Orientările 2/2023 privind domeniul tehnic de aplicare al articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice

Versiunea 2.0

Adoptate la 7 octombrie 2024

Istoricul versiunilor

Versiunea 1.0	14 noiembrie 2023	Adoptarea orientărilor pentru consultare publică
Versiunea 2.0	7 octombrie 2024	Adoptarea orientărilor în urma consultării publice

Rezumat

În prezentele orientări, CEPD abordează aplicabilitatea articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice în cazul unor soluții tehnice diferite. Prezentele orientări explică în mod detaliat Avizul nr. 9/2014 al Grupului de lucru „Articolul 29" referitor la aplicarea Directivei privind viața privată și comunicațiile electronice în ceea ce privește amprentarea dispozitivelor (*device fingerprinting*) și au scopul de a asigura o înțelegere clară a operațiunilor tehnice care intră sub incidența articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice.

Apariția unor metode de urmărire noi, atât pentru a înlocui instrumentele de urmărire existente (de exemplu, modulele cookie, din cauza întreruperii suportului pentru modulele cookie de la terți de către unii furnizori de browsere), cât și pentru a crea noi modele de afaceri, a devenit o preocupare majoră în ceea ce privește protecția datelor. În timp ce aplicabilitatea articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice este bine stabilită și implementată în cazul anumitor tehnologii de urmărire, cum ar fi modulele cookie, este necesar să se soluționeze ambiguitățile legate de aplicarea dispoziției menționate în cazul instrumentelor de urmărire emergente.

Orientările identifică trei elemente-cheie pentru aplicabilitatea articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice (secțiunea 2.1), și anume „informații", „echipamentul terminal al unui abonat sau utilizator" și „dobândirea accesului", „stocarea de informații" și „informații stocate". Orientările oferă și o analiză detaliată a fiecărui element (secțiunile 2.2-2.6).

În secțiunea 3, această analiză se aplică unei liste neexhaustive de cazuri de utilizare care reprezintă tehnici comune, și anume:

- Urmărirea prin URL și pixeli
- Prelucrarea locală
- Urmărirea bazată exclusiv pe IP
- Raportarea intermitentă și mediată prin internetul obiectelor (IoT)
- Identificatorul unic

Cuprins

Comitetul european pentru protecția datelor,

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul 2016/679/UE al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolul 15 alineatul (3) 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, astfel cum a fost modificată prin Directiva 2009/136/CE (denumită în continuare „Directiva privind viața privată și comunicațiile electronice” sau „ePD”),

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

ADOPTĂ URMĂTOARELE ORIENTĂRI:

1 INTRODUCERE

1. În conformitate cu articolul 5 alineatul (3) din ePD, *„stocarea de informații sau dobândirea accesului la informațiile deja stocate în echipamentul terminal al unui abonat sau utilizator”* este permisă doar pe bază de consimțământ sau de necesitate în scopuri specifice stabilite în articolul respectiv. După cum se amintește în considerentul 24 din ePD[2], scopul dispoziției respective este de a proteja echipamentul terminal al utilizatorilor, deoarece acesta face parte din sfera privată a utilizatorilor. Din formularea articolului rezultă că articolul 5 alineatul (3) din ePD nu se aplică exclusiv modulelor cookie, ci și „tehnologiilor similare”. Cu toate acestea, în prezent nu există o listă cuprinzătoare a operațiunilor tehnice care intră sub incidența articolului 5 alineatul (3) din ePD.

2. Avizul nr. 9/2014 al Grupului de lucru „Articolul 29” privind aplicarea Directivei privind viața privată și comunicațiile electronice în ceea ce privește amprentarea dispozitivelor (*device fingerprinting*) (denumit în continuare «Avizul nr. 9/2014 al Grupului de lucru „Articolul 29”») a clarificat deja că amprentarea se încadrează în domeniul tehnic de aplicare al articolului 5 alineatul (3) din ePD[3], însă, din cauza noilor progrese tehnologice, sunt necesare orientări suplimentare cu privire la tehnicile de urmărire observate în prezent. Peisajul tehnic a evoluat în ultimul deceniu, cu utilizarea tot mai frecventă a identificatorilor încorporați în sistemele de operare, precum și cu crearea unor noi instrumente care permit stocarea informațiilor în echipamentul terminal.

[1] Trimiterile la „statele membre” din acest document trebuie înțelese ca trimiteri la „statele membre ale SEE”.
[2] „Echipamentul terminal al utilizatorului de rețele de comunicații electronice și orice informație stocată în acesta fac parte din sfera privată a utilizatorului protejată conform Convenției europeane pentru apărarea drepturilor omului și a libertăților fundamentale. Așa-numitele spyware, web bugs, hidden identifiers și alte procedee similare pot să acceseze terminalul utilizatorului fără știrea acestuia și să acceadă la informații, să copieze informații ascunse sau să urmărească activitatea utilizatorului și pot încălca flagrant confidențialitatea datelor acestor utilizatori. Folosirea de astfel de procedee trebuie permisă doar în scopuri legitime, cu informarea utilizatorilor în cauză.”
[3] Avizul nr. 9/2014 al Grupului de lucru „Articolul 29”, p. 11.

3. Ambiguitățile privind domeniul de aplicare al articolului 5 alineatul (3) din ePD au creat stimulente pentru punerea în aplicare de soluții alternative de urmărire a utilizatorilor de internet și au condus la o tendință de eludare a obligațiilor legale prevăzute la articolul 5 alineatul (3) din ePD. Toate aceste situații generează preocupări și necesită o analiză suplimentară pentru a completa orientările anterioare ale CEPD.

4. Scopul prezentelor orientări este de a efectua o analiză tehnică a domeniului de aplicare al articolului 5 alineatul (3) din ePD, și anume de a clarifica ce acoperă din punct de vedere tehnic sintagma *„a stoca sau a accesa informații stocate în echipamentul terminal al unui abonat sau utilizator*". Prezentele orientări nu abordează circumstanțele în care o operațiune de prelucrare poate intra în domeniul de aplicare al exceptărilor de la cerința de consimțământ prevăzute de ePD[4], deoarece aceste circumstanțe ar trebui analizate de la caz la caz, ținând seama de transpunerea (transpunerile) din statul membru relevant și de orientările emise de autoritățile naționale competente.

5. În partea finală a prezentelor orientări va fi analizată o listă neexhaustivă de cazuri de utilizare specifice.

2 ANALIZĂ

2.1 Elemente-cheie pentru aplicabilitatea articolului 5 alineatul (3) din ePD

6. Articolul 5 alineatul (3) din ePD se aplică în cazul în care:

   a. **CRITERIUL A:** operațiunile efectuate se referă la *„informații*". Ar trebui remarcat faptul că termenul utilizat nu este „date cu caracter personal", ci „informații".

   b. **CRITERIUL B:** operațiunile efectuate implică un *„echipament terminal*" al unui abonat sau utilizator (B.1), ceea ce implică necesitatea de a evalua noțiunea de *rețea de comunicații publice*" (B.2).

   c. **CRITERIUL C:** operațiunile efectuate constituie într-adevăr *„stocare*" (C.1) sau *„dobândire a accesului"* (C.2). Aceste două noțiuni pot fi analizate independent, astfel cum se reamintește în Avizul nr. 9/2014 al Grupului de lucru „Articolul 29": *«Utilizarea cuvintelor „stocate sau accesate" indică faptul că nu este necesar ca stocarea și accesul să aibă loc în cadrul aceleiași comunicări sau să fie realizate de aceeași parte»*[5].

   Din motive de claritate, entitatea care dobândește acces la informațiile stocate în echipamentul terminal al utilizatorului va fi denumită în continuare „entitatea care accesează informațiile".

2.2 Noțiunea de „informații" – Criteriul A

7. Astfel cum se indică la CRITERIUL A, această secțiune detaliază ce acoperă noțiunea de „informații". Alegerea termenului „informații", care cuprinde o categorie mai largă decât simpla noțiune de „date cu caracter personal", este legată de domeniul de aplicare al Directivei privind viața privată și comunicațiile electronice.

[4] Astfel cum se prevede la articolul 5 alineatul (3) din ePD: *„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.*"

[5] Avizul nr. 9/2014 al Grupului de lucru „Articolul 29", p. 8.

8. Scopul articolului 5 alineatul (3) din ePD este de a proteja sfera privată a utilizatorilor, astfel cum se menționează în considerentul 24 al acesteia: *„Echipamentul terminal al utilizatorului de rețele de comunicații electronice și orice informație stocată în acesta fac parte din sfera privată a utilizatorului protejată conform Convenției Europene pentru Protecția Drepturilor Omului și a Libertăților Fundamentale*". Aceasta este protejată și de articolul 7 din Carta drepturilor fundamentale a UE.

9. De fapt, scenariile care pătrund în această sferă privată, chiar și fără a implica date cu caracter personal, sunt acoperite în mod explicit de formularea articolului 5 alineatul (3) din ePD și de cea a considerentului 24 al acesteia, de exemplu stocarea de viruși pe echipamentul terminal al utilizatorului. Acest lucru arată că definiția termenului „informații" nu ar trebui să se limiteze la caracteristica de a avea legătură cu o persoană fizică identificată sau identificabilă.

10. Acest lucru a fost confirmat de Curtea de Justiție a Uniunii Europene: *„Această protecție se aplică oricărei informații stocate pe acest echipament terminal, indiferent dacă este vorba sau nu despre date cu caracter personal, și urmărește printre altele, astfel cum reiese din același considerent, să protejeze utilizatorii împotriva riscului ca hidden identifiers sau alte procedee similare să acceseze echipamentul terminal al acestor utilizatori fără știrea lor*"[6].

11. Întrebările referitoare la măsura în care originea acestor informații și motivele pentru care acestea sunt stocate în echipamentul terminal ar trebui luate în considerare atunci când se evaluează aplicabilitatea articolului 5 alineatul (3) din ePD au fost clarificate anterior. De exemplu, în Avizul nr. 9/2014 al Grupului de lucru „Articolul 29": *„Nu este corect să se interpreteze această situație ca o lipsă a obligației părții terțe de a obține consimțământul utilizatorului pentru a avea acces la aceste informații, doar pentru că nu ea este cea care le-a și stocat. Cerința privind consimțământul se aplică, de asemenea, în cazul în care se accesează o valoare care are doar drept de citire (de exemplu, solicitarea adresei MAC a unei interfețe de rețea prin intermediul API-ului SO)*"[7].

12. În concluzie, noțiunea de „informații" include atât date fără caracter personal, cât și date cu caracter personal, indiferent de modul în care aceste date au fost stocate și de către cine, și anume de către o entitate externă (inclusiv alte entități decât cea care are acces), de către utilizator, de către un producător sau în orice alt scenariu.

2.3 Noțiunea de „echipament terminal al unui abonat sau utilizator" – Criteriul B.1

13. Această secțiune se bazează pe definiția utilizată în Directiva 2008/63/CE și la care se face trimitere în articolul 2 din Directiva (UE) 2018/1972, în care „echipamentul terminal" este definit ca: *„echipamentul racordat în mod direct sau indirect la interfața unei rețele publice de telecomunicații, în scopul trimiterii, prelucrării sau recepționării de informații; în ambele cazuri de racordare (directă sau indirectă), aceasta se poate efectua prin cablu, fibre optice sau electromagnetic; racordarea este indirectă atunci când echipamentul este amplasat între terminal și interfața rețelei*"[8].

14. Considerentul 24 din ePD oferă o înțelegere clară a rolului echipamentului terminal pentru protecția oferită de articolul 5 alineatul (3) din ePD. ePD protejează viața privată a utilizatorilor nu numai în ceea ce privește confidențialitatea informațiilor lor, ci și prin protejarea integrității echipamentului terminal al utilizatorului. Această înțelegere va ghida interpretarea noțiunii de „echipament terminal" în cuprinsul prezentelor orientări.

[6] Hotărârea Curții de Justiție din 1 octombrie 2019, Planet49, cauza C-673/17, ECLI:EU:C:2019:801, punctul 70.
[7] Avizul nr. 9/2014 al Grupului de lucru „Articolul 29", p. 8.
[8] Directiva 2008/63/CE a Comisiei din 20 iunie 2008 privind concurența pe piețele echipamentelor terminale pentru telecomunicații (versiune codificată), articolul 1 punctul 1.

15. Articolul 3 din ePD prevede că, pentru ca directiva să se aplice, prelucrarea de date cu caracter personal trebuie să fie efectuată în legătură cu furnizarea de servicii de comunicații electronice destinate publicului prin intermediul rețelelor publice de comunicații. Acest lucru implică faptul că un dispozitiv trebuie să poată fi utilizat în legătură cu serviciul respectiv și că, pentru a fi considerat echipament terminal, trebuie să fie conectat sau să poată fi conectat[9] la interfața unei rețele publice de comunicații. CEPD observă că modificările aduse în 2009[10] textului articolului 5 alineatul (3) din ePD au extins protecția echipamentului terminal prin eliminarea trimiterii la „folosirea rețelelor de comunicații electronice" ca mijloc de stocare a informațiilor sau de dobândire a accesului la informațiile stocate în echipamentul terminal. Prin urmare, atât timp cât un dispozitiv are o interfață de rețea care îl face eligibil pentru conectare (chiar dacă această conexiune nu există), articolul 5 alineatul (3) din ePD se aplică fiecărei entități care ar stoca și ar dobândi accesul la informațiile deja stocate în echipamentul terminal, indiferent de mijloacele de acces la echipamentul terminal și indiferent dacă acesta este conectat sau deconectat de la o rețea.

16. Echipamentele care fac parte chiar din rețeaua publică de comunicații electronice nu ar fi considerate echipamente terminale în temeiul articolului 5 alineatul (3) din ePD[11].

17. Un echipament terminal poate fi format din orice număr de echipamente hardware individuale, care împreună formează echipamentul terminal. Acesta poate lua sau nu forma unui dispozitiv închis fizic care găzduiește toate echipamentele hardware de afișare, prelucrare, stocare și periferice (de exemplu, telefoane inteligente, laptopuri, dispozitive de stocare conectate la rețea, automobile conectate sau televizoare conectate, ochelari inteligenți).

18. ePD recunoaște că protecția confidențialității informațiilor stocate în echipamentul terminal al unui utilizator și integritatea echipamentului terminal al utilizatorului nu se limitează la protecția sferei private a persoanelor fizice, ci vizează și dreptul la respectarea corespondenței acestora sau a intereselor legitime ale persoanelor juridice[12]. Ca atare, un echipament terminal care permite realizarea acestei corespondențe și a intereselor legitime ale persoanelor juridice este protejat în temeiul articolului 5 alineatul (3) din ePD.

19. Utilizatorul sau abonatul poate deține sau închiria sau poate să primească în alt mod echipamentul terminal. Mai mulți utilizatori sau abonați pot folosi în comun același echipament terminal.

20. Această protecție este garantată de ePD pentru echipamentul terminal asociat utilizatorului sau abonatului și nu depinde de stabilirea mijloacelor de acces de către utilizator (de exemplu, dacă a inițiat comunicațiile electronice) sau chiar de cunoașterea mijloacelor de acces respective de către utilizator).

[9] Adică să dispună de capacitățile tehnice necesare pentru a fi conectat la rețea, chiar dacă această conexiune nu există în prezent.

[10] Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului (Text cu relevanță pentru SEE), JO L 337, 18.12.2009, articolul 2 punctul 5 și considerentul 65.

[11] Pentru a identifica limitele rețelei în diferite contexte, consultați Orientările OAREC privind abordări comune de identificare a punctului terminal al rețelei în diferitele topologii de rețea [BoR (20) 46].

[12] Într-adevăr, astfel cum se reamintește la articolul 2 punctul 13 din Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice, utilizatorul poate fi o persoană fizică sau juridică.

2.4 Noțiunea de „rețea publică de comunicații” – Criteriul B.2

21. Întrucât situația reglementată de ePD este cea legată de „*furnizarea de servicii de comunicații electronice destinate publicului prin intermediul rețelelor publice de comunicații din cadrul Comunității*”[13], iar definiția unui echipament terminal menționează în mod specific noțiunea de „*rețea publică de comunicații*”, este esențial să se clarifice această noțiune pentru a identifica contextul în care se aplică articolul 5 alineatul (3) din ePD.

22. Noțiunea de rețea de comunicații electronice nu este definită în cadrul ePD în sine. Acest concept a fost menționat inițial în Directiva 2002/21/CE (directiva-cadru) privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice[14], înlocuit ulterior de articolul 2 punctul 1 din Directiva (UE) 2018/1972 (Codul european al comunicațiilor electronice). Acesta are, în prezent, următorul conținut:

> *„rețea de comunicații electronice” înseamnă sisteme de transmisie, indiferent dacă sunt bazate sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată, și, după caz, echipamente de comutare sau de rutare și alte resurse, inclusiv elemente de rețea care nu sunt active, care permit transmiterea semnalelor prin cablu, unde radio, prin mijloace optice sau prin alte mijloace electromagnetice, inclusiv rețele de comunicații prin satelit, rețele fixe (cu comutare de circuite și cu comutare de pachete, inclusiv internet) și mobile, rețele electrice, în măsura în care sunt utilizate pentru transmiterea de semnale, rețele utilizate pentru difuzarea programelor de radio și de televiziune și rețele de televiziune prin cablu, indiferent de tipul de informație transmisă*[15].

23. Această definiție este neutră în ceea ce privește tehnologiile de transmisie. Conform acestei definiții, o rețea de comunicații electronice este orice sistem de rețea care permite transmisia semnalelor electronice între nodurile sale, indiferent de echipamentul și protocoalele utilizate.

24. Noțiunea de rețea de comunicații electronice în temeiul Directivei (UE) 2018/1972 nu depinde de caracterul public sau privat al infrastructurii, și nici de modul în care este instalată sau gestionată rețeaua (*„indiferent dacă sunt bazate sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată”*[16]). Prin urmare, definiția rețelei de comunicații electronice, prevăzută la articolul 2 din Directiva (UE) 2018/1972, este suficient de amplă pentru a acoperi orice tip de infrastructură. Aceasta include rețele gestionate sau nu de un operator, rețele co-gestionate de un grup de operatori sau chiar rețele ad-hoc în care un echipament terminal se poate alătura sau poate părăsi în mod dinamic o rețea de alte echipamente terminale care utilizează protocoale de transmisie pe o rază mică de acțiune.

25. Această definiție a rețelei nu prevede nicio limitare cu privire la numărul de echipamente terminale prezente în rețea în orice moment. Unele scheme de interconectare se bazează pe noduri care transmit informații în mod ad-hoc către nodurile conectate în prezent[17] și pot, la un moment dat, să asigure

[13] Articolul 3 din ePD.
[14] Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (directiva-cadru).
[15] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (reformare) (Text cu relevanță pentru SEE), articolul 2 punctul 1.
[16] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (reformare) (Text cu relevanță pentru SEE), articolul 2 punctul 1.
[17] De exemplu, în contextul schemelor de interconectare tolerante la întârziere care implementează „tehnici de stocare și redirecționare", cum ar fi proiectul cu sursă deschisă Briar.

comunicarea doar între două noduri pereche. Astfel de cazuri s-ar încadra în domeniul general de aplicare al ePD, atât timp cât protocolul de rețea permite includerea ulterioară a nodurilor pereche.

26. Disponibilitatea publică a rețelei de comunicații este necesară pentru ca dispozitivul să fie considerat un echipament terminal și, în consecință, pentru ca articolul 5 alineatul (3) din ePD să fie aplicabil. Trebuie remarcat faptul că punerea la dispoziție a rețelei pentru o subcategorie limitată a publicului (de exemplu, abonații, indiferent dacă plătesc sau nu, sub rezerva condițiilor de eligibilitate) nu face ca rețeaua respectivă să fie privată[18].

2.5 Noțiunea de „dobândire a accesului” – Criteriul C.1

27. Pentru a încadra în mod corect noțiunea de „dobândire a accesului”, este important să se ia în considerare domeniul de aplicare al ePD, prevăzut la articolul 1 din ePD: „*în vederea asigurării unui nivel echivalent de protecție a drepturilor și libertăților fundamentale, mai ales a dreptului la confidențialitatea datelor personale, în domeniul prelucrării de date personale în sectorul comunicațiilor electronice și a liberei circulații a acestor date și a serviciilor și echipamentelor de comunicații electronice în interiorul Comunității*”.

28. Pe scurt, ePD este un instrument juridic de protejare a confidențialității datelor, menit să protejeze confidențialitatea comunicațiilor și integritatea dispozitivelor. În considerentul 24 din ePD, se clarifică faptul că, în cazul persoanelor fizice, echipamentul terminal al utilizatorului face parte din sfera privată a utilizatorului și că accesul la informațiile stocate pe echipament fără știrea utilizatorului poate încălca flagrant confidențialitatea datelor acestuia.

29. Și persoanele juridice sunt protejate de ePD[19]. În consecință, noțiunea de „dobândire a accesului” prevăzută la articolul 5 alineatul (3) din ePD trebuie să fie interpretată astfel încât să protejeze aceste drepturi împotriva încălcării de către terțe părți.

30. Stocarea informațiilor sau dobândirea accesului pot fi operațiuni independente și pot fi efectuate de către entități independente. Pentru ca articolul 5 alineatul (3) din ePD să se aplice, nu este necesar să existe atât stocarea informațiilor, cât și accesul la informațiile deja stocate.

31. Astfel cum se observă în Avizul nr. 9/2014 al Grupului de lucru „Articolul 29”: «*Utilizarea cuvintelor „stocate sau accesate” indică faptul că nu este necesar ca stocarea și accesul să aibă loc în cadrul aceleiași comunicări sau să fie realizate de aceeași parte. Informațiile care sunt stocate de către una dintre părți (inclusiv informațiile stocate de către utilizator sau de către fabricantul dispozitivului) și care sunt accesate ulterior de către o altă parte intră, prin urmare, în sfera de aplicare a articolului 5 alineatul (3)*»[20]. În consecință, pentru ca noțiunea de acces să se aplice, nu există restricții privind originea informațiilor referitoare la echipamentul terminal.

32. Ori de câte ori o entitate ia măsuri pentru a dobândi acces la informațiile stocate în echipamentul terminal, se aplică articolul 5 alineatul (3) din ePD. De obicei, acest lucru presupune ca entitatea care accesează informațiile să trimită proactiv instrucțiuni specifice către echipamentul terminal, pentru a primi înapoi informațiile vizate. De exemplu, acesta este cazul modulelor cookie, în care entitatea care accesează informațiile dă instrucțiuni echipamentului terminal să trimită în mod proactiv informații la fiecare apel ulterior al Hypertext Transfer Protocol („HTTP”).

[18] Pentru o analiză suplimentară privind identificarea rețelelor publice de comunicații, vezi Orientările OAREC privind punerea în aplicare a Regulamentului privind internetul deschis [BoR (20) 112].
[19] Considerentul 26 din ePD, a se vedea punctul 17 de mai sus.
[20] Avizul nr. 9/2014 al Grupului de lucru „Articolul 29”, p. 8.

33. Același lucru este valabil și atunci când entitatea care accesează informațiile distribuie software pe echipamentul terminal al utilizatorului care este stocat și va apela apoi în mod proactiv un punct terminal al interfeței de programare a aplicațiilor („API”) prin rețea. Alte exemple ar include codul JavaScript, în care entitatea care accesează informațiile dă instrucțiuni browserului utilizatorului să trimită cereri asincrone cu informațiile vizate. Un astfel de acces se încadrează clar în domeniul de aplicare al articolului 5 alineatul (3) din ePD, deoarece entitatea care accesează informațiile dă instrucțiuni în mod explicit echipamentului terminal să trimită informațiile.

34. În unele cazuri, entitatea care dă instrucțiuni echipamentului terminal să trimită înapoi datele vizate și entitatea care primește informațiile ar putea să nu fie aceleași. Acest lucru poate rezulta din furnizarea și/sau utilizarea unui mecanism comun între cele două entități. Instruirea dispozitivului să trimită informații deja stocate (de exemplu, prin utilizarea unui protocol sau a unui SDK[21] ce implică trimiterea proactivă de informații de către echipamentul terminal) face posibilă o intruziune în echipamentul terminal, prin urmare, un astfel de acces declanșează aplicabilitatea articolului 5 alineatul (3) din ePD. Astfel cum se observă în Avizul nr. 9/2014 al Grupului de lucru „Articolul 29”, acest lucru poate fi valabil atunci când un site dă instrucțiuni echipamentului terminal să trimită informații către servicii de publicitate terțe prin includerea unui pixel de urmărire[22]. Acest caz de utilizare este dezvoltat în continuare în secțiunea 3.1.

2.6 Noțiunile de „stocare a informațiilor” și „informații stocate” – Criteriul C.2

35. Stocarea informațiilor în sensul articolului 5 alineatul (3) din ePD se referă la plasarea informațiilor pe un suport de stocare electronic fizic care face parte din echipamentul terminal[23] al unui utilizator sau abonat.

36. În mod tipic, informațiile nu sunt stocate în echipamentul terminal al unui utilizator sau abonat prin acces direct la memoria dispozitivului de către o altă parte, ci mai degrabă prin instruirea software-ului de pe echipamentul terminal de a genera informații specifice. Se consideră că stocarea ce are loc prin intermediul unor astfel de instrucțiuni este inițiată direct de cealaltă parte. Aceasta include utilizarea unor protocoale stabilite, cum ar fi stocarea de module cookie în browser, precum și software-ul personalizat, indiferent cine a creat sau a instalat protocoalele sau software-ul pe echipamentul terminal.

37. ePD nu stabilește nicio limită superioară sau inferioară privind durata în care informațiile trebuie să rămână pe un suport de stocare pentru a fi considerate stocate și nu există nici o limită superioară sau inferioară privind cantitatea de informații care trebuie stocate.

38. În mod similar, noțiunea de stocare nu depinde de tipul de suport pe care sunt stocate informațiile. Exemplele tipice ar include unitățile de hard disk („HDD”), unitățile SSD („SSD”), memoria numai pentru citire, programabilă, care poate fi ștearsă electric („EEPROM”) și memoria cu acces aleatoriu („RAM”), dar scenariile mai puțin tipice, care implică un suport precum banda magnetică sau cache-ul unității centrale de procesare („CPU”), nu sunt excluse din domeniul de aplicare. Suportul de stocare poate fi conectat intern (de exemplu, printr-o conexiune SATA) sau extern (de exemplu, printr-o conexiune USB).

[21] Un SDK („kit de dezvoltare de software”) este un set de instrumente de dezvoltare de software puse la dispoziție pentru a facilita crearea de aplicații software.
[22] Avizul nr. 9/2014 al Grupului de lucru „Articolul 29”, p. 9.
[23] Astfel cum este definit în secțiunea 2.3 din prezentele orientări.

39. „Informațiile stocate” se referă la informațiile existente deja pe echipamentul terminal, indiferent de sursa sau natura acestor informații. Acestea includ orice rezultat al stocării informațiilor în sensul articolului 5 alineatul (3) din ePD, astfel cum se descrie mai sus (fie de către aceeași parte care ar dobândi ulterior accesul, fie de către o altă terță parte). Acestea includ, de asemenea, rezultatele proceselor de stocare a informațiilor care nu intră în domeniul de aplicare al articolului 5 alineatul (3) din ePD, cum ar fi: stocarea pe echipamentul terminal chiar de către utilizator sau abonat ori de către un producător de hardware (cum ar fi adresele MAC ale controlerelor de interfață de rețea), senzorii integrați în echipamentul terminal sau procesele și programele executate pe echipamentul terminal, care pot sau nu să producă informații care depind de informațiile stocate sau sunt obținute din acestea.

3 CAZURI DE UTILIZARE

40. Astfel cum se subliniază în introducerea la prezentele orientări[24], acestea nu analizează aplicarea exceptărilor de la obligația de a obține consimțământul, prevăzută la articolul 5 alineatul (3) din ePD. CEPD reamintește că, pentru toate cazurile în care are loc stocarea de informații sau dobândirea accesului la informații deja stocate, ar trebui să se evalueze dacă este necesar consimțământul sau dacă s-ar putea aplica o exceptare în temeiul articolului 5 alineatul (3) din ePD. Prin urmare, cititorul trebuie să ia în considerare exceptările în cazul său de utilizare, împreună cu această analiză tehnică.

41. Fără a aduce atingere contextului specific în care pot fi utilizate acele categorii tehnice care sunt necesare pentru a stabili dacă articolul 5 alineatul (3) din ePD este aplicabil, este posibil să se identifice, într-o manieră neexhaustivă, categorii ample de identificatori și informații care sunt utilizate pe scară largă și care pot fi supuse aplicabilității articolului 5 alineatul (3) din ePD.

42. Comunicarea în rețea se bazează de obicei pe un model stratificat care necesită utilizarea unor identificatori pentru a permite stabilirea și desfășurarea corespunzătoare a comunicării. Instrucțiunea de comunicare a acestor identificatori către actorii de la distanță este transmisă prin intermediul unui software care respectă protocoalele de comunicare convenite. Astfel cum s-a subliniat mai sus, faptul că entitatea care primește informațiile ar putea să nu fie entitatea care dă instrucțiuni de transmitere a informațiilor nu exclude aplicarea articolului 5 alineatul (3) din ePD. Acest lucru poate să vizeze identificatori de rutare, cum ar fi adresa MAC sau IP a echipamentului terminal, dar și identificatori de sesiune (SSRC, identificator Websocket) sau dispozitive de autentificare electronică.

43. În același mod, protocolul de aplicare poate include mai multe mecanisme de furnizare a datelor contextuale (cum ar fi antetul HTTP, inclusiv câmpul „acceptare” sau agentul utilizator), mecanismul de înmagazinare cache (cum ar fi ETag[25]) sau alte funcționalități (modulele cookie fiind una dintre acestea sau HSTS[26]). Din nou, recurgerea la aceste mecanisme pentru a colecta informații (de exemplu, în contextul amprentării[27] sau al urmăririi identificatorilor de resurse) poate duce la aplicarea articolului 5 alineatul (3) din ePD.

[24] A se vedea punctul 4 de mai sus.
[25] HTTP ETag este un identificator care permite efectuarea de cereri condiționate pe baza validității datelor clientului memorate în cache.
[26] HTTP Strict Transport Security (HSTS) permite serverelor să specifice ce resurse trebuie solicitate întotdeauna prin conexiuni HTTPS.
[27] Astfel cum se observă în introducere, consultați Avizul nr. 9/2014 al Grupului de lucru „Articolul 29” privind aplicarea Directivei privind viața privată și comunicațiile electronice în ceea ce privește amprentarea dispozitivelor.

44. Pe de altă parte, există unele contexte în care aplicațiile locale instalate în echipamentul terminal utilizează unele informații strict în interiorul terminalului, după cum ar putea fi cazul interfețelor de programare a aplicațiilor pentru sistemul telefoanelor inteligente (acces la cameră, microfon, senzor GPS, cip accelerator, cip radio, acces la fișiere locale, listă de contacte, acces la identificatori etc.). Acest lucru ar putea fi valabil și pentru browserele care prelucrează informații stocate sau informații generate în interiorul dispozitivului (cum ar fi modulele cookie, stocarea locală, WebSQL sau chiar informațiile furnizate chiar de utilizatori). Utilizarea acestor informații de către o aplicație nu ar constitui o „[dobândire a] accesului la informațiile deja stocate" în sensul articolului 5 alineatul (3) din ePD, atât timp cât informațiile nu părăsesc dispozitivul, dar atunci când aceste informații sau orice informații derivate din acestea sunt accesate, se aplică articolul 5 alineatul (3) din ePD.

45. În sfârșit, în unele cazuri, actorii distribuie elemente de software malițios, de exemplu software de extracție de criptomonede sau, în general, programe malware, exploatând capacitățile de prelucrare ale echipamentului terminal în beneficiul actorului care le distribuie. Distribuirea respectivului software malițios în echipamentul terminal al utilizatorului ar constitui „stocare" în sensul articolului 5 alineatul (3) din ePD. În plus, în cazul în care software-ul stabilește o conexiune de rețea pentru a transmite informații într-o etapă ulterioară, aceasta ar constitui „dobândirea accesului" în sensul articolului 5 alineatul (3) din ePD.

46. Pentru un subansamblu al acestor categorii care prezintă un interes specific, fie din cauza utilizării lor pe scară largă, fie pentru că un studiu specific este justificat în ceea ce privește circumstanțele utilizării lor, este prezentată o analiză specifică mai jos.

3.1 Urmărirea prin URL și pixeli

47. Un pixel de urmărire este un hyperlink la o resursă, de obicei un fișier imagine, încorporat într-un conținut, cum ar fi un site sau un e-mail. De obicei, acest pixel nu îndeplinește niciun scop legat de conținutul solicitat în sine; singurul său scop este de a stabili automat o comunicare de către client cu gazda pixelului, care altfel nu ar fi avut loc. Acest lucru nu este totuși sistematic, iar pixelii de urmărire pot fi creați și prin adăugarea unor informații suplimentare la imaginile de încărcare a hyperlinkurilor care sunt relevante pentru conținutul afișat utilizatorului. Stabilirea comunicării transmite diverse informații gazdei pixelului, în funcție de cazul specific de utilizare.

48. În cazul unui e-mail, expeditorul poate include un pixel de urmărire pentru a detecta momentul în care destinatarul citește e-mailul. Pixelii de urmărire de pe site-uri pot face legătura cu o entitate care colectează numeroase astfel de cereri și poate, așadar, să urmărească comportamentul utilizatorilor. Acești pixeli de urmărire pot conține și identificatori suplimentari, metadate suplimentare sau conținut suplimentar ca parte a linkului. Aceste puncte de date pot fi adăugate de către proprietarul site-ului, eventual legate de activitatea utilizatorului pe site-ul respectiv, astfel încât să poată fi generate rapoarte analitice de utilizare. De asemenea, acestea pot fi generate în mod dinamic prin logica aplicativă la nivel de client furnizată de entitate.

49. Linkurile de urmărire pot funcționa în același mod, dar identificatorul este adăugat la adresa site-ului. Când localizatorul uniform de resurse („URL") este vizitat de către utilizator, site-ul vizat încarcă resursa solicitată, dar colectează și un identificator care nu este relevant în ceea ce privește identificarea resurselor. Linkurile de urmărire sunt utilizate foarte frecvent de site-urile de comerț electronic pentru a identifica originea sursei lor de trafic de intrare. De exemplu, aceste site-uri pot furniza partenerilor link-uri urmărite pentru a le utiliza pe domeniul lor, astfel încât site-ul de comerț electronic să știe care dintre partenerii săi este responsabil pentru o vânzare și să plătească un comision, o practică cunoscută sub denumirea de „marketing afiliat".

50. Atât linkurile de urmărire, cât și pixelii de urmărire pot fi distribuiți printr-o gamă largă de canale, de exemplu prin e-mailuri, site-uri sau chiar, în cazul linkurilor de urmărire, prin orice tip de sisteme de transmitere de mesaje text. Această distribuire către echipamentul terminal al utilizatorului constituie stocare, cel puțin prin intermediul mecanismului de înmagazinare cache al software-ului la nivel de client. Ca atare, se aplică articolul 5 alineatul (3) din ePD, chiar dacă această stocare nu este permanentă.

51. Adăugarea informațiilor de urmărire la URL-uri sau imagini (pixeli) trimise utilizatorului constituie o instrucțiune pentru echipamentul terminal de a trimite înapoi informațiile vizate (identificatorul specificat). În cazul pixelilor de urmărire construiți în mod dinamic, distribuția logicii aplicative (de obicei un cod JavaScript) constituie instrucțiunea. În consecință, se poate considera că colectarea identificatorilor furnizați prin aceste mecanisme de urmărire constituie o „dobândire a accesului” în sensul articolului 5 alineatul (3) din ePD, așadar se aplică și acestei etape.

3.2 Prelucrarea locală

52. Unele tehnologii se bazează pe prelucrarea locală solicitată de un software distribuit pe echipamentul terminal al utilizatorilor, unde informațiile produse prin prelucrarea locală sunt puse apoi la dispoziția actorilor selectați, prin intermediul API la nivel de client. Acest lucru poate fi valabil, de exemplu, pentru o API furnizată de browser, în care rezultatele generate la nivel local pot fi accesate de la distanță.

53. În cazul în care, în orice moment și, de exemplu, în codul la nivel de client, informațiile prelucrate sunt puse la dispoziția unei terțe părți, de exemplu sunt trimise înapoi prin rețea către un server, o astfel de operațiune (solicitată de entitatea care produce codul la nivel de client distribuit pe echipamentul terminal al utilizatorului) ar constitui o „[dobândire a] accesului la informațiile deja stocate”. Faptul că aceste informații sunt produse la nivel local nu exclude aplicarea articolului 5 alineatul (3) din ePD.

3.3 Urmărirea bazată exclusiv pe IP

54. Unii furnizori dezvoltă soluții care se bazează doar pe colectarea unei singure componente, și anume adresa IP, pentru a urmări navigarea[28] utilizatorului, în unele cazuri în mai multe domenii. În acest context, articolul 5 alineatul (3) din ePD s-ar putea aplica chiar dacă instrucțiunea de a pune la dispoziție IP a fost dată de o altă entitate decât cea care primește informațiile.

55. Cu toate acestea, dobândirea accesului la adresele IP ar declanșa aplicarea articolului 5 alineatul (3) din ePD numai în cazurile în care aceste informații provin de la echipamentul terminal al unui abonat sau utilizator. Deși nu este cazul în mod sistematic (de exemplu, atunci când CGNAT[29] este activat), IPv4 static de ieșire provenit de la routerul unui utilizator s-ar încadra în acest caz, precum și adresele IPV6, deoarece acestea sunt definite parțial de către gazdă. Cu excepția cazului în care poate garanta că adresa IP nu provine de la echipamentul terminal al unui utilizator sau abonat, entitatea trebuie să ia toate măsurile prevăzute la articolul 5 alineatul (3) din ePD.

56. Deși prezentele orientări nu analizează aplicarea exceptărilor de la obligația de a obține consimțământul prevăzută la articolul 5 alineatul (3) din ePD, este important să reamintim încă o dată că aplicabilitatea acestui articol nu înseamnă în mod sistematic că trebuie obținut consimțământul.

[28] Acest lucru este suplimentar și independent de utilizarea și funcția unei adrese IP pentru stabilirea și transmisia comunicațiilor tehnice subiacente sau de faptul că poate fi vorba sau nu de date cu caracter personal (în ceea ce privește analiza privind viața privată și comunicațiile electronice, este vorba despre „informații”).

[29] NAT de nivel operator sau CGNAT este utilizat de furnizorii de servicii de internet pentru a maximiza utilizarea spațiului limitat de adrese IP. Acesta grupează un număr de abonați sub aceeași adresă IP publică.

Astfel, CEPD reamintește că, în fiecare caz, ar trebui să se evalueze dacă este necesar consimțământul sau dacă s-ar putea aplica o exceptare în temeiul articolului 5 alineatul (3) din ePD[30].

3.4 Raportarea intermitentă și mediată prin IoT

57. Dispozitivele IoT (internetul obiectelor) produc informații în mod continuu în timp, de exemplu prin intermediul senzorilor încorporați în dispozitiv, care pot sau nu să fie prelucrate în prealabil la nivel local. În multe cazuri, informațiile sunt puse la dispoziția unui server la distanță, dar modalitățile de colectare pot varia.

58. Unele dispozitive IoT au o conexiune directă la o rețea publică de comunicații cu o cartelă SIM celulară. Altele pot avea o conexiune indirectă la o rețea publică de comunicații, de exemplu prin utilizarea Wi-Fi sau prin transmiterea de informații către un alt dispozitiv printr-o conexiune punct la punct (de exemplu, prin Bluetooth). Celălalt dispozitiv poate fi, de exemplu, un telefon inteligent sau un gateway dedicat care poate sau nu să prelucreze în prealabil informațiile, înainte de a le trimite către server.

59. Dispozitivele IoT ar putea fi instruite de producător să transmită în flux întotdeauna informațiile colectate, dar să memoreze mai întâi informațiile în cache la nivel local, de exemplu până când este disponibilă o conexiune.

60. În orice caz, dispozitivul IoT, în cazul în care este conectat (în mod direct sau indirect) la o rețea publică de comunicații, ar fi considerat în sine un echipament terminal. Faptul că informațiile sunt transmise în flux sau sunt memorate în cache pentru raportarea intermitentă nu schimbă caracterul informațiilor respective. În ambele situații, s-ar aplica articolul 5 alineatul (3) din ePD, deoarece, prin instruirea codului de pe dispozitivul IoT pentru a trimite datele stocate în mod dinamic către serverul la distanță, are loc o „dobândire a accesului”.

3.5 Identificatorul unic

61. Un instrument comun utilizat de întreprinderi este noțiunea de „identificatori unici” sau „identificatori permanenți”. Acești identificatori pot fi obținuți din date cu caracter personal permanente (prenume și nume, e-mail, număr de telefon etc.), care sunt dispersate pe dispozitivul utilizatorului, colectate și partajate între mai mulți operatori pentru a identifica în mod unic o persoană în diferite seturi de date [date de utilizare colectate prin utilizarea site-ului sau a aplicației, date de gestionare a relațiilor cu clienții (CRM) legate de achiziționarea sau abonamentul online sau offline etc.]. Pe site-uri, datele cu caracter personal permanente sunt obținute, în general, în contextul autentificării sau al abonării la buletine informative.

62. Astfel cum s-a subliniat anterior, faptul că informațiile sunt introduse de utilizator nu ar exclude aplicarea articolului 5 alineatul (3) din ePD în ceea ce privește stocarea, deoarece aceste informații sunt stocate temporar pe echipamentul terminal înainte de a fi colectate.

63. În contextul colectării unui „identificator unic” pe site-uri sau pe aplicații pentru dispozitive mobile, entitatea care colectează informațiile dă instrucțiuni browserului (prin distribuirea codului la nivel de client) să trimită informațiile respective. Ca atare, are loc o „dobândire a accesului” și se aplică articolul 5 alineatul (3) din ePD.

[30] Avizul nr. 9/2014 al Grupului de lucru „Articolul 29” furnizează câteva exemple de cazuri în care consimțământul ar putea să nu fie necesar.