Smernice

Smernice 2/2023 o tehničnem področju uporabe tretjega odstavka 5. člena Direktive o zasebnosti in elektronskih komunikacijah

Različica 2.0

Sprejete 7. oktobra 2024

Zgodovina različic

Različica 1.0	14. november 2023	Sprejetje smernic za javno posvetovanje
Različica 2.0	7. oktober 2024	Sprejetje smernic po javnem posvetovanju

Povzetek

EOVP v teh smernicah obravnava uporabnost tretjega odstavka 5. člena Direktive o zasebnosti in elektronskih komunikacijah za različne tehnične rešitve. Te smernice dopolnjujejo Mnenje št. 9/2014 delovne skupine iz člena 29 o uporabi Direktive o zasebnosti in elektronskih komunikacijah v zvezi z napravami za odvzem prstnih odtisov, njihov cilj pa je zagotoviti jasno razumevanje tehničnih postopkov iz tretjega odstavka 5. člena Direktive o zasebnosti in elektronskih komunikacijah.

Pojav novih metod sledenja, ki nadomeščajo obstoječa orodja za sledenje (na primer piškotke, kjer nekateri ponudniki brskalnikov ne podpirajo več piškotkov tretjih oseb) in ustvarjajo nove poslovne modele, je postal ključni problem varstva osebnih podatkov. Čeprav je uporabnost tretjega odstavka 5. člena Direktive o zasebnosti in elektronskih komunikacijah dobro uveljavljena in se v praksi pogosto aplicira na vrsto metod sledenja, kot so npr. piškotki, je treba odpraviti nejasnosti, povezane z uporabo navedene določbe glede na nova orodja, ki podobno omogočajosledenje posameznikov.

Smernice opredeljujejo tri ključne elemente za uporabnost tretjega odstavka 5. člena Direktive o zasebnosti in elektronskih komunikacijah (oddelek 2.1), in sicer „podatke“, „terminalsko opremo naročnika ali uporabnika“ ter „pridobivanje dostopa in shranjevanje podatkov in shranjene podatke“. Smernice nadalje vsebujejo podrobno analizo vsakega elementa (oddelki 2.2 do 2.6).

V oddelku 3 se ta analiza uporablja kot neizčrpni seznam primerov uporabe, ki pomenijo skupne tehnike, in sicer:

- spletni naslov (URL) in sledenje slikovnim pikam,
- lokalna obdelava,
- sledenje samo na podlagi naslova IP,
- občasno in posredovano poročanje o internetu stvari (IoT),
- enolični identifikator.

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju točke (e) prvega odstavka 70. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju tretjega odstavka 5. člena Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, kakor je bila spremenjena z Direktivo 2009/136/ES (v nadaljevanju: Direktiva o zasebnosti in elektronskih komunikacijah ali Direktiva o e-zasebnosti),

ob upoštevanju 12. in 22. člena svojega poslovnika –

SPREJEL NASLEDNJE SMERNICE:

1 UVOD

1. V skladu s tretjim odstavkom 5. člena Direktive o e-zasebnosti je *„shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika“* dovoljeno le na podlagi privolitve ali potrebe za specifične namene opredeljene v navedenem členu. Kot je opozorjeno v uvodni izjavi 24 Direktive o e-zasebnosti[2], je cilj te določbe zaščititi terminalsko opremo uporabnikov, saj ta spada v njihovov zasebno sfero. Iz besedila člena izhaja, da se tretji odstavek 5. člena Direktive o e-zasebnosti ne uporablja izključno za piškotke, temveč tudi za „podobne tehnologije“. Vendar izčrpen seznam tehničnih operacij, zajetih v tretjem odstavku 5. člena Direktive o e-zasebnosti, trenutno ne obstaja.

2. V Mnenju št. 9/2014 delovne skupine iz člena 29 o uporabi Direktive o e-zasebnosti v zvezi z napravami za odvzem prstnih odtisov je že pojasnjeno, da odvzemanje prstnih odtisov spada na tehnično področje uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti[3], vendar so zaradi precejšnega tehnološkega napredka potrebne dodatne smernice v zvezi s trenutno opaženimi tehnikami sledenja. Tehnično okolje se je v zadnjem desetletju razvilo z vse večjo uporabo identifikatorjev, vgrajenih v operacijske sisteme, pa tudi z oblikovanjem novih orodij, ki omogočajo shranjevanje podatkov v terminalski opremi.

[1] Sklicevanje na „države članice“ v tem dokumentu je treba razumeti kot sklicevanje na „države članice EGP“.

[2] „Terminalna oprema uporabnikov omrežij elektronskih komunikacij in vsak podatek, shranjen na taki opremi, sta del zasebnega področja uporabnikov, ki zahteva varstvo v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin. Tako imenovana vohunska programska oprema, program za prikriti nadzor računalnika, omrežni hrošči, skriti identifikatorji in druge podobne naprave lahko vdrejo v uporabnikov terminal brez njegove vednosti, da bi pridobili dostop do podatkov, shranili skrite podatke ali izsledili uporabnikove dejavnosti, in lahko resno motijo zasebnost teh uporabnikov. Uporaba takih naprav mora biti dovoljena samo za zakonite namene, z vednostjo zadevnih uporabnikov.“

[3] Mnenje št. 9/2014 delovne skupine iz člena 29, str. 11.

3. Dvoumnosti glede področja uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti so spodbudile uvajanje alternativnih rešitev za sledenje internetnim uporabnikom in vodile k izogibanju pravnim obveznostim iz tretjega odstavka 5. člena Direktive o e-zasebnosti. Vsi taki primeri zbujajo zaskrbljenost in zahtevajo dodatno analizo za dopolnitev prejšnjih smernic EOVP.

4. Namen teh smernic je izvesti tehnično analizo področja uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti, in sicer pojasniti, kaj je tehnično zajeto s stavkom „*shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika*“. Te smernice ne obravnavajo okoliščin, v katerih lahko za dejanje obdelave veljajo izjeme od zahteve po privolitvi, določene v Direktivi o e-zasebnosti[4], saj je treba te okoliščine analizirati od primera do primera, pri čemer je treba upoštevati prenos(-e) zadevne države članice in smernice, ki jih izdajo nacionalni pristojni organi.

5. Neizčrpen seznam posebnih primerov uporabe bo analiziran v zadnjem delu teh smernic.

2 ANALIZA

2.1 Ključni elementi za uporabnost tretjega odstavka 5. člena Direktive o e-zasebnosti

6. Tretji odstavek 5. člena Direktive o e-zasebnosti se uporablja, če:

   a. **MERILO A:** se izvedene operacije nanašajo na „*podatke*“. Opozoriti je treba, da se ne uporablja izraz „osebni podatki“, temveč „podatki“.

   b. **MERILO B:** izvedene operacije vključujejo „*terminalsko opremo*“ naročnika ali uporabnika (B.1), kar pomeni, da je treba oceniti pojem „*javno komunikacijsko omrežje*“ (B.2).

   c. **MERILO C** izvedene operacije dejansko pomenijo „*shranjevanje*“ (C.1) ali „*pridobivanje dostopa*“ (C.2). Ta dva pojma je mogoče proučevati neodvisno, kot je opozorjeno v Mnenju št. 9/2014 delovne skupine iz člena 29: *Uporaba besed „shranjen ali dostopen“ pomeni, da ni nujno, da se shranjevanje in dostop zgodita v isti komunikaciji in da ju opravi ista stranka*[5]*.*

   Zaradi berljivosti se subjekt, ki pridobi dostop do podatkov, shranjenih v uporabnikovi terminalski opremi, v nadaljevanju imenuje „subjekt, ki dostopa“.

2.2 Pojem „podatki“ – merilo A

7. Kot je navedeno pod MERILOM A, ta oddelek podrobno opisuje, kaj zajema pojem „podatki“. Izbira izraza „podatki“, ki zajema širšo kategorijo kot zgolj pojem „osebni podatki“, je povezana s področjem uporabe Direktive o e-zasebnosti.

8. Cilj tretjega odstavka 5. člena Direktive o e-zasebnosti je zaščititi zasebno sfero uporabnikov, kot je navedeno v uvodni izjavi 24: „*Terminalna oprema uporabnikov omrežij elektronskih komunikacij in vsak podatek, shranjen na taki opremi, sta del zasebnega področja uporabnikov, ki zahteva varstvo v*

[4] Kot je navedeno v tretjem odstavku 5. člena Direktive o e-zasebnosti: „*To ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja, ali, če je nujno potrebno, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata.*“

[5] Mnenje št. 9/2014 delovne skupine iz člena 29, str. 8.

skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin“. Zaščitena je tudi s 7. členom Listine EU o temeljnih pravicah.

9. Dejansko so scenariji, ki posegajo v to zasebno sfero, čeprav ne vključujejo osebnih podatkov, izrecno zajeti v besedilu tretjega odstavka 5. člena in uvodne izjave 24 Direktive o e-zasebnosti, na primer shranjevanje virusov v uporabnikovi terminalski opremi. To kaže, da opredelitev pojma „podatki“ ne bi smela biti omejena na lastnost, da je povezana z določeno ali določljivo fizično osebo.

10. Slednje je potrdilo tudi Sodišče EU: „*To varstvo velja za vse podatke, shranjene v tej terminalni opremi, ne glede na to, ali gre za osebne podatke, in njegov namen je, kot je razvidno iz iste uvodne izjave, varstvo uporabnikov pred nevarnostjo vdorov skritih identifikatorjev ali drugih podobnih naprav v terminalno opremo teh uporabnikov brez njihove vednosti*“[6].

11. Vprašanja o tem, ali bi bilo treba pri ocenjevanju uporabnosti tretjega odstavka 5. člena Direktive o e-zasebnosti upoštevati izvor teh podatkov in razloge, zakaj so shranjeni v terminalski opremi, so bila predhodno pojasnjena. Na primer v Mnenju št. 9/2014 delovne skupine iz člena 29: „*Razlaga, da tretja oseba ne potrebuje privolitve za dostop do teh podatkov samo zato, ker jih ni shranila, ni pravilna. Zahteva glede privolitve se uporablja tudi, kadar se dostopa do različice, ki je namenjena samo za branje (na primer zahteva po naslovu MAC omrežnega vmesnika prek OS API)*“[7].

12. Skratka, pojem podatka vključuje neosebne in osebne podatke, ne glede na to, kako so bili shranjeni in kdo jih je hranil, tj. zunanji subjekt (vključno z drugimi subjekti, ki nimajo dostopa), uporabnik, proizvajalec ali kako drugače.

2.3 Pojem „terminalna oprema naročnika ali uporabnika“ – merilo B.1

13. Ta oddelek temelji na opredelitvi iz Direktive 2008/63/ES in na katero se sklicuje opredelitev v 2. členu Direktive (EU) 2018/1972, v kateri „terminalska oprema“ pomeni: „*vso opremo, ki je neposredno ali posredno priključena na mrežni vmesnik javnega telekomunikacijskega omrežja za pošiljanje, obdelovanje ali sprejemanje informacij; v obeh primerih (neposredna ali posredna) se lahko priključitev izvede z žico, optičnim kablom ali elektromagnetno; priključitev je posredna, če je oprema nameščena med terminalom in javnim mrežnim vmesnikom*“[8].

14. Uvodna izjava 24 Direktive o e-zasebnosti zagotavlja jasno razumevanje vloge terminalske opreme pri varstvu, ki ga zagotavlja tretji odstavek 5. člena Direktive o e-zasebnosti. Direktiva o e-zasebnosti varuje zasebnost uporabnikov ne le v zvezi z zaupnostjo njihovih podatkov, temveč tudi z varovanjem celovitosti njihove terminalske opreme. To razumevanje bo vodilo pri razlagi pojma terminalske opreme v vseh teh smernicah.

15. Člen 3 Direktive o e-zasebnosti določa, da mora biti obdelava osebnih podatkov izvedena v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih, da bi se Direktiva o e-zasebnosti lahko uporabljala. To pomeni, da bi morala biti naprava uporabna v povezavi s tovrstno storitvijo in da bi morala biti povezana ali povezljiva[9] z vmesnikom javnega komunikacijskega omrežja, da bi jo lahko opredelili kot terminalsko opremo. EOVP ugotavlja,

[6] Sodba Sodišča z dne 1. oktobra 2019, *Planet 49*, zadeva C-673/17, ECLI:EU:C:2019:801, točka 70.
[7] Mnenje št. 9/2014 delovne skupine iz člena 29, str. 8.
[8] Direktiva Komisije 2008/63/ES z dne 20. junija 2008 o konkurenci na trgih za telekomunikacijsko terminalsko opremo (kodificirano besedilo), prvi odstavek 1. člena.
[9] To pomeni, da ima tehnične zmogljivosti za priključitev na omrežje, tudi če ta povezava trenutno ni vzpostavljena.

da so spremembe iz leta 2009[10] v besedilu tretjega odstavka 5. člena Direktive o e-zasebnosti razširile varstvo terminalske opreme s črtanjem sklicevanja na „uporabo elektronskega komunikacijskega omrežja“ kot sredstva za shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi. Dokler ima naprava omrežni vmesnik, ki mu omogoča priključitev (tudi če taka povezava ni vzpostavljena), se tretji odstavek 5. člena Direktive o e-zasebnosti uporablja za vse subjekte, ki bi hranili in pridobivali dostop do podatkov, ki so že shranjeni v terminalski opremi, ne glede na sredstvo dostopa do terminalske opreme in ne glede na to, ali je povezano z omrežjem ali odklopljeno z njega.

16. Oprema, ki je del javnega elektronskega komunikacijskega omrežja, se ne bi štela za terminalsko opremo v skladu s tretjim odstavkom 5. člena Direktive o e-zasebnosti[11].

17. Terminalska oprema je lahko sestavljena iz poljubnega števila posameznih delov strojne opreme, ki skupaj tvorijo terminalsko opremo. Ta je lahko (ali ne) v obliki fizično zaprte naprave, ki vsebuje vso strojno opremo za prikazovanje, obdelavo, shranjevanje in periferno opremo (na primer pametni telefoni, prenosni računalniki, na omrežje priključene naprave za shranjevanje, povezani avtomobili ali povezani televizorji, pametna očala).

18. Direktiva o e-zasebnosti priznava, da varstvo zaupnosti podatkov, shranjenih v uporabnikovi terminalski opremi, in celovitosti uporabnikove terminalske opreme ni omejeno na varovanje zasebne sfere fizičnih oseb, temveč se nanaša tudi na pravico do spoštovanja njegove korespondence ali na zakonite interese pravnih oseb[12]. Terminalsko opremo, ki omogoča korespondenco in izvajanje zakonitih interesov pravnih oseb, kot takšno varuje tretji odstavek 5. člena Direktive o e-zasebnosti.

19. Uporabnik ali naročnik ima lahko terminalsko opremo v lasti, jo najame ali kako drugače pridobi. Več uporabnikov ali naročnikov lahko deli isto terminalsko opremo.

20. Direktiva o e-zasebnosti tovrstno varstvo daje terminalski opremi, povezani z uporabnikom ali naročnikom, in ni odvisno od tega, ali uporabnik vzpostavi sredstvo dostopa (na primer, če je začel elektronsko komunikacijo), niti od tega, ali je seznanjen z navedenim načinom dostopa.

2.4 Pojem „javno komunikacijsko omrežje“ – merilo B.2

21. Ker je položaj, ki ga ureja Direktiva o e-zasebnosti, povezan z „ *javno razpoložljivimi elektronskimi komunikacijskimi storitvami v javnih komunikacijskih omrežjih v Skupnosti*“[13], opredelitev terminalske opreme pa izrecno omenja pojem „*javno komunikacijsko omrežje*“, je bistveno pojasniti ta pojem, da se določi okvir, v katerem se uporablja tretji odstavek 5. člena Direktive o e-zasebnosti.

22. Pojem elektronskega komunikacijskega omrežja v Direktivi o e-zasebnosti ni opredeljen. Ta pojem je bil prvotno omenjen v Direktivi 2002/21/ES (okvirna direktiva) o skupnem regulativnem okviru za

[10] Direktiva 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov (besedilo velja za EGP), UL L 337, 18. 12. 2009, peti odstavek 2. člena in uvodna izjava 65.

[11] Za opredelitev omejitev omrežja v različnih okoljih glejte Smernice organa BEREC o skupnih pristopih k opredelitvi omrežne priključne točke v različnih omrežnih topologijah (BoR (20) 46).

[12] Kot sledi iz trinajstega odstavka 2. člena Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah, je uporabnik lahko fizična ali pravna oseba.

[13] Člen 3 Direktive o e-zasebnosti.

elektronska komunikacijska omrežja in storitve[14], ki ga je pozneje nadomestila opredelitev iz prvega odstavka 2. člena Direktive 2018/1972 (Evropski zakonik o elektronskih komunikacijah). Zdaj se glasi:

> *„elektronsko komunikacijsko omrežje“ pomeni prenosne sisteme, ne glede na to, ali temeljijo na stalni infrastrukturi ali centralizirani upravni zmogljivosti, in, kjer je primerno, komutacijsko ali usmerjalno opremo ter druge vire, vključno z omrežnimi elementi, ki niso aktivni, ki omogočajo prenos signalov po žicah, z radijskimi valovi, z optičnimi ali drugimi elektromagnetnimi sredstvi, vključno s satelitskimi omrežji, fiksnimi (vodovno in paketno komutiranimi, vključno z internetom) in mobilnimi omrežji, električnimi kabelskimi sistemi, če se uporabljajo za prenos signalov, omrežji, ki se uporabljajo za radijsko in televizijsko radiodifuzijo, ter z omrežji kabelske televizije, ne glede na vrsto prenesenih informacij.*[15]

23. Ta opredelitev je nevtralna kar zadeva tehnologije prenosa. Elektronsko komunikacijsko omrežje je v skladu s to opredelitvijo vsak omrežni sistem, ki omogoča prenos elektronskih signalov med svojimi vozlišči ne glede na uporabljeno opremo in protokole.

24. Pojem elektronskega komunikacijskega omrežja v skladu z Direktivo 2018/1972 ni odvisen niti od javne ali zasebne narave infrastrukture niti od načina njegove uvedbe ali upravljanja („*ne glede na to, ali temeljijo na stalni infrastrukturi ali centralizirani upravni zmogljivosti*“[16]). Zato je opredelitev elektronskega komunikacijskega omrežja iz 2. člena Direktive 2018/1972 dovolj široka, da zajema katero koli vrsto infrastrukture. Vključuje omrežja, ki jih upravlja ali ne upravlja operater, omrežja, ki jih soupravlja skupina operaterjev, ali celo priložnostna omrežja, v katerih se lahko terminalska oprema dinamično pridruži mreži druge terminalske opreme ali jo zapusti s pomočjo protokolov za prenos na kratke razdalje.

25. Ta opredelitev omrežja ne določa nobene omejitve glede števila terminalske opreme, ki je kadar koli prisotna v omrežju. Nekatere omrežne sheme se zanašajo na vozlišča, ki priložnostno posredujejo podatke vozliščem, ki so trenutno povezana[17], v nekem trenutku pa lahko komunicirata le dva enakovredna uporabnika. Taki primeri bi spadali v splošno področje uporabe Direktive o e-zasebnosti, če bi omrežni protokol omogočal nadaljnjo vključitev enakovrednih uporabnikov.

26. Za to, da se naprava šteje za terminalsko opremo, in posledično za uporabnost tretjega odstavka 5. člena Direktive o e-zasebnosti je potrebna javna uporabnost komunikacijskega omrežja. Opozoriti je treba, da dejstvo, da je omrežje na voljo omejeni podskupini javnosti (na primer naročnikom, ki plačujejo ali ne, pod pogoji upravičenosti), ne pomeni, da je tako omrežje zasebno[18].

2.5 Pojem „pridobivanje dostopa“ – merilo C.1

27. Za pravilno opredelitev pojma „pridobivanje dostopa“ je pomembno upoštevati področje uporabe Direktive o e-zasebnosti, navedeno v njenem 1. členu: „*enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih*

[14] Direktiva Evropskega parlamenta in Sveta 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva)
[15] Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (prenovitev) (besedilo velja za EGP, člen 2(1).)
[16] Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (prenovitev) (besedilo velja za EGP, člen 2(1).)
[17] Na primer v okviru sheme mrežnega povezovanja, odporne proti zamudam, ki izvaja „tehnike shranjevanja in posredovanja“, kot je projekt odprtega vira Briar.
[18] Za nadaljnjo analizo identifikacije javnih komunikacijskih omrežij glejte Smernice BEREC o izvajanju Uredbe o dostopu do odprtega interneta (BoR (20) 112).

komunikacij in za zagotovitev prostega pretoka takih podatkov ter elektronske komunikacijske opreme in storitev v Skupnosti“.

28. Na kratko, Direktiva o e-zasebnosti je pravni instrument za ohranjanje zasebnosti, s ciljem zaščititi zaupnost komunikacij in celovitosti naprav. V uvodni izjavi 24 Direktive o e-zasebnosti je pojasnjeno, da je v primeru fizičnih oseb terminalska oprema uporabnikov del njihove zasebne sfere in da lahko dostop do podatkov, shranjenih v njej brez njihove vednosti, resno posega v njihovo zasebnost.

29. Tudi pravne osebe so zaščitene z Direktivo o e-zasebnosti[19]. Zato je treba pojem „pridobivanje dostopa“ iz tretjega odstavka 5. člena Direktive o e-zasebnosti razlagati na način, ki varuje te pravice pred kršitvami s strani tretjih oseb.

30. Shranjevanje podatkov ali pridobivanje dostopa sta lahko neodvisni operaciji, ki ju izvajajo neodvisni subjekti. Ni nujno, da sta prisotna tako shranjevanje podatkov kot tudi dostop do že shranjenih podatkov, da bi se lahko uporabljal tretji odstavek 5. člena Direktive o e-zasebnosti.

31. Kot je navedeno v Mnenju 9/2014 delovne skupine iz člena 29: „*Uporaba besed 'shranjen ali dostopen' pomeni, da ni nujno, da se shranjevanje in dostop zgodita v isti komunikaciji in da ju opravi ista stranka. Podatki, ki jih hrani ena stranka (vključno s podatki, ki jih hrani uporabnik ali proizvajalec naprave), do katerih pozneje dostopa druga stranka, zato spadajo na področje uporabe člena 5(3)*“[20]. Zato za uporabo pojma dostopa ni nobenih omejitev glede izvora podatkov v terminalski opremi.

32. Kadar koli subjekt sprejme ukrepe za pridobivanje dostopa do podatkov, shranjenih v terminalski opremi, bi se uporabljal tretji odstavek 5. člena Direktive o e-zasebnosti. To običajno pomeni, da mora subjekt, ki dostopa, proaktivno pošiljati posebna navodila terminalski opremi, da bi pridobil ciljne podatke. To velja na primer za piškotke, pri katerih subjekt, ki dostopa, naroči terminalski opremi, naj proaktivno pošilja podatke ob vsakem naslednjem klicu protokola za prenos hiperteksta („HTTP“).

33. To velja tudi takrat, ko subjekt, ki dostopa, v terminalski opremi uporabnika distribuira programsko opremo, ki je shranjena, in nato prek omrežja proaktivno pokliče končno točko vmesnika za programiranje aplikacij („API“). Dodatni primeri vključujejo kodo JavaScript, pri kateri subjekt, ki dostopa, naroči brskalniku uporabnika, naj pošlje asinhrone zahtevke s ciljno usmerjenimi podatki. Tak dostop očitno spada na področje uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti, saj subjekt, ki dostopa, terminalski opremi izrecno naroči, naj pošlje podatke.

34. V nekaterih primerih subjekt, ki daje navodila terminalski opremi za pridobitev ciljnih podatkov, in subjekt, ki prejema podatke, morda nista ista. To lahko izhaja iz določbe in/ali uporabe skupnega mehanizma med obema subjektoma. Navodilo napravi za pošiljanje že shranjenih podatkov (na primer z uporabo protokola ali SDK, ki pomeni,[21] da terminalska oprema proaktivno pošilja podatke) omogoča vdor v terminalsko opremo, zato tak dostop sproži uporabnost tretjega odstavka 5. člena Direktive o e-zasebnosti. Kot je navedeno v Mnenju št. 09/2014 delovne skupine iz člena 29, se to lahko zgodi, kadar spletno mesto naroči terminalski opremi, da pošlje informacije oglaševalskim storitvam tretjih oseb z vključitvijo sledilnih pikslev (t.i. tracking pixel)[22]. Ta primer uporabe je podrobneje opisan v oddelku 3.1.

[19] Uvodna izjava 26 Direktive o e-zasebnosti, glejte odstavek 17 zgoraj.
[20] Mnenje št. 9/2014 delovne skupine iz člena 29, str. 8.
[21] SDK („komplet za razvoj programske opreme“) je sklop orodij za razvoj programske opreme, ki so na voljo za lažje ustvarjanje aplikativne programske opreme.
[22] Mnenje št. 9/2014 delovne skupine iz člena 29, str. 9.

2.6 Pojma „shranjevanje podatkov“ in „shranjeni podatki“ – merilo C.2

35. Shranjevanje podatkov v smislu tretjega odstavka 5. člena Direktive o e-zasebnosti se nanaša na dajanje podatkov na fizični elektronski pomnilniški medij, ki je del terminalske opreme uporabnika ali naročnika[23].

36. Običajno se podatki ne shranjujejo v terminalski opremi uporabnika ali naročnika z neposrednim dostopom do pomnilnika naprave s strani druge osebe, temveč z navodili za ustvarjanje določenih podatkov s programsko opremo na terminalski opremi. Šteje se, da je shranjevanje, ki poteka prek takih navodil, neposredno sprožila druga stranka. To vključuje uporabo uveljavljenih protokolov, kot sta shranjevanje piškotkov v brskalniku in prilagojena programska oprema, ne glede na to, kdo je ustvaril ali namestil protokole ali programsko opremo v terminalski opremi.

37. V Direktivi o e-zasebnosti ni določena zgornja ali spodnja meja meja, kako dolgo morajo podatki ostati na pomnilniškem mediju, da se šteje, da so shranjeni, niti ni zgornje ali spodnje meje količine podatkov, ki jih je treba shraniti.

38. Prav tako pojem shranjevanja ni odvisen od vrste nosilca, na katerem so shranjeni podatki. Tipični primeri vključujejo trde diske („HDD“), polprevodniške pogone („SSD“), električno izmenljivi programirljivi bralni pomnilnik („EEPROM“) in pomnilnik z naključnim dostopom („RAM“), vendar s področja uporabe niso izključeni tudi manj tipični scenariji, ki vključujejo medij, kot je magnetni trak ali predpomnilnik centralne procesne enote („CPU“). Pomnilniški medij je lahko povezan interno (na primer prek povezave SATA) ali zunanje (na primer prek povezave USB).

39. „Shranjeni podatki“ se nanašajo na podatke, ki že obstajajo na terminalski opremi, ne glede na vir ali naravo teh podatkov. To vključuje vse rezultate shranjevanja podatkov v smislu tretjega odstavka 5. člena Direktive o e-zasebnosti, kot je opisano zgoraj (bodisi s strani iste stranke, ki bo pozneje pridobila dostop, bodisi s strani druge tretje osebe). Poleg tega vključuje rezultate postopkov shranjevanja podatkov, ki presegajo področje uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti, kot so: shranjevanje na terminalski opremi s strani uporabnika ali naročnika ali proizvajalca strojne opreme (kot so naslovi MAC krmilnikov omrežnih vmesnikov), senzorji, vgrajeni v terminalsko opremo, ali postopki in programi, izvedeni na terminalski opremi, ki lahko dajejo podatke, ki so odvisni od shranjenih podatkov ali izhajajo iz njih, ali pa tudi ne.

3 PRIMERI UPORABE

40. Kot je poudarjeno v uvodu teh smernic[24], v njih ni analizirana uporaba izjem od obveznosti pridobitve privolitve iz tretjega odstavka 5. člena Direktive o e-zasebnosti. EOVP opozarja, da bi bilo treba v vseh primerih shranjevanja podatkov ali pridobivanja dostopa do že shranjenih podatkov oceniti, ali je potrebna privolitev oziroma ali bi se lahko uporabila izjema na podlagi tretjega odstavka 5. člena Direktive o e-zasebnosti. Zato mora bralec v povezavi s to tehnično analizo proučiti izjeme glede na svoj primer uporabe.

41. Brez poseganja v posebne okoliščine, v katerih se lahko uporabljajo tiste tehnične kategorije, ki so potrebne za opredelitev, ali se uporablja tretji odstavek 5. člena Direktive o e-zasebnosti, je mogoče neizčrpno opredeliti splošne kategorije identifikatorjev in podatkov, ki se pogosto uporabljajo in za katere se lahko uporablja tretji odstavek 5. člena Direktive o e-zasebnosti.

[23] Kot je opredeljeno v oddelku 2.3 teh smernic.
[24] Glejte odstavek 4 zgoraj.

42. Omrežna komunikacija običajno temelji na večplastnem modelu, ki zahteva uporabo identifikatorjev, da se omogoči pravilna vzpostavitev in izvajanje komunikacije. Posredovanje teh identifikatorjev oddaljenim akterjem se izvaja prek programske opreme v skladu z dogovorjenimi komunikacijskimi protokoli. Kot je navedeno zgoraj, dejstvo, da subjekt prejemnik morda ni subjekt, ki daje navodila za pošiljanje podatkov, ne izključuje uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti. To se lahko nanaša na usmerjevalne identifikatorje, kot sta naslova MAC ali IP terminalske opreme, pa tudi na identifikatorje seje (SSRC, identifikator spletnega vtičnika) ali avtentikacijske žetone.

43. Na enak način lahko aplikacijski protokol vključuje več mehanizmov za zagotavljanje podatkov o okoliščinah (na primer glavo HTTP, vključno s poljem „sprejmi“, ali uporabniškega agenta), mehanizem predpomnilnika (na primer ETag[25]) ali druge funkcije (med njimi so piškotki ali HSTS[26]). Vnovič lahko uporaba teh mehanizmov za zbiranje podatkov (na primer v okviru odvzema prstnih odtisov[27] ali sledenja identifikatorjem vira) privede do uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti.

44. Po drugi strani pa obstajajo nekatere okoliščine, v katerih lokalne aplikacije, nameščene v terminalski opremi, uporabljajo nekatere podatke izključno znotraj terminala, kot se lahko zgodi pri vmesnikih API za sisteme pametnih telefonov (dostop do kamere, mikrofona, senzorja GPS, čipa za merjenje pospeškov, radijskega čipa, lokalnega dostopa do datotek, seznama kontaktnih podatkov, dostopa do identifikatorjev itd.). To bi lahko veljalo tudi za spletne brskalnike, ki obdelujejo podatke, shranjene ali ustvarjene znotraj naprave (kot so piškotki, lokalno shranjevanje, WebSQL ali celo podatke, ki jih zagotovijo uporabniki sami). Uporaba takih podatkov v aplikaciji ne bi pomenila „pridobivanje dostopa do že shranjenih podatkov“ v smislu tretjega odstavka 5. člena Direktive o e-zasebnosti, dokler podatki ne zapustijo naprave, vendar bi se ob dostopu do teh podatkov ali kakršne koli izpeljave teh podatkov uporabljal tretji odstavek 5. člena Direktive o e-zasebnosti.

45. V nekaterih primerih akteriji distribuirajo zlonamerne elemente programske opreme, na primer programsko opremo za rudarjenje kriptovalut ali, splošneje, zlonamerno programsko opremo, ki izrablja zmožnosti obdelave terminalske opreme v korist akterja distribucije. Distribucija navedene zlonamerne programske opreme v uporabnikovi terminalski opremi bi pomenila „shranjevanje“ v smislu tretjega odstavka 5. člena Direktive o e-zasebnosti. Poleg tega bi programska oprema, če bi vzpostavila omrežno povezavo za poznejše pošiljanje podatkov, pomenila „pridobivanje dostopa“ v smislu tretjega odstavka 5. člena Direktive o e-zasebnosti.

46. Za podskupino teh kategorij, ki pomenijo poseben interes, bodisi zaradi njihove razširjene uporabe bodisi zato, ker je glede na okoliščine njihove uporabe upravičena posebna študija, je v nadaljevanju navedena posebna analiza.

3.1 Spletni naslov (URL) in sledenje slikovnim pikam

47. Slikovna pika (ang. pixel) za sledenje je hiperpovezava na vir, običajno slikovno datoteko, ki je vstavljena v del vsebine, kot sta spletno mesto ali e-poštno sporočilo. Ta slikovna pika običajno nima nobenega namena, povezanega z zahtevano vsebino; njen edini namen je samodejno vzpostaviti komunikacijo med stranko in gostiteljem slikovne pike, do katere sicer ne bi prišlo. Vendar to ni sistematično, slikovne pike za sledenje pa je mogoče ustvariti tudi z dodajanjem dodatnih podatkov

[25] HTTP ETag je identifikator, ki omogoča, da se na podlagi veljavnosti v predpomnilniku shranjenih podatkov o strankah vloži pogojna zahteva.
[26] HTTP Strict Transport Security (HSTS) omogoča strežnikom, da opredelijo, katere vire je treba vedno zahtevati z uporabo povezav HTTPS.
[27] Kot je navedeno v uvodu, glejte Mnenje št. 9/2014 delovne skupine iz člena 29 o uporabi direktive o e-zasebnosti v zvezi z napravami za odvzem prstnih odtisov.

slikam za nalaganje hiperpovezav, ki so pomembne za vsebino, prikazano uporabniku. Vzpostavitev komunikacije posreduje različne podatke gostitelju slikovne pike, odvisno od konkretnega primera uporabe.

48. V primeru elektronskega sporočila lahko pošiljatelj vključi slikovno piko za sledenje, da zazna, kdaj prejemnik prebere elektronsko sporočilo. Slikovne pike za sledenje na spletnih mestih so lahko povezane s subjektom, ki zbira številne tovrstne zahteve in tako lahko sledi vedenju uporabnikov. Take slikovne pike za sledenje lahko kot del povezave vsebujejo tudi dodatne identifikatorje, metapodatke ali vsebino. Te podatkovne točke lahko doda lastnik spletnega mesta, po možnosti v zvezi z dejavnostjo uporabnika na tem spletnem mestu, da se lahko pripravijo analitična poročila o uporabi. Dinamično jih je mogoče ustvariti tudi z aplikativno logiko na strani stranke, ki jo zagotovi subjekt.

49. Povezave za sledenje (ang. tracking links) lahko delujejo na podoben način, vendar je identifikator priložen naslovu spletišča. Kadar uporabnik obišče enotni naslov vira (URL), ciljno usmerjeno spletišče naloži zahtevani vir, vendar zbira tudi identifikator, ki ni pomemben v smislu identifikacije vira. Spletne strani e-trgovin jih zelo pogosto uporabljajo za ugotavljanje izvora vhodnega vira prometa. Taka spletna mesta lahko na primer partnerjem zagotovijo sledljive povezave, ki jih lahko uporabijo na svoji domeni, tako da spletno mesto e-trgovine ve, kateri od njihovih partnerjev je odgovoren za prodajo, in plača provizijo, kar je praksa, znana kot trženje, povezano s pridruženimi podjetji.

50. Povezave za sledenje in slikovne pike za sledenje se lahko razpošiljajo po najrazličnejših kanalih, na primer prek elektronske pošte, spletnih mest ali, v primeru povezav za sledenje, prek kakršnih koli sistemov za pošiljanje besedilnih sporočil. Ta distribucija na uporabnikovo terminalsko opremo pomeni shranjevanje, vsaj prek mehanizma predpomnilnika programske opreme na odjemalčevi strani. Kot tak se uporablja tretji odstavek 5. člena Direktive o e-zasebnosti, tudi če to shranjevanje ni trajno.

51. Dodajanje informacij o sledenju URL-jem ali slikam (slikovnim pikam), poslanim uporabniku, pomeni navodilo terminalski opremi, naj pošlje nazaj ciljne podatke (določen identifikator). Pri dinamično oblikovanih slikovnih pikah za sledenje je navodilo distribucija aplikativne logike (običajno koda JavaScript). Posledično se lahko šteje, da zbiranje identifikatorjev, zagotovljenih s takimi mehanizmi sledenja, pomeni „pridobivanje dostopa“ v smislu tretjega odstavka 5. člena Direktive o e-zasebnosti, zato se uporablja tudi za ta korak.

3.2 Lokalna obdelava

52. Nekatere tehnologije temeljijo na lokalni obdelavi, ki jo izvaja programska oprema, distribuirana na terminalski opremi uporabnikov, pri čemer so podatki, pridobljeni z lokalno obdelavo, nato na voljo izbranim akterjem prek API na strani odjemalca. To lahko na primer velja za API, ki ga zagotavlja spletni brskalnik, kjer je mogoče do lokalno ustvarjenih rezultatov dostopati na daljavo.

53. Če so obdelani podatki kadar koli in na primer v kodi na strani odjemalca dani na voljo tretji osebi, na primer poslani nazaj prek omrežja na strežnik, bi taka operacija (ki jo je spodbudil subjekt, ki proizvaja kodo na strani odjemalca, distribuirano na uporabniški terminalski opremi) pomenila „pridobivanje dostopa do že shranjenih informacij“. Dejstvo, da se ti podatki pripravljajo lokalno, ne izključuje uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti.

3.3 Sledenje samo na podlagi naslova IP

54. Nekateri ponudniki razvijajo rešitve, ki temeljijo le na zbiranju enega elementa, in sicer naslova IP, da bi spremljali navigacijo[28] uporabnika, v nekaterih primerih prek več domen. V tem okviru bi se lahko uporabljal tretji odstavek 5. člena Direktive o e-zasebnosti, čeprav je navodilo za dajanje na voljo naslova IP dal drug subjekt kot prejemnik.

55. Vendar bi pridobitev dostopa do naslovov IP sprožila uporabo tretjega odstavka 5. člena Direktive o e-zasebnosti le v primerih, ko ti podatki izvirajo iz terminalske opreme naročnika ali uporabnika. Čeprav se to ne dogaja sistematično (na primer, ko je aktiviran CGNAT[29]), bi statični izhodni IPv4, ki izvira iz uporabnikovega usmerjevalnika, spadal v ta primer, prav tako pa tudi naslovi IPv6, saj jih deloma določi gostitelj. Razen če lahko subjekt zagotovi, da naslov IP ne izvira iz terminalske opreme uporabnika ali naročnika, mora sprejeti vse ukrepe v skladu s tretjim odstavkom 5. člena Direktive o e-zasebnosti.

56. Čeprav te smernice ne analizirajo uporabe izjem od obveznosti pridobivanja privolitve iz tretjega odstavka 5. člena Direktive o e-zasebnosti, je pomembno vnovič opozoriti, da uporabnost tega člena ne pomeni sistematično, da je treba pridobiti privolitev. EOVP zato opozarja, da bi bilo treba v vsakem primeru oceniti, ali je potrebna privolitev ali pa bi se lahko uporabila izjema na podlagi tretjega odstavka 5. člena Direktive o e-zasebnosti[30].

3.4 Občasno in posredovano poročanje o internetu stvari (IoT)

57. Naprave IoT (interneta stvari) neprekinjeno zbirajo podatke, na primer prek senzorjev, vgrajenih v napravo, ki so lahko lokalno predhodno obdelani ali ne. V številnih primerih so podatki na voljo oddaljenemu strežniku, vendar se lahko načini tega zbiranja razlikujejo.

58. Nekatere naprave interneta stvari imajo neposredno povezavo z javnim komunikacijskim omrežjem z mobilno kartico SIM. Druge imajo lahko posredno povezavo z javnim komunikacijskim omrežjem, na primer prek uporabe brezžičnega omrežja ali prenosa informacij na drugo napravo prek povezave od točke do točke (na primer prek Bluetootha). Druga naprava je lahko na primer pametni telefon ali namenski prehod, ki lahko podatke pred pošiljanjem v strežnik prej obdela ali ne.

59. Proizvajalec lahko napravam interneta stvari naroči, naj vedno prenašajo zbrane informacije, vendar jih najprej shranijo v lokalni predpomnilnik, na primer dokler ni na voljo povezava.

60. V vsakem primeru bi se naprava interneta stvari, če je (neposredno ali posredno) povezana z javnim komunikacijskim omrežjem, sama štela za terminalsko opremo. Dejstvo, da so informacije pretočne ali shranjene v predpomnilniku za občasno poročanje, ne spremeni narave teh informacij. V obeh primerih bi se uporabljal tretji odstavek 5. člena Direktive o e-zasebnosti, saj z navodilom o kodi na napravi interneta stvari za pošiljanje dinamično shranjenih podatkov oddaljenemu strežniku obstaja „pridobivanje dostopa“.

3.5 Enolični identifikator

61. Skupno orodje, ki ga uporabljajo podjetja, je pojem „enoličnih identifikatorjev“ ali „stalnih identifikatorjev“. Taki identifikatorji lahko izhajajo iz trajnih osebnih podatkov (ime in priimek, e-pošta,

[28] To je dodatno in neodvisno od uporabe in funkcije naslova IP za vzpostavitev in prenos ali prenos osnovnih tehničnih komunikacij ali od dejstva, da gre lahko za osebne podatke ali ne (v zvezi z analizo zasebnosti in elektronskih komunikacij gre za „podatke“).

[29] Ponudniki internetnih storitev uporabljajo NAT ali CGNAT stopnje prenašalca, da bi čim bolj povečali uporabo omejenega prostora za naslove IP. Združuje več naročnikov pod istim javnim naslovom IP.

[30] Mnenje št. 9/2014 Delovne skupine iz člena 29 navaja nekaj primerov, pri katerih privolitev morda ni potrebna.

telefonska številka itd.), ki so zgoščeni v napravi uporabnika, zbrani in deljeni med več upravljavci za enolično identifikacijo osebe v različnih naborih podatkov (podatki o uporabi, zbrani z uporabo spletnega mesta ali aplikacije, podatki o upravljanju odnosov s strankami (CRM), povezani s spletnim ali nespletnim nakupom ali naročnino itd.). Na spletnih mestih se trajni osebni podatki običajno pridobijo v okviru avtentikacije ali naročnine na e-novice.

62. Kot je bilo že navedeno, dejstvo, da uporabnik vnese podatke, ne izključuje uporabe tretjega odstavka 5. člena Direktive o e-zasebnosti v zvezi s shranjevanjem, saj se ti podatki pred zbiranjem začasno shranijo v terminalski opremi.

63. Pri zbiranju „enoličnih identifikatorjev“ na spletnih mestih ali v mobilnih aplikacijah subjekt, ki zbira podatke, naroča brskalniku (z distribucijo kode na strani odjemalca), naj mu pošlje te podatke. Tako poteka „pridobivanje dostopa“ in se uporablja tretji odstavek 5. člena Direktive o e-zasebnosti.