiectul unei utilizări în scopul reproducerii, al reprezentării, al punerii la

[4] JORF din 7 martie 2010, textul nr. 19.

dispoziție sau al comunicării publice de opere sau de obiecte protejate de un drept de autor sau de un drept conex fără autorizarea titularilor […] atunci când aceasta este necesară.

Neîndeplinirea de către persoana titulară a accesului a obligației definite la primul paragraf nu are ca efect angajarea răspunderii penale a persoanei în cauză […]”

2. Decretul din 5 martie 2010

21. Decretul din 5 martie 2010, în versiunea aplicabilă situației de fapt din litigiul principal, prevede la articolul 1:

„Prelucrarea datelor cu caracter personal, denumită «Sistemul de gestionare a măsurilor pentru protecția operelor pe internet», are ca scop punerea în aplicare de către comisia pentru protecția drepturilor din cadrul [Hadopi]:

1° A măsurilor prevăzute în volumul III din partea legislativă din [CPI] (titlul III capitolul I secțiunea 3 subsecțiunea 3) și în volumul III din partea administrativă din același cod (titlul III capitolul I secțiunea 2 subsecțiunea 2);

2° A sesizărilor procurorului Republicii cu privire la fapte care pot constitui infracțiuni prevăzute la articolele L. 335-2, L. 335-3, L. 335-4 și R. 335-5 din același cod, precum și a informării organismelor de apărare a intereselor profesionale și a organismelor de gestiune colectivă cu privire la aceste sesizări;

[…]”

22. Articolul 4 din acest decret prevede:

„I.– Au acces direct la datele cu caracter personal și la informațiile menționate în anexa la prezentul decret angajații publici autorizați, împuterniciți de președintele [Hadopi] în temeiul articolului L. 331-21 din [CPI], și membrii comisiei pentru protecția drepturilor menționate la articolul 1.

II.– Operatorii de comunicații electronice și prestatorii de servicii menționați la punctul 2 din anexa la prezentul decret sunt destinatari:

– ai datelor tehnice necesare pentru identificarea abonatului;

– ai recomandărilor prevăzute la articolul L. 331-25 din [CPI] în vederea transmiterii pe cale electronică a acestora către abonații lor;

– ai elementelor necesare pentru punerea în aplicare a pedepselor complementare de suspendare a accesului la un serviciu de comunicații publice online aduse la cunoștința comisiei pentru protecția drepturilor de către procurorul Republicii.

III.– Organismele de apărare a intereselor profesionale și organismele de gestiune colectivă sunt destinatare ale unei informații referitoare la sesizarea procurorului Republicii.

IV.– Autoritățile judiciare sunt destinatare ale proceselor-verbale de constatare a faptelor care pot constitui infracțiuni prevăzute la articolele L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 și R. 335-5 din [CPI].

Cazierul judiciar automatizat este informat cu privire la executarea pedepsei de suspendare."

23. Anexa la Decretul din 5 martie 2010 prevede:

„Datele cu caracter personal și informațiile înregistrate în prelucrarea denumită «Sistemul de gestionare a măsurilor pentru protecția operelor pe internet» sunt următoarele:

1° Date cu caracter personal și informații provenite de la organismele de apărare a intereselor profesionale constituite periodic, de la organismele de gestiune colectivă, de la Centrul național al cinematografiei și al imaginii animate, precum și cele provenite de la procurorul Republicii:

În ceea ce privește faptele care pot constitui o neîndeplinire a obligației definite la articolul L. 336-3 din [CPI]:

Data și ora faptelor;

Adresa IP a abonaților în cauză;

Protocolul peer-to-peer utilizat;

Pseudonimul utilizat de abonat;

Informații referitoare la operele sau la obiectele protejate care fac obiectul faptelor;

Denumirea fișierului, astfel cum se regăsește pe calculatorul abonatului (dacă este cazul);

Furnizorul de acces la internet de la care a fost achiziționat accesul sau care a furnizat resursa tehnică IP.

[…]

2° Date cu caracter personal și informații referitoare la abonat colectate de la operatorii de comunicații electronice […] și de la prestatorii de servicii […]:

Numele de familie, prenumele;

Adresa poștală și adresele electronice;

Coordonatele telefonice;

Adresa postului telefonic al abonatului;

Furnizorul de acces la internet, care utilizează resursele tehnice ale furnizorului de acces menționat la punctul 1, cu care abonatul a încheiat contractul; numărul de dosar;

data de la care începe suspendarea accesului la un serviciu de comunicații publice online.

[…]”

3. Codul poștal și al comunicațiilor electronice

24. Articolul L. 34-1 din Codul poștal și al comunicațiilor electronice, astfel cum a fost modificat prin articolul 17 din Legea nr. 2021-998 din 30 iulie 2021 [5], prevede la alineatul II bis:

„[O]peratorii de comunicații electronice sunt obligați să păstreze:

1° În scopul desfășurării procedurilor penale, al prevenirii amenințărilor împotriva siguranței publice și al apărării securității naționale, informațiile referitoare la identitatea civilă a utilizatorului, până la împlinirea unui termen de cinci ani de la încetarea validității contractului său;

2° În aceleași scopuri precum cele enunțate la punctul 1 al prezentului alineat II bis, celelalte informații furnizate de utilizator la momentul încheierii unui contract sau al creării unui cont, precum și informațiile referitoare la plată până la împlinirea unui termen de un an de la încetarea validității contractului său sau de la închiderea contului său;

3° În scopul combaterii criminalității și infracționalității grave, al prevenirii amenințărilor grave împotriva siguranței publice și al apărării securității naționale, datele tehnice care permit identificarea sursei de conectare sau cele referitoare la echipamentele terminale utilizate, până la expirarea unui termen de un an de la conectare sau de la utilizarea echipamentelor terminale.”

III. Procedura în fața Curții

25. Ca răspuns la invitația adresată persoanelor interesate menționate la articolul 23 din Statutul Curții de Justiție a Uniunii Europene, reclamantele din litigiul principal, guvernele francez, danez, estonian, irlandez, neerlandez, finlandez, suedez, precum și Comisia Europeană au răspuns la întrebările scrise adresate de Curte.

26. Aceleași părți, cu excepția guvernului finlandez, guvernele ceh, spaniol, cipriot, leton și norvegian, precum și AEPD și ENISA au participat la ședința care a avut loc la 15 mai 2023.

[5] JORF din 31 iulie 2021, textul nr. 1. Această versiune a articolului L. 34-1 din codul menționat, în vigoare de la data de 31 iulie 2021, a fost adoptată în urma Deciziei nr. 393099 a Conseil d'État (Consiliul de Stat, Franța) din 21 aprilie 2021 (JORF din 25 aprilie 2021), care a înlăturat versiunea precedentă a acestei dispoziții ce includea o obligație de păstrare a datelor cu caracter personal „în vederea investigării, constatării și urmăririi penale a infracțiunilor sau a unei încălcări a obligației definite la articolul L. 336-3 [din CPI]” numai pentru a permite, atât cât era necesar, punerea la dispoziția printre altele a Hadopi. Prin Decizia nr. 2021-976-977 QPC din 25 februarie 2022 (domnul Habib A. și alții), Conseil constitutionnel (Consiliul Constituțional, Franța) a declarat neconstituțională această versiune anterioară a articolului L. 34-1 din codul menționat pentru motivul esențial că, „prin autorizarea păstrării generale și nediferențiate a datelor de conectare, dispozițiile contestate aduc o atingere disproporționată dreptului la respectarea vieții private” (punctul 13). Astfel, această instanță a considerat că datele de conectare care trebuie păstrate în temeiul acestor dispoziții privesc nu doar identificarea utilizatorilor serviciilor de comunicații electronice, ci și alte date care, „ținând seama de natura lor, de diversitatea lor și de prelucrările la care pot fi supuse […] furnizează cu privire la acești utilizatori și, dacă este cazul, cu privire la terți numeroase informații precise care aduc atingere în mod special vieții lor private” (punctul 11).

IV. Analiză

27. Analiza noastră cu privire la întrebările preliminare din primele noastre concluzii ne-a determinat să propunem Curții să statueze că articolul 15 alineatul (1) din Directiva 2002/58 trebuie interpretat în sensul că nu se opune unei reglementări naționale ce permite păstrarea de către furnizorii de servicii de comunicații electronice și accesul unei autorități administrative precum Hadopi[6] limitate la date de identitate civilă corespunzătoare unor adrese IP pentru ca respectiva autoritate să poată identifica titularii acestor adrese suspectați a fi responsabili de încălcări ale dreptului de autor și ale drepturilor conexe și să poată lua, dacă este cazul, măsuri împotriva lor, fără ca acest acces să fie condiționat de un control prealabil din partea unei instanțe sau a unei entități administrative independente, atunci când aceste date constituie singurul mijloc de investigare ce permite identificarea persoanei căreia îi era atribuită această adresă la momentul săvârșirii infracțiunii.

28. În prezentele concluzii, vom încerca să aprofundăm anumite elemente din analiza noastră anterioară și punctele dezbătute în ședința care a avut loc la 15 mai 2023, pentru a expune motivele pentru care menținem atât propunerea noastră de răspuns la întrebările preliminare, cât și raționamentul care a condus la aceasta[7].

29. Mai precis, vom demonstra că faptul de a permite păstrarea și accesul la date de identitate civilă corespunzătoare unor adrese IP, fără un control prealabil, pentru a identifica autorii unei infracțiuni atunci când aceste date constituie singurul mijloc de identificare a acestora întrunește cerințele stabilite de Curte în ceea ce privește examinarea măsurilor adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58 (secțiunea B).

30. Astfel, vom evidenția faptul că o asemenea soluție nu constituie un reviriment al jurisprudenței dezvoltate de Curte începând cu Hotărârile Tele2 Sverige și Watson și alții[8] și La Quadrature du Net și alții[9], care impune respectarea și protejarea drepturilor fundamentale, ci o dezvoltare necesară a acesteia care, în opinia noastră, reprezintă o extensie a principiilor stabilite de Curte. Această distincție nu este doar semantică. Astfel, soluția pe care o propunem nu urmărește să repună în discuție jurisprudența existentă, ci să permită, în numele unui anumit pragmatism, adaptarea sa în împrejurări speciale și foarte limitate (secțiunea C).

31. Din motive de claritate și în măsura în care dezbaterile din ședință au demonstrat necesitatea unor precizări în această privință, vom începe analiza noastră printr-o reamintire a modului de funcționare a mecanismului de răspuns gradual operat de Hadopi (secțiunea A).

6 La 1 ianuarie 2022, Consiliul Superior al Audiovizualului (CSA) și Hadopi au devenit Autoritatea de reglementare a comunicațiilor audiovizuale și digitale (Arcom). Ținând seama de perioada în care s-au desfășurat faptele din litigiul principal, ne vom referi totuși, în prezentele concluzii, la Hadopi.

7 În această privință, menținem și propunerea noastră de reformulare a întrebărilor preliminare, precum și modul în care înțelegem obiectul lor. Astfel, deși, în textul întrebărilor preliminare, se menționează numai accesul la datele de identitate civilă corespunzătoare unor adrese IP, problema accesului la aceste date este totuși indisociabilă de cea a păstrării lor de către furnizorii de servicii de comunicații electronice, astfel încât analiza compatibilității cu dreptul Uniunii a păstrării datelor este o condiție prealabilă necesară pentru cea a compatibilității accesului. Cu privire la acest aspect, a se vedea punctul 45 și următoarele din primele noastre concluzii. De asemenea, deși întrebările preliminare vizează „datele de identitate civilă corespunzătoare unei adrese IP”, acestea trebuie înțelese în sensul că vizează și accesul la adresele IP care permit identificarea sursei unei conexiuni. Cu privire la acest aspect, a se vedea punctul 41 și următoarele din primele noastre concluzii.

8 Hotărârea din 21 decembrie 2016 (C-203/15 și C-698/15, denumită în continuare „Hotărârea Tele2”, EU:C:2016:970).

9 Hotărârea din 6 octombrie 2020 (C-511/18, C-512/18 și C-520/18, denumită în continuare „Hotărârea La Quadrature du Net și alții”, EU:C:2020:791).

A. Mecanismul de răspuns gradual operat de Hadopi

32. Hadopi este o autoritate administrativă independentă responsabilă de protecția dreptului de autor și a drepturilor conexe împotriva încălcărilor acestor drepturi săvârșite pe internet. În acest scop, a fost instituit așa-numitul mecanism de „răspuns gradual”, a cărui punere în aplicare este încredințată comisiei pentru protecția drepturilor din cadrul Hadopi.

33. Această comisie este sesizată de organisme ale titularilor de drepturi, în cadrul cărora anumiți agenți autorizați și acreditați de ministrul culturii colectează, pe rețelele peer-to-peer, adresele IP ale utilizatorilor de internet care pun la dispoziția publicului opere fără autorizarea titularilor lor. Se întocmesc atunci procese-verbale. Acestea conțin printre altele adresa IP a accesului la internet utilizat pentru săvârșirea acestor încălcări ale dreptului de autor, data și ora încălcării constatate, precum și titlul operei în discuție și sunt transmise comisiei pentru protecția drepturilor din cadrul Hadopi. Trebuie subliniat în această privință și astfel cum a arătat AEPD că prelucrarea datelor cu caracter personal de către agenți în cadrul organismelor titularilor de drepturi face obiectul unei autorizări din partea Commission nationale de l'informatique et des libertés (Comisia Națională pentru Informatică și Libertăți) (CNIL), autoritatea franceză de supraveghere în materie de protecție a datelor [10].

34. La primirea proceselor-verbale și după un control automatizat pentru a se asigura că acestea conțin toate datele necesare, comisia pentru protecția drepturilor din cadrul Hadopi poate obține de la furnizorii de servicii de comunicații electronice identitatea, adresa poștală, adresa electronică și datele de contact telefonic ale titularului abonamentului utilizat pentru săvârșirea unei încălcări a dreptului de autor.

35. Hadopi poate atunci să adreseze acestei persoane o „recomandare” prin care este informată cu privire la faptul că accesul său la internet a făcut obiectul unei utilizări contrare dreptului de autor și care constă în obligarea persoanei suspectate de neîndeplinirea obligației de vigilență în ceea ce privește respectarea pe internet a operelor protejate de dreptul de autor sau de un drept conex să se conformeze acesteia. Cu alte cuvinte, recomandarea este adresată titularului accesului la internet, care poate fi, în realitate, o persoană diferită de cea care a pus la dispoziție opera cu încălcarea dreptului de autor. O a doua recomandare poate fi emisă în cazul unei a doua constatări a contrafacerii prin intermediul aceluiași acces la internet. În cazul unor repetări, comisia pentru protecția drepturilor din cadrul Hadopi poate decide să sesizeze procurorul Republicii în vederea începerii urmăririi penale. În această privință, astfel cum a precizat guvernul francez în primele sale observații, agenții Hadopi însărcinați cu mecanismul de răspuns gradual sunt agenți autorizați și împuterniciți de președintele Hadopi, supuși secretului profesional și singurii din cadrul Hadopi care sunt autorizați să aibă acces la datele personale prelucrate potrivit acestui mecanism.

36. Trebuie să precizăm, în această privință, că nu sunt colectate și transmise către Hadopi datele tuturor utilizatorilor rețelelor peer-to-peer atunci când aceștia din urmă se limitează să descarce astfel de conținuturi [11], ci numai cele ale persoanelor care au pus la dispoziție conținuturi contrafăcute, cu alte cuvinte care au *încărcat* astfel de conținuturi.

[10] A se vedea în această privință deliberarea nr. 2010-225 a CNIL din 10 iunie 2010, prin care se modifică autorizația pentru efectuarea unei prelucrări de date cu caracter personal de către Société des auteurs, compositeurs et éditeurs de muzique (Societatea autorilor, compozitorilor și editorilor de muzică) (SACEM), având ca scop identificarea și constatarea infracțiunilor de contrafacere săvârșite prin rețelele de schimb de fișiere denumite „peer-to-peer” (autorizația nr. 1425421).

[11] Cu privire la funcționarea rețelelor peer-to-peer și la diferitele profiluri de utilizatori de internet pe aceste rețele, a se vedea Concluziile noastre prezentate în cauza M.I.C.M. (C-597/19, EU:C:2020:1063, punctul 37 și urm.).

37. Astfel, cu titlu ilustrativ, pentru anul 2021, Hadopi a primit din partea organismelor titularilor de drepturi aproape patru milioane de procese-verbale, a trimis 210 595 de prime recomandări și 53 564 de ultime recomandări și a sesizat procurorul Republicii în 1 484 de cazuri.

38. Odată făcute aceste mențiuni, vom demonstra de ce un astfel de mecanism, care presupune păstrarea și accesul la date de identitate civilă corespunzătoare unor adrese IP, îndeplinește, în opinia noastră, cerințele jurisprudenței referitoare la măsurile naționale adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58.

B. Respectarea cerințelor rezultate din jurisprudența Curții referitoare la interpretarea articolului 15 alineatul (1) din Directiva 2002/58

39. Întrucât am amintit deja, în primele noastre concluzii, jurisprudența Curții referitoare la păstrarea adreselor IP atribuite sursei unei conexiuni și la accesul la ele [12], ne vom concentra în prezentele concluzii asupra a ceea ce constituie, în opinia noastră, esența acestei jurisprudențe, și anume, pe de o parte, cerința proporționalității și, pe de altă parte, în ceea ce privește accesul la aceste date, eventuala necesitate a unui control prealabil din partea unei instanțe sau a unei autorități administrative independente.

1. Cu privire la proporționalitatea măsurii în cauză

40. Pentru a stabili compatibilitatea cu dreptul Uniunii a unei măsuri de păstrare sau de acces la date de identitate civilă corespunzătoare unei adrese IP, trebuie, astfel cum subliniază Curtea în mod repetat, să se realizeze o conciliere a diverselor interese legitime și drepturi în cauză, care sunt, pe de o parte, drepturile la protecția vieții private, precum și la protecția datelor personale [13] garantate la articolele 7 și 8 din cartă și, pe de altă parte, protecția drepturilor și libertăților celorlalți și a drepturilor consacrate la articolele 3, 4, 6 și 7 din cartă [14]. Vom adăuga că, în prezenta cauză, drepturile la protecția vieții private și la protecția datelor personale trebuie să fie de asemenea conciliate cu dreptul de proprietate consacrat la articolul 17 din cartă, întrucât mecanismul de răspuns gradual vizează în cele din urmă protecția drepturilor de autor și a drepturilor conexe.

41. Curtea precizează în această privință că această conciliere efectuată în temeiul articolului 15 alineatul (1) din Directiva 2002/58 permite statelor membre să adopte o măsură derogatorie de la principiul confidențialității în cazul în care o asemenea măsură este „*necesară, corespunzătoare și proporțională* în cadrul unei societăți democratice” (sublinierea noastră). Considerentul (11) al acestei directive precizează că o măsură de această natură trebuie să fie „strict” *proporțională* cu scopul urmărit [15].

[12] Punctul 53 și următoarele din primele noastre concluzii.

[13] Drepturile la protecția vieții private și la protecția datelor personale se concretizează, în Directiva 2002/58, în principiile confidențialității comunicațiilor și interzicerii stocării datelor aferente pe care aceasta le prevede.

[14] Hotărârea La Quadrature du Net și alții (punctele 120-122, precum și 127 și 128), Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, denumită în continuare „Hotărârea Commissioner of An Garda Síochána și alții”, EU:C:2022:258, punctele 48 și 50), precum și Hotărârea din 20 septembrie 2022, SpaceNet și Telekom Deutschland (C-793/19 și C-794/19, denumită în continuare „Hotărârea SpaceNet și Telekom Deutschland”, EU:C:2022:702, punctele 63 și 65).

[15] Hotărârile La Quadrature du Net și alții (punctul 129), Commissioner of An Garda Síochána și alții (punctul 51) și SpaceNet și Telekom Deutschland și alții (punctul 66).

42. Pe de altă parte, Curtea se referă la principiul proporționalității pe tot parcursul raționamentului său referitor la interpretarea articolului 15 alineatul (1) din Directiva 2002/58 și, prin urmare, face din acesta cheia de boltă a examinării unei măsuri naționale de păstrare sau de acces la date personale, adoptată în temeiul acestei dispoziții.

43. O lectură mai aprofundată a acestui raționament arată că principiul proporționalității acoperă, în contextul articolului 15 alineatul (1) din Directiva 2002/58, diferite aspecte legate, pe de o parte, de gravitatea ingerinței în drepturile fundamentale pe care o implică păstrarea sau accesul la datele de transfer și, pe de altă parte, de necesitatea măsurii în cauză.

44. În ceea ce privește păstrarea și accesul la datele de identitate civilă corespunzătoare unor adrese IP de către Hadopi, considerăm că atât gravitatea ingerinței, cât și caracterul indispensabil al acestor date ar trebui să determine Curtea să își adapteze analiza privind proporționalitatea unei măsuri naționale adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58.

a) Gravitatea relativă a ingerinței în drepturile fundamentale

45. Rezultă în mod clar din jurisprudența constantă a Curții că, în conformitate cu principiul proporționalității, importanța obiectivului urmărit de o măsură adoptată în temeiul articolului 15 alineatul (1) din Directiva 2002/58 trebuie să se raporteze la gravitatea ingerinței care rezultă din aceasta [16].

46. Mai precis, Curtea a statuat, astfel cum am subliniat în primele noastre concluzii, că o ingerință gravă nu se poate justifica, în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, decât prin obiectivul privind combaterea infracționalității care trebuie calificată drept „gravă” [17].

47. În ceea ce privește adresele IP, Curtea arată că, deși acestea prezintă un grad de sensibilitate mai redus decât celelalte date de transfer, păstrarea și analizarea lor constituie totuși ingerințe grave în drepturile fundamentale din moment ce ele pot fi utilizate pentru a se realiza o reconstituire exhaustivă a parcursului de navigare al unui utilizator de internet și, prin urmare, pentru a se stabili profilul detaliat al acestuia din urmă și pentru a se desprinde concluzii precise asupra vieții sale private [18].

48. În cauza principală, păstrarea și accesul la date de identitate civilă corespunzătoare unor adrese IP vizează combaterea încălcărilor dreptului de autor și ale drepturilor conexe. Or, este clar, în opinia noastră, că această combatere nu se poate încadra în combaterea infracționalității grave [19], chiar dacă volumul acestor încălcări ar avea un caracter masiv. Prin urmare, ar exista un decalaj între gravitatea ingerinței în drepturile fundamentale pe care o implică măsura în cauză și obiectivul pe care aceasta îl urmărește.

[16] Hotărârile Commissioner of An Garda Síochána și alții (punctul 56) și SpaceNet și Telekom Deutschland (punctul 71).

[17] Hotărârea Tele2 (punctul 115), Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punctul 56), și Hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice) (C-746/18, denumită în continuare „Hotărârea Prokuratuur”, EU:C:2021:152, punctul 33). A se vedea de asemenea punctul 92 din primele noastre concluzii.

[18] A se vedea Hotărârile La Quadrature du Net și alții (punctele 152 și 153), Commissioner of An Garda Síochána și alții (punctul 73) și SpaceNet și Telekom Deutschland (punctul 103). A se vedea de asemenea punctele 63, 64 și 93 din primele noastre concluzii.

[19] Am susținut, în primele noastre concluzii, că noțiunea de „infracționalitate gravă” ar trebui să primească o interpretare autonomă pentru a împiedica orice eludare de către statele membre a cerințelor prevăzute la articolul 15 alineatul (1) din Directiva 2002/58. Ne menținem această poziție. Cu toate acestea, trebuie să subliniem că, chiar dacă Curtea ar statua că definiția noțiunii de „infracționalitate gravă” este lăsată la latitudinea statelor membre, aceasta ar trebui, în orice caz, să fie stabilită în limitele dreptului Uniunii și nu ar putea fi extinsă până la a goli de conținut această dispoziție.

49. În primele noastre concluzii, am apreciat, în conformitate cu jurisprudența Curții, că accesul Hadopi la datele de identitate civilă corespunzătoare unei adrese IP constituie o ingerință gravă în drepturile fundamentale. Deși am considerat de asemenea că păstrarea și accesul la aceste date trebuiau totuși să fie permise în speță, în urma ședinței, suntem nevoiți să aducem câteva precizări suplimentare.

50. Mecanismul de răspuns gradual permite Hadopi să coreleze adresa IP, comunicată de organizațiile titularilor de drepturi, a persoanelor suspectate că ar fi utilizat accesul lor la internet pentru a săvârși o încălcare a dreptului de autor pe o rețea peer-to-peer, precum și un extras din fișierul încărcat fără respectarea dreptului de autor cu identitatea civilă a acestei persoane. După cum au arătat Comisia și AEPD în ședință, asemenea elemente, deși permit să se obțină cu siguranță mai multe informații decât simpla identitate a autorului prezumat al unei încălcări, nu conduc totuși la desprinderea unor concluzii foarte precise asupra vieții private a acestei persoane. Astfel, după cum am menționat în primele noastre concluzii[20], este vorba numai despre dezvăluirea unei consultări punctuale a unui conținut care, luat în considerare în mod izolat, nu poate permite stabilirea profilului detaliat al persoanei care a efectuat această consultare.

51. Acest lucru este valabil cu atât mai mult cu cât, mai întâi, marea majoritate a adreselor IP comunicate Hadopi sunt adrese IP denumite „dinamice”, care, prin natura lor, sunt schimbătoare și nu corespund unei identități precise decât într-un singur moment care coincide cu punerea la dispoziție a conținutului în cauză. Prin urmare, acestea exclud orice reconstituire exhaustivă.

52. În continuare, trebuie să subliniem că, în opinia noastră, protecția drepturilor fundamentale pe internet nu poate justifica imposibilitatea unui acces la simplele datele referitoare la adresa IP, la conținutul unei opere și la identitatea persoanei care a procedat la punerea la dispoziție a acesteia cu încălcarea drepturilor de autor, ci doar faptul că păstrarea și accesul la acestea din urmă trebuie să fie însoțite de garanții. În această privință, considerăm că o analogie cu lumea reală este elocventă: o persoană suspectată că ar fi săvârșit un furt nu poate invoca dreptul său la protecția vieții private pentru ca persoanele însărcinate cu urmărirea penală a acestei infracțiuni să nu poată lua cunoștință de conținutul furat. În schimb, această persoană poate în mod întemeiat să invoce drepturile sale fundamentale pentru a împiedica accesul, în cursul procedurii, la un ansamblu de date mai largi decât simplele date necesare pentru calificarea pretinsei infracțiuni.

53. În sfârșit, arătăm că, contrar celor susținute de reclamanți, mecanismul de răspuns gradual nu pare să presupună o supraveghere generalizată a utilizatorilor rețelelor peer-to-peer. Astfel, nu este vorba despre verificarea ansamblului activității lor pe o anumită rețea pentru a stabili dacă au pus la dispoziție o operă cu încălcarea dreptului de autor, ci mai degrabă despre determinarea, pornind de la un fișier identificat ca fiind o contrafacere, a persoanei care deține accesul la [adresa de] internet de la care utilizatorul de internet a efectuat punerea la dispoziție. De asemenea, astfel cum a subliniat AEPD în ședință, nu este vorba despre supravegherea activității tuturor utilizatorilor rețelelor peer-to-peer, ci numai a activității persoanelor care încărcă fișiere contrafăcute, încărcarea acestor fișiere dezvăluind cu atât mai puțin elemente referitoare la viața privată a persoanei cu cât se poate efectua numai pentru a permite acestor utilizatori de internet să descarce ulterior alte fișiere.

[20] Punctul 101 din primele noastre concluzii.

54. În aceste condiții, apreciem că motivele care au determinat Curtea să considere că păstrarea și accesul la adresele IP constituie o ingerință gravă în drepturile fundamentale nu se aplică în ceea ce privește un mecanism de răspuns gradual precum cel operat de Hadopi. Rezultă că gravitatea ingerinței pe care o implică această păstrare și acest acces ar trebui nuanțată în momentul examinării principiului proporționalității.

55. Cu alte cuvinte, considerăm că jurisprudența Curții referitoare la gravitatea ingerinței în drepturile fundamentale cauzată de păstrarea și de accesul la adresele IP nu trebuie interpretată în sensul că această ingerință este întotdeauna una gravă, ci în sensul că există o ingerință gravă numai atunci când adresele IP pot conduce la o reconstituire exhaustivă a parcursului de navigare al unui utilizator de internet și la desprinderea unor concluzii foarte precise asupra vieții sale private.

56. Întrucât acest lucru nu este valabil într-o situație precum cea în discuție în litigiul principal, rezultă că ingerința pe care le implică păstrarea și accesul la datele de identitate civilă corespunzătoare unei adrese IP utilizate pentru punerea la dispoziție a unui conținut cu încălcarea dreptului de autor ar trebui să poată fi justificată de un obiectiv de combatere a infracționalității în sens mai larg decât simpla infracționalitate gravă.

57. Precizăm în plus că ingerința în drepturile fundamentale pe care o implică păstrarea și accesul la date de identitate civilă corespunzătoare unei adrese IP într-o situație precum cea în discuție în litigiul principal nu este agravată de împrejurarea că titularul accesului la [adresa de] internet utilizată pentru punerea la dispoziție a unui conținut contrafăcut nu se află în mod necesar la originea acestei puneri la dispoziție, astfel încât recomandarea adresată de Hadopi ar putea conduce la dezvăluirea către acest titular a conținutului menționat la care a putut avea acces un terț. Pe de o parte, amintim că încălcarea investigată de Hadopi este cea privind neîndeplinirea obligației de a se asigura că accesul nu face obiectul unei utilizări în scopul punerii la dispoziție a unui conținut cu încălcarea dreptului de autor. Prin urmare, este necesar ca informațiile care permit calificarea sa să fie transmise autorului prezumat al acesteia. Pe de altă parte, astfel cum am menționat deja, considerăm că informațiile referitoare la opera în discuție nu permit să se desprindă concluzii precise asupra vieții private a persoanei aflate la originea punerii la dispoziție. Prin urmare, eventuala transmitere a acestor informații titularului conexiunii internet nu depășește ceea ce este necesar pentru a permite urmărirea încălcării dreptului de autor în discuție.

b) Caracterul indispensabil al datelor în cauză pentru detectarea și urmărirea penală a unei infracțiuni

58. Pentru a asigura faptul că o măsură de păstrare și de acces la date de transfer, cum sunt datele de identitate civilă corespunzătoare unei adrese IP adoptate în temeiul articolului 15 alineatul (1) din Directiva 2002/58, este una proporțională, este necesar, potrivit jurisprudenței Curții, ca ingerința pe care o implică să fie limitată la strictul necesar pentru a permite realizarea obiectivului urmărit[21]. Considerăm că tocmai aceasta este situația în ceea ce privește măsura în discuție în litigiul principal.

[21] Hotărârile La Quadrature du Net și alții (punctele 120-122 și 132), Commissioner of An Garda Síochána și alții (punctele 48 și 54), precum și SpaceNet și Telekom Deutschland (punctele 63 și 69).

59. Astfel cum am subliniat în primele noastre concluzii [22], din însăși jurisprudența Curții reiese că, în cazul unei infracțiuni săvârșite exclusiv online, precum o încălcare a dreptului de autor pe o rețea peer-to-peer, adresa IP poate constitui singurul mijloc de investigare care permite identificarea persoanei căreia îi era atribuită această adresă la momentul săvârșirii infracțiunii [23]. Rezultă, în opinia noastră, că păstrarea și accesul la datele de identitate civilă corespunzătoare unor adrese IP în scopul detectării și al urmăririi încălcărilor dreptului de autor săvârșite online sunt, în conformitate cu jurisprudența, strict necesare pentru realizarea obiectivului urmărit.

60. Este adevărat că orice cerință privind protecția datelor personale presupune o limitare a competențelor de investigare. Acest lucru rezultă din însuși principiul concilierii intereselor contrare, iar un asemenea rezultat nu poate fi contestat ca atare. Totuși, în ipoteza în care adresa IP constituie singurul mijloc de identificare a persoanei suspectate că ar fi săvârșit online o încălcare a unui drept de proprietate intelectuală, o astfel de situație se distinge de majoritatea urmăririlor penale cu privire la care Curtea arată că „eficacitatea […] nu depinde în general de un singur instrument de investigație, ci de toate instrumentele de investigație de care dispun autoritățile naționale competente în acest scop” [24]. A admite că datele de identitate civilă corespunzătoare unor adrese IP nu ar trebui să facă obiectul unei păstrări și al unui acces într-o situație precum cea în discuție în litigiul principal nu ar determina, la fel ca orice măsură care asigură protecția datelor de transfer, o simplă limitare a competențelor de investigare, ci privarea autorităților naționale de singurul mijloc de detectare și de urmărire penală a anumitor infracțiuni.

61. Cu alte cuvinte, nu este vorba, potrivit interpretării pe care o propunem cu privire la articolul 15 alineatul (1) din Directiva 2002/58, despre a permite, prin examinarea necesității unei astfel de măsuri, păstrarea și accesul la date care doar *facilitează* detectarea și urmărirea penală a infracțiunilor, atunci când aceste infracțiuni pot fi detectate și urmărite penal și prin mijloace concurente, fie ele chiar mai puțin eficiente. În schimb, este vorba despre a permite păstrarea și accesul la datele menționate atunci când acestea sunt *indispensabile* pentru identificarea persoanei suspectate că ar fi săvârșit o infracțiune, care nu ar putea fi urmărită penal fără aceste mijloace din moment ce datele în cauză constituie unicul instrument de identificare a utilizatorului de internet întrucât infracțiunea este săvârșită exclusiv online.

62. O astfel de interpretare se impune, în opinia noastră, cu excepția situației în care se admite că o serie întreagă de infracțiuni nu poate face niciodată obiectul urmăririi penale [25].

63. Rezultă din tot ceea ce precedă că, în opinia noastră, o reglementare națională ce permite păstrarea de către furnizorii de servicii de comunicații electronice și accesul unei autorități administrative, limitate la date de identitate civilă corespunzătoare unor adrese IP, este pe deplin proporțională cu obiectivul urmărit, și anume urmărirea încălcărilor dreptului de autor și ale drepturilor conexe pe internet, întrucât ingerința în drepturile fundamentale pe care o implică este de o gravitate limitată, iar aceste date constituie singurul mijloc de investigare ce permite identificarea persoanei căreia îi era atribuită această adresă la momentul săvârșirii infracțiunii.

[22] Punctul 78 din primele noastre concluzii.

[23] Hotărârile La Quadrature du Net și alții (punctul 154), Commissioner of An Garda Síochána și alții (punctul 73) și SpaceNet și Telekom Deutschland (punctul 100),.

[24] Hotărârea Commissioner of An Garda Síochána și alții (punctul 69).

[25] Punctul 81 din primele noastre concluzii. A se vedea de asemenea, cu privire la acest aspect, punctul 79 și următoarele din prezentele concluzii.

64. Prin urmare, considerăm că articolul 15 alineatul (1) din Directiva 2002/58 ar trebui interpretat în sensul că nu se opune unei astfel de reglementări.

2. Cu privire la existența unor garanții materiale și procedurale adecvate

65. În ceea ce privește în mod specific accesul la date de identitate civilă corespunzătoare unor adrese IP, reiese din jurisprudența Curții că doar caracterul strict proporțional al măsurii nu este suficient pentru ca aceasta să devină compatibilă cu articolul 15 alineatul (1) din Directiva 2002/58.

66. Astfel, pentru a se asigura că accesul la datele de transfer și de localizare este limitat la strictul necesar, Curtea a statuat că este esențial ca acest acces să fie condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă care dispune de toate atribuțiile și care prezintă toate garanțiile necesare în vederea asigurării unei concilieri a diferitelor interese legitime și drepturi în cauză [26].

67. O interpretare strictă a jurisprudenței ar conduce, prin urmare, la aprecierea că accesul Hadopi la datele de identitate civilă corespunzătoare adreselor IP ale persoanelor suspectate că ar fi săvârșit o încălcare a dreptului de autor pe internet ar trebui să fie condiționat de un asemenea control prealabil care lipsește în cazul mecanismului de răspuns gradual, în forma sa actuală.

68. Cu toate acestea, astfel cum a arătat guvernul irlandez în ședință și cum am susținut în primele noastre concluzii, considerăm că cerința privind un control prealabil din partea unei instanțe sau a unei entități administrative independente nu este o cerință sistematică, ci depinde de o analiză mai globală a măsurii în cauză care ia în considerare atât gravitatea ingerinței pe care o implică, cât și garanțiile pe care le prevede.

69. Astfel, subliniem că, în fiecare dintre hotărârile în care s-a enunțat această cerință privind un control prealabil din partea unei instanțe sau a unei entități administrative independente, erau în discuție reglementări naționale ce permiteau accesul la ansamblul datelor de transfer și de localizare ale utilizatorilor care au legătură cu toate mijloacele de comunicații electronice ale utilizatorilor [27] sau, cel puțin, cu telefonia fixă și mobilă [28] a utilizatorilor identificați.

70. Deducem de aici că cerința privind un astfel de control prealabil este ghidată de gravitatea ingerinței în discuție în cauzele respective. Astfel cum a subliniat Curtea, era vorba despre date „efectiv susceptibil[e] să permită deducerea unor concluzii precise, chiar foarte precise, privind viața privată a persoanelor […] precum obiceiurile din viața cotidiană, locurile de ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele” [29]. În plus, erau vizate datele unor persoane deja identificate și suspectate că ar fi săvârșit o infracțiune pe baza altor indicii, datele în cauză permițând, prin urmare, consolidarea elementelor incriminatoare împotriva utilizatorului în discuție prin extinderea sferei datelor care îl privesc.

[26] Hotărârile Tele2 (punctul 120), Prokuratuur (punctele 51 și 52), precum și Commissioner of An Garda Síochána și alții (punctele 106 și 107).

[27] Hotărârile Tele2 și Commissioner of An Garda Síochána și alții.

[28] Hotărârea Prokuratuur.

[29] Hotărârea Prokuratuur (punctul 36).

71. Or, în ceea ce privește reglementarea în discuție în litigiul principal și astfel cum am subliniat, gravitatea ingerinței pe care o presupune corelarea unei date de identitate civilă și cu o adresă IP este mult mai redusă decât cea care rezultă din accesul la ansamblul datelor de transfer și de localizare ale unei persoane, întrucât această corelare nu aduce vreun element din care să se poată trage concluzii precise privind viața privată a persoanei vizate.

72. În plus, astfel cum am arătat în primele noastre concluzii [30], aceste date nu privesc decât persoanele care, în urma unei constatări obiective privind utilizarea adresei IP cu încălcarea unui drept de autor stabilite de organismele titularilor de drepturi, au săvârșit fapte de natură să constituie o neîndeplinire a obligației de vigilență prevăzute la articolul L. 336-3 din CPI. Acestea nu sunt identificate în prealabil prin alte mijloace, corelarea adresei IP cu datele de identitate civilă fiind singurul mijloc de identificare a persoanei în cauză. Prin urmare, accesul la aceste date nu permite, astfel cum se întâmpla în cauzele în care Curtea s-a pronunțat anterior, obținerea de informații suplimentare și precise cu privire la activitatea unor persoane deja suspectate pe baza altor elemente, ci doar să devină utilizabilă adresa IP, care altfel nu ar prezenta vreun interes. În aceste condiții, datele la care Hadopi are acces sunt *de facto* limitate.

73. În opinia noastră, există o diferență fundamentală între faptul de a avea acces la date cu caracter personal referitoare la o persoană suspectată că ar fi săvârșit o infracțiune pentru a-i demonstra vinovăția și faptul de a permite dezvăluirea identității autorului unei infracțiuni deja constatate.

74. În opinia noastră, acest lucru este valabil cu atât mai mult cu cât colectarea adreselor IP pe rețelele peer-to-peer face obiectul unei autorizări prealabile limitate numai la aceste date, astfel încât Hadopi nu este niciodată în posesia unui ansamblu nelimitat de date în ceea ce privește utilizatorii de internet suspectați că ar fi săvârșit o încălcare a dreptului de autor pe internet [31].

75. Prin urmare, logica ce stă la baza cerinței privind un control prealabil efectuat de o instanță sau de o entitate administrativă independentă nu se aplică în ceea ce privește mecanismul de răspuns gradual precum cel în discuție în litigiul principal, astfel încât considerăm că o asemenea cerință nu este necesară pentru a se asigura că ingerința în drepturile fundamentale pe care o implică acest mecanism este limitată la strictul necesar.

76. Din tot ceea ce precedă rezultă că o reglementare națională ce permite păstrarea și accesul unei autorități administrative independente precum Hadopi la date de identitate civilă corespunzătoare unor adrese IP pentru a identifica titularii acestor adrese suspectați a fi responsabili de încălcări ale dreptului de autor, fără ca acest acces să fie condiționat de un control prealabil din partea unei instanțe sau a unei entități administrative independente, respectă în cele din urmă principiile stabilite de jurisprudența Curții, atunci când aceste date constituie singurul mijloc de identificare a persoanei căreia îi era atribuită adresa IP la momentul săvârșirii infracțiunii, astfel încât articolul 15 alineatul (1) din Directiva 2002/58 ar trebui interpretat în sensul că nu se opune unei asemenea reglementări.

77. Dincolo de aceste considerații specifice cauzei care face obiectul litigiului principal, trebuie să formulăm și considerații mai generale cu privire la necesitatea de a dezvolta jurisprudența Curții.

[30] Punctul 102 din primele noastre concluzii.

[31] Punctul 33 din prezentele concluzii.

C. O dezvoltare necesară și limitată a jurisprudenței

78. Există mai multe argumente care militează pentru o clarificare a jurisprudenței Curții referitoare la păstrarea și la accesul la date precum adresele IP corelate cu date de identitate civilă.

79. În primul rând și astfel cum am subliniat deja [32], în situația în discuție în litigiul principal, obținerea datelor de identitate civilă corespunzătoare unei adrese IP este singurul mijloc de investigare ce permite identificarea persoanei căreia îi era atribuită această adresă la momentul săvârșirii infracțiunii în discuție.

80. Rezultă în mod necesar că, în cazul în care Curtea ar considera că articolul 15 alineatul (1) din Directiva 2002/58 se opune totuși păstrării și accesului la acestea, autoritățile naționale ar fi private *de facto* de acest unic mijloc de identificare și, prin urmare, autorii infracțiunii în discuție nu ar putea fi niciodată urmăriți penal [33]. Acest lucru ne-a determinat, în primele noastre concluzii, să evocăm posibilitatea unei impunități sistemice pentru această infracțiune [34].

81. Riscul unei impunități sistemice nu se limitează la încălcările dreptului de autor săvârșite pe rețelele peer-to-peer, ci se extinde, astfel cum a arătat guvernul ceh în ședință, la toate infracțiunile săvârșite exclusiv online.

82. Astfel, infracțiunile al căror autor poate fi identificat numai prin intermediul adresei sale IP nu ar putea fi niciodată urmărite penal, iar textele care le sancționează nu ar putea fi niciodată aplicate dacă s-ar considera că atât păstrarea datelor, cât și accesul la acestea sunt contrare dreptului Uniunii.

83. În această privință, menționăm că este adevărat, astfel cum au susținut reclamantele din litigiul principal, că alte mijloace ar putea permite, teoretic, identificarea autorilor anumitor infracțiuni săvârșite exclusiv online. Astfel, acestea se referă în special la identificatorul utilizat pe rețelele sociale și la datele asociate contului utilizatorului, adresa sa de e-mail, numărul său de telefon sau un element privind viața sa privată pe care persoana le-ar fi dezvăluit. Cu toate acestea, astfel de date necesită, pentru a le corela cu identitatea persoanei, investigații aprofundate în cursul cărora este examinată activitatea online a utilizatorului de internet. Prin urmare, considerăm că recurgerea la asemenea mijloace de investigare este susceptibilă să permită, spre deosebire de simpla adresă IP, desprinderea unor concluzii foarte precise asupra vieții private a persoanelor, astfel încât păstrarea și accesul la aceste date ar fi, în acest sens, contrare articolului 15 alineatul (1) din Directiva 2002/58.

84. În aceste condiții, accesul la date de identitate civilă corespunzătoare adresei IP a unui utilizator de internet nu este, desigur, unicul mijloc teoretic de investigare ce permite identificarea persoanei titulare a acestei adrese la momentul săvârșirii infracțiunii, dar este cel care permite urmărirea sa penală, implicând în același timp cea mai mică ingerință în drepturile fundamentale ale acesteia și, prin urmare, evitarea impunității generale.

[32] Punctul 59 din prezentele concluzii.

[33] Punctul 62 din prezentele concluzii.

[34] Punctul 78 și următoarele din primele noastre concluzii.

85. În al doilea rând, subliniem din nou că o astfel de soluție ar permite, în opinia noastră, reconcilierea a două linii jurisprudențiale ale Curții, surse ale unei anumite tensiuni pe care am identificat-o în primele noastre concluzii [35] și în concluziile referitoare la cauza M.I.C.M. [36], și anume, pe de o parte, jurisprudența referitoare la păstrarea și la accesul la date și, pe de altă parte, cea referitoare la comunicarea adreselor IP atribuite sursei unei conexiuni în cadrul acțiunilor în apărarea drepturilor de proprietate intelectuală inițiate de persoane private.

86. În al treilea rând, deși jurisprudența Curții începând cu Hotărârile Tele2 și La Quadrature du Net și alții trebuie salutată întrucât a permis instituirea unui cadru vizând protecția drepturilor fundamentale ale utilizatorilor de servicii de comunicații electronice, ea este totuși marcată de o anumită cazuistică. Astfel, pe parcursul cauzelor supuse examinării sale, Curtea a dat o claritate progresivă jurisprudenței sale care i-a permis să examineze diverse reglementări naționale în lumina articolului 15 alineatul (1) din Directiva 2002/58. Cu toate acestea, este imposibil pentru Curte să anticipeze virtual toate măsurile care ar putea face obiectul unei analize în lumina acestei dispoziții. Acest lucru este demonstrat de altfel de numărul trimiterilor preliminare [37] al căror obiect îl face această dispoziție începând cu Hotărârea Tele2, care atestă, în opinia noastră, dificultatea pe care o pot întâmpina instanțele naționale în aplicarea principiilor enunțate în jurisprudența Curții în cazul unor situații diferite de cele care au condus la pronunțarea hotărârilor în discuție [38].

87. Prin urmare, rezultă că este necesară, în opinia noastră, o anumită flexibilitate atunci când sunt supuse examinării Curții măsuri care nu puteau fi avute în vedere în cadrul hotărârilor anterioare, precum reglementări ce vizează infracțiuni care pot fi urmărite penal numai în măsura în care datele de identitate civilă corespunzătoare unor adrese IP sunt păstrate și accesibile, cu privire la care Curtea nu a trebuit niciodată să se pronunțe până în prezent.

88. Prin urmare, nu este vorba, astfel cum a susținut guvernul danez, despre a reconsidera jurisprudența Curții, ci despre a admite că, pe baza principiilor care stau la baza acesteia, se poate ajunge la o soluție mai nuanțată, în împrejurări foarte limitate.

89. Astfel, interpretarea pe care o propunem pentru articolul 15 alineatul (1) din Directiva 2002/58 permite păstrarea și accesul la date de identitate civilă corespunzătoare unor adrese IP numai în ceea ce privește urmărirea penală a infracțiunilor ai căror autori nu ar putea fi identificați în lipsa acestor date. Prin urmare, ea vizează numai infracțiunile săvârșite exclusiv pe internet și nu contestă soluțiile enunțate în jurisprudența referitoare la păstrarea și la accesul la date mai largi și care urmăresc alte obiective.

[35] Punctul 69 și următoarele din primele noastre concluzii.

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

[37] Hotărârea din 2 octombrie 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), și Hotărârile La Quadrature du Net și alții, Prokuratuur, Commissioner of An Garda Síochána și alții, precum și SpaceNet și Telekom Deutschland.

[38] În această privință, creșterea numărului de cereri de decizii preliminare având ca obiect interpretarea articolului 15 alineatul (1) din Directiva 2002/58 poate indica de asemenea o anumită formă de reticență din partea instanțelor naționale în a aplica principiile stabilite de Curte în cazul unor situații ușor diferite ca urmare a particularităților ordinilor juridice naționale. Cu privire la acest aspect, a se vedea în special Cameron, I., „Metadata retention and national security: *Privacy international* and *La Quadrature du Net*”, în *Common Market Law Review*, 2021, vol. 58, nr. 5, p. 1433-1471, sau de asemenea Bertrand, B., „L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin?”, în *Dalloz IP/IT*, 2021, nr. 9, p. 468-472. Prin urmare, considerăm cu atât mai esențial, în perspectiva menținerii unui dialog fructuos între Curte și instanțele din statele membre, ca Curtea să poată da dovadă de adaptare atunci când împrejurările o impun. Astfel cum au arătat autorii doctrinei, standardul ridicat de protecție instituit de jurisprudența Curții nu poate fi cu adevărat eficace fără sprijinul instanțelor naționale, care sunt principalele responsabile de punerea lui în aplicare. Cu privire la acest aspect, a se vedea în special Teyssedre, J., „Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Siochana*”, în *Common Market Law Review*, vol. 60, nr. 2, 2023, p. 569-588, și Sirinelli, J., „La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite”, în *Revue trimestrielle de droit européen*, vol. 57, nr. 2, 2021, p. 313-329.

V. Concluzie

90. Având în vedere ansamblul considerațiilor care precedă, propunem Curții să răspundă la întrebările preliminare adresate de Conseil d'État (Consiliul de Stat, Franța) după cum urmează:

Articolul 15 alineatul (1) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), astfel cum a fost modificată prin Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene,

trebuie interpretat în sensul că

nu se opune unei reglementări naționale ce permite păstrarea de către furnizorii de servicii de comunicații electronice și accesul unei autorități administrative responsabile de protecția drepturilor de autor și a drepturilor conexe împotriva încălcărilor acestor drepturi săvârșite pe internet limitat la date de identitate civilă corespunzătoare unor adrese IP pentru ca respectiva autoritate să poată identifica titularii acestor adrese suspectați a fi responsabili de aceste încălcări și să poată lua, dacă este cazul, măsuri împotriva lor, fără ca acest acces să fie condiționat de un control prealabil din partea unei instanțe sau a unei entități administrative independente, atunci când aceste date constituie singurul mijloc de investigare ce permite identificarea persoanelor cărora le erau atribuite aceste adrese la momentul săvârșirii infracțiunii.