CONCLUZIILE AVOCATULUI GENERAL
M. CAMPOS SÁNCHEZ-BORDONA
prezentate la 12 mai 2016[1]

Cauza C-582/14

Patrick Breyer
împotriva
Bundesrepublik Deutschland[cerere de decizie preliminară formulată de

Bundesgerichtshof (Curtea Federală de Justiție, Germania)]

„Prelucrarea datelor cu caracter personal — Directiva 95/46/CE — Articolul 2 litera (a) și articolul 7 litera (f) — Noțiunea «date cu caracter personal» — Adrese IP — Păstrarea datelor de către un furnizor de servicii de comunicații electronice — Reglementare națională care nu permite luarea în considerare a interesului legitim al operatorului”

1. Adresa de protocol internet (denumită în continuare „adresă IP”) este o succesiune de numere binare care, odată atribuită unui dispozitiv (calculator, tabletă, smartphone), îl identifică și permite accesul acestuia la rețeaua de comunicații electronice. Pentru a se conecta la internet, dispozitivul trebuie să utilizeze secvența numerică pusă la dispoziție de furnizorii serviciului de acces la rețea. Adresa IP este transmisă serverului pe care este găzduită pagina web care este accesată.

2. În special, furnizorii de acces la rețea (în general, companiile de telefonie) atribuie clienților așa-numitele „adrese IP dinamice”, în mod temporar, pentru fiecare conexiune la internet, și le schimbă la fiecare conectare ulterioară. Aceste companii țin un registru al adreselor IP atribuite la fiecare moment unui anumit dispozitiv[2].

3. În general, titularii site-urilor internet care sunt accesate prin intermediul adreselor IP dinamice țin de asemenea registre în care sunt indicate paginile consultate, data accesării acestora și adresa IP dinamică folosită. Din punct de vedere tehnic, după încheierea conexiunii la internet a fiecărui utilizator, aceste registre pot fi păstrate pe durată nedeterminată.

4. Prestatorul de servicii nu poate identifica utilizatorul paginii sale web doar prin intermediul unei adrese IP dinamice, ci numai dacă utilizează și alte informații suplimentare aflate în posesia furnizorului de acces la rețea.

1 — Limba originală: spaniola.

2 — Articolul 5 din Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO 2006, L 105, p. 54, Ediție specială, 13/vol. 53, p. 51) impunea printre altele obligația de a păstra, în vederea prevenirii, cercetării, detectării și sancționării infracțiunilor grave, „data și ora conectării și deconectării din serviciul de accesare a internetului, […] împreună cu adresa IP alocată de furnizorul de servicii de accesare a internetului, indiferent dacă aceasta este dinamică sau statică, precum și identificatorul de utilizator al abonatului sau al utilizatorului înregistrat”.

5. În cadrul litigiului se analizează dacă adresele IP dinamice constituie date cu caracter personal, în sensul articolului 2 litera (a) din Directiva 95/46/CE[3]. Pentru a propune o soluție, trebuie să stabilim, în prealabil, relevanța pe care o are în acest scop faptul că informațiile suplimentare necesare pentru identificarea utilizatorului nu se află în posesia titularului site-ului internet, ci a unui terț (în concret, a furnizorului serviciului de acces la rețea).

6. Aceasta reprezintă o problemă inedită pentru Curte, având în vedere că la punctul 51 din Hotărârea Scarlet Extended[4] a statuat că adresele IP „reprez[intă] date protejate cu caracter personal, deoarece permit identificarea precisă a utilizatorilor respectivi", însă într-un context în care colectarea și identificarea adreselor IP era efectuată de furnizorul de acces la rețea[5], iar nu de către un furnizor de conținut, precum în prezenta cauză.

7. În cazul în care adresele IP dinamice constituie date cu caracter personal pentru furnizorul de servicii internet, ar trebui să se examineze ulterior dacă prelucrarea acestora intră în domeniul de aplicare al Directivei 95/46.

8. Este posibil ca aceste date, deși au caracter personal, să nu beneficieze de protecția conferită de Directiva 95/46 dacă, de exemplu, sunt prelucrate în vederea urmăririi penale a unor posibili autori ai unor atacuri asupra paginii web. În această ipoteză, Directiva 95/46 nu este aplicabilă, conform articolului 3 alineatul (2) prima liniuță din aceasta.

9. În plus, trebuie să se stabilească dacă furnizorul de servicii care înregistrează adresele IP dinamice atunci când un utilizator accesează paginile sale web (în speță, Republica Federală Germania) acționează în calitate de autoritate publică sau mai degrabă ca particular.

10. În cazul în care Directiva 95/46 ar fi aplicabilă, ar trebui să se clarifice, în ultimul rând, în ce măsură articolul 7 litera (f) din aceasta este compatibil cu o reglementare națională care limitează domeniul de aplicare al uneia dintre condițiile prevăzute la articolul respectiv cu scopul de a justifica prelucrarea datelor cu caracter personal.

I – **Cadrul normativ**

A – *Dreptul Uniunii*

11. Considerentul (26) al Directivei 95/46 are următorul cuprins:

„(26) întrucât principiile protecției trebuie să se aplice oricărei informații privind o persoană identificată sau identificabilă; întrucât pentru a determina dacă o persoană este identificabilă este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată; întrucât principiile protecției nu se aplică datelor anonime astfel încât persoana vizată să nu mai fie identificabilă; întrucât codurile de conduită în sensul articolului 27 pot fi un instrument util pentru a furniza indicații asupra modului în care datele pot fi transformate în date anonime și stocate într-o formă în care nu mai pot permite identificarea persoanei vizate".

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 L 281, p. 31, Ediție specială, 13/vol. 17, p. 10).

4 — Hotărârea din 24 noiembrie 2011 (C-70/10, EU:C:2011:771, punctul 51).

5 — Această situație se regăsește și în Hotărârea din 19 aprilie 2012, Bonnier Audio și alții (C-461/10, EU:C:2012:219, punctele 51 și 52).

12. Conform articolului 1 din Directiva 95/46:

„(1) Statele membre asigură, în conformitate cu prezenta directivă, protejarea drepturilor și libertăților fundamentale ale persoanei și în special a dreptului la viața privată în ceea ce privește prelucrarea datelor cu caracter personal.

(2) Statele membre nu pot limita sau interzice libera circulație a datelor cu caracter personal între statele membre din motive legate de protecția asigurată în conformitate cu alineatul (1).”

13. Potrivit articolului 2 din Directiva 95/46:

„În sensul prezentei directive:

(a) «date cu caracter personal» înseamnă orice informație referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

(b) «prelucrarea datelor cu caracter personal» (prelucrare) înseamnă orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

[…]

(d) «operator» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin acte cu putere de lege sau norme administrative interne sau comunitare, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul intern sau comunitar;

[…]

(f) «terț» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice organism altul decât persoana vizată, operatorul, persoana împuternicită și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date;

[…]”

14. Articolul 3 din Directiva 95/46, intitulat „Domeniul de aplicare”, prevede:

„(1) Prezenta directivă se aplică prelucrării automate, în totalitate sau parțial, precum și prelucrării neautomate a datelor cu caracter personal, conținute sau care urmează să fie conținute într-un sistem de evidență a datelor cu caracter personal.

(2) Prezenta directivă nu se aplică prelucrării datelor cu caracter personal:

— puse în practică pentru exercitarea activităților din afara domeniului de aplicare a dreptului comunitar, cum ar fi cele prevăzute în titlurile V și VI din Tratatul privind Uniunea Europeană, și, în orice caz, prelucrărilor care au ca obiect siguranța publică, apărarea, securitatea statului (inclusiv bunăstarea economică a statului atunci când aceste prelucrări sunt legate de probleme de securitate a statului) și activitățile statului în domeniul dreptului penal;

[…]”

15. Capitolul II din Directiva 95/46, privind „condițiile generale de legalitate a prelucrării datelor cu caracter personal”, începe cu articolul 5, conform căruia „statele membre precizează, în limitele dispozițiilor prezentului capitol, condițiile în care operațiunile de prelucrare a datelor cu caracter personal sunt legale”.

16. Potrivit articolului 6 din Directiva 95/46:

„(1) Statele membre stabilesc că datele cu caracter personal trebuie să fie:

(a) prelucrate în mod corect și legal;

(b) colectate în scopuri determinate, explicite și legitime și să nu mai fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor în scopuri istorice, statistice sau științifice nu este considerată incompatibilă atât timp cât statele membre prevăd garanții corespunzătoare;

(c) adecvate, pertinente și neexcesive în ceea ce privește scopurile pentru care sunt colectate și prelucrate ulterior;

(d) exacte și, dacă este necesar, actualizate; trebuie luate toate măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate sau pentru care vor fi prelucrate ulterior să fie șterse sau rectificate;

(e) păstrate într-o formă care permite identificarea persoanelor vizate o perioadă nu mai lungă decât este necesar în vederea atingerii scopurilor pentru care au fost colectate sau pentru care vor fi prelucrate ulterior. Statele membre stabilesc garanțiile corespunzătoare pentru datele cu caracter personal care sunt stocate pe o perioadă mai mare decât cea menționată, în scopuri istorice, statistice sau științifice.

(2) Operatorul are obligația să asigure respectarea alineatului (1).”

17. Conform articolului 7 din Directiva 95/46:

„Statele membre prevăd ca datele cu caracter personal să fie prelucrate numai dacă:

(a) persoana vizată și-a dat consimțământul neechivoc sau

(b) prelucrarea este necesară pentru executarea unui contract la care subiectul datelor este parte sau în vederea luării unor măsuri, la cererea acestuia, înainte de încheierea contractului sau

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului sau

(d) prelucrarea este necesară în scopul protejării interesului vital al persoanei vizate sau

(e) prelucrarea este necesară pentru aducerea la îndeplinire a unei sarcini de interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul sau terțul căruia îi sunt comunicate datele sau

(f) prelucrarea este necesară pentru realizarea interesului legitim urmărit de operator sau de către unul sau mai mulți terți, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protecție în temeiul articolului 1 alineatul (1).”

18. Potrivit articolului 13 din Directiva 95/46:

„(1) Statele membre pot adopta măsuri legislative pentru a restrânge domeniul obligațiilor și drepturilor prevăzute la articolul 6 alineatul (1), articolul 10, articolul 11 alineatul (1), articolul 12 și articolul 21, dacă o astfel de restricție constituie o măsură necesară pentru a proteja:

(a) securitatea statului;

(b) apărarea;

(c) siguranța publică;

(d) prevenirea, investigarea, detectarea și punerea sub urmărire a infracțiunilor sau a încălcării eticii în cazul profesiunilor reglementate;

(e) un interes economic sau financiar important al unui stat membru sau al Uniunii Europene, inclusiv în domeniile monetar, bugetar și fiscal;

(f) o funcție de monitorizare, inspecție sau de reglementare legată, chiar și ocazional, de exercitarea autorității publice în cazurile menționate la literele (c), (d) și (e);

(g) protecția persoanei vizate sau a drepturilor și libertăților altora.

[…]”

B – *Dreptul național*

19. Articolul 12 din Telemediengesetz (Legea privind serviciile de telecomunicații, denumită în continuare „TMG”)[6] prevede:

„(1) Furnizorul de servicii poate colecta și utiliza datele cu caracter personal pentru furnizarea serviciilor de telecomunicații numai dacă acest lucru este permis în temeiul prezentei legi sau al altor dispoziții care fac referire în mod expres la serviciile respective sau dacă utilizatorul și-a dat consimțământul în acest sens.

(2) Furnizorul de servicii poate utiliza în alte scopuri datele cu caracter personal colectate pentru furnizarea serviciilor de telecomunicații numai dacă acest lucru este permis în temeiul prezentei legi sau al altor dispoziții care fac referire în mod expres la serviciile respective sau dacă utilizatorul și-a dat consimțământul în acest sens.

(3) În lipsa unor prevederi contrare, sunt aplicabile dispozițiile privind protecția datelor cu caracter personal, chiar dacă datele nu sunt prelucrate în mod automat.”

20. Conform articolului 15 din TMG:

„(1) Furnizorul de servicii poate colecta și utiliza datele cu caracter personal ale unui utilizator numai dacă este necesar pentru a permite utilizarea și facturarea serviciilor de telecomunicații (date de utilizare). Datele de utilizare sunt în special:

1. datele de identificare a utilizatorului;

6 — Legea din 26 februarie 2007 (BGBl. 2007 I, p. 179).

2. informațiile privind începutul și sfârșitul fiecărei utilizări, precum și întinderea acesteia și

3. informațiile privind serviciile de telecomunicații folosite de utilizator.

(2) Furnizorul de servicii poate grupa datele de utilizare ale unui utilizator referitoare la folosirea diferitor servicii de telecomunicații în măsura în care este necesar pentru emiterea de facturi către acest utilizator.

[…]

(4) Furnizorul de servicii poate folosi datele de utilizare după încheierea sesiunii, în măsura în care este necesar pentru facturarea serviciului către utilizator (date pentru facturare). Pentru a respecta termenele de conservare legale în vigoare, statutare sau contractuale, furnizorul de servicii poate bloca datele. […]"

21. Conform articolului 3 din Bundesdatenschutzgesetz (Legea federală privind protecția datelor, denumită în continuare „BDSG")[7], „datele cu caracter personal constituie informații concrete privind situația personală sau materială a unei persoane fizice identificate sau identificabile (persoana vizată). […]".

II – **Situația de fapt**

22. Domnul Breyer a introdus o acțiune împotriva Republicii Federale Germania prin care a solicitat încetarea înregistrării adreselor IP.

23. Numeroase instituții publice germane administrează portaluri de internet accesibile publicului, prin intermediul cărora pun la dispoziție informații actualizate. Pentru a preveni atacurile și a face posibilă urmărirea penală a autorilor atacurilor, majoritatea acestor portaluri înregistrează toate accesările în fișiere sau registre de protocol. În cuprinsul acestora sunt păstrate, inclusiv după încheierea sesiunii, numele fișierului sau al paginii consultate, termenii introduși în câmpurile de căutare, momentul la care a avut loc consultarea, volumul datelor transferate, indicarea accesării cu succes a site-ului și adresa IP a calculatorului de pe care s-a solicitat accesul.

24. Prin cererea sa, domnul Breyer, care a consultat mai multe dintre paginile menționate, a solicitat obligarea Republicii Federale Germania să înceteze să înregistreze, pe cont propriu sau prin intermediul unor terți, adresa IP a sistemului *host* de pe care a solicitat accesul, în măsura în care această înregistrare nu este necesară pentru restabilirea disponibilității serviciului de telecomunicații în cazul defectării acestuia.

25. Cererea formulată de domnul Breyer a fost respinsă în primă instanță. Totuși, apelul introdus de acesta a fost admis în parte, iar Republica Federală Germania a fost obligată să înceteze înregistrarea după încheierea fiecărei sesiuni de acces. Ordinul de încetare a fost emis cu condiția ca reclamantul să fi furnizat datele sale personale în cadrul sesiunii de acces, inclusiv sub forma unei adrese de e-mail, iar această înregistrare să nu fie necesară pentru restabilirea disponibilității serviciului de telecomunicații.

7 — Legea din 20 decembrie 1990 (BGBl. 1990 I, p. 2954).

III – **Întrebările preliminare adresate**

26. Ambele părți au declarat apel, iar Camera VI a Bundesgerichtshof (Curtea Federală de Justiție, Germania) a formulat următoarele întrebări preliminare, pe care le-a adresat la 17 decembrie 2014:

„1) Articolul 2 litera (a) din Directiva 95/46/CE […] trebuie interpretat în sensul că o adresă de protocol internet (adresă IP) care este înregistrată de un furnizor de servicii cu ocazia accesului la site-ul său internet constituie pentru acesta o dată cu caracter personal, în cazul în care un terț (în speță furnizorul de acces) dispune de informațiile suplimentare necesare pentru identificarea persoanei vizate?

2) Articolul 7 litera (f) din Directiva privind protecția datelor se opune unei dispoziții de drept național potrivit căreia furnizorul de servicii poate colecta și utiliza datele personale ale unui utilizator fără consimțământul acestuia numai în măsura în care este necesar pentru a permite și a factura utilizarea efectivă a serviciului de comunicații electronice de către respectivul utilizator și potrivit căreia scopul asigurării unei funcționalități generale a serviciului respectiv nu poate justifica utilizarea datelor după terminarea sesiunii în curs?”

27. Potrivit instanței de trimitere, reclamantul ar putea solicita încetarea înregistrării adreselor IP, în conformitate cu dreptul german, în cazul în care păstrarea acestora constituie o ingerință nelegală, din perspectiva legislației în materia protecției datelor, în dreptul său general al personalității, mai precis în dreptul său la „autodeterminare informațională” [articolul 1004 alineatul 1 și articolul 823 alineatul 1 din Bürgerliches Gesetzbuch (Codul civil german) coroborate cu articolele 1 și 2 din Grundgesetz (Legea fundamentală)].

28. Această situație ar fi aplicabilă în cazul în care: a) adresa IP (în orice caz, împreună cu momentul accesării unui site internet) ar putea fi considerată „dată cu caracter personal” în sensul articolului 2 litera (a) coroborat cu a doua teză a considerentului (26) al Directivei 95/46 sau în sensul articolului 12 alineatele 1 și 3 din TMG coroborat cu articolul 3 alineatul 1 din BDSG și b) nu ar exista nicio situație de autorizare în sensul articolului 7 litera (f) din Directiva 95/46 sau în sensul articolului 12 alineatele 1 și 3 și al articolului 15 alineatele 1 și 4 din TMG.

29. Potrivit Bundesgerichtshof (Curtea Federală de Justiție), este indispensabil pentru interpretarea dreptului național (articolul 12 alineatul 1 din TMG) să se stabilească ce se înțelege prin caracterul personal al datelor, la care face referire articolul 2 litera (a) din Directiva 95/46.

30. În plus, instanța *a quo* subliniază că, întrucât articolul 15 alineatul 1 din TMG prevede că furnizorul de servicii poate colecta și utiliza datele cu caracter personal ale unui utilizator numai dacă este necesar pentru a permite utilizarea și facturarea serviciilor de telecomunicații (date de utilizare) [8], interpretarea acestei dispoziții naționale depinde de cea a articolului 7 litera (f) din Directiva 95/46.

IV – **Procedura în fața Curții. Argumentele părților**

31. Au prezentat observații scrise guvernul german, guvernul austriac, guvernul portughez și Comisia. Doar această din urmă instituție, precum și domnul Breyer s-au prezentat în ședința publică desfășurată la 25 februarie 2016, la care guvernul german nu a dorit să participe.

8 — Potrivit Bundesgerichtshof (Curtea Federală de Justiție), datele de utilizare sunt datele de identificare a utilizatorului, informațiile privind începutul și sfârșitul fiecărei utilizări, precum și întinderea acesteia și informațiile privind serviciile de telecomunicații folosite de utilizator.

A – *Argumentele părților cu privire la prima întrebare preliminară*

32. Potrivit domnului Breyer, constituie date cu caracter personal inclusiv acelea care pot fi grupate numai din punct de vedere teoretic, cu alte cuvinte pornind de la premisa unui potențial pericol abstract, fiind mai puțin relevant dacă în practică acestea sunt grupate efectiv. În opinia sa, faptul că un organism poate fi relativ incapabil să identifice o persoană utilizând adresa IP nu înseamnă că nu există un pericol pentru persoana respectivă. În plus, acesta consideră că este relevant faptul că Germania păstrează datele sale IP pentru identificarea, dacă este cazul, a eventualelor atacuri sau în vederea inițierii procedurilor penale, în temeiul articolului 113 din Telekommunikationsgesetz (Legea privind telecomunicațiile), iar astfel de situații s-au produs în numeroase ocazii.

33. Potrivit guvernului german, prima întrebare preliminară trebuie să primească un răspuns negativ. Acesta consideră că adresele IP dinamice nu dezvăluie o persoană „identificată", în sensul articolului 2 litera (a) din Directiva 95/46. Pentru a stabili dacă acestea oferă informații cu privire la o persoană „identificabilă", în sensul aceleiași dispoziții, *caracterul identificabil* trebuie examinat în conformitate cu un criteriu „relativ", astfel cum reiese, în opinia sa, din cuprinsul considerentului (26) al Directivei 95/46, conform căruia trebuie să se ia în considerare doar mijloacele care pot fi utilizate „în mod rezonabil" fie de operator, fie de un terț pentru a identifica o persoană. O astfel de precizare ar indica faptul că legiuitorul Uniunii nu a dorit să includă în domeniul de aplicare al Directivei 95/46 situațiile în care orice terț are posibilitatea obiectivă de a efectua identificarea.

34. Guvernul german consideră de asemenea că noțiunea „date cu caracter personal", în sensul articolului 2 litera (a) din Directiva 95/46, trebuie interpretată în lumina obiectivului acestei directive, care constă în asigurarea respectării drepturilor fundamentale. Necesitatea protejării persoanelor fizice ar putea fi interpretată în moduri diferite, în funcție de posesorii datelor și de aspectul dacă dețin sau nu dețin mijloacele necesare pentru utilizarea acestora în vederea identificării respectivelor persoane.

35. Guvernul german susține că domnul Breyer nu este identificabil pe baza adreselor IP grupate cu alte informații păstrate de furnizorii de conținut. În acest scop, ar trebui să se gestioneze informațiile deținute de furnizorii de acces la internet, care, în lipsa unui temei legal, nu le pot pune la dispoziția furnizorilor de conținut.

36. În opinia guvernului austriac, trebuie, dimpotrivă, să se răspundă afirmativ la această întrebare. Conform considerentului (26) al Directivei 95/46, pentru ca o persoană să fie considerată identificabilă, nu este necesar ca toate datele de identificare să fie deținute de o singură entitate. Astfel, o adresă IP ar putea fi o dată cu caracter personal dacă un terț (precum, de exemplu, furnizorul de acces la internet) dispune de mijloacele necesare pentru identificarea titularului acestei adrese fără să depună eforturi considerabile.

37. Guvernul portughez înclină de asemenea în favoarea unui răspuns afirmativ. Acesta consideră că adresa IP, în combinație cu data la care a fost consultat site-ul, constituie o dată cu caracter personal, întrucât poate conduce la identificarea utilizatorului de către o altă entitate decât cea care a păstrat adresa IP.

38. Comisia propune de asemenea să se răspundă afirmativ, pe baza soluției adoptate de Curte în cauza Scarlet Extended[9]. În opinia Comisiei, având în vedere că adresele IP sunt păstrate tocmai pentru identificarea utilizatorilor în cazul atacurilor cibernetice, utilizarea informațiilor suplimentare înregistrate de furnizorii de acces la internet ar presupune un mijloc care poate fi utilizat „în mod

9 — Hotărârea din 24 noiembrie 2011 (C-70/10, EU:C:2011:771, punctul 51).

rezonabil”, în sensul considerentului (26) al Directivei 95/46. În definitiv, potrivit Comisiei, atât obiectivul urmărit de această directivă, cât și articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”) ar fi în favoarea unei interpretări ample a articolului 2 litera (a) din Directiva 95/46.

B – *Argumentele părților cu privire la a doua întrebare preliminară*

39. Domnul Breyer consideră că articolul 7 litera (f) din Directiva 95/46 constituie o clauză generală care trebuie pusă în aplicare în mod concret. Potrivit jurisprudenței Curții, ar trebui, prin urmare, să se analizeze circumstanțele fiecărui caz în parte și să se determine dacă există grupuri cu un interes legitim, în sensul dispoziției respective, astfel încât stabilirea unor reguli specifice pentru aceste grupuri nu numai că este permisă, ci este esențială pentru aplicarea articolului menționat. În această ipoteză, în opinia domnului Breyer, reglementarea națională este conformă cu articolul 7 litera (f) din Directiva 95/46, întrucât nu există un interes al portalului public pentru păstrarea datelor cu caracter personal sau pentru că interesul pentru protejarea anonimatului este mai important. Cu toate acestea, în opinia sa, o păstrare sistematică și cu caracter personal a datelor nu este în spiritul unei societăți democratice și nici nu este necesară sau proporțională pentru a asigura funcționarea comunicațiilor electronice, care este perfect posibilă fără înregistrarea acestor date cu caracter personal, după cum o demonstrează unele site-uri internet ale anumitor ministere federale.

40. Guvernul german susține că nu se impune analizarea celei de a doua întrebări, care a fost adresată doar în ipoteza în care s-ar răspunde afirmativ la prima întrebare, ceea ce nu este cazul, în opinia sa, având în vedere motivele prezentate anterior.

41. Guvernul austriac propune să se răspundă în sensul că Directiva 95/46 nu se opune în mod general păstrării unor date precum cele în discuție în procedura principală, atunci când aceasta este esențială pentru a asigura buna funcționare a comunicațiilor electronice. În opinia acestui guvern, păstrarea limitată a adresei IP pentru o perioadă mai mare decât cea în care a fost consultată pagina web poate fi legală, sub aspectul respectării obligației operatorului datelor cu caracter personal de a aplica măsurile de protecție a acestora, prevăzută la articolul 17 alineatul (1) din Directiva 95/46. Lupta împotriva atacurilor cibernetice poate justifica analiza datelor referitoare la atacurile anterioare și împiedicarea accesului la un site internet a anumitor adrese IP. Caracterul proporțional al păstrării unor date precum cele din procedura principală, din punctul de vedere al obiectivului de asigurare a bunei funcționări a comunicațiilor electronice, ar trebui să fie apreciat de la caz la caz, luându-se în considerare principiile menționate la articolul 6 alineatul (1) din Directiva 95/46.

42. Guvernul portughez susține că articolul 7 alineatul (f) din Directiva 95/46 nu se opune normelor naționale vizate în procedura principală, deoarece legiuitorul german a efectuat deja evaluarea comparativă, prevăzută la acest articol, a intereselor legitime ale operatorului de date cu caracter personal, pe de o parte, și a drepturilor și a libertăților titularilor acestor date, pe de altă parte.

43. În opinia Comisiei, legislația națională care transpune articolul 7 litera (f) din Directiva 95/46 trebuie să stabilească obiectivele prelucrării datelor cu caracter personal astfel încât acestea să fie previzibile pentru particularul afectat. Comisia consideră că legislația germană nu respectă această cerință, întrucât articolul 15 alineatul 1 din TMG prevede că păstrarea adreselor IP este autorizată „dacă este necesar pentru a permite utilizarea […] serviciilor de telecomunicații”.

44. Prin urmare, Comisia propune să se răspundă la cea de a doua întrebare preliminară în sensul că această prevedere se opune interpretării unei dispoziții naționale conform căreia o autoritate publică ce acționează în calitate de furnizor de servicii poate să grupeze și să utilizeze datele cu caracter personal ale unui utilizator fără consimțământul acestuia, chiar dacă obiectivul urmărit este de a asigura buna funcționare generală a comunicațiilor electronice, dacă dispoziția națională respectivă nu prevede acest obiectiv în mod suficient de clar și de precis.

V – **Analiză**

A – *Prima întrebare preliminară*

1. Delimitarea întrebării adresate

45. Având în vedere modul în care Bundesgerichtshof (Curtea Federală de Justiție) a formulat prima întrebare preliminară, scopul acesteia este de a se stabili dacă o adresă IP prin intermediul căreia se accesează o pagină web constituie o dată cu caracter personal [în sensul articolului 2 litera (a) din Directiva 95/46/CE] pentru entitatea publică titulară a acestei pagini, în cazul în care furnizorul de acces la rețea deține informații suplimentare care permit identificarea persoanei vizate.

46. Redactată în această formă, întrebarea este suficient de clară pentru a elimina cu ușurință alte probleme care s-ar putea ridica *in abstracto* cu privire la natura juridică a adreselor IP, în contextul protecției datelor cu caracter personal.

47. În primul rând, Bundesgerichtshof (Curtea Federală de Justiție) se referă exclusiv la „adresele IP dinamice”, și anume la acelea care sunt atribuite în mod temporar fiecărei conexiuni la rețea și care se modifică odată cu conexiunile ulterioare. Prin urmare, acestea sunt diferite de „adresele IP fixe sau statice”, care au caracter invariabil și permit identificarea permanentă a dispozitivului conectat la rețea.

48. În al doilea rând, instanța de trimitere pornește de la premisa că, în procedura *a quo*, furnizorul site-ului internet nu poate identifica vizitatorii paginilor sale web prin intermediul adresei IP dinamice și nici nu deține informații suplimentare proprii care, dacă sunt grupate cu adresa IP respectivă, facilitează identificarea acestora. Bundesgerichtshof (Curtea Federală de Justiție) pare să aprecieze că, în acest context, adresa IP dinamică nu este o dată cu caracter personal, în sensul articolului 2 litera (a) din Directiva 95/46, *în ceea ce privește furnizorul site-ului internet*.

49. Îndoiala instanței de trimitere se referă la posibilitatea calificării adresei IP dinamice, în ceea ce privește furnizorul site-ului internet, ca dată cu caracter personal *în cazul în care un terț deține informații suplimentare care*, dacă sunt grupate cu această dată, permit identificarea vizitatorilor paginilor sale web. Or – iar această mențiune este mai relevantă – Bundesgerichtshof (Curtea Federală de Justiție) nu face referire la orice terț care deține informațiile suplimentare, ci doar la furnizorul de acces la rețea (excluzând, prin urmare, alți eventuali posesori ai acestui tip de date).

50. Prin urmare, nu fac obiectul analizei, printre altele, următoarele aspecte: a) dacă adresele IP statice constituie date cu caracter personal, conform Directivei 95/46[10]; b) dacă adresele IP dinamice constituie, în orice moment și în orice circumstanțe, date cu caracter personal în sensul acestei directivei și, în sfârșit, c) în ce măsură calificarea adreselor IP dinamice ca date cu caracter personal este inevitabilă, în cazul în care există un terț, indiferent de calitatea acestuia, care le poate utiliza pentru identificarea utilizatorilor rețelei.

10 — Problemă soluționată de Curte în Hotărârea din 24 noiembrie 2011, Scarlet Extended (C-70/10, EU:C:2011:771, punctul 51), și în Hotărârea din 19 aprilie 2012, Bonnier Audio și alții (C-461/10, EU:C:2012:219). La punctele 51 și 52 din aceasta din urmă, Curtea a concluzionat că comunicarea, „pentru identificarea acestuia, a numelui și a adresei […] unui utilizator de internet care utilizează adresa IP de la care se prezumă că au fost schimbate ilegal fișiere care conțin opere protejate reprezintă o prelucrare a datelor cu caracter personal în sensul articolului 2 primul paragraf din Directiva 2002/58 coroborat cu articolul 2 litera (b) din Directiva 95/46”.

51. Prin urmare, trebuie să se stabilească numai dacă o adresă IP dinamică reprezintă o dată cu caracter personal în ceea ce privește furnizorul unui serviciu de internet, în cazul în care compania de comunicații care oferă acces la rețea (furnizorul de acces) gestionează informații suplimentare care, grupate cu adresa respectivă, permit identificarea persoanelor care accesează pagina web administrată de furnizorul serviciului de internet.

2. Cu privire la fond

52. Problema ridicată prin intermediul acestei trimiteri preliminare face obiectul unei dezbateri ample în doctrina și în jurisprudența germane, polarizată în două curente de opinie [11]. Potrivit unuia dintre acestea (care optează pentru un criteriu „obiectiv" sau „absolut"), un utilizator este identificabil – și, prin urmare, adresa IP constituie o dată cu caracter personal care poate fi protejată – în cazul în care, indiferent de posibilitățile și de mijloacele furnizorului serviciului de internet, identificarea utilizatorului este posibilă doar dacă această adresă IP dinamică este grupată cu alte informații furnizate de un terț (de exemplu furnizorul de acces la rețea).

53. Pentru adepții celuilalt curent (care adoptă un criteriu „relativ"), posibilitatea de a fi asistați de un terț pentru identificarea finală a utilizatorului nu este suficientă pentru a conferi caracter personal adresei IP dinamice. Ceea ce contează este capacitatea persoanei care are acces la această informație de a o utiliza, cu propriile mijloace, și de a identifica astfel o persoană.

54. Indiferent de termenii acestui litigiu în contextul dreptului național, răspunsul Curții trebuie să se limiteze la interpretarea celor două dispoziții din Directiva 95/46 la care au făcut trimitere atât instanța *a quo*, cât și părțile din procedură, și anume articolul 2 litera (a) [12] din directiva menționată și considerentul (26) [13] al acesteia.

55. Prin simplul fapt că facilitează obținerea de informații cu privire la data și ora la care a fost accesată o pagină web de pe un calculator (sau alt dispozitiv), adresele IP dinamice relevă anumite modele de comportament al utilizatorilor de internet și, prin urmare, implică o posibilă ingerință în dreptul la viață privată [14], garantat la articolul 8 din Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale și la articolul 7 din cartă, iar Directiva 95/46 [15] trebuie interpretată în lumina acestuia din urmă coroborat cu articolul 8 din cartă. În realitate, părțile din procedură nu contestă premisa respectivă, astfel încât, prin urmare, nici aceasta nu face obiectul întrebării preliminare.

56. Persoana la care se referă aceste detalii nu este o „persoană fizică identificată". Data și ora unei conexiuni, precum și originea sa numerică nu dezvăluie, în mod direct sau imediat, identitatea persoanei fizice căreia îi aparține dispozitivul de pe care este accesată pagina web și nici identitatea utilizatorului care îl folosește (poate fi orice persoană fizică).

11 — Cu privire la cele două opinii din doctrină, a se vedea de exemplu Schreibauer, M., în *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., și von Lewinski, K. (editori), Carl Heymanns Verlag/Wolters Kluwer, Köln, 2014, ediția a patra, § 11 Telemediengesetz (4-10). Nink, J., și Pohle, J.: „Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze", în *Multimedia und Recht*, 9/2015, p. 563-567. Heidrich, J., și Wegener, C.: „Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging", în *Multimedia und Recht*, 8/2015, p. 487-492. Leisterer, H.: „Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr", în *Computer und Recht*, 10/2015, p. 665-670.

12 — Reprodus la punctul 13.

13 — Reprodus la punctul 11.

14 — Acest aspect a fost amintit de avocatul general Cruz Villalón în Concluziile prezentate în cauza Scarlet Extended (C-70/10, EU:C:2011:255, punctul 76) și este în acord cu poziția exprimată de Autoritatea Europeană pentru Protecția Datelor în Avizul din 22 februarie 2010 privind negocierile curente purtate de Uniunea Europeană pentru un Acord comercial de combatere a contrafacerii (ACTA) (JO 2010, C 147, p. 1, punctul 24) și în Avizul din 10 mai 2010 privind Propunerea de directivă a Parlamentului European și a Consiliului privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile, de abrogare a Deciziei-cadru 2004/68/JAI (JO 2010, C 323, p. 6, punctul 11).

15 — A se vedea în acest sens Hotărârea din 20 mai 2003, Österreichischer Rundfunk (C-465/00, C-138/01 și C-139/01, EU:C:2003:294, punctul 68), și Concluziile avocatului general Kokott prezentate în cauza Promusicae (C-275/06, EU:C:2007:454, punctul 51 și următoarele).

57. Cu toate acestea, în măsura în care o adresă IP dinamică contribuie la identificarea – fie ca atare, fie prin asociere cu alte informații – titularului dispozitivului utilizat pentru accesarea paginii web, aceasta poate fi considerată o informație referitoare la o „persoană identificabilă” [16].

58. Potrivit Bundesgerichtshof (Curtea Federală de Justiție), adresa IP dinamică nu este suficientă, în sine, pentru identificarea utilizatorului care a accesat prin intermediul acesteia o pagină web. Dacă, dimpotrivă, furnizorul de servicii de internet ar putea să identifice utilizatorul prin intermediul adresei IP dinamice, ar fi vorba, fără nicio îndoială, despre o dată cu caracter personal în sensul Directivei 95/46. Totuși, nu acesta pare să fie scopul în care a fost formulată întrebarea preliminară, din care reiese că furnizorii de servicii de internet din procedura *a quo* nu pot identifica utilizatorul exclusiv pe baza adresei IP dinamice.

59. Dacă este grupată cu alte informații, adresa IP dinamică facilitează identificarea „indirectă” a utilizatorului, iar această opinie este unanim acceptată. Posibila existență a acestor informații suplimentare, care pot fi grupate cu adresa IP dinamică, permite, pur și simplu, calificarea acestora din urmă ca date cu caracter personal în temeiul directivei? Trebuie să se stabilească dacă este suficientă, în acest sens, simpla posibilitate, în abstract, de a cunoaște informațiile respective sau dacă, dimpotrivă, este necesar ca acestea să se afle la dispoziția unei persoane care cunoaște deja adresa IP dinamică sau a unui terț.

60. Părțile și-au concentrat observațiile pe interpretarea considerentului (26) al Directivei 95/46 și în special pe expresia „mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată”. Întrebarea adresată de instanța de trimitere nu vizează informațiile suplimentare deținute de furnizorii de servicii din procedura principală și nici vreun terț care se află în posesia unor astfel de informații suplimentare (a căror grupare cu adresa IP dinamică facilitează identificarea utilizatorului), ci se referă la furnizorul de acces la rețea.

61. Prin urmare, în prezenta cauză, Curtea nu trebuie să analizeze toate mijloacele pe care pârâta din procedura *a quo* le-ar putea utiliza „în mod rezonabil” pentru ca adresele IP dinamice pe care le deține să poată fi considerate date cu caracter personal. Având în vedere că Bundesgerichtshof (Curtea Federală de Justiție) se referă exclusiv la informații suplimentare aflate în posesia unui terț, poate rezulta a) fie că pârâta nu deține informații suplimentare proprii care să îi permită identificarea utilizatorului, b) fie că, în cazul în care deține astfel de informații, nu le poate utiliza în mod rezonabil în acest scop, în calitate de operator al acestora, conform considerentului (26) al Directivei 95/46.

62. Ambele ipoteze depind de o constatare de natură factuală, care este de competența exclusivă a instanței de trimitere. În cazul în care Bundesgerichtshof (Curtea Federală de Justiție) ar avea vreo îndoială cu privire la capacitatea pârâtei de a utiliza în mod rezonabil informațiile suplimentare proprii, Curtea ar putea să îi furnizeze criterii generale pentru interpretarea noțiunii „mijloacele care pot fi utilizate în mod rezonabil […] de operator”. Având în vedere că nu aceasta este situația în speță, considerăm că este exclus ca, în acest context, Curtea să stabilească anumite criterii de interpretare de care instanța de trimitere nu are nevoie și pe care nu le-a solicitat.

16 — Trebuie să se pornească de la premisa că, exceptând cazul în care există probe contrare, această persoană este cea care a navigat pe internet și a accesat respectiva pagină web. Totuși, chiar și fără a ține seama de această ipoteză, informația privind data, ora și originea numerică a accesului la o pagină web ar permite stabilirea unei legături între accesarea respectivă și titularul dispozitivului, precum și asocierea indirectă a acestuia cu modelul său comportamental din cadrul rețelei. O posibilă excepție ar putea fi adresele IP atribuite calculatoarelor din locuri precum internet café-urile, ai căror utilizatori anonimi sunt neidentificabili, iar în ceea ce privește proprietarii acestora, traficul generat în cadrul lor nu oferă nicio informație personală relevantă. În rest, aceasta este singura excepție de la principiul conform căruia adresele IP reprezintă date cu caracter personal admise de grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, constituit în conformitate cu Directiva 95/46 (așa-numitul „Grupul de lucru «Articolul 29»”). Avizul nr. 4/2007 din 20 iunie 2007 privind conceptul de date cu caracter personal, WP 136, emis de acest grup, poate fi consultat la adresa http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

63. Prin urmare, nucleul întrebării adresate se reduce la stabilirea aspectului dacă este relevantă, în vederea calificării adreselor IP dinamice ca date cu caracter personal, împrejurarea că un terț bine determinat – furnizorul de acces la internet – deține informații suplimentare care, grupate cu aceste adrese, pot conduce la identificarea utilizatorului care a accesat o anumită pagină web.

64. Se impune încă o dată să facem trimitere la considerentul (26) al Directivei 95/46. Noțiunea „mijloacele care pot fi utilizate în mod rezonabil […] *de orice altă persoană*” [17] ar putea conduce la o interpretare conform căreia ar fi suficient ca un terț să poată obține informații suplimentare (care pot fi grupate cu o adresă IP dinamică în vederea identificării unei persoane) pentru a considera că această adresă constituie *eo ipso* o dată cu caracter personal.

65. În practică, această interpretare extensivă ar determina calificarea ca dată cu caracter personal a oricărui tip de informație, chiar dacă ar fi insuficientă în sine pentru a facilita identificarea unui utilizator. Nu s-ar putea elimina în niciun caz, cu o certitudine absolută, eventualitatea existenței unui terț care deține informații suplimentare care pot fi grupate cu informația respectivă și care, prin urmare, ar putea dezvălui identitatea unei persoane.

66. În opinia noastră, posibilitatea ca progresul mijloacelor tehnice să deschidă considerabil, în viitorul mai mult sau mai puțin apropiat, calea accesului la instrumente de obținere și de prelucrare a informațiilor din ce în ce mai complexe justifică prudența anticipată în ceea ce privește apărarea intimității. Prin definirea categoriilor juridice relevante din materia protecției datelor s-a urmărit includerea unor ipoteze comportamentale suficient de ample și de flexibile pentru a acoperi orice situație imaginabilă [18].

67. Totuși, considerăm că această preocupare – care, în rest, este justificată – nu permite ignorarea voinței legiuitorului, iar interpretarea sistematică a considerentului (26) al Directivei 95/46 se rezumă la „mijloacele care pot fi utilizate în mod rezonabil” *de anumiți terți*.

68. Întrucât considerentul (26) nu face referire la orice mijloace care pot fi folosite de operator (în acest caz, furnizorul de servicii de internet), ci doar la cele pe care acesta le poate utiliza „în mod rezonabil”, tot astfel trebuie să se înțeleagă că legiuitorul se referă la „terții” la care, *tot în mod rezonabil*, poate apela operatorul care dorește să obțină informațiile suplimentare pentru identificare. Această situație nu se regăsește în cazul în care contactul cu acești terți este, de fapt, foarte costisitor din punctul de vedere al resurselor umane și economice sau practic imposibil ori interzis prin lege. În caz contrar, după cum am arătat deja, ar fi practic imposibil să se facă distincție între aceste mijloace, deoarece întotdeauna s-ar putea imagina existența ipotezei unui terț care, oricât de inaccesibil ar fi pentru furnizorul de servicii de internet, ar putea deține – în prezent sau în viitor – informații suplimentare relevante care să contribuie la identificarea unui utilizator.

69. După cum am arătat, terțul la care face referire Bundesgerichtshof (Curtea Federală de Justiție) este un furnizor de acces la rețea. Acesta este, fără îndoială, terțul la care este cel mai rezonabil să credem că apelează furnizorul de servicii pentru a obține informațiile suplimentare necesare, în cazul în care dorește să identifice în modul cel mai eficient, practic și direct utilizatorul care a accesat pagina sa web prin intermediul adresei IP dinamice. Acesta nu este în niciun caz un terț ipotetic, necunoscut și inaccesibil, ci un personaj principal în rețeaua de internet, despre care se cunoaște cu certitudine că se află în posesia informațiilor de care are nevoie furnizorul de servicii pentru identificarea unui utilizator. De fapt, potrivit instanței de trimitere, acesta este terțul concret la care dorește să apeleze pârâta din procedura principală pentru a obține informațiile suplimentare de care are nevoie.

17 — Sublinierea noastră.

18 — Această vocație de protecție și de prevenție stă la baza poziției adoptate de Grupul de lucru „Articolul 29”, în interpretarea căruia, după cum am arătat, trebuie să se plece de la principiul conform căruia adresele IP constituie date cu caracter personal, fiind admisă ca unică excepție ipoteza în care furnizorul serviciului poate stabili cu o certitudine absolută că acestea constituie adrese aferente unor persoane neidentificabile, precum utilizatorii unui internet café. A se vedea nota de subsol 16, *in fine*.

70. Furnizorul de acces la internet este, în mod obișnuit, terțul menționat în considerentul (26) al Directivei 95/46, la care poate apela în modul cel mai „rezonabil” furnizorul de servicii din procedura *a quo*. Cu toate acestea, trebuie să se determine dacă obținerea informațiilor suplimentare deținute de acest terț poate fi considerată posibilă sau realizabilă „în mod rezonabil”.

71. Guvernul german susține că, întrucât informațiile deținute de furnizorul de acces la internet constituie date cu caracter personal, acesta din urmă nu le poate divulga pur și simplu, ci în conformitate cu legislația care reglementează prelucrarea unor astfel de date [19].

72. Într-adevăr, este evident că, pentru a beneficia de aceste informații, trebuie să se respecte legislația aplicabilă în materia datelor cu caracter personal. O informație poate fi obținută „în mod rezonabil” numai dacă sunt îndeplinite condițiile privind accesul la acest tip de date, prima dintre aceste condiții referindu-se la posibilitatea legală de păstrare și de transmitere a datelor către terți. Desigur, furnizorul de acces la internet poate să refuze divulgarea datelor respective, însă este la fel de posibil să accepte. Simpla posibilitate a transmiterii datelor, perfect „rezonabilă”, transformă adresa IP dinamică, în conformitate cu considerentul (26) al Directivei 95/46, într-o dată cu caracter personal în ceea ce privește furnizorul de servicii de internet.

73. Este vorba despre o posibilitate reală *în cadrul legii* și, prin urmare, „rezonabilă”. Mijloacele de acces rezonabile prevăzute de Directiva 95/46 trebuie să fie, prin definiție, mijloace legale [20]. Aceasta este și premisa de la care, în mod firesc, pornește instanța de trimitere, după cum amintește guvernul german [21]. Astfel, se reduc în mod semnificativ căile de acces relevante din punct de vedere juridic, deoarece acestea trebuie să aibă caracter exclusiv legal. Însă atât timp cât acestea există, oricât de restrictive ar putea fi în ceea ce privește aplicarea lor practică, constituie un „mijloc rezonabil” în sensul Directivei 95/46.

74. Prin urmare, considerăm că, astfel cum a fost formulată de Bundesgerichtshof (Curtea Federală de Justiție), prima întrebare preliminară trebuie să primească un răspuns afirmativ. Adresa IP dinamică trebuie calificată, în ceea ce privește furnizorul de servicii de internet, ca dată cu caracter personal, având în vedere existența unui terț (furnizorul de acces la rețea) la care se poate apela în mod rezonabil pentru obținerea unor informații suplimentare care, grupate cu data respectivă, permit identificarea unui utilizator.

75. În opinia noastră, rezultatul la care ar conduce soluția contrară celei propuse o confirmă pe aceasta din urmă. Dacă adresele IP dinamice nu ar constitui date cu caracter personal în ceea ce privește furnizorul de servicii de internet, acesta le-ar putea păstra pe perioadă nedeterminată și ar putea solicita în orice moment furnizorului de acces la internet informații suplimentare, în vederea grupării cu aceste date și a identificării utilizatorului. În aceste circumstanțe, astfel cum admite guvernul german [22], adresa IP dinamică ar deveni o dată cu caracter personal, deoarece acesta ar deține deja informațiile suplimentare pentru identificarea utilizatorului, în acest sens fiind aplicabilă legislația în materia protecției datelor.

76. Cu toate acestea, ar fi vorba despre o informație care ar fi putut să fie păstrată numai dacă până la acel moment nu ar fi fost considerată dată cu caracter personal în ceea ce privește furnizorul de servicii. Astfel, calificarea adresei IP dinamice, din punct de vedere juridic, ca dată cu caracter personal, ar depinde de furnizorul de servicii, și anume de eventualitatea în care acesta ar decide să o utilizeze pentru identificarea utilizatorului prin gruparea sa cu informații suplimentare pe care va

19 — Punctele 40 și 45 din observațiile sale scrise.

20 — În acest context, este irelevant că accesul la o dată cu caracter personal este posibil *de facto*, prin încălcarea normelor privind protecția datelor.

21 — Punctele 47 și 48 din observațiile sale scrise.

22 — Punctul 36 din observațiile sale scrise.

trebui să le obțină de la un terț. Totuși, în opinia noastră, factorul determinant, în contextul Directivei 95/46, îl constituie posibilitatea – rezonabilă – existenței unui terț „accesibil”, care deține mijloacele necesare pentru a permite identificarea unei persoane, iar nu concretizarea posibilității de a apela la acest terț.

77. S-ar putea admite inclusiv că, astfel cum susține guvernul german, adresa IP dinamică devine o dată cu caracter personal numai atunci când o primește furnizorul de acces la internet. Totuși, în acest caz ar trebui să se accepte că o astfel de calificare va fi efectuată retroactiv, în funcție de termenul de păstrare a adresei IP, și, în consecință, calificarea respectivă ar trebui considerată inexistentă în cazul în care a fost depășită perioada în care putea fi păstrată dacă ar fi fost calificată încă de la început ca dată cu caracter personal. În această ipoteză, soluția ar fi contrară spiritului legislației în materia protecției datelor cu caracter personal. Faptul de a nu recunoaște de la bun început relevanța unei caracteristici inerente datelor respective ar fi incompatibil cu motivul care justifică păstrarea exclusiv temporară a acestora: potențialul lor de a servi ca mijloc de identificare – prin ele însele sau împreună cu alte informații – a unei persoane fizice. De asemenea, pentru acest motiv pur economic este mai rezonabil să li se atribuie de la început acest caracter.

78. Prin urmare, ca primă concluzie, considerăm că articolul 2 litera (a) din Directiva 95/46 trebuie interpretat în sensul că o adresă IP păstrată de un furnizor de servicii în legătură cu un acces la pagina sa web constituie pentru acesta o dată cu caracter personal, în măsura în care un furnizor de acces la rețea (internet) deține informații suplimentare care permit identificarea persoanei vizate.

B – *A doua întrebare preliminară*

79. Prin intermediul celei de a doua întrebări preliminare, Bundesgerichtshof (Curtea Federală de Justiție) dorește să afle dacă articolul 7 litera (f) din Directiva 95/46 se opune unei reglementări naționale care autorizează colectarea și utilizarea datelor cu caracter personal ale unui utilizator fără consimțământul acestuia numai dacă este necesar pentru a permite și a factura utilizarea efectivă a serviciului de telecomunicații de către respectivul utilizator, obiectivul privind asigurarea funcționării acestui serviciu neputând justifica utilizarea datelor menționate după încheierea fiecărei sesiuni.

80. Răspunsul trebuie să fie precedat de o precizare cu privire la informația furnizată de Bundesgerichtshof (Curtea Federală de Justiție) conform căreia datele în litigiu sunt păstrate pentru asigurarea bunei funcționări a site-urilor internet din procedura principală, facilitând, în acest caz, urmărirea penală în cazul atacurilor cibernetice care le-ar putea viza.

81. Prin urmare, trebuie să se stabilească, în primul rând, dacă prelucrarea adreselor IP la care face referire trimiterea preliminară intră sub incidența excepției prevăzute la articolul 3 alineatul (2) prima liniuță din Directiva 95/46 [23].

1. Cu privire la aplicabilitatea Directivei 95/46 în ceea ce privește prelucrarea datelor în litigiu

82. Aparent, în procedura principală, Republica Federală Germania acționează ca simplu furnizor de servicii de internet, cu alte cuvinte ca particular (și, prin urmare, *sine imperio*). Prin urmare, în principiu, prelucrarea datelor care fac obiectul acestui litigiu nu este exclusă din domeniul de aplicare al Directivei 95/46.

23 — Directiva 95/46 nu se aplică „prelucrărilor care au ca obiect siguranța publică, apărarea, securitatea statului [...] *și activitățile statului în domeniul dreptului penal*” (sublinierea noastră).

83. Astfel cum a statuat Curtea în Hotărârea Lindqvist [24], activitățile menționate la articolul 3 alineatul (2) din Directiva 95/46 „sunt, în toate cazurile, activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor” [25]. Având în vedere că prelucrarea datelor în discuție îi revine celui care, în pofida calității sale de autoritate publică, acționează în realitate ca persoană privată, Directiva 95/46 este aplicabilă.

84. Instanța de trimitere subliniază scopul principal pe care administrația germană îl urmărește prin înregistrarea adreselor IP dinamice, și anume, „garantarea și menținerea securității și a bunei funcționări a serviciilor sale de telecomunicații” și în special promovarea „detectării și a protecției împotriva frecventelor atacuri de tipul «denial of service», în cadrul cărora infrastructura de telecomunicații este paralizată prin asaltarea deliberată și coordonată a anumitor servere de rețea cu un număr mare de cereri” [26]. Păstrarea adreselor IP dinamice în acest scop este obișnuită pentru orice titular de site-uri internet de o anumită importanță și nu presupune, direct sau indirect, exercitarea autorității publice, astfel încât includerea acestor date în domeniul de aplicare al Directivei 95/46 nu implică dificultăți majore.

85. Cu toate acestea, Bundesgerichtshof (Curtea Federală de Justiție) susține că păstrarea adreselor IP dinamice de către furnizorii de servicii din procedura principală are de asemenea ca scop să contribuie la urmărirea penală, dacă este cazul, a autorilor eventualelor atacuri cibernetice. Acest scop este suficient pentru a exclude prelucrarea datelor respective din domeniul de aplicare al Directivei 95/46?

86. În opinia noastră, dacă „urmărire penală” înseamnă exercitarea *ius puniendi* aparținând statului de către furnizorii de servicii care au calitatea de pârâți în procedura principală, ar fi vorba despre o „activitate a statului în domeniul dreptului penal” și, prin urmare, despre una dintre excepțiile prevăzute la articolul 3 alineatul (2) prima liniuță din Directiva 95/46.

87. În aceste împrejurări, potrivit jurisprudenței stabilite de Curte în cauza Huber [27], prelucrarea datelor cu caracter personal de către furnizorii de servicii din motive de securitate și de funcționare tehnică a serviciilor de telecomunicații ale acestora s-ar încadra în domeniul de aplicare al Directivei 95/46, în timp ce prelucrarea de date care vizează activitatea statului în domeniul penal nu ar intra sub incidența acestuia.

88. În mod analog, chiar dacă urmărirea penală propriu-zisă nu ar fi de competența Republicii Federale Germania în calitate de simplu furnizor de servicii care nu acționează în exercitarea puterii publice, iar aceasta s-ar limita, ca orice particular, la transmiterea adreselor IP în litigiu către un organ de stat în vederea efectuării urmăririi penale, prelucrarea adreselor IP dinamice ar avea de asemenea ca obiect o activitate exclusă din domeniul de aplicare al Directivei 95/46.

24 — Hotărârea din 6 noiembrie 2003 (C-101/01, EU:C:2003:596, punctul 43).

25 — În același sens, Hotărârea din 16 decembrie 2008, Satakunnan Markkinapörssi și Satamedia (C-73/07, EU:C:2008:727, punctul 41).

26 — Punctul 36 din ordonanța de trimitere.

27 — Hotărârea din 16 decembrie 2008 (C-524/06, EU:C:2008:724, punctul 45).

89. Astfel, rezultă din jurisprudența stabilită în cauza Parlamentul/Consiliul și Comisia [28], în care Curtea a statuat că faptul că anumite date cu caracter personal „sunt colectate de operatori privați în scopuri comerciale și că aceștia sunt cei care organizează transferul lor către o țară terță” nu înseamnă că acest transfer „nu face parte din domeniul de aplicare” al articolului 3 alineatul 2 a doua liniuță din Directiva 95/46 atunci când obiectivul său privește activitățile statului în domeniul dreptului penal, cu toate că în acest caz „se înscrie într-un cadru instituit de autoritățile publice și care vizează protecția siguranței publice” [29].

90. Dacă, dimpotrivă, astfel cum considerăm, prin „urmărire penală” trebuie să se înțeleagă, după cum rezultă din ordonanța de trimitere, o procedură specifică unui particular care are calitate de persoană autorizată să inițieze procedura de *ius puniendi* aparținând statului, prin acțiunea corespunzătoare, atunci nu se poate susține că prelucrarea adreselor IP dinamice are ca obiect activitatea statului în domeniul dreptului penal, care este exclusă din domeniul de aplicare al Directivei 95/46.

91. Astfel, păstrarea și înregistrarea acestor date ar servi ca mijloc de probă suplimentar prin intermediul căruia titularul paginii web poate solicita statului, la cererea părții, urmărirea penală a unui comportament ilicit. În definitiv, acestea ar constitui un instrument de apărare, pe cale penală, a drepturilor conferite de ordinea juridică unei persoane particulare (în acest caz, unei entități publice care acționează în regim de drept privat). Din această perspectivă, ele nu se diferențiază de inițiativa oricărui alt furnizor de servicii de internet care urmărește să fie protejat de stat în conformitate cu procedurile de exercitare a acțiunii penale, prevăzute de ordinea juridică.

92. În consecință, dacă administrația germană acționează în calitate de furnizor de servicii de internet lipsit de autoritate publică, aspect care trebuie apreciat de instanța de trimitere, prelucrarea pe care o efectuează acesta în privința adreselor IP dinamice, ca date cu caracter personal, este inclusă în domeniul de aplicare al Directivei 95/46.

2. Cu privire la fond

93. Articolul 15 alineatul 1 din TMG autorizează colectarea și utilizarea datelor cu caracter personal ale unui utilizator numai atunci când acestea sunt necesare pentru a permite și a factura folosirea efectivă a serviciului de telecomunicații. Mai exact, furnizorul de servicii poate colecta și utiliza numai așa-numitele „date de utilizare”, și anume datele cu caracter personal ale unui utilizator care sunt indispensabile pentru a permite „utilizarea și facturarea serviciilor de telecomunicații”. Aceste date trebuie eliminate imediat după încheierea sesiunii (cu alte cuvinte imediat după ce se încheie utilizarea efectivă a serviciului de telecomunicații), cu excepția cazului în care trebuie păstrate „în vederea facturării”, în conformitate cu dispozițiile articolului 15 alineatul 4 din TMG.

94. După încheierea conexiunii, articolul 15 din TMG pare să nu permită păstrarea datelor de utilizare din alte motive, inclusiv pentru a asigura „utilizarea serviciilor de telecomunicații” cu caracter general. Atunci când se referă exclusiv la scopurile de facturare drept motiv justificativ pentru păstrarea datelor, dispoziția respectivă din TMG ar putea fi interpretată (deși interpretarea sa definitivă este de competența instanței de trimitere) în sensul că impune folosirea datelor de utilizare numai pentru a face posibilă o utilizare concretă și eliminarea lor odată cu încheierea acesteia.

28 — Hotărârea din 30 mai 2006 (C-317/04 și C-318/04, EU:C:2006:346, punctele 54-59).

29 — *Ibidem*, punctul 59. Era vorba de date cu caracter personal a căror prelucrare nu era necesară pentru furnizarea serviciilor care reprezenta activitatea operatorilor privați afectați (companii aeriene), dar pe care aceștia erau obligați să le transmită autorităților americane în scopul prevenirii și al combaterii terorismului.

95. Articolul 7 litera (f) din Directiva 95/46 [30] permite prelucrarea datelor cu caracter personal în termeni pe care îi considerăm mai permisivi (pentru operator) decât cei prevăzuți în cuprinsul articolului 15 din TMG. Din această perspectivă, norma germană poate fi considerată mai restrictivă decât reglementarea Uniunii, deoarece, în principiu, nu prevede satisfacerea altui interes legitim decât cel privind facturarea serviciului, astfel încât Republica Federală Germania, în calitate de furnizor de servicii de internet, ar putea să aibă de asemenea un interes legitim în ceea ce privește asigurarea bunei funcționări a paginilor sale web, care depășește fiecare utilizare concretă [31].

96. Jurisprudența stabilită de Curte în Hotărârea ASNEF și FECEMD [32] furnizează orientările necesare pentru oferirea unui răspuns la cea de a doua întrebare preliminară. În această cauză, Curtea a statuat că din obiectivul urmărit de Directiva 95/46 „rezultă că articolul 7 din Directiva 95/46 prevede o listă exhaustivă și limitativă de cazuri în care o prelucrare de date cu caracter personal poate fi considerată ca fiind legală” [33]. Prin urmare, „statele membre nu pot nici să adauge principii noi privind legitimarea prelucrărilor de date cu caracter personal la articolul 7 din Directiva 95/46, nici să prevadă cerințe suplimentare care să modifice conținutul unuia dintre cele șase principii prevăzute la acest articol” [34].

97. Articolul 15 din TMG nu adaugă o condiție suplimentară față de cele prevăzute la articolul 7 din Directiva 95/46 pentru ca prelucrarea datelor să fie considerată legală – precum în cazul Hotărârii ASNEF și FECEMD [35] –, însă, dacă acesta este interpretat în sensul restrictiv pe care îl propune instanța *a quo*, conținutul condiției prevăzute la litera (f) a dispoziției respective este redus: acolo unde legiuitorul Uniunii face referire, cu caracter general, la realizarea „[…] interesului legitim urmărit de operator sau de către unul sau mai mulți terți”, articolul 15 din TMG vizează doar necesitatea „de a permite utilizarea [concretă] și facturarea serviciilor de telecomunicații”.

98. La fel ca în cauzele ASNEF și FECEMD [36], și în prezenta cauză o măsură națională – din nou, dacă se optează pentru interpretarea restrictivă expusă anterior – ar modifica domeniul de aplicare al principiului prevăzut la articolul 7 din Directiva 95/46 și nu s-ar rezuma doar la explicitarea sa, acesta fiind singurul aspect în privința căruia autoritățile fiecărui stat membru dispun de o anumită marjă de apreciere, în conformitate cu articolul 5 din Directiva 95/46.

99. Astfel, conform acestei din urmă prevederi, „statele membre precizează, în limitele dispozițiilor prezentului capitol[[37]], condițiile în care operațiunile de prelucrare a datelor cu caracter personal sunt legale”. Cu toate acestea, după cum a statuat Curtea în cauzele ASNEF și FECEMD [38], „în temeiul [prevederii respective], statele membre nu pot nici să introducă alte principii referitoare la legitimarea operațiunilor de prelucrare a datelor cu caracter personal decât cele prevăzute la articolul 7 din această directivă, nici să modifice, prin cerințe suplimentare, conținutul celor șase principii prevăzute la articolul 7 menționat”.

30 — Reprodus la punctul 17.

31 — A se vedea punctul 84. Desigur, titularii paginilor web au un interes legitim în ceea ce privește prevenirea și combaterea blocărilor accesului („denials of service”) menționate de instanța de trimitere, cu alte cuvinte a atacurilor masive săvârșite uneori în mod concertat împotriva anumitor site-uri internet cu scopul de a le suprasolicita și a le face inoperante.

32 — Hotărârea din 24 noiembrie 2011 (C-468/10 și C-469/10, EU:C:2011:777).

33 — *Ibidem*, punctul 30.

34 — *Ibidem*, punctul 32.

35 — În această cauză, legislația națională adăuga, printre condițiile prevăzute la articolul 7 litera (f) din Directiva 95/46, faptul că datele care fac obiectul prelucrării trebuie să figureze în surse accesibile publicului.

36 — Hotărârea din 24 noiembrie 2011 (C-468/10 și C-469/10, EU:C:2011:777).

37 — Capitolul II, intitulat „Condițiile generale de legalitate a prelucrării datelor cu caracter personal”, în cuprinsul căruia se regăsesc articolele 5-21 din Directiva 95/46.

38 — Hotărârea din 24 noiembrie 2011 (C-468/10 și C-469/10, EU:C:2011:777, punctul 36).

100. Articolul 15 din TMG ar reduce în mod considerabil, în raport cu articolul 7 litera (f) din Directiva 95/46, întinderea interesului legitim relevant pentru justificarea prelucrării datelor, fără a se limita la clarificarea sau la nuanțarea acestuia în contextul limitelor permise de articolul 5 din aceeași directivă. În plus, ar fi vorba despre o reducere categorică și absolută, care nu ar permite ca protecția și garantarea utilizării generale a serviciului de telecomunicații să facă obiectul unei evaluări comparative privind „interesul sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protecție în temeiul articolului 1 alineatul (1)” din Directiva 95/46, astfel cum prevede articolul 7 litera (f) din aceasta.

101. În definitiv, la fel ca în cauzele ASNEF și FECEMD [39], legiuitorul național a stabilit „în mod definitiv […] rezultat[ul] ponderării drepturilor și intereselor opuse, [pentru anumite categorii de date cu caracter personal], fără a permite un rezultat diferit în funcție de împrejurările speciale ale unui caz concret”, astfel încât „nu mai este vorba despre o precizare în sensul articolului 5” din Directiva 95/46.

102. În aceste împrejurări, considerăm că Bundesgerichtshof (Curtea Federală de Justiție) trebuie să interpreteze legislația națională în conformitate cu Directiva 95/46, ceea ce presupune: a) că printre motivele care justifică prelucrarea așa-numitelor „date de utilizare” poate fi inclus interesul legitim al furnizorului de servicii de telecomunicații în vederea protejării utilizării generale a acestora și b) se poate efectua o evaluare comparativă, *ad casum*, privind acest interes al furnizorului serviciului și interesul sau drepturile și libertățile fundamentale ale utilizatorului, în vederea identificării persoanei care trebuie protejată în sensul articolului 1 alineatul (1) din Directiva 95/46 [40].

103. În opinia noastră, nu mai este nimic de adăugat cu privire la termenii în care trebuie să se efectueze această evaluare comparativă în litigiul aflat la originea trimiterii preliminare. Bundesgerichtshof (Curtea Federală de Justiție) nu adresează nicio întrebare referitoare la acest aspect, fiind preocupată de răspunsul la o întrebare prealabilă evaluării comparative, și anume dacă aceasta poate fi efectuată.

104. În sfârșit, este inutil să subliniem că instanța *a quo* va putea lua în considerare eventualele dispoziții legale adoptate de statul membru în cadrul autorizației prevăzute la articolul 13 alineatul (1) litera (d) din Directiva 95/46 pentru a restrânge domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolul 6 din aceeași directivă, dacă o astfel de restricție este necesară pentru a asigura printre altele „[…] prevenirea, investigarea, detectarea și punerea sub urmărire a infracțiunilor […]”. Instanța de trimitere nu face referire nici la această situație, având cunoștință, fără îndoială, despre existența ambelor articole.

105. Prin urmare, sugerăm să se răspundă la cea de a doua întrebare preliminară în sensul că articolul 7 litera (f) din Directiva 95/46 se opune unei reglementări naționale a cărei interpretare împiedică un furnizor de servicii să colecteze și să prelucreze datele cu caracter personal ale unui utilizator fără consimțământul acestuia, cu scopul de a asigura funcționarea serviciului de telecomunicații, după încheierea fiecărei sesiuni de utilizare.

39 — *Ibidem*, punctul 47.

40 — În ședință, reprezentantul domnului Breyer a contestat faptul că înregistrarea adreselor IP dinamice este necesară pentru a proteja buna funcționare a serviciilor de internet față de posibile atacuri. În opinia noastră, această problemă nu poate fi soluționată în termeni absoluți, ci, dimpotrivă, răspunsul trebuie să fie precedat, în fiecare caz, de evaluarea comparativă a interesului titularului site-ului internet și a drepturilor și intereselor utilizatorilor.

VI – **Concluzie**

106. Având în vedere considerațiile anterioare, propunem Curții să răspundă la întrebările preliminare adresate după cum urmează:

„1) Conform articolului 2 litera (a) Directiva 95/46/CE a 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, o adresă IP dinamică prin intermediul căreia un utilizator a accesat pagina web a unui furnizor de servicii de telecomunicații constituie pentru acesta din urmă o «dată cu caracter personal» în măsura în care un furnizor de acces la rețea deține informații suplimentare care, dacă sunt asociate cu adresa IP dinamică, permit identificarea utilizatorului.

2) Articolul 7 litera (f) din Directiva 95/46 trebuie interpretat în sensul că obiectivul privind asigurarea funcționării serviciului de telecomunicații poate fi considerat, în principiu, drept un interes legitim, a cărui realizare justifică prelucrarea acestei date cu caracter personal, sub rezerva analizei privind prevalența sa asupra interesului sau a drepturilor fundamentale ale persoanei vizate. O dispoziție națională care nu ar permite să se ia în considerare interesul legitim ar fi incompatibilă cu articolul menționat.”