Smjernice

Smjernice 2/2023 o tehničkom području primjene članka 5. stavka 3. Direktive o e-privatnosti

Inačica 2.0

Doneseno 7. listopada 2024.

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Povijest inačice

Inačica 1.0	14. studenoga 2023.	Donošenje Smjernica za potrebe savjetovanja s javnošću
Inačica 2.0	7. listopada 2024.	Donošenje Smjernica nakon savjetovanja s javnošću

Sažetak

U ovim Smjernicama Europski odbor za zaštitu podataka razmatra primjenjivost članka 5. stavka 3. Direktive o e-privatnosti na različita tehnička rješenja. Ovim se smjernicama dopunjuje Mišljenje 9/2014 Radne skupine iz članka 29. o primjeni Direktive o e-privatnosti na prikupljanje informacija o uređaju u svrhu njegove identifikacije i praćenja te se nastoji osigurati jasno razumijevanje tehničkih operacija obuhvaćenih člankom 5. stavkom 3. Direktive o e-privatnosti.

Pojava novih metoda praćenja kako bi se zamijenili postojeći alati za praćenje (na primjer, kolačići, zbog toga što neki dobavljači preglednika više ne podržavaju kolačiće trećih strana) i stvorili novi poslovni modeli postali su jedan od glavnih razloga za zabrinutost u pogledu zaštite podataka. Iako je primjenjivost članka 5. stavka 3. Direktive o e-privatnosti dobro utvrđena i provedena za neke tehnologije praćenja kao što su kolačići, potrebno je riješiti nejasnoće u vezi s primjenom navedene odredbe na nove alate za praćenje.

U Smjernicama se utvrđuju tri ključna elementa za primjenjivost članka 5. stavka 3. Direktive o e-privatnosti (odjeljak 2.1.), odnosno „informacije”, „terminalna oprema pretplatnika ili korisnika” i „dobivanje pristupa” i „pohrana informacija i pohranjenih informacija”. U Smjernicama se nadalje navodi detaljna analiza svakog elementa (odjeljci od 2.2. do 2.6.).

U odjeljku 3. ta se analiza primjenjuje na neiscrpan popis slučajeva uporabe koji predstavljaju zajedničke tehnike, a to su:

- URL i piksel za praćenje
- Lokalna obrada
- Praćenje samo na osnovi IP-a.
- Izvješćivanje o internetu stvari povremeno i s posredovanjem
- Jedinstveni identifikator

Sadržaj

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „Opća uredba o zaštiti podataka"),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članak 15. stavak 3. Direktive 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija, kako je izmijenjena Direktivom 2009/136/EZ (dalje u tekstu „Direktiva o e-privatnosti" ili „ePD"),

uzimajući u obzir članak 12. i članak 22. Poslovnika,

DONIO JE SLJEDEĆE SMJERNICE:

1 UVOD

1. U skladu s člankom 5. stavkom 3. Direktive o e-privatnosti *„ pohrana informacija ili za pristup informacijama pohranjenima u terminalnoj opremi pretplatnika ili korisnika"* dopuštena je samo na osnovi privole ili nužnosti u posebne svrhe utvrđene u tom članku. Kako se podsjeća u uvodnoj izjavi 24. Direktive o e-privatnosti[2], cilj je te odredbe zaštititi terminalnu opremu korisnika jer je ona dio privatne sfere korisnika. Iz teksta tog članka proizlazi da se članak 5. stavak 3. Direktive o e-privatnosti ne primjenjuje isključivo na kolačiće, nego i na „slične tehnologije". Međutim, trenutačno ne postoji sveobuhvatan popis tehničkih operacija obuhvaćenih člankom 5. stavkom 3. Direktive o e-privatnosti.

2. Radna skupina iz članka 29. (dalje u tekstu „WP29"), Mišljenje 9/2014 o primjeni Direktive o e-privatnosti na prikupljanje informacija o uređaju u svrhu njegove identifikacije i praćenja (dalje u tekstu „Mišljenje 9/2014 Radne skupine iz članka 29.") već je pojasnila da je prikupljanje informacija obuhvaćeno tehničkim područjem primjene članka 5. stavka 3. Direktive o e-privatnosti[3], no zbog novih napredaka u tehnologijama potrebne su dodatne smjernice u pogledu tehnika praćenja koje se trenutačno poštuju. Tehničko se okruženje razvilo tijekom posljednjeg desetljeća, uz sve veću uporabu identifikatora ugrađenih u operativne sustave, kao i stvaranje novih alata koji omogućuju pohranu informacija u terminalnoj opremi.

[1] Upućivanja na „države članice" u ovom dokumentu trebala bi se tumačiti kao upućivanja na „države članice EGP-a".

[2] „Terminalna oprema korisnika elektroničkih komunikacijskih mreža te informacije pohranjene na takvoj opremi dio su privatnog područja korisnika koje zahtijeva zaštitu prema Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda. Takozvani špijunski programi (spyware), mrežne greške (web bugs), skriveni identifikatori i druga slična sredstva mogu ući u korisnikov terminal bez njegova znanja s ciljem dobivanja pristupa informacijama, pohranjivanja skrivenih informacija ili ulaženja u trag aktivnostima korisnika, te mogu ozbiljno narušiti privatnost korisnika. Uporaba takvih sredstava treba se dopustiti isključivo u legitimne svrhe, uz znanje dotičnih korisnika."

[3] Mišljenje 9/2014 Radne skupine iz članka 29., str. 11.

3. Nejasnoće u pogledu područja primjene članka 5. stavka 3. Direktive o e-privatnosti stvorile su poticaje za provedbu alternativnih rješenja za praćenje korisnika interneta i dovele do tendencije zaobilaženja pravnih obveza predviđenih člankom 5. stavkom 3. Direktive o e-privatnosti. Sve takve situacije izazivaju zabrinutost i zahtijevaju dodatnu analizu kako bi se dopunile prethodne smjernice Europskog odbora za zaštitu podataka.

4. Cilj je ovih Smjernica provesti tehničku analizu područja primjene članka 5. stavka 3. Direktive o e-privatnosti, odnosno pojasniti što je tehnički obuhvaćeno izrazom *„pohranjivati informacije ili dobiti pristup informacijama pohranjenima u terminalnoj opremi pretplatnika ili korisnika*". Ove se Smjernice ne odnose na okolnosti u kojima postupak obrade može biti obuhvaćen izuzećima od zahtjeva za privolu predviđenu Direktivom o e-privatnosti[4] jer bi te okolnosti trebalo analizirati na pojedinačnoj osnovi, uzimajući u obzir prenošenje/provedbe relevantnih država članica, te smjernice koje izdaju nacionalna nadležna tijela.

5. Nepotpuni popis specifičnih slučajeva uporabe analizirat će se u završnom dijelu ovih Smjernica.

2 ANALIZA

2.1 Ključni elementi za primjenjivost članka 5. stavka 3. Direktive o e-privatnosti

6. Članak 5. stavak 3. Direktive o e-privatnosti primjenjuje se:

   a. **KRITERIJ A:** ako se provedene operacije odnose na „*informacije*". Treba napomenuti da se pojam koji se upotrebljava ne odnosi na „osobne podatke", već na „informacije".

   b. **KRITERIJ B:** ako obavljene operacije uključuju „*terminalnu opremu*" pretplatnika ili korisnika (B.1), što podrazumijeva potrebu za procjenom pojma *„javne komunikacijske mreže*" (B.2).

   c. **KRITERIJ C**: ako postupci koji se provode doista predstavljaju „*pohranu*" (C.1) ili „*dobivanja pristupa*" (C.2). Ta se dva pojma mogu neovisno proučiti, kako se podsjeća u Mišljenju 9/2014 Radne skupine iz članka 29.: *„Uporaba riječi ,pohranjeno ili pristupljeno' ukazuje na to da se pohrana i pristup ne moraju odvijati u okviru iste komunikacije i da ih ne mora obavljati ista strana"*[5]*.*

   Radi čitljivosti, subjekt koji dobije pristup informacijama pohranjenima u korisnikovoj terminalnoj opremi u daljnjem se tekstu naziva „subjekt koji dobiva pristup".

2.2 Pojam „informacije" – kriterij A

7. Kako je navedeno u KRITERIJU A, u ovom se odjeljku detaljno opisuje što je obuhvaćeno pojmom „informacije". Odabir pojma „informacije", koji obuhvaća širu kategoriju od samog pojma osobnih podataka, povezan je s područjem primjene Direktive o e-privatnosti.

8. Cilj je članka 5. stavka 3. Direktive o e-privatnosti zaštititi privatnu sferu korisnika, kako je navedeno u uvodnoj izjavi 24.: *„Terminalna oprema korisnika elektroničkih komunikacijskih mreža te informacije pohranjene na takvoj opremi dio su privatnog područja korisnika koje zahtijeva zaštitu prema Europskoj*

[4] Kako je navedeno u članku 5. stavku 3. Direktive o e-privatnosti: *„Ovo ne sprečava tehničko pohranjivanje ili pristup isključivo u svrhu provođenja ili olakšavanja prijenosa komunikacija preko elektroničke komunikacijske mreže ili ako je strogo nužno kako bi se pružila neka usluga informacijskog društva koju je pretplatnik ili korisnik izričito zatražio.*"

[5] Mišljenje 9/2014 Radne skupine iz članka 29., str. 8.

konvenciji za zaštitu ljudskih prava i temeljnih sloboda.". Zaštićena je i člankom 7. Povelje EU-a o temeljnim pravima.

9. Zapravo, scenariji koji zadiru u tu privatnu sferu, čak i ako ne uključuju osobne podatke, izričito su obuhvaćeni tekstom članka 5. stavka 3. i uvodne izjave 24. Direktive o e-privatnosti, primjerice pohranjivanje virusa u terminalnoj opremi korisnika. To pokazuje da definicija pojma „informacije" ne bi trebala biti ograničena na imovinu koja je povezana s fizičkom osobom čiji je identitet utvrđen ili se može utvrditi.

10. To je potvrdio Sud Europske unije: „*Ta se zaštita primjenjuje na sve informacije pohranjene na toj terminalnoj opremi, neovisno o tome je li riječ o osobnim podacima, a cilj joj je, kao što to proizlazi iz te iste uvodne izjave, među ostalim, zaštita korisnika od opasnosti da skriveni identifikatori ili druga slična sredstva uđu u terminalnu opremu tih korisnika bez njihova znanja*."[6]

11. Pri procjeni primjenjivosti članka 5. stavka 3. Direktive o e-privatnosti trebalo bi uzeti u obzir pitanja o tome jesu li izvor tih informacija i razlozi zbog kojih su pohranjene u terminalnoj opremi prethodno razjašnjeni. Na primjer, u Mišljenju 9/2014 Radne skupine iz članka 29.: „*Nije ispravno tumačiti to na način da to znači da treća strana ne zahtijeva privolu za pristup tim informacijama samo zato što ih nije pohranila. Zahtjev za privolu primjenjuje se i kada se pristupa vrijednosti koja se upotrebljava samo za čitanje (npr. traženje adrese MAC mrežnog sučelja putem sučelja OS API)*."[7]

12. Zaključno, pojam informacija uključuje i neosobne podatke i osobne podatke, bez obzira na to kako su ti podatci pohranjeni i tko ih pohranjuje, tj. je li ih pohranio vanjski subjekt (uključujući i subjekte koji nisu subjekti koji imaju pristup), korisnik, proizvođač ili bilo koji drugi scenarij.

2.3 Pojam „terminalna oprema pretplatnika ili korisnika" – kriterij B.1

13. Ovaj se odjeljak zasniva na definiciji koja se upotrebljava u Direktivi 2008/63/EZ i kako je navedena u članku 2. Direktive (EU) 2018/1972, u kojoj je „terminalna oprema" definirana kao: „*oprema koja je izravno ili neizravno povezana sa sučeljem javne telekomunikacijske mreže s ciljem slanja, obrade ili primanja informacija; u svakom slučaju (izravno ili neizravno), povezivanje se može ostvariti žicom, optičkim vlaknom ili elektromagnetski; povezivanje je neizravno ako je oprema smještena između terminala i sučelja mreže*"[8].

14. U uvodnoj izjavi 24. Direktive o e-privatnosti pruža se jasno razumijevanje uloge terminalne opreme za zaštitu koju pruža članak 5. stavak 3. Direktive o e-privatnosti. Direktiva o e-privatnosti štiti privatnost korisnika ne samo u odnosu na povjerljivost njihovih podataka, već i čuvanjem cjelovitosti korisničke terminalne opreme. To će razumijevanje usmjeravati tumačenje pojma terminalne opreme u svim ovim Smjernicama.

15. U članku 3. Direktive o e-privatnosti navodi se da se za primjenu Direktive o e-privatnosti obrada osobnih podataka mora provoditi u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama. To podrazumijeva da bi uređaj trebao biti upotrebljiv u vezi s takvom uslugom i da bi, kako bi se kvalificirao kao terminalna oprema, trebao biti[9] povezan ili povezan sa sučeljem javne komunikacijske mreže. Europski odbor za zaštitu podataka napominje da je

[6] Presuda Suda od 1. listopada 2019., Planet49, predmet C-673/17, ECLI:EU:C:2019:801, točka 70.
[7] Mišljenje 9/2014 Radne skupine iz članka 29., str. 8.
[8] Direktiva Komisije 2008/63/EZ od 20. lipnja 2008. o tržišnom natjecanju na tržištima telekomunikacijske terminalne opreme (Kodificirana inačica), članak 1. stavak 1.
[9] To znači da ima tehničke sposobnosti za priključenje na mrežu čak i ako to povezivanje trenutačno nije uspostavljeno.

izmjenama iz 2009.[10] u tekstu članka 5. stavka 3. Direktive o e-privatnosti proširena zaštita terminalne opreme brisanjem upućivanja na „uporabu elektroničke komunikacijske mreže" kao sredstva za pohranu informacija ili za dobivanje pristupa informacijama pohranjenima u terminalnoj opremi. Stoga, sve dok uređaj ima mrežno sučelje koje ga čini prihvatljivim za povezivanje (čak i ako takva veza nije uspostavljena), članak 5. stavak 3. Direktive o e-privatnosti primjenjuje se na svaki subjekt koji bi pohranio i dobio pristup informacijama koje su već pohranjene u terminalnoj opremi bez obzira na način pristupa terminalnoj opremi te na to je li povezan ili isključen s mreže

16. Oprema koja je dio same javne elektroničke komunikacijske mreže ne bi se smatrala terminalnom opremom u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti[11].

17. Terminalna oprema može se sastojati od bilo kojeg broja pojedinačnih dijelova hardvera koji zajedno čine terminalnu opremu. To može ili ne mora biti u obliku fizički zatvorenog uređaja na kojem se nalazi sva oprema za prikaz, obradu, pohranu i periferni hardver (na primjer, pametni telefoni, prijenosna računala, uređaj za pohranu u mreži, povezani automobili ili povezani televizori, pametne naočale).

18. Direktiva o e-privatnosti potvrđuje da zaštita povjerljivosti informacija pohranjenih u terminalnoj opremi korisnika i integriteta terminalne opreme korisnika nije ograničena na zaštitu privatne sfere fizičkih osoba, već se odnosi i na pravo na poštovanje njihove korespondencije ili legitimnih interesa pravnih osoba[12]. Kao takva, terminalna oprema koja omogućuje tu korespondenciju i legitimne interese pravnih osoba zaštićena je na temelju članka 5. stavka 3. Direktive o e-privatnosti.

19. Korisnik ili pretplatnik može posjedovati terminalnu opremu, unajmiti je ili na drugi način biti opremljen s terminalnom opremom. Više korisnika ili pretplatnika može dijeliti istu terminalnu opremu.

20. Ta je zaštita zajamčena Direktivom o e-privatnosti za terminalnu opremu povezanu s korisnikom ili pretplatnikom i ne ovisi o tome je li korisnik postavio sredstva pristupa (na primjer, ako je pokrenuo elektroničku komunikaciju) ili čak o tome je li korisnik upoznat s navedenim sredstvima pristupa.

2.4 Pojam „javne komunikacijske mreže" – kriterij B.2

21. Budući da je situacija uređena Direktivom o e-privatnosti ona koja je u vezi s *„pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama u Zajednici"*[13] i da se u definiciji terminalne opreme izričito spominje pojam *„javne komunikacijske mreže"*, ključno je pojasniti taj pojam kako bi se utvrdio kontekst u kojem se primjenjuje članak 5. stavak 3. Direktive o e-privatnosti.

22. Pojam elektroničke komunikacijske mreže nije definiran u samoj Direktivi o e-privatnosti. Na taj se koncept izvorno upućivalo u Direktivi 2002/21/EZ (Okvirna direktiva) o zajedničkom regulatornom

[10] Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektroničke komunikacijske mreže i usluge, Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija i Uredba (EZ) br. 2006/2004 o suradnji između nacionalnih tijela odgovornih za provedbu zakona o zaštiti potrošača (Tekst značajan za EGP), SL L 337, 18.12.2009., članak 2. stavak 5. i uvodna izjava 65.

[11] Kako bi se utvrdila ograničenja mreže u različitim kontekstima, vidjeti Smjernice BEREC-a o zajedničkim pristupima utvrđivanju mrežne točke za prekid u različitim topologijama mreže (BoR (20) 46).

[12] Naime, kako je navedeno u članku 2. stavku 13. Direktive (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija, korisnik može biti fizička ili pravna osoba.

[13] Članak 3. Direktive o e-privatnosti.

okviru za elektroničke komunikacijske mreže i usluge[14], koja je naknadno zamijenjena člankom 2. stavkom 1. Direktive 2018/1972 (Europski zakonik elektroničkih komunikacija). Sad glasi:

> *„elektronička komunikacijska mreža" znači sustavi prijenosa, bez obzira na to temelje li se na stalnoj infrastrukturi ili centraliziranom upravljačkom kapacitetu, i, ako je to primjenjivo, opremu za prespajanje ili usmjeravanje te druga sredstva, uključujući mrežne elemente koji nisu aktivni, a koji dopuštaju prijenos signala žičanim, radijskim, optičkim ili drugim elektromagnetskim sredstvom, što uključuje satelitske mreže, zemaljske nepokretne (s prespajanjem kanala, prespajanjem paketa podataka, uključujući internet) i pokretne mreže, elektroenergetske kabelske sustave, u mjeri u kojoj se rabe za prijenos signala, mreže koje se rabe za radijsku i televizijsku radiodifuziju te mreže kabelske televizije, bez obzira na vrstu informacija koju prenose;*[15]

23. Ova je definicija neutralna u odnosu na tehnologije prijenosa. Elektronička komunikacijska mreža, u skladu s tom definicijom, je svaki mrežni sustav koji omogućuje prijenos elektroničkih signala između svojih čvorova, bez obzira na korištenu opremu i protokole.

24. Pojam elektroničke komunikacijske mreže u skladu s Direktivom 2018/1972 ne ovisi o javnoj ili privatnoj prirodi infrastrukture ni o načinu na koji se mreža uvodi ili njome upravlja („*temelji li se na stalnoj infrastrukturi ili centraliziranom upravljačkom kapacitetu*"[16].) Stoga je definicija elektroničke komunikacijske mreže, u skladu s člankom 2. Direktive 2018/1972, dovoljno široka da obuhvaća bilo koju vrstu infrastrukture. To uključuje mreže kojima upravlja ili ne upravlja operator, mreže kojima zajednički upravlja skupina operatora ili čak *ad hoc* mreže u kojima se terminalna oprema može dinamički pridružiti drugoj terminalnoj opremi ili iz nje napustiti mrežu druge terminalne opreme primjenom protokola prijenosa kratkog dometa.

25. Ova definicija mreže ne daje nikakva ograničenja u pogledu broja terminalne opreme prisutne u mreži u bilo kojem trenutku. Neki programi umrežavanja oslanjaju se na to da čvorovi prenose informacije na *ad hoc* način čvorovima koji su trenutačno povezani[17] i u nekom trenutku mogu komunicirati samo dva istorazinska pristupa. Takvi bi slučajevi bili obuhvaćeni općim područjem primjene Direktive o e-privatnosti, pod uvjetom da mrežni protokol omogućuje daljnje uključivanje istorazinskih pristupa.

26. Javna dostupnost komunikacijske mreže potrebna je kako bi se uređaj smatrao terminalnom opremom, a time i za primjenjivost članka 5. stavka 3. Direktive o e-privatnosti. Treba napomenuti da činjenica da je mreža stavljena na raspolaganje ograničenom podskupu javnosti (na primjer, pretplatnicima, bez obzira na to plaćaju li ili ne, pod uvjetima prihvatljivosti) ne čini takvu mrežu privatnom[18].

[14] Direktiva 2002/21/EZ Europskog parlamenta i Vijeća od 7. ožujka 2002. o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge (Okvirna direktiva)

[15] Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (preinaka) (Tekst značajan za EGP), članak 2. stavak 1.

[16] Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća od 11. prosinca 2018. o Europskom zakoniku elektroničkih komunikacija (preinaka) (Tekst značajan za EGP), članak 2. stavak 1.

[17] Na primjer, u kontekstu sheme umrežavanja otporne na kašnjenje u kojoj se primjenjuju „tehnike pohrane i prosljeđivanja", kao što je projekt otvorenog koda Briar.

[18] Za daljnju analizu utvrđivanja javnih komunikacijskih mreža vidjeti Smjernice BEREC-a o provedbi Uredbe o otvorenom internetu (BoR (20) 112).

2.5 Pojam „dobivanje pristupa” – kriterij C.1

27. Kako bi se pravilno oblikovao pojam „dobivanja pristupa”, važno je razmotriti područje primjene Direktive o e-privatnosti navedeno u njezinu članku 1.: „*trebaju osigurati ujednačenu razinu zaštite temeljnih prava i sloboda, a posebno prava na privatnost u vezi s obradom osobnih podataka u području elektroničkih komunikacija i osigurati slobodan prijenos takvih podataka i elektroničke komunikacijske opreme i usluga u Zajednici*”.

28. Ukratko, Direktiva o e-privatnosti pravni je instrument za očuvanje privatnosti čiji je cilj zaštita povjerljivosti komunikacija i integriteta uređaja. U uvodnoj izjavi 24. Direktive o e-privatnosti pojašnjeno je da je, u slučaju fizičkih osoba, terminalna oprema korisnika dio njihove privatne sfere te da pristup informacijama pohranjenima na njoj bez njihova znanja može ozbiljno narušiti njihovu privatnost.

29. Pravne osobe isto su zaštićene Direktivom o e-privatnosti[19]. Slijedom toga, pojam „dobivanja pristupa” u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti mora se tumačiti na način kojim se ta prava štite od kršenja trećih strana.

30. Pohranjivanje informacija ili dobivanje pristupa mogu biti neovisne operacije koje provode neovisni subjekti. Pohrana informacija i pristup već pohranjenim informacijama ne moraju biti prisutni kako bi se primjenjivao članak 5. stavak 3. Direktive o e-privatnosti.

31. Kako je navedeno u Mišljenju 9/2014 Radne skupine iz članka 29.: „*Uporaba riječi ‚pohranjeno ili pristupljeno’ ukazuje na to da se pohrana i pristup ne moraju odvijati u okviru iste komunikacije i da ih ne mora obavljati ista strana. Informacije koje pohranjuje jedna strana (uključujući informacije koje pohranjuje korisnik ili proizvođač uređaja), a kojima kasnije pristupa druga strana, stoga su obuhvaćene područjem primjene članka 5. stavka 3.*”[20]. Slijedom toga, ne postoje ograničenja u pogledu podrijetla informacija u terminalnoj opremi za primjenu pojma pristupa.

32. Kad god subjekt poduzme korake za ostvarivanje pristupa informacijama pohranjenima u terminalnoj opremi, primjenjuje se članak 5. stavak 3. Direktive o e-privatnosti. To obično podrazumijeva da subjekt koji pristupa proaktivno šalje posebne upute terminalnoj opremi kako bi dobio natrag ciljane informacije. Na primjer, to je slučaj s kolačićima, za koje pristupni subjekt nalaže terminalnoj opremi da proaktivno šalje informacije o svakom sljedećem pozivu na protokol za prijenos hiperteksta („HTTP”).

33. To je jednako tako slučaj kad subjekt koji pristupa distribuira softver u terminalnoj opremi korisnika koji je pohranjen i koji će zatim proaktivno pozivati krajnju točku sučelja za programiranje aplikacija (engl. *Application Programming Interface*, „API”) putem mreže. Dodatni primjeri uključuju JavaScript kod, gdje subjekt koji pristupa nalaže pregledniku korisnika da pošalje asinkrone zahtjeve s ciljanim informacijama. Jasno je da je takav pristup obuhvaćen područjem primjene članka 5. stavka 3. Direktive o e-privatnosti jer subjekt koji pristupa izričito nalaže terminalnoj opremi da pošalje informacije.

34. U nekim slučajevima subjekt koji upućuje terminalnu opremu da pošalje ciljane podatke i subjekt koji prima informacije možda neće biti isti. To može biti posljedica pružanja i/ili upotrebe zajedničkog mehanizma između dvaju subjekata. Nalaganjem uređaju da pošalje već pohranjene informacije (na

[19] Uvodna izjava 26. Direktive o e-privatnosti, vidjeti prethodni stavak 17.
[20] Mišljenje 9/2014 Radne skupine iz članka 29., str. 8.

primjer, primjenom protokola ili SDK-a[21] koje podrazumijevaju proaktivno slanje informacija od strane terminalne opreme) omogućuje se zadiranje u terminalnu opremu, stoga takav pristup dovodi do primjene članka 5. stavka 3. Direktive o e-privatnosti. Kako je navedeno u Mišljenju 9/2014 Radne skupine iz članka 29., to može biti slučaj kada internetske stranice upute terminalnu opremu da pošalje informacije službama za oglašavanje trećih strana uključivanjem piksela za praćenje[22]. Ovaj slučaj uporabe dodatno je razrađen u odjeljku 3.1.

2.6 Pojmovi „pohrana informacija" i „pohranjene informacije" – kriterij C.2

35. Pohrana informacija u smislu članka 5. stavka 3. Direktive o e-privatnosti odnosi se na stavljanje informacija na fizički elektronički medij za pohranu koji je dio terminalne opreme korisnika ili pretplatnika[23].

36. Obično se informacije ne pohranjuju u terminalnoj opremi korisnika ili pretplatnika izravnim pristupom memoriji uređaja od strane druge strane, nego davanjem uputa softveru u terminalnoj opremi za generiranje određenih informacija. Smatra se da je pohranu koja se odvija na temelju takvih uputa izravno pokrenula druga strana. To uključuje upotrebu uspostavljenih protokola kao što je pohrana kolačića u pregledniku te prilagođenog softvera, bez obzira na to tko je izradio ili instalirao protokole ili softver u terminalnoj opremi.

37. U Direktivi o e-privatnosti ne postavlja se gornja ili donja granica razdoblja tijekom kojeg se informacije moraju zadržati na mediju za pohranu kako bi se smatrale pohranjenima, kao ni gornja ili donja granica količine informacija koje treba pohraniti.

38. Slično tome, pojam pohrane ne ovisi o vrsti medija na kojem se informacije pohranjuju. Tipični primjeri uključivali bi tvrde diskove („HDD"), pogone u čvrstom stanju („SSD"), električno izbrisivu programabilnu memoriju samo za čitanje („EEPROM") i memoriju s nasumičnim pristupom („RAM"), no manje tipični scenariji koji uključuju medij kao što su magnetska vrpca ili predmemorija središnje jedinice za obradu („CPU") nisu isključeni iz područja primjene. Medij za pohranu podataka može se povezati interno (npr. putem SATA veze), eksterno (npr. putem USB veze)

39. „Pohranjene informacije" odnose se na informacije koje već postoje u terminalnoj opremi, bez obzira na izvor ili prirodu tih informacija. To uključuje sve rezultate pohrane informacija u smislu članka 5. stavka 3. Direktive o e-privatnosti kako je prethodno opisano (neovisno o tome radi li se o istoj strani koja bi poslije dobila pristup ili o nekoj drugoj trećoj strani). Osim toga, uključuje rezultate postupaka pohrane informacija izvan područja primjene članka 5. stavka 3. Direktive o e-privatnosti, kao što su pohrana u terminalnoj opremi od strane samog korisnika ili pretplatnika ili proizvođača hardvera (kao što su MAC adrese kontrolora mrežnih sučelja), senzora integriranih u terminalnu opremu ili postupaka i programa izvršenih u terminalnoj opremi, koji mogu ili ne moraju proizvesti informacije koje ovise o pohranjenim informacijama ili iz njih proizlaze.

[21] SDK („komplet za razvoj softvera") skup je alata za razvoj softvera koji se stavljaju na raspolaganje kako bi se olakšalo stvaranje aplikacijskog softvera.
[22] Mišljenje 9/2014 Radne skupine iz članka 29., str. 9.
[23] Kako je definirano u odjeljku 2.3 ovih Smjernica.

3 PRIMJERI UPOTREBE

40. Kako je istaknuto u uvodu ovih Smjernica[24], one ne analiziraju primjenu izuzeća od obveze prikupljanja privole predviđene člankom 5. stavkom 3. Direktive o e-privatnosti. Europski odbor za zaštitu podataka podsjeća da bi za sve slučajeve pohrane informacija ili dobivanja pristupa već pohranjenim informacijama trebalo procijeniti je li potrebna privola ili bi se moglo primijeniti izuzeće u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti. Čitatelj bi stoga trebao razmotriti izuzeća u slučaju njihove primjene, zajedno s ovom tehničkom analizom.

41. Ne dovodeći u pitanje poseban kontekst u kojem se te tehničke kategorije mogu upotrebljavati, a koje su potrebne kako bi se utvrdilo primjenjuje li se članak 5. stavak 3. Direktive o e-privatnosti, moguće je na neiscrpan način utvrditi široke kategorije identifikatora i informacija koje su široko korištene i mogu podlijegati primjenjivosti članka 5. stavka 3. Direktive o e-privatnosti.

42. Mrežna komunikacija obično se oslanja na slojevit model koji zahtijeva upotrebu identifikatora kako bi se omogućilo pravilno uspostavljanje i provođenje komunikacije. Prijenos komunikacije tih identifikatora subjektima na daljinu vrši se putem softvera u skladu s dogovorenim komunikacijskim protokolima. Kako je prethodno navedeno, činjenica da subjekt primatelj možda nije subjekt koji upućuje na slanje informacija ne isključuje primjenu članka 5. stavka 3. Direktive o e-privatnosti. To se može odnositi na identifikatore usmjeravanja kao što su MAC ili IP adresa terminalne opreme, ali i identifikatore sesije (SSRC, identifikator Websocketa) ili tokene za autentifikaciju.

43. Na isti način, protokol aplikacije može uključivati nekoliko mehanizama za pružanje kontekstualnih podataka (kao što je HTTP zaglavlje, uključujući polje „prihvaćanje" ili korisnički agent), mehanizam za predmemoriranje (kao što je ETag[25]) ili druge funkcionalnosti (kolačići su jedan od njih ili HSTS[26]). Ponovno, oslanjanje na te mehanizme za prikupljanje informacija (na primjer u kontekstu prikupljanja informacija o uređaju u svrhu njegove identifikacije i praćenja[27] ili praćenja identifikatora resursa) može dovesti do primjene članka 5. stavka 3. Direktive o e-privatnosti.

44. S druge strane, postoje određeni konteksti u kojima lokalne aplikacije ugrađene u terminalnu opremu koriste neke informacije strogo unutar terminala, kao što bi moglo vrijediti za API-je sustava za pametne telefone (pristup kameri, mikrofon, senzor GPS-a, akcelerator, radijski čip, pristup lokalnoj dokumentaciji, popis kontakata, pristup identifikatorima itd.). To može vrijediti i za internetske preglednike koji obrađuju informacije pohranjene ili generirane informacije unutar uređaja (kao što su kolačići, lokalna pohrana, WebSQL ili čak informacije koje su dostavili sami korisnici). Uporaba takvih informacija putem aplikacije ne bi predstavljala „dobivanje pristupa već pohranjenim informacijama" u smislu članka 5. stavka 3. Direktive o e-privatnosti sve dok te informacije ne napuštaju uređaj, ali kada se pristupi tim informacijama ili bilo kakvom izvođenju tih informacija, primjenjivao bi se članak 5. stavak 3. Direktive o e-privatnosti.

45. Konačno, u nekim slučajevima akteri distribuiraju zlonamjerne softverske elemente, na primjer softver za rudarenje kriptomaterijala ili općenito zlonamjerni softver, koji iskorištavaju sposobnosti obrade terminalne opreme u korist distributera. Distribucija navedenog zlonamjernog softvera u terminalnoj

[24] Vidjeti prethodni stavak 4.

[25] HTTP ETag je identifikator koji omogućuje podnošenje uvjetnog zahtjeva na temelju valjanosti predmemoriranih podataka klijenta.

[26] HTTP Strict Transport Security (HSTS) omogućuje poslužiteljima da odrede koji bi se resursi uvijek trebali zatražiti putem HTTPS veza.

[27] Kako je navedeno u uvodu, vidjeti Mišljenje 9/2014 Radne skupine iz članka 29. o primjeni Direktive o e-privatnosti na prikupljanje informacija o uređaju u svrhu njegove identifikacije i praćenja

opremi korisnika predstavljala bi „pohranjivanje” u smislu članka 5. stavka 3. Direktive o e-privatnosti. Osim toga, ako softver uspostavi mrežnu vezu za slanje informacija u kasnijoj fazi, to bi predstavljalo „dobivanje pristupa” u smislu članka 5. stavka 3. Direktive o e-privatnosti.

46. Za podskup tih kategorija koje predstavljaju poseban interes, ili zbog njihove raširene upotrebe ili zato što je posebna studija opravdana s obzirom na okolnosti njihove upotrebe, u nastavku je navedena posebna analiza.

3.1 URL i piksel za praćenje

47. Piksel za praćenje je hiperveza na izvor, obično slikovnu datoteku, ugrađenu u sadržaj kao što su internetske stranice ili e-pošta. Taj piksel obično ne ispunjava nikakvu svrhu povezanu sa samim zatraženim sadržajem. Njegova je jedina svrha automatski uspostaviti komunikaciju klijenta s domaćinom piksela do koje inače ne bi došlo. Međutim, to nije sustavno, a pikseli za praćenje mogu se izraditi i dodavanjem dodatnih informacija u poveznice na učitavanje slika koje su relevantne za sadržaj koji se prikazuje korisniku. Uspostavljanje komunikacije prenosi različite informacije domaćinu piksela, ovisno o konkretnom slučaju uporabe.

48. U slučaju elektroničke pošte pošiljatelj može uključiti piksel za praćenje kako bi otkrio kad primatelj čita poruku e-pošte. Pikseli za praćenje na mrežnim stranicama mogu se povezati sa subjektom koji prikuplja mnoge takve zahtjeve i time može pratiti ponašanje korisnika. Takvi pikseli za praćenje također mogu sadržavati dodatne identifikatore, metapodatke ili sadržaj kao dio poveznice. Vlasnik mrežnog mjesta može dodati te podatkovne točke koje mogu biti povezane s korisnikovom aktivnošću na tom mrežnom mjestu kako bi se mogla generirati analitička izvješća o uporabi. Mogu se dinamički generirati i primjenom aplikativne logike na strani klijenta koju isporučuje subjekt.

49. Veze za praćenje mogu funkcionirati na isti način, ali identifikator je priložen adresi mrežnog mjesta. Kad korisnik posjeti jedinstveni lokator resursa („URL”), ciljano mrežno mjesto učitava traženi resurs, ali i prikuplja identifikator koji nije relevantan u smislu identifikacije resursa. Internetske stranice e-trgovine vrlo ih često upotrebljavaju za utvrđivanje podrijetla svojeg ulaznog izvora prometa. Na primjer, takve mrežne stranice mogu pružati praćene poveznice na partnere koje mogu upotrebljavati u svojoj domeni kako bi mrežne stranice za e-trgovinu znale koji su njihovi partneri odgovorni za prodaju i plaćaju proviziju, što je praksa poznata kao povezani marketing.

50. I veze za praćenje i pikseli za praćenje mogu se distribuirati putem različitih kanala, na primjer putem e-pošte, mrežnih stranica ili čak, u slučaju veza za praćenje, putem bilo koje vrste sustava za razmjenu tekstualnih poruka. Ta distribucija korisnikovoj terminalnoj opremi predstavlja pohranu, barem putem mehanizma za privremenu memoriju softvera na strani klijenta. Kao takav, primjenjuje se članak 5. stavak 3. Direktive o e-privatnosti, čak i ako ta pohrana nije trajna.

51. Dodavanje informacija o praćenju URL-ovima ili slikama (pikselima) koje se šalju korisniku predstavlja uputu terminalnoj opremi za vraćanje ciljanih informacija (određeni identifikator). U slučaju dinamički konstruiranih piksela za praćenje, uputa se sastoji od distribucije aplikativne logike (obično JavaScript koda). Slijedom toga, može se smatrati da prikupljanje identifikatora koji se pružaju putem takvih mehanizama praćenja predstavlja „navođenje pristupa” u smislu članka 5. stavka 3. Direktive o elektroničkoj praksi te se stoga primjenjuje i na taj korak.

3.2 Lokalna obrada

52. Neke se tehnologije oslanjaju na lokalnu obradu u skladu s uputama za softver koji se distribuira u terminalnu opremu korisnika, pri čemu se informacije dobivene lokalnom obradom zatim stavljaju na

raspolaganje odabranim subjektima putem API-ja na strani klijenta. To, na primjer, može biti slučaj s API-jem koji osigurava internetski preglednik, pri čemu se lokalno generiranim rezultatima može pristupiti na daljinu.

53. Ako se u bilo kojem trenutku i na primjer u kodu na strani klijenta obrađene informacije stave na raspolaganje trećoj strani, na primjer, šalju se natrag putem mreže poslužitelju, takva bi operacija (prema uputama subjekta koji proizvodi kôd na strani klijenta distribuiran na korisničkoj terminalnoj opremi) činila „dobivanje pristupa već pohranjenim informacijama". Činjenica da se te informacije proizvode lokalno ne isključuje primjenu članka 5. stavka 3. Direktive o e-privatnosti.

3.3 Praćenje samo na osnovi IP-a

54. Neki pružatelji usluga razvijaju rješenja koja se oslanjaju samo na prikupljanje jedne komponente, odnosno IP adrese, kako bi pratili navigaciju[28] korisnika, u nekim slučajevima u više domena. U tom kontekstu mogao bi se primjenjivati članak 5. stavak 3. Direktive o e-privatnosti iako je nalog za stavljanje intelektualnog vlasništva na raspolaganje dao subjekt koji nije subjekt primatelj.

55. Međutim, dobivanje pristupa IP adresama dovelo bi do primjene članka 5. stavka 3. Direktive o e-privatnosti samo u slučajevima kada te informacije potječu iz terminalne opreme pretplatnika ili korisnika. Iako to nije sustavno slučaj (na primjer, kad se aktivira CGNAT[29]), statični odlazni IPv4 koji potječe od usmjerivača korisnika spadao bi u taj slučaj, kao i adrese IPV6 jer ih djelomično definira domaćin. Osim ako subjekt može osigurati da IP adresa ne potječe iz terminalne opreme korisnika ili pretplatnika, mora poduzeti sve korake u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti.

56. Iako se u ovim smjernicama ne analizira primjena izuzeća od obveze prikupljanja privole iz članka 5. stavka 3. Direktive o e-privatnosti, važno je ponovno podsjetiti da primjenjivost tog članka ne znači da se privola mora sustavno pribavljati. EDPB stoga podsjeća da bi u svakom slučaju trebalo procijeniti je li potrebna privola ili bi se moglo primijeniti izuzeće iz članka 5. stavka 3. Direktive o e-privatnosti[30].

3.4 Izvješćivanje o IoT-u povremeno i s posredovanjem

57. Uređaji interneta stvari (IoT) kontinuirano proizvode informacije tijekom vremena, na primjer putem senzora ugrađenih u uređaj, koji mogu ili ne moraju biti prethodno obrađeni na lokalnoj razini. U mnogim se slučajevima informacije stavljaju na raspolaganje udaljenom poslužitelju, ali se modaliteti tog prikupljanja mogu razlikovati.

58. Neki uređaji interneta stvari imaju izravnu vezu s javnom komunikacijskom mrežom s mobilnom SIM karticom. Drugi mogu biti neizravno povezani s javnom komunikacijskom mrežom, na primjer uporabom bežične mreže ili prijenosom informacija na drugi uređaj putem povezivanja od točke do točke (na primjer, preko Bluetootha). Drugi uređaj može, na primjer, biti pametni telefon ili poseban pristupnik koji može ili ne mora prethodno obraditi informacije prije njihova slanja poslužitelju.

[28] To je dodatno i neovisno o upotrebi i funkciji IP adrese za uspostavu, isporuku ili prijenos temeljnih tehničkih komunikacija ili činjenici da to mogu ili ne moraju biti osobni podatci (u pogledu analize e-privatnosti riječ je o „informacijama").
[29] Pružatelj internetskih usluga upotrebljava sustav za prevođenje mrežnih adresa na nivou poslužitelja (engl. *Carrier-grade NAT, CGNAT*) kako bi maksimalno iskoristio ograničeni prostor za IP adresu. On grupira broj pretplatnika pod istom javnom IP adresom.
[30] U Mišljenju 9/2014 Radne skupine iz članka 29. predviđeni su neki primjeri kada privola možda neće biti potrebna.

59. Proizvođač može od uređaja za internet stvari zatražiti da uvijek usmjere prikupljene informacije, ali da prvo lokalno predmemoriraju informacije, na primjer dok veza ne bude dostupna.

60. U svakom slučaju, uređaj interneta stvari, kad je povezan (izravno ili neizravno) na javnu komunikacijsku mrežu, sam bi se smatrao terminalnom opremom. Činjenica da se informacije prenose putem interneta ili se pohranjuju u predmemoriju radi povremenog izvješćivanja ne mijenja prirodu tih informacija. U obje bi se situacije članak 5. stavak 3. Direktive o e-privatnosti primjenjivao jer postoji „dobivanje pristupa" u obliku naputka koda na uređaju interneta stvari za slanje dinamički pohranjenih podataka na udaljeni poslužitelj.

3.5 Jedinstveni identifikator

61. Zajednički alat koji upotrebljavaju poduzeća jest pojam „jedinstveni identifikator" ili „trajni identifikator". Takvi identifikatori mogu se dobiti iz trajnih osobnih podataka (ime i prezime, e-adresa, telefonski broj itd.) koji se raspršuju na korisnikov uređaj, prikupljaju i dijele među nekoliko voditelja obrade kako bi se osoba na jedinstven način identificirala putem različitih skupova podataka (podatci o upotrebi prikupljeni upotrebom mrežnog mjesta ili aplikacije, podatci o upravljanju odnosima s klijentima povezani s kupnjom ili pretplatom na internetu ili izvan njega itd.). Trajni osobni podatci na mrežnim mjestima obično se prikupljaju u kontekstu autentifikacije ili pretplate na biltene.

62. Kako je prethodno navedeno, činjenica da korisnik unosi informacije ne bi spriječila primjenu članka 5. stavka 3. Direktive o e-privatnosti u pogledu pohrane jer se te informacije privremeno pohranjuju u terminalnoj opremi prije njihova prikupljanja.

63. U kontekstu prikupljanja „jedinstvenih identifikatora" na mrežnim stranicama ili mobilnim aplikacijama, subjekt koji prikuplja daje upute pregledniku (putem distribucije kôda na strani klijenta) da pošalje te podatke. Stoga je u tijeku „odobrenje pristupa" i primjenjuje se članak 5. stavak 3. Direktive o e-privatnosti.