Pokyny 2/2023 týkající se technické oblasti působnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích

Verze 2.0

Přijato dne 7. října 2024

Historie verze

Verze 1.0	14. listopadu 2023	Přijetí pokynů k veřejné konzultaci
Verze 2.0	7. října 2024	Přijetí pokynů po veřejné konzultaci

Shrnutí

V těchto pokynech se Evropský sbor pro ochranu osobních údajů (EDPB) zabývá použitelností čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích na různá technická řešení. V těchto pokynech se dále rozpracovává stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29 o uplatňování směrnice o soukromí a elektronických komunikacích na snímání otisků zařízení a jejich cílem je zajistit jasné chápání technických operací, na něž se vztahuje čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

Vznik nových metod sledování, které nahrazují stávající nástroje sledování (například soubory cookie, protože někteří dodavatelé prohlížečů přestali podporovat soubory cookie třetích stran) a vytvářejí nové obchodní modely, se stal jedním ze zásadních problémů v oblasti ochrany údajů. Zatímco u některých sledovacích technologií, jako jsou soubory cookie, je použitelnost čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích dobře zavedená a uplatňovaná, je nutno zabývat se nejasnostmi souvisejícími s uplatňováním uvedeného ustanovení na nově vznikající nástroje sloužící ke sledování.

Pokyny rozlišují tři klíčové prvky pro použitelnost čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích (oddíl 2.1), a sice „informace“, „koncové zařízení účastníka nebo uživatele“ a „získávání přístupu a uchovávání informací a uchovávané informace“. Pokyny dále obsahují podrobnou analýzu každého prvku (oddíly 2.2–2.6).

V oddíle 3 se tato analýza použije na nevyčerpávající seznam případů použití představujících běžné techniky, a to:

- sledování URL a pixelů,
- místní zpracování,
- sledování pouze na základě IP adresy,
- občasné a zprostředkované podávání zpráv o internetu věcí (IoT),
- jedinečný identifikátor.

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. e) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“),

s ohledem na Dohodu o EHP a zejména přílohu XI a protokol 37 k uvedené dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, ve znění směrnice 2009/136/ES (dále jen „směrnice o soukromí a elektronických komunikacích“),

s ohledem na články 12 a 22 svého jednacího řádu,

PŘIJAL TYTO POKYNY:

1 ÚVOD

1. Podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích je *„uchovávání informací nebo získávání přístupu k již uchovávaným informacím (...) v koncovém zařízení účastníka nebo uživatele“* povoleno pouze pod podmínkou souhlasu pro konkrétní účely stanovené v uvedeném článku. Jak se připomíná ve 24. bodě odůvodnění směrnice o soukromí a elektronických komunikacích[2], cílem tohoto ustanovení je chránit koncová zařízení uživatelů, neboť jsou součástí soukromí uživatelů. Ze znění článku vyplývá, že čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích se nevztahuje výlučně na soubory cookie, ale také na „podobné technologie“. V současné době však neexistuje úplný seznam technických operací, na něž se vztahuje čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

2. Ve stanovisku č. 9/2014 pracovní skupiny zřízené podle článku 29 k uplatňování směrnice o soukromí a elektronických komunikacích na snímání otisků zařízení (dále jen „stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29“) se již objasnilo, že snímání otisků zařízení spadá do technické oblasti působnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích[3], ale vzhledem k novému pokroku v oblasti technologií je zapotřebí dalších pokynů, pokud jde o techniky sledování, které jsou v současnosti pozorovány. Technické prostředí se v posledním desetiletí vyvíjelo a stále častěji se využívají identifikátory začleněné do operačních systémů a také se vytvářejí nové nástroje umožňující uchovávání informací v koncových zařízeních.

[1] Pokud se v tomto dokumentu hovoří o „členských státech”, rozumějí se tím „členské státy EHP“.

[2] „Koncové zařízení uživatelů sítí elektronických komunikací a jakékoli informace uchovávané na takovém zařízení tvoří součást soukromí uživatelů, které vyžaduje ochranu v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod. Tzv. špionážní software („spyware“), webové štěnice („web bugs“), skryté identifikátory a jiné podobné nástroje mohou pronikat do koncového zařízení uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele a mohou vážně narušit soukromí těchto uživatelů. Použití takových nástrojů by mělo být povoleno pouze k oprávněným účelům s vědomím uživatelů, kterých se dotýká.“

[3] Stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29, s. 11.

3. Nejasnosti týkající se oblasti působnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích vytvořily pobídky k zavádění alternativních řešení pro sledování uživatelů internetu a vedou k tendenci obcházet právní povinnosti stanovené v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Všechny takové situace vyvolávají obavy a vyžadují doplňující analýzu, která doplní předchozí pokyny EDPB.

4. Cílem těchto pokynů je provést technickou analýzu oblasti působnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, konkrétně objasnit, co technicky zahrnuje formulace „*k uchovávání informací nebo získávání přístupu k informacím uchovávaným v koncovém zařízení účastníka nebo uživatele*“. Tyto pokyny se nezabývají okolnostmi, za nichž se na operaci zpracování mohou vztahovat výjimky z požadavku souhlasu stanovené ve směrnici o soukromí a elektronických komunikacích[4], neboť tyto okolnosti by měly být analyzovány případ od případu s ohledem na provedení právních předpisů příslušným členským státem a na pokyny vydané příslušnými vnitrostátními orgány.

5. Nevyčerpávající seznam konkrétních případů použití bude analyzován v závěrečné části těchto pokynů.

2 ANALÝZA

2.1 Klíčové prvky pro použitelnost čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích

6. Ustanovení čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích se použije, pokud:

   a. **KRITÉRIUM A:** prováděné operace se týkají „*informací*“. Je třeba připomenout, že použitým pojmem nejsou „osobní údaje“, ale „informace“.

   b. **KRITÉRIUM B:** prováděné operace zahrnují „*koncové zařízení*“ účastníka nebo uživatele (B.1), což znamená potřebu posoudit pojem „*veřejná komunikační síť*“ (B.2).

   c. **KRITÉRIUM C:** provedené operace skutečně představují „*uchovávání*“ (C.1) nebo „*získávání přístupu*“ (C.2). Tyto dva pojmy lze zkoumat odděleně, jak se připomíná ve stanovisku č. 9/2014 pracovní skupiny zřízené podle článku 29: „*Použití slov ‚které jsou uchovávány nebo k nimž je získán přístup‘ naznačuje, že k uchovávání a přístupu nemusí dojít v rámci stejné komunikace a nemusí je provést tatáž strana.*“[5]

   Z důvodu srozumitelnosti bude subjekt, který získá přístup k informacím uloženým v koncovém zařízení uživatele, dále v textu označován jako „přistupující subjekt“.

2.2 Pojem „informace“ – kritérium A

7. Jak je uvedeno v KRITÉRIU A, v tomto oddíle se podrobně popisuje, co zahrnuje pojem „informace“. Výběr pojmu „informace“, který zahrnuje širší kategorii než pouhý pojem osobní údaje, souvisí s oblastí působnosti směrnice o soukromí a elektronických komunikacích.

8. Cílem čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích je chránit soukromí uživatelů, jak je uvedeno ve 24. bodě odůvodnění: „*Koncové zařízení uživatelů sítí elektronických komunikací a*

[4] Jak je uvedeno v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích: „*To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal.*“

[5] Stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29, s. 8.

jakékoli informace uchovávané na takovém zařízení tvoří součást soukromí uživatelů, které vyžaduje ochranu v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod.“ Je rovněž chráněno článkem 7 Listiny základních práv EU.

9. Na scénáře, které narušují soukromí i bez zahrnutí osobních údajů, se totiž výslovně vztahuje znění čl. 5 odst. 3 a 24. bodu odůvodnění směrnice o soukromí a elektronických komunikacích, například uchovávání virů v koncovém zařízení uživatele. Z toho vyplývá, že definice pojmu „informace“ by neměla být omezena na to, že se vztahuje k identifikované nebo identifikovatelné fyzické osobě.

10. To potvrdil i Soudní dvůr EU: „*Tato ochrana se vztahuje na veškeré informace uložené na tomto koncovém zařízení, bez ohledu na to, zda se týkají osobních údajů či nikoliv, a má za cíl zejména, jak vyplývá z tohoto bodu odůvodnění, chránit uživatele před rizikem pronikání skrytých identifikátorů nebo jiných podobných nástrojů do koncového zařízení těchto uživatelů bez jejich vědomí.*“[6]

11. Otázky, zda je třeba při posuzování použitelnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích zvážit původ těchto informací a důvody jejich uchovávání v koncovém zařízení, byly vyjasněny již dříve. Například ve stanovisku č. 9/2014 pracovní skupiny zřízené podle článku 29: „*To nelze vykládat v tom smyslu, že třetí osoba nepotřebuje souhlas s přístupem k těmto informacím pouze z toho důvodu, že je neuložila. Požadavek na souhlas platí rovněž v případě přístupu k hodnotě určené pouze ke čtení (např. žádost o MAC adresu síťového rozhraní prostřednictvím API operačního systému)*.“[7]

12. Závěrem lze říci, že pojem informace zahrnuje jak neosobní, tak osobní údaje bez ohledu na to, jak a kým byly tyto údaje uloženy, tj. zda je uložil externí subjekt (rovněž včetně jiných subjektů, než je subjekt, který má přístup), uživatel, výrobce nebo zda nastal jakýkoli jiný scénář.

2.3 Pojem „koncové zařízení účastníka nebo uživatele“ – kritérium B.1

13. Tento oddíl vychází z definice použité ve směrnici 2008/63/ES a uvedené v článku 2 směrnice (EU) 2018/1972, kde je „koncové zařízení“ definováno jako: „*zařízení přímo nebo nepřímo připojené k rozhraní veřejné telekomunikační sítě, které může vysílat, zpracovávat nebo přijímat informace; připojení přímé či nepřímé může být provedeno kabelově, za použití optického paprsku nebo elektromagnetických vln; připojení je nepřímé, jestliže je mezi rozhraní sítě a koncové zařízení připojeno další zařízení*“[8].

14. Ve 24. bodě odůvodnění směrnice o soukromí a elektronických komunikacích se jasně vykládá chápání úlohy koncového zařízení pro ochranu podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Směrnice o soukromí a elektronických komunikacích chrání soukromí uživatelů, nejen pokud jde o důvěrnost jejich informací, ale také tím, že chrání integritu koncového zařízení uživatele. Toto chápání bude vodítkem pro výklad pojmu koncového zařízení v rámci těchto pokynů.

15. Článek 3 směrnice o soukromí a elektronických komunikacích stanoví, že aby se směrnice o soukromí a elektronických komunikacích mohla použít, musí být zpracování osobních údajů prováděno ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích. To znamená, že zařízení by mělo být použitelné ve spojení s takovou službou, a že má-li naplňovat znaky koncového zařízení, mělo by být připojeno nebo připojitelné[9] k rozhraní

[6] Rozsudek Soudního dvora ze dne 1. října 2019, Planet 49, věc C-673/17, ECLI:EU:C:2019:801, bod 70.
[7] Stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29, s. 8.
[8] Směrnice Komise 2008/63/ES ze dne 20. června 2008 o hospodářské soutěži na trhu s telekomunikačními koncovými zařízeními (kodifikované znění), čl. 1 bod 1.
[9] To znamená mít technické možnosti pro připojení k síti, i když k tomuto připojení aktuálně nedochází.

veřejné komunikační sítě. EDPB konstatuje, že změny provedené v roce 2009[10] ve znění čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích rozšířily ochranu koncových zařízení zrušením odkazu na „užívání sítí elektronických komunikací“ jako prostředku pro uchovávání informací nebo získání přístupu k informacím uchovávaným v koncovém zařízení. Pokud má tedy zařízení síťové rozhraní, které jej činí způsobilým pro připojení (i když k takovému připojení nedojde), použije se čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích na každý subjekt, který by uchovával informace již uchovávané v koncovém zařízení a získal by k nim přístup, a to bez ohledu na způsob přístupu ke koncovému zařízení a na to, zda je propojen, či odpojen od sítě.

16. Zařízení, která jsou součástí samotné veřejné sítě elektronických komunikací, by podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích nebyla považována za koncová zařízení[11].

17. Koncové zařízení může sestávat z libovolného počtu jednotlivých hardwarových prvků, které dohromady tvoří koncové zařízení. To může, ale nemusí mít podobu fyzicky uzavřeného zařízení, které obsahuje veškerý zobrazovací, výpočetní, úložný a periferní hardware (například chytré telefony, notebooky, síťová úložná zařízení, propojené automobily nebo televizory s internetem, chytré brýle).

18. Ve směrnici o soukromí a elektronických komunikacích se uznává, že ochrana důvěrnosti informací uchovávaných v koncovém zařízení uživatele a integrity koncového zařízení uživatele není omezena na ochranu soukromí fyzických osob, ale týká se rovněž práva na respektování jejich korespondence nebo oprávněných zájmů právnických osob[12]. Koncová zařízení, která umožňují tuto korespondenci a oprávněné zájmy právnických osob, jsou jako taková chráněna podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

19. Uživatel nebo účastník může koncové zařízení vlastnit nebo si je pronajímat nebo mu může být jinak poskytnuto. Stejné koncové zařízení může sdílet více uživatelů nebo účastníků.

20. Tuto ochranu zaručuje směrnice o soukromí a elektronických komunikacích koncovému zařízení přidruženému k uživateli nebo účastníkovi a nezávisí na tom, zda uživatel nastavil prostředky přístupu (například zda inicioval elektronickou komunikaci), nebo dokonce na tom, zda si je uživatel vědom uvedených prostředků přístupu).

2.4 Pojem „veřejná komunikační síť“ – kritérium B.2

21. Vzhledem k tomu, že situace upravená směrnicí o soukromí a elektronických komunikacích se týká *„poskytování veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích ve Společenství“*[13] a v definici koncového zařízení se výslovně zmiňuje pojem *„veřejné komunikační sítě“*, je zásadní tento pojem vyjasnit, aby bylo možné určit kontext, v němž se čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích použije.

[10] Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele (text s významem pro EHP), Úř. věst. L 337, 18.12.2009, čl. 2 odst. 5 a 65. bod odůvodnění.

[11] Pro určení limitů sítě v různých kontextech viz pokyny sdružení BEREC ke společným přístupům k identifikaci koncového bodu sítě v různých topologiích sítí (BoR (20) 46).

[12] Jak je připomenuto v čl. 2 bodě 13 směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace, uživatelem totiž může být fyzická nebo právnická osoba.

[13] Článek 3 směrnice o soukromí a elektronických komunikacích.

22. Pojem „sítí elektronických komunikací“ není v samotné směrnici o soukromí a elektronických komunikacích definován. Tento pojem byl původně uveden ve směrnici 2002/21/ES (rámcová směrnice) o společném předpisovém rámci pro sítě a služby elektronických komunikací[14], která byla následně nahrazena čl. 2 odst. 1 směrnice 2018/1972 (evropský kodex elektronických komunikací). Nyní zní takto:

> *„sítí elektronických komunikací“ [se rozumí] přenosové systémy, ať jsou založeny na trvalé infrastruktuře nebo centralizované správní kapacitě, či nikoli, a popřípadě i spojovací nebo směrovací zařízení a jiné prostředky, včetně neaktivních síťových prvků, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných (okruhově nebo paketově komutovaných, včetně internetu) a mobilních sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na typ přenášené informace.*[15]

23. Tato definice je neutrální ve vztahu k přenosovým technologiím. Síť elektronických komunikací je podle této definice jakýkoli síťový systém, který umožňuje přenos elektronických signálů mezi svými uzly, bez ohledu na použité zařízení a protokoly.

24. Pojem síť elektronických komunikací podle směrnice 2018/1972 nezávisí na veřejné nebo soukromé povaze infrastruktury ani na způsobu zavedení nebo správy sítě („*ať jsou založeny na trvalé infrastruktuře nebo centralizované správní kapacitě, či nikoli*“[16].) Definice sítě elektronických komunikací podle článku 2 směrnice 2018/1972 je tedy dostatečně široká na to, aby zahrnovala jakýkoli druh infrastruktury. Zahrnuje sítě spravované nebo nespravované operátorem, sítě společně spravované skupinou operátorů, nebo dokonce sítě ad hoc, v jejichž rámci se koncové zařízení může dynamicky připojovat k síti jiných koncových zařízení nebo ji opouštět pomocí přenosových protokolů krátkého dosahu.

25. Tato definice sítě nestanoví žádné omezení, pokud jde o počet koncových zařízení přítomných v síti v jakémkoliv okamžiku. Některé síťové struktury jsou založeny na tom, že uzly předávají informace ad hoc uzlům, které jsou právě připojeny[17], a v určitém okamžiku mohou komunikovat pouze dva uzly na stejné úrovni. Takové případy by spadaly do obecné působnosti směrnice o soukromí a elektronických komunikacích, pokud by síťový protokol umožňoval začlenění dalších podobných subjektů.

26. Veřejná dostupnost komunikační sítě je nezbytnou podmínkou, má-li být zařízení považováno za koncové zařízení, a tudíž i použitelnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Je třeba poznamenat, že skutečnost, že síť je zpřístupněna omezené podskupině veřejnosti (například účastníkům, bez ohledu na to, zda platí, či nikoli, na základě podmínek způsobilosti), neznamená, že je tato síť soukromá[18].

---

[14] Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).

[15] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění), text s významem pro EHP, čl. 2 bod 1.

[16] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění), text s významem pro EHP, čl. 2 bod 1.

[17] Například v kontextu síťových struktur tolerujících zpoždění, kterými se zavádějí „techniky uchovávání a dalšího předávání (store and forward)“, jako je projekt s otevřeným zdrojovým kódem Briar.

[18] Další analýzu identifikace veřejných komunikačních sítí naleznete v pokynech sdružení BEREC k provádění nařízení o otevřeném internetu (BoR (20) 112).

2.5 Pojem „získávání přístupu“ – kritérium C.1

27. Pro správné zasazení pojmu „získávání přístupu“ do kontextu je důležité vzít v úvahu oblast působnosti směrnice o soukromí a elektronických komunikacích uvedenou v jejím článku 1: *„zajištění rovnocenné úrovně ochrany základních práv a svobod, zejména práva na soukromí a zachování důvěrnosti informací, se zřetelem na zpracování osobních údajů v odvětví elektronických komunikací, a (...) zajištění volného pohybu těchto údajů a elektronických komunikačních zařízení a služeb ve Společenství.*“

28. Stručně řečeno, směrnice o soukromí a elektronických komunikacích je právní nástroj na ochranu soukromí, jehož cílem je chránit důvěrnost komunikace a integritu zařízení. Ve 24. bodě odůvodnění směrnice o soukromí a elektronických komunikacích se objasňuje, že v případě fyzických osob je koncové zařízení uživatele součástí jejich soukromí a že přístup k informacím na něm uchovávaným bez jejich vědomí může jejich soukromí vážně narušit.

29. Směrnicí o soukromí a elektronických komunikacích jsou rovněž chráněny právnické osoby[19]. Proto musí být pojem „získávání přístupu“ podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích vykládán způsobem, který tato práva chrání před porušováním třetími stranami.

30. Uchovávání informací nebo získávání přístupu mohou být nezávislé operace a mohou je provádět nezávislé subjekty. Aby se použil čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, nemusí současně docházet k uchovávání informací a k přístupu k již uchovávaným informacím.

31. Jak je uvedeno ve stanovisku č. 9/2014 pracovní skupiny zřízené podle článku 29: „*Použití slov ‚které jsou uchovávány nebo k nimž je získán přístup' naznačuje, že k uchovávání a přístupu nemusí dojít v rámci stejné komunikace a nemusí je provést tatáž strana. Informace, které uchovává jedna strana (včetně informací uchovávaných uživatelem nebo výrobcem zařízení) a k nimž později získá přístup jiná strana, proto spadají do oblasti působnosti čl. 5 odst. 3.*“[20] Z toho vyplývá, že pro uplatnění pojmu přístupu neplatí žádná omezení týkající se původu informací na koncovém zařízení.

32. Kdykoli subjekt podnikne kroky k získání přístupu k informacím uchovávaným v koncovém zařízení, použije se čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. To obvykle znamená, že přistupující subjekt musí aktivně odesílat konkrétní pokyny koncovým zařízením, aby mohl zpět přijmout cílené informace. Tak je tomu například v případě souborů cookie, kdy přistupující subjekt dává koncovému zařízení pokyn, aby aktivně odesílalo informace při každém dalším zavolání protokolu HTTP (Hypertext Transfer Protocol).

33. Stejně tak je tomu v případě, kdy přistupující subjekt distribuuje na koncovém zařízení uživatele software, který je uložen, a následně aktivně zavolá prostřednictvím sítě koncový bod rozhraní pro programování aplikací („API“). Jako další příklady lze uvést kód v jazyce JavaScript, kdy přistupující subjekt udělí pokyny prohlížeči uživatele, aby zasílal asynchronní žádosti s cílovými informacemi. Takový přístup zjevně spadá do oblasti působnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, neboť přistupující subjekt výslovně udílí pokyny koncovému zařízení, aby odesílalo informace.

34. V některých případech nemusí být subjekt, který dává koncovému zařízení pokyn k odeslání cílových údajů, a subjekt, který informace přijímá, totožný. To může vyplývat z ustanovení a/nebo používání společného mechanismu mezi oběma subjekty. Udílení pokynů zařízení k odesílání již uchovávaných

[19] 26. bod odůvodnění směrnice o soukromí a elektronických komunikacích, viz bod 17 výše.
[20] Stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29, s. 8.

informací (například použitím protokolu nebo SDK[21], které implikuje aktivní odesílání informací ze strany koncového zařízení) umožňuje vniknutí do koncového zařízení, a proto takový přístup zakládá použitelnost čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Jak je uvedeno ve stanovisku č. 9/2014 pracovní skupiny zřízené podle článku 29, může tomu tak být v případě, kdy webová stránka dá koncovému zařízení pokyn k odesílání informací reklamním službám třetích stran prostřednictvím začlenění sledovacího pixelu[22]. Tento případ použití je dále rozpracován v oddíle 3.1.

2.6 Pojmy „uchovávání informací“ a „uchovávané informace“ – kritérium C.2

35. Uchováváním informací ve smyslu čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích se rozumí ukládání informací na fyzickém elektronickém paměťovém médiu, které je součástí koncového zařízení uživatele nebo účastníka[23].

36. Informace se obvykle neuchovávají v koncovém zařízení uživatele nebo účastníka prostřednictvím přímého přístupu k paměti zařízení třetí stranou, ale spíše pokynem uděleným softwaru, aby vytvářel na koncovém zařízení konkrétní informace. Uchovávání, ke kterému dochází prostřednictvím těchto pokynů, se považuje za iniciované přímo druhou stranou. To zahrnuje používání zavedených protokolů, jako je ukládání souborů cookie v prohlížeči, jakož i individualizovaného softwaru bez ohledu na to, kdo protokoly nebo software na koncovém zařízení vytvořil nebo nainstaloval.

37. Směrnice o soukromí a elektronických komunikacích nestanoví žádnou horní ani dolní hranici doby, po kterou musí informace být přechovávány v paměťovém médiu, aby mohly být považovány za uložené, ani neexistuje horní nebo dolní hranice pro množství informací, které mají být uchovávány.

38. Stejně tak pojem uchovávání nezávisí na typu média, na kterém jsou informace uchovávány. Typickými příklady jsou pevné disky („HDD“), polovodičové disky („SSD“), elektricky vymazatelná programovatelná paměť pouze pro čtení („EEPROM“) a paměť s náhodným přístupem („RAM“), ale z oblasti působnosti nejsou vyloučeny ani méně typické scénáře zahrnující médium, jako je magnetická páska nebo mezipaměť centrální procesorové jednotky („CPU“). Paměťové médium může být připojeno interně (např. prostřednictvím připojení SATA), externě (např. prostřednictvím připojení USB).

39. „Uchovávanými informacemi“ se rozumí informace, které již existují v koncovém zařízení, bez ohledu na zdroj nebo povahu těchto informací, a to včetně jakéhokoli výsledku uchovávání informací ve smyslu čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, jak je popsáno výše (buď stejnou stranou, která později získá přístup, nebo jinou třetí stranou). Dále zahrnuje výsledky procesů uchovávání informací mimo oblast působnosti čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, jako jsou: uchovávání v koncovém zařízení samotným uživatelem nebo účastníkem nebo výrobcem hardwaru (například adresy MAC síťového rozhraní), senzory integrované do koncového zařízení nebo procesy a programy prováděné na koncovém zařízení, které mohou, ale nemusí vytvářet informace závislé na uchovávaných informacích nebo z nich odvozené.

[21] SDK („software development kit“) je soubor nástrojů pro vývoj softwaru, které jsou k dispozici pro usnadnění tvorby softwaru aplikace.
[22] Stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29, s. 9.
[23] Jak je definováno v oddíle 2.3 těchto pokynů.

3 PŘÍPADY POUŽITÍ

40. Jak bylo zdůrazněno v úvodu těchto pokynů[24], neanalyzuje se zde uplatňování výjimek z povinnosti získat souhlas stanovený v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. EDPB připomíná, že ve všech případech, kdy dochází k uchovávání informací nebo získávání přístupu k již uchovávaným informacím, je třeba posoudit, zda je nutný souhlas nebo zda by se mohla uplatnit výjimka podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Čtenář by proto měl ve svém případě použití zvážit výjimky ve spojení s touto technickou analýzou.

41. Aniž je dotčen zvláštní kontext, v němž lze použít tyto technické kategorie, které jsou nezbytné k posouzení, zda se použije čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, je možné orientačně určit široké kategorie identifikátorů a informací, které jsou běžně používány a může se na ně vztahovat čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

42. Síťová komunikace se obvykle opírá o několikavrstvý model, který vyžaduje použití identifikátorů umožňujících správné navázání a průběh komunikace. Předání těchto identifikátorů vzdáleným účastníkům je řízeno prostřednictvím softwaru podle dohodnutých komunikačních protokolů. Jak bylo uvedeno výše, skutečnost, že přijímajícím subjektem nemusí být subjekt, který udílí pokyny k odesílání informací, nevylučuje použití čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Může jít o směrovací identifikátory, jako je adresa MAC nebo IP koncového zařízení, ale také o identifikátory relace (SSRC, identifikátor webového socketu) nebo autentizační tokeny.

43. Stejně tak může protokol aplikace obsahovat několik mechanismů pro poskytování kontextových údajů (například hlavičku HTTP včetně pole „accept“ (přijmout) nebo user agent), mechanismus ukládání do mezipaměti (například ETag[25]) nebo jiné funkce (jednou z nich jsou soubory cookie nebo HSTS[26]). Opět platí, že spoléhání se na tyto mechanismy při shromažďování informací (například v souvislosti se snímáním otisků zařízení[27] nebo sledováním identifikátorů zdrojů) může vést k tomu, že se použije čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

44. Na druhou stranu za určitých situací používají místní aplikace nainstalované v koncovém zařízení některé informace výhradně uvnitř koncového zařízení, jako tomu může být v případě systémových rozhraní API chytrého telefonu (přístup k fotoaparátu, mikrofonu, snímači GPS, akceleračnímu čipu, rádiovému čipu, přístup k místním souborům, seznamu kontaktů, přístup k identifikátorům atd.). To může platit i pro webové prohlížeče, které zpracovávají informace uchovávané nebo vytvářené uvnitř zařízení (například soubory cookie, místní úložiště, WebSQL, nebo dokonce informace poskytnuté samotnými uživateli). Použití těchto informací ze strany aplikace by nepředstavovalo „získávání přístupu k již uchovávaným informacím“ ve smyslu čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, pokud informace neopustí zařízení, ale pokud se získává přístup k těmto informacím nebo k jakýmkoli informacím z nich odvozených, použije se čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

45. V neposlední řadě pak v některých případech distribuují subjekty škodlivé softwarové prvky, jako je například software pro těžbu kryptoměn nebo obecněji malware, a využívají tak výpočetní schopnosti

[24] Viz bod 4 výše.

[25] HTTP ETag je identifikátor, který umožňuje provádět podmíněné požadavky na základě platnosti dat uložených v mezipaměti klienta.

[26] HTTP Strict Transport Security (HSTS) umožňuje serverům určit, které zdroje mají být vždy vyžadovány pomocí připojení HTTPS.

[27] Jak je uvedeno v úvodu, viz stanovisko č. 9/2014 pracovní skupiny zřízené podle článku 29 k uplatňování směrnice o soukromí a elektronických komunikacích na snímání otisků zařízení.

koncového zařízení ve prospěch distribuujícího subjektu. Distribuce uvedeného škodlivého softwaru v koncovém zařízení uživatele představuje „uchovávání“ ve smyslu čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Pokud by navíc software navázal síťové připojení za účelem pozdějšího odesílání informací, představuje toto jednání „získávání přístupu“ ve smyslu čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

46. Pro podskupinu těchto kategorií, které představují zvláštní zájem, buď z důvodu jejich rozšířeného využití, nebo proto, že je zapotřebí zvláštní studie s ohledem na okolnosti jejich použití, uvádíme níže zvláštní analýzu.

3.1 Sledování URL a pixelů

47. Sledovací pixel je hypertextový odkaz na zdroj, obvykle soubor s obrázkem, vložený do obsahu, jako je webová stránka nebo e-mail. Tento pixel obvykle neplní žádný účel související s požadovaným obsahem jako takovým; jeho jediným účelem je automatické navázání komunikace klienta s hostitelem pixelu, ke které by jinak nedošlo. To však není systematické a sledovací pixely lze vytvořit také přidáním dalších informací k obrázkům načítajícím hypertextové odkazy, které jsou relevantní pro obsah zobrazený uživateli. Při navázání komunikace se přenáší různé informace hostiteli pixelu v závislosti na konkrétním případu použití.

48. V případě e-mailu může odesílatel přiložit sledovací pixel, aby zjistil, kdy si příjemce e-mail přečte. Sledovací pixely na webových stránkách mohou odkazovat na subjekt, který shromažďuje mnoho takových požadavků, a může tak sledovat chování uživatelů. Takové sledovací pixely mohou jako součást odkazu obsahovat také další identifikátory, metadata nebo obsah. Tyto datové body může přidat vlastník internetových stránek, a to i v souvislosti s činností uživatele na těchto internetových stránkách, aby bylo možné vytvářet analytické zprávy o používání. Mohou být také dynamicky generovány prostřednictvím aplikační logiky na straně klienta, kterou dodává daný subjekt.

49. Sledovací odkazy mohou fungovat stejným způsobem, ale identifikátor je připojen k adrese webové stránky. Když uživatel navštíví adresu URL (Uniform Resource Locator, jednotný lokátor zdroje), cílová webová stránka načte požadovaný zdroj, ale zároveň shromáždí identifikátor, který není relevantní z hlediska identifikace zdroje. Webové stránky elektronických obchodů je velmi často používají k identifikaci původu příchozího zdroje návštěvnosti. Takové webové stránky mohou například poskytovat partnerům sledované odkazy, které mohou používat na své doméně, aby webová stránka elektronického obchodu věděla, který z jeho partnerů je zodpovědný za prodej, a vyplatit provizi, což je praxe známá jako „partnerský (affiliate) marketing“.

50. Sledovací odkazy i sledovací pixely mohou být distribuovány prostřednictvím široké škály kanálů, například prostřednictvím e-mailů, internetových stránek, nebo v případě sledovacích odkazů dokonce prostřednictvím jakýchkoli systémů zasílání textových zpráv. Tato distribuce do koncového zařízení uživatele představuje uchovávání, přinejmenším prostřednictvím mechanismu ukládání do mezipaměti softwaru na straně klienta. Proto se použije čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, i když toto uchovávání není trvalé.

51. Doplnění informací o sledování do adres URL nebo obrázků (pixelů) zaslaných uživateli představuje pokyn koncovému zařízení, aby odeslalo zpět cílené informace (specifikovaný identifikátor). V případě dynamicky konstruovaných sledovacích pixelů je pokynem distribuce aplikační logiky (obvykle kód v jazyce JavaScript). Lze tedy mít za to, že shromažďování identifikátorů poskytovaných prostřednictvím těchto sledovacích mechanismů představuje „získávání přístupu“ ve smyslu čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, a proto se použije i na tento krok.

3.2 Místní zpracování

52. Některé technologie jsou založeny na místním zpracování podle pokynů softwaru distribuovaného na koncové zařízení uživatelů, přičemž informace vytvořené místním zpracováním jsou následně zpřístupněny vybraným subjektům prostřednictvím API na straně klienta. To může být například případ rozhraní API poskytovaného webovým prohlížečem, díky kterému lze k výsledkům generovaným lokálně přistupovat na dálku.

53. Pokud jsou zpracované informace v kterémkoli okamžiku a například v kódu na straně klienta zpřístupněny třetí straně, například odeslány po síti zpět na server, představuje taková operace (podle pokynu subjektu, který vytváří kód na straně klienta distribuovaný na koncové zařízení uživatele) „získávání přístupu k již uchovávaným informacím“. Skutečnost, že tyto informace jsou vytvářeny na místní úrovni, nebrání použití čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

3.3 Sledování pouze na základě IP adresy

54. Někteří poskytovatelé vyvíjejí řešení, která jsou založena na shromažďování pouze jedné složky, a to IP adresy, aby mohli sledovat prohlížení stránek[28] uživatelem, v některých případech ve více doménách. V této souvislosti by se mohl použít čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, i když pokyn zpřístupnit IP adresu udělil jiný subjekt než přijímající.

55. Získávání přístupu k IP adresám by však vedlo k použití čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích pouze v případech, kdy tyto informace pocházejí z koncového zařízení účastníka nebo uživatele. I když tomu tak není systematicky (například při aktivaci CGNAT[29]), statické odchozí adresy IPv4 vycházející ze směrovače uživatele by do tohoto případu spadaly, stejně jako adresy IPV6, protože jsou částečně definovány hostitelem. Pokud subjekt nemůže zajistit, že IP adresa nepochází z koncového zařízení uživatele nebo účastníka, musí podniknout všechny kroky podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

56. Ačkoli v těchto pokynech neanalyzujeme uplatňování výjimek z povinnosti získat souhlas stanovené v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, je důležité znovu upozornit, že použitelnost tohoto článku systematicky neznamená, že je třeba získat souhlas. EDPB proto připomíná, že v každém případě je třeba posoudit, zda je nutný souhlas nebo zda by se mohla uplatnit výjimka podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích[30].

3.4 Občasné a zprostředkované podávání zpráv o IoT

57. Zařízení v rámci internetu věcí (IoT) vytvářejí informace nepřetržitě, například prostřednictvím čidel zabudovaných v zařízení, a ty mohou, ale nemusí být lokálně předem zpracovány. V mnoha případech jsou informace zpřístupněny vzdálenému serveru, ale podmínky tohoto shromažďování se mohou lišit.

58. Některá zařízení IoT jsou přímo připojena k veřejné komunikační síti pomocí mobilní SIM karty. Jiná mohou mít nepřímé připojení k veřejné komunikační síti, například prostřednictvím WIFI nebo předávání informací jinému zařízení prostřednictvím připojení point-to-point (například

[28] Jedná se o doplňkový postup nezávislý na použití a funkci IP adresy pro navázání a předání nebo přenos výchozí technické komunikace nebo na skutečnosti, že se může či nemusí jednat o osobní údaje (pokud jde o analýzu soukromí v oblasti elektronických komunikací, jedná se o „informace“).

[29] Službu Carrier-grade NAT neboli CGNAT používají poskytovatelé internetových služeb k maximalizaci využití omezeného počtu IP adres. Pod stejnou veřejnou IP adresu sdružuje několik účastníků.

[30] Ve stanovisku č. 9/2014 pracovní skupiny zřízené podle článku 29 se uvádí několik příkladů, kdy souhlas nemusí být nutný.

prostřednictvím Bluetooth). Druhým zařízením může být například chytrý telefon nebo vyhrazená brána, která může, ale nemusí informace před odesláním na server předem zpracovávat.

59. Zařízení IoT mohou od výrobce dostat pokyn, aby shromážděné informace vždy streamovala, ale přesto je nejprve lokálně ukládala do mezipaměti, například dokud nebude k dispozici připojení.

60. V každém případě by zařízení IoT, pokud je připojeno (přímo či nepřímo) k veřejné komunikační síti, bylo samo o sobě považováno za koncové zařízení. Skutečnost, že informace jsou přenášeny nebo ukládány do mezipaměti za účelem občasného podávání zpráv, nemění povahu těchto informací. V obou případech by se použil čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, protože prostřednictvím pokynu kódu v zařízení IoT k odeslání dynamicky uchovávaných údajů na vzdálený server dochází k „získávání přístupu“.

3.5 Jedinečný identifikátor

61. Pojem „jedinečné identifikátory“ nebo „perzistentní identifikátory“ označuje nástroj, který podniky běžně používají. Tyto identifikátory mohou být odvozeny z trvalých osobních údajů (jméno a příjmení, e-mail, telefonní číslo atd.), které jsou v zařízení uživatele hašovány, shromážděny a sdíleny mezi několika správci za účelem jedinečné identifikace osoby v různých souborech údajů (údaje o používání shromážděné prostřednictvím používání webových stránek nebo aplikací, údaje o řízení vztahů se zákazníky (CRM) související s on-line nebo off-line nákupem nebo předplatným atd.). Na internetových stránkách se perzistentní osobní údaje obvykle získávají v souvislosti s ověřením totožnosti nebo přihlášením k odběru zpravodajů.

62. Jak bylo uvedeno výše, skutečnost, že informace vkládá uživatel, nevylučuje použití čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, pokud jde o uchovávání, neboť tyto informace jsou před shromážděním dočasně uchovávány na koncovém zařízení.

63. V souvislosti se shromažďováním „jedinečných identifikátorů“ na internetových stránkách nebo v mobilních aplikacích dává shromažďující subjekt pokyny prohlížeči (prostřednictvím distribuce kódu na straně klienta), aby tyto informace odeslal. Proto dochází k „získávání přístupu“ a použije se čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.