Usmernenia

Usmernenia 2/2023 o Technickom rozsahu pôsobnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách

Verzia 2.0

Prijaté 7. októbra 2024

História verzií

Verzia 1.0	14. novembra 2023	Prijatie usmernení na účely verejnej konzultácie
Verzia 2.0	07. októbra 2024	Prijatie usmernení po verejnej konzultácii

Zhrnutie

EDPB sa v týchto usmerneniach zaoberá uplatniteľnosťou článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách na rôzne technické riešenia. V týchto usmerneniach sa ďalej rozvádza stanovisko 9/2014 pracovnej skupiny zriadenej podľa článku 29 k uplatňovaniu smernice o súkromí a elektronických komunikáciách na zariadenia na získavanie jedinečných identifikačných údajov (fingerprinting) a ich cieľom je poskytnúť jasné pochopenie technických operácií, na ktoré sa vzťahuje článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

Vznik nových metód sledovania, ktoré nahrádzajú existujúce nástroje sledovania (napríklad súbory cookie, pretože niektorí výrobcovia prehliadačov prestali podporovať súbory cookie tretích strán) a vytvárajú nové obchodné modely, sa stal vážnym problémom v oblasti ochrany údajov. Zatiaľ čo uplatniteľnosť článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách je dobre zavedená a implementovaná pre niektoré technológie sledovania, ako sú napríklad súbory cookie, je potrebné riešiť nejasnosti súvisiace s uplatňovaním uvedeného ustanovenia na nové nástroje sledovania.

V usmerneniach sa stanovujú tri kľúčové prvky uplatniteľnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách (oddiel 2.1), a to „informácie“, „koncové zariadenia účastníka alebo užívateľa“ a „získanie prístupu a „uloženie informácií a uložených informácií“. Usmernenia ďalej poskytujú podrobnú analýzu každého prvku (oddiel 2.2-2.6).

V oddiele 3 sa táto analýza uplatňuje na neúplný zoznam prípadov použitia, ktoré predstavujú bežné techniky, a to:

- Sledovanie URL a pixelov
- Miestne spracovanie
- Sledovanie len na základe duševného vlastníctva
- občasné a sprostredkované podávanie správ o internete vecí (IoT)
- Jedinečný identifikátor

Obsah

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, a najmä na jej prílohu XI a protokol 37, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018[1],

so zreteľom na článok 15 ods. 3 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, ktorá sa týka spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií, zmenenej smernicou 2009/136/ES (ďalej len „smernica o súkromí a elektronických komunikáciách“),

so zreteľom na články 12 a 22 svojho rokovacieho poriadku,

PRIJAL TIETO USMERNENIA:

1 ÚVOD

1. Podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách „*ukladanie informácií alebo získavanie prístupu k informáciám, ktoré už boli uložené, v koncovom zariadení účastníka alebo užívateľa“* je povolené len na základe súhlasu alebo potreby na osobitné účely stanovené v uvedenom článku. Ako sa pripomína v odôvodnení 24 smernice o súkromí a elektronických komunikáciách[2], cieľom tohto ustanovenia je chrániť koncové zariadenia užívateľov, keďže sú súčasťou súkromnej sféry užívateľov. Zo znenia článku vyplýva, že článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách sa nevzťahuje výlučne na súbory cookie, ale aj na „podobné technológie“. V súčasnosti však neexistuje úplný zoznam technických operácií, na ktoré sa vzťahuje článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

2. Pracovná skupina zriadená podľa článku 29 (ďalej len „WP29“) vo svojom stanovisku 9/2014 k uplatňovaniu smernice o súkromí a elektronických komunikáciách (ďalej len „stanovisko č. 9/2014 WP29) už objasnila, že fingerprinting patrí do technického rozsahu pôsobnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách[3], ale vzhľadom na nový pokrok v oblasti technológií sú potrebné ďalšie usmernenia, pokiaľ ide o sledovacie techniky, ktoré sa v súčasnosti pozorujú. V posledných desiatich rokoch došlo k rozvoju technického prostredia, pričom čoraz viac sa používajú identifikátory zabudované v operačných systémoch a vznikli nové nástroje umožňujúcich uloženie informácií v koncových zariadeniach.

[1] Odkazy na „členské štáty“ uvedené v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.
[2] „Koncové zariadenie užívateľov elektronických komunikačných sietí a akékoľvek informácie uložené v takom zariadení, sú súčasťou súkromnej sféry užívateľov podliehajúcich ochrane podľa Európskeho dohovoru na ochranu ľudských práv a základných slobôd. Takzvané spyware, web bugs, hidden identifiers a ostatné podobné zariadenia môžu vstúpiť do koncového zriadenia užívateľa bez ich vedomia, aby získali prístup k informáciám, ukladali tajné informácie alebo zistili aktivity užívateľa a môžu vážne narušiť súkromie užívateľa. Používanie takých zariadení by malo byť povolené len na legitímne účely, s vedomím príslušných užívateľov.“
[3] Stanovisko č. 9/2014 WP29, s. 11.

3. Nejednoznačnosti týkajúce sa rozsahu uplatňovania článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách vytvorili stimuly na zavedenie alternatívnych riešení na sledovanie užívateľov internetu a viedli k tendencii obchádzať právne povinnosti stanovené v článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Všetky takéto situácie vyvolávajú obavy a vyžadujú si dodatočnú analýzu s cieľom doplniť predchádzajúce usmernenia EDPB.

4. Cieľom týchto usmernení je vykonať technickú analýzu rozsahu uplatňovania článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, a to objasniť, na čo sa z technického hľadiska vzťahuje slovné spojenie „*uložiť informácie alebo získať prístup k informáciám uloženým v koncovom zariadení účastníka alebo užívateľa*“. V rámci týchto usmernení sa neriešia okolnosti, za ktorých sa na spracovateľskú operáciu môžu vzťahovať výnimky z požiadavky súhlasu stanovené v smernici o súkromí a elektronických komunikáciách[4], keďže tieto okolnosti by sa mali analyzovať individuálne, pričom by sa mala zohľadniť príslušná transpozícia (transpozície) členského štátu a usmernenia vydané príslušnými vnútroštátnymi orgánmi.

5. Neúplný zoznam konkrétnych prípadov použitia sa analyzuje v záverečnej časti týchto usmernení.

2 ANALÝZA

2.1 Kľúčové prvky uplatniteľnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách

6. Článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách sa uplatňuje, ak:

   a. **KRITÉRIUM A:** vykonané operácie sa týkajú „*informácií*“. Treba poznamenať, že použitý pojem nie je „osobné údaje“, ale „informácie“.

   b. **Kritérium B:** vykonané operácie zahŕňajú „*koncové zariadenie*“ účastníka alebo užívateľa (B.1), z čoho vyplýva potreba posúdiť pojem „*verejná komunikačná sieť*“ (B.2).

   c. **KRITÉRIUM C** vykonávané operácie skutočne predstavujú „*uloženie*“ (C.1) alebo „*získanie prístupu*“ (C.2). Tieto dva pojmy možno skúmať nezávisle, ako sa pripomína v stanovisku č. 9/2014 WP29: „*Použitie výrazu „uložené [...] alebo ku ktorým sa získava prístup“ naznačuje, že ukladanie a získavanie prístupu nemusí prebiehať v rámci tej istej komunikácie a nemusí ich vykonávať tá istá strana*“[5].

   V záujme čitateľnosti sa subjekt získavajúci prístup k informáciám uloženým v koncovom zariadení užívateľa bude ďalej označovať ako „subjekt s prístupom k informáciám“.

2.2 Pojem „informácie“ – kritérium A

7. Ako sa uvádza v KRITÉRIU A, v tejto časti sa podrobne vysvetľuje, čo zahŕňa pojem „informácie“. Výber pojmu „informácie“, ktorý zahŕňa širšiu kategóriu, než je samotný pojem osobných údajov, súvisí s rozsahom pôsobnosti smernice o súkromí a elektronických komunikáciách.

[4] Ako sa uvádza v článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách: „*To nebráni nijakému technickému uloženiu ani prístupu výhradne na účely výkonu prenosu správy prostredníctvom elektronickej komunikačnej siete alebo ak je to nevyhnutne potrebné na to, aby poskytovateľ služieb informačnej spoločnosti, ktoré si účastník alebo užívateľ výslovne vyžiadal, mohol tieto služby poskytnúť.*“

[5] Stanovisko č. 9/2014 WP29, s. 8.

8. Cieľom článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách je chrániť súkromnú sféru užívateľov, ako sa uvádza v jeho odôvodnení 24: „*Koncové zariadenie užívateľov elektronických komunikačných sietí a akékoľvek informácie uložené v takom zariadení, sú súčasťou súkromnej sféry užívateľov podliehajúcich ochrane podľa Európskeho dohovoru na ochranu ľudských práv a základných slobôd*“. Je chránená aj článkom 7 Charty základných práv EÚ.

9. Na scenáre, ktoré zasahujú do tejto súkromnej sféry aj bez toho, aby zahŕňali osobné údaje, sa v skutočnosti výslovne vzťahuje znenie článku 5 ods. 3 a odôvodnenia 24 smernice o súkromí a elektronických komunikáciách, napríklad ukladanie vírusov na koncové zariadenie užívateľa. Z toho vyplýva, že vymedzenie pojmu „informácie“ by sa nemalo obmedzovať len na vlastnosť, ktorá znamená, že súvisia s identifikovanou alebo identifikovateľnou fyzickou osobou.

10. Potvrdil to aj Súdny dvor EÚ: „*Táto ochrana sa uplatňuje na všetky informácie uložené na danom koncovom zariadení bez ohľadu na to, či ide o osobné údaje, a ako vyplýva z toho istého odôvodnenia, jej cieľom je predovšetkým chrániť používateľov pred nebezpečenstvom, že skryté identifikátory alebo iné podobné zariadenia preniknú do koncového zariadenia týchto užívateľov bez ich vedomia*“[6].

11. Otázky, či by sa pri posudzovaní uplatniteľnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách mali zvážiť pôvod týchto informácií a dôvody, prečo sú uložené v koncovom zariadení, boli predtým objasnené. Napríklad v stanovisku č. 9/2014 WP29: „*Nie je správne vykladať túto situáciu tak, že tretia strana nežiada o súhlas so získaním prístupu k týmto informáciám len preto, lebo to nebola ona, kto tieto informácie uložil*. *Požiadavka na získanie súhlasu sa uplatňuje aj v prípade, keď sa získava prístup k hodnote len na čítanie (napr. žiadosť o MAC adresu sieťového rozhrania prostredníctvom rozhrania API operačného systému)*“[7].

12. Na záver, pojem informácie zahŕňa iné ako osobné údaje aj osobné údaje bez ohľadu na to, ako boli tieto údaje uložené a kto ich uložil, t. j. či ich uložil externý subjekt (vrátane iných subjektov, ako je ten, ktorý má k nim prístup), používateľ, výrobca alebo akýkoľvek iný scenár.

2.3 Pojem „terminálne vybavenie účastníka alebo užívateľa“ – kritérium B.1

13. Tento oddiel vychádza z vymedzenia pojmu použitého v smernici 2008/63/ES, ako sa uvádza v článku 2 smernice (EÚ) 2018/1972, kde je „koncové zariadenie“ vymedzené ako: „*zariadenie priamo alebo nepriamo pripojené k rozhraniu verejnej telekomunikačnej siete na vysielanie, spracovanie alebo prijatie informácií; v oboch prípadoch (priamom alebo nepriamom) pripojenie môže byť urobené vodičom, optickým vláknom alebo elektromagneticky; pripojenie je nepriame, ak je zariadenie umiestnené medzi terminál a rozhranie verejnej siete*“[8].

14. V odôvodnení 24 smernice o súkromí a elektronických komunikáciách sa uvádza jasné pochopenie úlohy koncového zariadenia pre ochranu poskytovanú článkom 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Smernica o súkromí a elektronických komunikáciách chráni súkromie používateľov nielen v súvislosti s dôvernosťou ich informácií, ale aj zabezpečením integrity koncového zariadenia užívateľa. Týmto pochopením sa bude riadiť výklad pojmu koncového zariadenia v rámci týchto usmernení.

15. V článku 3 smernice o súkromí a elektronických komunikáciách sa uvádza, že na to, aby sa smernica o elektronických komunikáciách uplatňovala, spracovanie osobných údajov sa musí vykonávať v

[6] Rozsudok Súdneho dvora z 1. októbra 2019, Planet 49, vec C-673/17, ECLI:EU:C:2019:801, bod 70.
[7] Stanovisko č. 9/2014 WP29, s. 8.
[8] Smernica Komisie 2008/63/ES z 20. júna 2008 o hospodárskej súťaži na trhoch s koncovými telekomunikačnými zariadeniami (kodifikované znenie), článok 1 ods.1.

súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach. To znamená, že zariadenie by malo byť použiteľné v spojení s takouto službou a že na to, aby bolo kvalifikované ako koncové zariadenie, by malo byť pripojené alebo pripojiteľné[9] k rozhraniu verejnej komunikačnej siete. EDPB poznamenáva, že zmenami vykonanými v roku 2009[10] v znení článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách sa rozšírila ochranu koncových zariadení vypustením odkazu na „používanie elektronickej komunikačnej siete" ako prostriedku na ukladanie informácií alebo na získanie prístupu k informáciám uloženým v koncovom zariadení. Preto, pokiaľ má zariadenie sieťové rozhranie, ktoré ho oprávňuje na pripojenie (aj keď takéto pripojenie nie je zavedené), článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách sa vzťahuje na každý subjekt, ktorý by mohol ukladať informácie a získavať prístup k informáciám, ktoré sú už uložené v koncovom zariadení, bez ohľadu na to, aký je spôsob prístupu ku koncovému zariadeniu a či je pripojené alebo odpojené od siete

16. Zariadenia, ktoré sú súčasťou samotnej verejnej elektronickej komunikačnej siete, by sa podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách nepovažovali za koncové zariadenia[11].

17. Koncové zariadenie môže pozostávať z akéhokoľvek počtu jednotlivých častí hardvéru, ktoré spolu tvoria koncové zariadenie. Môže, ale nemusí mať podobu fyzicky uzavretého zariadenia, v ktorom sa nachádza všetok zobrazovací, spracovateľský, úložný a periférny hardvér (napríklad smartfóny, notebooky, sieťové úložné zariadenie, pripojené autá alebo pripojené televízory, inteligentné okuliare).

18. V smernici o súkromí a elektronických komunikáciách sa uznáva, že ochrana dôvernosti informácií uložených v koncovom zariadení používateľa a integrity koncového zariadenia používateľa sa neobmedzuje len na ochranu súkromnej sféry fyzických osôb, ale týka sa aj práva na rešpektovanie ich korešpondencie alebo oprávnených záujmov právnických osôb[12]. Ako také je podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách chránené koncové zariadenie, ktoré umožňuje vykonať túto korešpondenciu a oprávnené záujmy právnických osôb.

19. Užívateľ alebo predplatiteľ môže vlastniť alebo prenajímať alebo inak nadobudnúť koncové zariadenie. Viacero užívateľov alebo predplatiteľov môže mať spoločné koncové zariadenie.

20. Túto ochranu zaručuje smernica o súkromí a elektronických komunikáciách koncovému zariadeniu pridruženému k užívateľovi alebo predplatiteľovi a nezávisí od toho, či užívateľ nastaví prostriedky prístupu (napríklad ak inicioval elektronickú komunikáciu), ani od toho, či je užívateľ oboznámený s uvedenými prostriedkami prístupu).

[9] To znamená, že majú technické možnosti na pripojenie k sieti, aj keď toto pripojenie nie je v súčasnosti k dispozícii.

[10] Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa (Text s významom pre EHP), Ú. v. EÚ L 337, 18.12.2009, článok 2 ods. 5 a odôvodnenie 65.

[11] Na určenie hraníc siete v rôznych kontextoch pozri Usmernenia BEREC o spoločných prístupoch k určovaniu koncového bodu siete v rôznych topológiách siete (BoR (20) 46).

[12] Skutočne, ako sa pripomína v článku 2 ods. 13 smernice Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií, užívateľom môže byť fyzická alebo právnická osoba.

2.4 Pojem „verejná komunikačná sieť“ – kritérium B.2

21. Keďže situácia, ktorú upravuje smernica o súkromí a elektronických komunikáciách, sa týka *„poskytovania verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Spoločenstve“*[13], a v definícii koncového zariadenia sa výslovne uvádza pojem *„verejná komunikačná sieť“*, je nevyhnutné objasniť tento pojem, aby sa určil kontext, v ktorom sa uplatňuje článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

22. Pojem elektronickej komunikačnej siete nie je vymedzený v samotnej smernici o súkromí a elektronických komunikáciách. Tento pojem bol pôvodne uvedený v smernici 2002/21/ES (rámcová smernica) o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby[14], a následne nahradený článkom 2 ods. 1 smernice (EÚ) 2018/1972 (európsky kódex elektronických komunikácií). Súčasné znenie:

> *„elektronická komunikačná sieť“ sú prenosové systémy, ktoré môžu ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej administratívnej kapacite, prípadne prepájacie alebo smerovacie zariadenie a iné prostriedky vrátane neaktívnych prvkov siete, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných (s prepájaním okruhov a paketov vrátane internetu) a mobilných sietí, elektrických káblových systémov v rozsahu, v ktorom sa používajú na prenos signálov, sietí používaných na rozhlasové a televízne vysielanie a sietí káblovej televízie bez ohľadu na typ prenášaných informácií*[15]

23. Toto vymedzenie je neutrálne, pokiaľ ide o prenosové technológie. Elektronická komunikačná sieť je podľa tohto vymedzenia akýkoľvek sieťový systém, ktorý umožňuje prenos elektronických signálov medzi jej uzlami bez ohľadu na použité zariadenia a protokoly.

24. Pojem elektronickej komunikačnej siete podľa smernice 2018/1972 nezávisí od verejnej alebo súkromnej povahy infraštruktúry, ani od spôsobu, akým sa sieť zavádza alebo spravuje (*„ktoré môžu ale nemusia byť založené na trvalej infraštruktúre alebo centralizovanej administratívnej kapacite“*[16].) V dôsledku toho je vymedzenie pojmu elektronickej komunikačnej siete podľa článku 2 smernice 2018/1972 dostatočne široké na to, aby zahŕňalo akýkoľvek druh infraštruktúry. Zahŕňa siete spravované alebo nespravované operátorom, siete spoločne spravované skupinou operátorov alebo dokonca siete ad-hoc, v ktorých sa koncové zariadenie môže dynamicky pripojiť alebo opustiť sieť iných koncových zariadení pomocou prenosových protokolov krátkeho dosahu.

25. Toto vymedzenie pojmu siete neobsahuje žiadne obmedzenia, pokiaľ ide o počet koncových zariadení nachádzajúcich sa v sieti v akomkoľvek čase. Niektoré sieťové schémy sa spoliehajú na to, že uzly odovzdávajú informácie ad-hoc spôsobom uzlom, ktoré sú v súčasnosti pripojené[17] a v určitom okamihu môžu komunikovať len dva uzly na rovnocennej úrovni. Takéto prípady by patrili do

[13] Článok 3 smernice o súkromí a elektronických komunikáciách.

[14] Smernica Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica)

[15] Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (prepracované znenie) (Text s významom pre EHP), článok 2 ods. 1.

[16] Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (prepracované znenie) (Text s významom pre EHP), článok 2 ods. 1.

[17] Napríklad v súvislosti so systémom vytvárania sietí tolerujúcich oneskorenie, v ktorom sa zavádzajú „techniky ukladania a šírenia“, ako je napríklad projekt s otvoreným zdrojovým kódom Briar.

všeobecného rozsahu pôsobnosti smernice o súkromí a elektronických komunikáciách, pokiaľ sieťový protokol umožňuje ďalšie začlenenie uzlov.

26. Verejná dostupnosť komunikačnej siete je potrebná na to, aby sa zariadenie mohlo považovať za koncové zariadenie a v dôsledku toho pre uplatniteľnosť článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Treba poznamenať, že skutočnosť, že sieť je sprístupnená obmedzenej podskupine verejnosti (napríklad predplatitelia, či už platiaci alebo nie, v závislosti od podmienok účasti) neznamená, že takáto sieť je súkromná[18].

2.5 Pojem „získanie prístupu“ – kritérium C.1

27. Na správne vymedzenie pojmu „získanie prístupu“ je dôležité zohľadniť rozsah pôsobnosti smernice o súkromí a elektronických komunikáciách, ktorý je uvedený v jej článku 1: „*na zabezpečenie primeranej úrovne ochrany základných práv a slobôd a najmä práva na súkromie, z hľadiska spracovávania osobných údajov v elektronickom komunikačnom sektore a zabezpečenia voľného pohybu takých údajov a elektronického komunikačného zariadenia a služieb v spoločenstve*“.

28. V skratke je smernica o súkromí a elektronických komunikáciách právnym nástrojom, ktorý sa zameriava na ochranu dôvernosti komunikácií a integrity zariadení. V odôvodnení 24 smernice o súkromí a elektronických komunikáciách sa objasňuje, že v prípade fyzických osôb je koncové zariadenie užívateľa súčasťou ich súkromnej sféry a že prístup k informáciám, ktoré sú na ňom uložené bez ich vedomia, môže vážne narušiť ich súkromie.

29. Právnické osoby sú takisto chránené smernicou o súkromí a elektronických komunikáciách[19]. V dôsledku toho sa pojem „získanie prístupu“ podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách musí vykladať spôsobom, ktorý chráni tieto práva pred porušením zo strany tretích strán.

30. Uloženie informácií alebo získavanie prístupu k nim môžu byť nezávislé operácie, ktoré vykonávajú nezávislé subjekty. Na uplatnenie článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách nemusí dochádzať súčasne k uloženiu informácií a prístupu k už uloženým informáciám.

31. Ako sa uvádza v stanovisku č. 9/2014 WP29: „*Použitie výrazu „uložené [...] alebo ku ktorým sa získava prístup“ naznačuje, že ukladanie a získavanie prístupu nemusí prebiehať v rámci tej istej komunikácie a nemusí ich vykonávať tá istá strana. Informácie, ktoré uloží jedna strana (vrátane informácií, ktoré uložil používateľ alebo výrobca zariadenia) a ku ktorým neskôr získa prístup iná strana, teda patria do rozsahu pôsobnosti článku 5 ods. 3*“[20]. Na účely uplatnenie pojmu prístup preto neexistujú žiadne obmedzenia týkajúce sa pôvodu informácií o koncových zariadeniach.

32. Vždy, keď subjekt podnikne kroky na získanie prístupu k informáciám uloženým v koncovom zariadení, uplatňuje sa článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Zvyčajne to znamená, že pristupujúci subjekt musí proaktívne posielať špecifické pokyny koncovému zariadeniu, aby dostal späť cielené informácie. Ide napríklad o súbory cookie, pri ktorých pristupujúci subjekt dáva koncovému zariadeniu pokyn, aby proaktívne odosielalo informácie pri každom nasledujúcom volaní protokolu HTTP (Hypertext Transfer Protocol).

[18] Na ďalšiu analýzu identifikácie verejných komunikačných sietí pozri usmernenia orgánu BEREC o vykonávaní nariadenia o otvorenom internete (BoR (20) 112).
[19] Odôvodnenie 26 smernice o súkromí a elektronických komunikáciách, pozri bod 17 vyššie.
[20] Stanovisko č. 9/2014 WP29, s. 8.

33. Je to tak aj v prípade, keď pristupujúci subjekt distribuuje softvér na koncovom zariadení užívateľa, ktorý je uložený, a potom proaktívne zavolá cez sieť koncový bod aplikačného programovacieho rozhrania (ďalej len „API“). Medzi ďalšie príklady by mohol patriť kód JavaScript, v ktorom pristupujúci subjekt dáva pokyn prehliadaču používateľa, aby odoslal asynchrónne požiadavky s cielenými informáciami. Takýto prístup jednoznačne patrí do rozsahu pôsobnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, keďže pristupujúci subjekt výslovne nariaďuje koncovému zariadeniu zaslať informácie.

34. V niektorých prípadoch nemusí byť subjekt, ktorý dáva koncovému zariadeniu pokyn, aby odoslal cieľové údaje späť, a subjekt prijímajúci informácie to isté. Môže to vyplývať z poskytovania a/alebo používania spoločného mechanizmu medzi týmito dvoma subjektmi. Pokyn zariadeniu, aby posielalo už uložené informácie (napríklad prostredníctvom protokolu alebo SDK[21], čo znamená proaktívne zasielanie informácií koncovým zariadením) umožňuje vniknutie do koncového zariadenia, a preto takýto prístup vedie k uplatniteľnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Ako sa uvádza v stanovisku č. 09/2014 WP29, môže to byť prípad, keď webová stránka dá koncovému zariadeniu pokyn na odosielanie informácií reklamným službám tretích strán prostredníctvom začlenenia sledovacieho pixelu[22]. Tento prípad použitia je ďalej rozpracovaný v oddiele 3.1.

2.6 Pojmy „uloženie informácií“ a „uložené informácie“ – kritérium C.2

35. Uloženie informácií v zmysle článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách sa vzťahuje na umiestnenie informácií na fyzické elektronické pamäťové médium, ktoré je súčasťou koncového zariadenia užívateľa alebo účastníka[23].

36. Informácie sa zvyčajne neukladajú v koncovom zariadení užívateľa alebo účastníka prostredníctvom priameho prístupu inej strany do pamäte zariadenia, ale skôr prostredníctvom pokynov softvéru na koncovom zariadení na generovanie konkrétnych informácií. Ukladanie, ktoré sa uskutočňuje na základe takýchto pokynov, sa považuje za iniciované priamo druhou stranou. To zahŕňa používanie zavedených protokolov, ako je ukladanie súborov cookie v prehliadači, ako aj prispôsobeného softvéru bez ohľadu na to, kto vytvoril alebo nainštaloval protokoly alebo softvér na koncové zariadenie.

37. V smernici o súkromí a elektronických komunikáciách sa nestanovuje žiadna horná ani dolná hranica dĺžky trvania informácie na pamäťovom médiu, aby sa mohla považovať za uloženú, ani hornú či dolnú hranicu množstva informácií, ktoré sa majú uložiť.

38. Podobne, pojem uloženie nezávisí od typu média, na ktorom sú informácie uložené. Typickými príkladmi by boli pevné disky (ďalej len „HDD“), mechaniky s nepohyblivým médiom (ďalej len „SSD“), elektricky mazateľná programovateľná pamäť len na čítanie (ďalej len „EEPROM“) a pamäť s priamym prístupom („RAM“), ale menej typické scenáre zahŕňajúce také médium, ako je magnetická páska alebo vyrovnávacia pamäť centrálnej procesorovej jednotky (CPU), nie sú vylúčené z rozsahu pôsobnosti. Pamäťové médium môže byť prepojené interne (napr. prostredníctvom pripojenia SATA), externe (napr. prostredníctvom pripojenia USB).

39. „Uložené informácie“ sa vzťahujú na informácie, ktoré už existujú na koncových zariadeniach bez ohľadu na zdroj alebo povahu týchto informácií. To zahŕňa akýkoľvek výsledok uloženia informácií

[21] SDP (ďalej len „súbor nástrojov pre vývoj softvéru“) je súbor nástrojov pre vývoj softvéru, ktoré sú k dispozícii na uľahčenie vytvorenia aplikačného softvéru.
[22] Stanovisko č. 9/2014 WP29, s. 9.
[23] Ako je vymedzené v oddiele 2.3 týchto usmernení.

v zmysle článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, ako sa uvádza vyššie (buď tou istou stranou, ktorá by neskôr získala prístup, alebo inou treťou stranou). Okrem toho zahŕňa výsledky postupov ukladania informácií, ktoré presahujú rozsah pôsobnosti článku 5 ods. 3,) smernice o súkromní a elektronických komunikáciách, ako napríklad: uchovávanie v koncovom zariadení samotným užívateľom alebo účastníkom alebo výrobcom hardvéru (ako sú MAC adresy riadiacich prvkov sieťového rozhrania), snímače integrované do koncového zariadenia alebo procesy a programy vykonávané na koncovom zariadení, ktoré môžu, ale nemusia poskytovať informácie, ktoré závisia od uložených informácií alebo z nich vyplývajú.

3 PRÍPADY POUŽITIA

40. Ako sa uvádza v úvode týchto usmernení[24], neanalyzujú sa v nich uplatňovanie výnimiek z povinnosti získať súhlas podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. EDPB pripomína, že vo všetkých prípadoch uloženia informácií alebo získania prístupu k už uloženým informáciám by sa muselo posúdiť, či je potrebný súhlas alebo či by sa mohla uplatniť výnimka podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Čitateľ by preto mal zvážiť výnimky v prípade ich použitia v spojení s touto technickou analýzou.

41. Bez toho, aby bol dotknutý osobitný kontext, v ktorom sa môžu používať tieto technické kategórie, ktoré sú potrebné na to, aby sa kvalifikovali, či sa uplatňuje článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách, je možné nevyčerpávajúcim spôsobom identifikovať široké kategórie identifikátorov a informácií, ktoré sa bežne používajú a môžu podliehať uplatniteľnosti článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

42. Sieťová komunikácia sa zvyčajne spolieha na vrstvený model, ktorý si vyžaduje použitie identifikátorov, aby sa umožnilo správne vytvorenie a uskutočnenie komunikácie. Komunikácia týchto identifikátorov so vzdialenými aktérmi je riadená prostredníctvom softvéru podľa dohodnutých komunikačných protokolov. Ako už bolo uvedené, skutočnosť, že prijímajúci subjekt nemusí byť subjektom, ktorý dáva pokyn na zaslanie informácií, nebráni uplatneniu článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. To by sa mohlo týkať smerovacích identifikátorov, ako je napríklad MAC alebo IP adresa koncového zariadenia, ale aj identifikátory relácie (SSRC, identifikátor webového socketu) alebo autentifikačné tokeny.

43. Rovnako môže aplikačný protokol obsahovať niekoľko mechanizmov na poskytovanie kontextových údajov (napríklad hlavičku HTTP vrátane poľa „accept“ alebo používateľský agent), mechanizmus ukladania do vyrovnávacej pamäte (napríklad ETag[25]) alebo iné funkcie (jednou z nich sú súbory cookie alebo HSTS[26]). Opäť platí, že spoliehanie sa na tieto mechanizmy pri zhromažďovaní informácií (napríklad v kontexte fingerprintingu[27] alebo sledovania identifikátorov zdrojov) môže viesť k uplatneniu článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

44. Na druhej strane existujú určité súvislosti, v ktorých miestne aplikácie inštalované v koncovom zariadení používajú niektoré informácie prísne vnútri terminálu, ako by to mohlo byť v prípade

[24] Pozri bod 44 vyššie.
[25] HTTP ETag je identifikátor, ktorý umožňuje vykonať podmienenú žiadosť na základe platnosti údajov o klientovi vo vyrovnávacej pamäti.
[26] HTTP Strict Transport Security (HSTS) umožňuje serverom špecifikovať, ktoré zdroje by sa mali vždy požadovať pomocou pripojení HTTPS.
[27] Ako sa uvádza v úvode, pozri stanovisko č. 9/2014 WP29 k uplatňovaniu smernice o súkromí a elektronických komunikáciách na získavanie jedinečných identifikačných údajov zariadenia (tzv. device fingerprinting).

systémového rozhrania API smartfónu (prístup ku kamere, mikrofónu, snímaču GPS, akceleračnému čipu, rádiovému čipu, prístup k miestnym súborom, zoznamu kontaktov, prístup k identifikátorom atď.). Môže to platiť aj v prípade internetových prehliadačov, ktoré spracúvajú uložené alebo generované informácie vo vnútri zariadenia (ako sú súbory cookie, miestne úložisko, WebSQL alebo dokonca aj informácie poskytnuté samotnými užívateľmi). Použitie takýchto informácií aplikáciou by nepredstavovalo „získavanie prístupu k informáciám, ktoré už boli uložené“ v zmysle článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, pokiaľ tieto informácie neopustia zariadenie, ale keď sa k týmto informáciám alebo k akýmkoľvek odvodeným informáciám získa prístup, uplatní sa článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

45. Napokon v niektorých prípadoch aktéri distribuujú škodlivé softvérové prvky, napríklad softvér na kryptoťažbu alebo všeobecnejšie malvér, pričom využívajú výpočtové schopnosti koncového zariadenia v prospech distribuujúceho subjektu. Distribúcia uvedeného škodlivého softvéru v koncových zariadeniach užívateľa by predstavovala „uloženie“ v zmysle článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Okrem toho, ak by softvér vytvoril sieťové pripojenie na zasielanie informácií v neskoršej fáze, predstavovalo by to „získavanie prístupu“ v zmysle článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

46. Pre podskupinu týchto kategórií, ktoré predstavujú osobitný záujem, buď z dôvodu ich rozšíreného používania, alebo preto, že je potrebná osobitná štúdia vzhľadom na okolnosti ich používania, sa ďalej uvádza osobitná analýza.

3.1 Sledovanie URL a pixelov

47. Sledovací pixel je hypertextový odkaz na zdroj, zvyčajne obrazový súbor, vložený do časti obsahu, ako je webové sídlo alebo e-mail. Tento pixel zvyčajne neplní žiadny účel, ktorý by súvisel so samotným obsahom. Jeho jediným účelom je automatické nadviazanie komunikácie klienta s hostiteľom pixelu, ku ktorej by inak nedošlo. Nie je to však systematické a sledovacie pixely možno vytvoriť aj pridaním dodatočných informácií do obrázkov načítavajúcich hypertextové odkazy, ktoré sú relevantné pre obsah, ktorý sa zobrazuje užívateľovi. Vytvorením komunikácie sa prenášajú rôzne informácie hostiteľovi pixelu v závislosti od konkrétneho prípadu použitia.

48. V prípade e-mailu môže odosielateľ priložiť sledovací pixel, aby zistil, kedy si príjemca e-mail prečíta. Sledovacie pixely na webových stránkach môžu odkazovať na subjekt, ktorý zhromažďuje veľa takýchto požiadaviek, a tak môže sledovať správanie používateľov. Takéto sledovacie pixely môžu akú súčasť odkazu obsahovať aj ďalšie identifikátory, metadáta alebo obsah. Tieto údajové body môže pridať vlastník webového sídla, a to aj prípadne v súvislosti s činnosťou užívateľa na tomto webovom sídle, aby bolo možné vytvárať analytické správy o používaní. Môžu byť takisto dynamicky generované prostredníctvom aplikatívnej logiky na strane klienta, ktorú dodáva daný subjekt.

49. Sledovacie odkazy môžu fungovať rovnakým spôsobom, ale identifikátor je pripojený k adrese webového sídla. Keď užívateľ navštívi adresu URL (Uniform Resource Locator), cieľová webová lokalita načíta požadovaný zdroj, zároveň však zhromaždí identifikátor, ktorý nie je relevantný z hľadiska identifikácie zdroja. Webové stránky elektronického obchodu ich veľmi často používajú na identifikáciu pôvodu prichádzajúceho zdroja návštevnosti. Takéto webové sídla môžu napríklad poskytovať partnerom sledované odkazy, ktoré môžu používať na svojej doméne, aby webové sídlo elektronického obchodu vedelo, ktorý z ich partnerov je zodpovedný za predaj, a vyplatilo províziu, čo je postup známy ako tzv. affiliate marketing (partnerský marketing).

50. Sledovacie odkazy aj sledovacie pixely možno distribuovať prostredníctvom širokej škály kanálov, napríklad prostredníctvom e-mailov, webových stránok alebo dokonca v prípade sledovacích odkazov

prostredníctvom akýchkoľvek systémov odosielania textových správ. Táto distribúcia do koncového zariadenia užívateľa predstavuje ukladanie, prinajmenšom prostredníctvom mechanizmu ukladania do vyrovnávacej pamäte softvéru na strane klienta. Ako taký sa uplatňuje článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách, aj keď toto uloženie nie je trvalé.

51. Pridanie informácií o sledovaní k adresám URL alebo obrázkom (pixelom) odoslaným užívateľovi predstavuje pokyn koncovému zariadeniu, aby odoslalo späť cielené informácie (špecifikovaný identifikátor). V prípade dynamicky vytvorených sledovacích pixelov je pokynom distribúcia aplikačnej logiky (zvyčajne kód JavaScriptu). V dôsledku toho sa možno domnievať, že zhromažďovanie identifikačných údajov poskytovaných prostredníctvom takýchto mechanizmov sledovania predstavuje „získanie prístupu“ v zmysle článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, a preto sa vzťahuje aj na tento krok.

3.2 Miestne spracovanie

52. Niektoré technológie sa spoliehajú na miestne spracovanie podľa pokynov softvéru distribuovaného na koncových zariadeniach užívateľov, pričom informácie získané miestnym spracovaním sa následne sprístupňujú vybraným aktérom prostredníctvom API na strane klienta. Môže to byť napríklad prípad API poskytovaného webovým prehliadačom, kde sa k lokálne generovaným výsledkom môže pristupovať na diaľku.

53. Ak sa kedykoľvek, napríklad v kóde na strane klienta, spracované informácie sprístupnia tretej strane, napríklad sa pošlú späť cez sieť na server, takáto operácia (nariadená subjektom, ktorý vytvára kód na strane klienta distribuovaný na koncovom zariadení užívateľa) by predstavovala „získanie prístupu k už uloženým informáciám“. Skutočnosť, že tieto informácie sa vytvárajú na miestnej úrovni, nebráni uplatneniu článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

3.3 Sledovanie len na základe duševného vlastníctva

54. Niektorí poskytovatelia vyvíjajú riešenia, ktoré sa spoliehajú len na zber jednej zložky, konkrétne IP adresy, s cieľom sledovať navigáciu[28] užívateľa, v niektorých prípadoch vo viacerých oblastiach. V tejto súvislosti by sa mohol uplatniť článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách aj napriek tomu, že pokyn na sprístupnenie IP adresy poskytol iný ako prijímajúci subjekt.

55. Získanie prístupu k IP adresám by však viedlo k uplatneniu článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách len v prípadoch, keď tieto informácie pochádzajú z koncového zariadenia účastníka alebo užívateľa. Aj keď tomu tak nie je systematicky (napríklad keď je aktivovaný CGNAT[29]), statické odchádzajúce adresy IPv4 pochádzajúce zo smerovača užívateľa by do tohto prípadu patrili, rovnako ako adresy IPV6, pretože sú čiastočne definované hostiteľom. Pokiaľ subjekt nemôže zabezpečiť, aby IP adresa nepochádzala z koncového zariadenia užívateľa alebo účastníka, musí vykonať všetky kroky podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

56. Hoci sa v týchto usmerneniach neanalyzuje uplatňovanie výnimiek z povinnosti získať súhlas podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, je dôležité opätovne pripomenúť, že uplatniteľnosť tohto článku systematicky neznamená, že je potrebné získať súhlas. EDPB preto

[28] Ide o doplnkový postup nezávislý od použitia a funkcie IP adresy na vytvorenie a prenos základnej technickej komunikácie alebo od skutočnosti, že môže alebo nemusí ísť o osobné údaje (pokiaľ ide o analýzu súkromia v elektronických komunikáciách, ide o „informácie“).

[29] Poskytovatelia internetových služieb používajú širokoškálový preklad sieťových adries (CGNAT – Carrier-grade NAT) na maximalizáciu využitia obmedzeného počtu IP adries. Zoskupuje niekoľko účastníkov pod tou istou verejnou IP adresou.

pripomína, že v každom prípade by sa muselo posúdiť, či je potrebný súhlas alebo či by sa mohla uplatniť výnimka podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách[30].

3.4 Občasné a sprostredkované podávanie správ o internete vecí

57. Zariadenia v rámci internetu vecí (IoT) vytvárajú informácie nepretržite, napríklad prostredníctvom snímačov zabudovaných v zariadení, ktoré môžu, ale nemusia byť lokálne vopred spracované. V mnohých prípadoch sa informácie sprístupňujú vzdialenému serveru, ale spôsoby tohto zberu sa môžu líšiť.

58. Niektoré zariadenia v rámci internetu vecí majú priame pripojenie k verejnej komunikačnej sieti pomocou mobilnej karty SIM. Iné môžu mať nepriame pripojenie k verejnej komunikačnej sieti, napríklad prostredníctvom WIFI alebo odovzdávania informácií inému zariadeniu prostredníctvom pripojenia point-to-point (napríklad prostredníctvom Bluetooth). Druhým zariadením môže byť napríklad smartfón alebo vyhradená brána, ktorá môže, ale nemusí informácie pred ich zaslaním na server vopred spracovať.

59. Zariadenia v rámci IoT môžu mať od výrobcu pokyn, aby zozbierané informácie vždy streamovali, ale zároveň ich najprv lokálne ukladali do vyrovnávacej pamäte, napríklad kým nebude k dispozícii pripojenie.

60. V každom prípade by sa zariadenie v rámci IoT, ak je pripojené (priamo alebo nepriamo) k verejnej komunikačnej sieti, samo osebe považovalo za koncové zariadenie. Skutočnosť, že informácie sú streamované alebo ukladané do vyrovnávacej pamäte na účely občasného podávania správ, nemení povahu týchto informácií. V oboch prípadoch by sa uplatnil článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách, pretože prostredníctvom pokynov kódu v zariadení v rámci IoT na odoslanie dynamicky uložených údajov na vzdialený server dochádza k „získaniu prístupu“.

3.5 Jedinečný identifikátor

61. Pojem „jedinečné identifikátory“ alebo „perzistentné identifikátory“ označujú nástroj, ktorý spoločnosti bežne používajú. Takéto identifikátory môžu byť odvodené z trvalých osobných údajov (meno a priezvisko, e-mail, telefónne číslo atď.), ktoré sú v zariadení užívateľa hašované, zhromaždené a zdieľané medzi viacerými správcami s cieľom jednoznačne identifikovať osobu v rôznych súboroch údajov (údaje o používaní zhromaždené prostredníctvom používania webovej lokality alebo aplikácie, údaje o riadení vzťahov so zákazníkmi (CRM) týkajúce sa online alebo offline nákupu alebo predplatného atď.). Na webových sídlach sa trvalé osobné údaje zvyčajne získavajú v súvislosti s overením totožnosti alebo prihlásením sa na odber informačných bulletinov.

62. Ako už bolo uvedené, skutočnosť, že informácie zadáva užívateľ, by nebránila uplatneniu článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, pokiaľ ide o uchovávanie, keďže tieto informácie sú pred ich zberom dočasne uložené v koncovom zariadení.

63. V súvislosti so zhromažďovaním „jedinečných identifikátorov“ na webových stránkach alebo v mobilných aplikáciách dáva subjekt, ktorý údaje zhromažďuje, pokyn prehliadaču (prostredníctvom kódu na strane klienta), aby tieto informácie odoslal. Dochádza tak k „získaniu prístupu“ a uplatňuje sa článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

[30] V stanovisku č. 9/2014 WP29 sa uvádza niekoľko príkladov, kedy súhlas nemusí byť potrebný.