



**17/CS**

**WP 247**

**Stanovisko č. 1/2017  
k návrhu nařízení o soukromí a elektronických komunikacích (2002/58/ES)**

**Přijaté dne 4. dubna 2017**

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Je nezávislým evropským poradním orgánem pro ochranu údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát zajišťuje ředitelství C (Základní práva a právní stát) Evropské komise, Generální ředitelství pro spravedlnost a spotřebitele, B-1049 Brusel, Belgie, kancelář č. MO-59 05/035.

Internet: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE  
ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ**

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem zejména na články 29 a 30 uvedené směrnice,

s ohledem na svůj jednací řád,

**PŘIJALA TOTO STANOVISKO:**

## SHRNUTÍ

Pracovní skupina vítá návrh nařízení o soukromí a elektronických komunikacích, který předložila Evropská komise dne 10. ledna 2017. Pracovní skupina vítá **volbu nařízení** jako regulačního nástroje. Zajistí to jednotná pravidla v celé EU a vyjasní situaci pro dozorové úřady a obdobné organizace. Pomůže to rovněž zajistit soudržnost s obecným nařízením o ochraně osobních údajů. Tato soudržnost je dále podpořena rozhodnutím učinit **stejný orgán, který je odpovědný za monitorování souladu s obecným nařízením o ochraně osobních údajů**, odpovědným za prosazování pravidel týkajících se soukromí a elektronických komunikací.

Zároveň je pozitivní volba (zachování) **doplňkového právního nástroje**. Ochrana důvěrné komunikace a koncových zařízení má zvláštní charakteristiky, které obecné nařízení o ochraně osobních údajů neupravuje. Pokud jde o tyto druhy služeb, jsou tedy zapotřebí doplňková ustanovení, aby se zajistila odpovídající ochrana základního práva na soukromí a důvěrný charakter sdělení, včetně důvěrnosti koncových zařízení. V tomto ohledu pracovní skupina velmi podporuje **zásadový přístup** zvolený v navrhovaném nařízení, jenž spočívá v **obecných zákazech a omezených výjimkách a cíleném uplatňování konceptu souhlasu**.

Pracovní skupina vítá **rozšíření** působnosti navrhovaného nařízení **na poskytovatele služeb „Over-The-Top“ (OTT)**, služeb, které jsou funkčně rovnocenné tradičnějším komunikačním prostředkům, a mají tedy obdobný potenciál dopadu na soukromí osob v EU a na jejich právo na důvěrnost sdělení. Je rovněž pozitivní, že se navrhované nařízení jednoznačně vztahuje na **obsah a související metadata** a uznává, že **metadata mohou odhalit velmi citlivé údaje**.

Pracovní skupina však také uvádí čtyři body, které k nimž má **vážné výhrady**. Pokud jde o **sledování umístění koncových zařízení, podmínky, za kterých je analýza obsahu a metadat přípustná, standardní nastavení koncových zařízení a softwaru a takzvané „tracking walls“**, navrhované nařízení by snížilo úroveň ochrany poskytované podle obecného nařízení o ochraně osobních údajů. V tomto stanovisku pracovní skupina předkládá konkrétní návrhy s cílem zajistit, aby nařízení o soukromí a elektronických komunikacích zaručilo stejnou nebo vyšší úroveň ochrany odpovídající citlivé povaze dat komunikací (obsahu i metadat).

Pokud jde o **sledování prostřednictvím Wi-Fi**, v závislosti na okolnostech a účelu shromažďování údajů bude takovéto sledování podle obecného nařízení o ochraně osobních údajů pravděpodobně buď podléhat souhlasu, nebo může být prováděno pouze v případě, že budou shromažďované údaje anonymizovány. V tomto druhém případě musí být splněny následující čtyři podmínky: účel shromažďování údajů z koncového zařízení je omezen na čistě statistické počítání, sledování je omezeno v čase a prostoru na rozsah nezbytně nutný pro daný účel, údaje budou neprodleně poté vymazány nebo anonymizovány a existují účinné možnosti neúčastnit se takového shromažďování. Evropská komise se vyzývá, aby podpořila technickou normu pro mobilní zařízení týkající se automatické signalizace námitky vůči tomuto sledování.

Pokud jde o **analýzu obsahu a metadat**, výchozím bodem by mělo být, že je zakázáno zpracovávat data komunikací bez souhlasu všech koncových uživatelů (odesílatelů a příjemců). Aby mohly poskytovatelé poskytovat služby, které uživatel výslovně požaduje,

například funkce vyhledávání a indexování nebo služby převodu textu na řeč, měla by existovat vnitrostátní výjimka pro zpracování obsahu a metadat pro čistě osobní účely samotného uživatele.

Pokud jde o **souhlas se sledováním**, pracovní skupina vyzývá k výslovnému zákazu tzv. „tracking walls“, tj. volby „ber nebo nech být“, která nutí uživatele souhlasit se sledováním, pokud chtějí mít přístup ke službě.

V neposlední řadě pracovní skupina doporučuje, aby koncová zařízení a software musely **standardně nabízet nastavení ochrany soukromí** a dávat uživatelům jasnou možnost potvrdit nebo změnit tato standardní nastavení během instalace. Nastavení musí být snadno přístupná během používání. Uživatelům musí být povoleno signalizovat konkrétní obsah prostřednictvím nastavení jejich internetového prohlížeče. Nastavení ochrany osobních údajů by nemělo být omezeno na zásah třetích stran ani na tzv. „cookies“. Pracovní skupina velmi doporučuje, aby se dodržování normy *Do Not Track* (Nesledovat) stalo povinným.

Pracovní skupina také určila další body, k nimž má výhrady, například v souvislosti s oblastí působnosti, ochranou koncových zařízení a přímým marketingem. V neposlední řadě pracovní skupina určila otázky, které si zaslouží vyjasnění, s cílem lépe chránit koncové uživatele a nastolit větší právní jistotu pro všechny zúčastněné strany.

## OBSAH

<b>1. ÚVOD.....</b>	<b>6</b>
<b>2. Kladné aspekty navrhovaného nařízení .....</b>	<b>6</b>
<i>Harmonizace v rámci celé EU, sjednocení pokut a výlučné prosazování práva úřady pro ochranu údajů .....</i>	<i>6</i>
<i>Rozšíření oblasti působnosti v porovnání se směrnicí o soukromí a elektronických komunikacích 8</i>	
<i>Cílené uplatňování konceptu souhlasu .....</i>	<i>10</i>
<b>3. BODY, K NIMŽ JSOU VÁŽNÉ VÝHRADY .....</b>	<b>10</b>
<i>Ochrana podle obecného nařízení o ochraně osobních údajů je navrhovaným nařízením oslabena .....</i>	<i>10</i>
<b>4. DALŠÍ BODY, K NIMŽ JSOU VÝHRADY .....</b>	<b>16</b>
<i>Územní a věcnou oblast působnosti je třeba rozšířit .....</i>	<i>16</i>
<i>Ochrana koncových zařízení musí být posílena .....</i>	<i>17</i>
<i>Přímý marketing .....</i>	<i>21</i>
<i>Časový harmonogram.....</i>	<i>24</i>
<i>Další výhrady.....</i>	<i>24</i>
<b>5. NÁVRHY NA VYJASNĚNÍ PRO ZAJIŠTĚNÍ PRÁVNÍ JISTOTY .....</b>	<b>27</b>
<i>Vyjasnění působnosti .....</i>	<i>27</i>
<i>Vyjasnění konceptu a použití souhlasu .....</i>	<i>30</i>
<i>Vyjasnění lokalizačních údajů a jiných metadat.....</i>	<i>31</i>
<i>Vyjasnění týkající se nevyžádaných sdělení .....</i>	<i>33</i>
<i>Vyjasnění týkající se použití nástrojů v oblasti základních práv .....</i>	<i>34</i>
<i>Další vyjasnění .....</i>	<i>35</i>

## 1. ÚVOD

1. Pracovní skupina pro ochranu údajů zřízená podle článku 29 (dále jen „pracovní skupina“ nebo „pracovní skupina podle článku 29“) vítá navrhované nařízení Evropské komise (EK) týkající se soukromí a elektronických komunikací (dále jen „navrhované nařízení“ nebo „navrhované nařízení o soukromí a elektronických komunikacích“)<sup>1</sup>, které má nahradit směrnici o soukromí a elektronických komunikacích (dále jen „směrnice o soukromí a elektronických komunikacích“)<sup>2</sup>.
2. Mnoho aspektů navrhovaného nařízení je kladných a představením navrhovaného nařízení podnikla Evropská komise významný krok. Navrhované nařízení však může být dále vylepšeno. Přispělo by to nejen k lepší ochraně koncových uživatelů, ale přineslo by to také větší právní jistotu pro všechny zúčastněné strany.
3. Pracovní skupina chce tedy nadnést několik bodů, k nimž má výhrady a jež doporučuje vyjasnit v Evropském parlamentu a Radě ministrů při projednávání navrhovaného nařízení. Toto stanovisko nejdříve posoudí kladné aspekty navrhovaného nařízení a poté zdůrazní problematické otázky a body, které je třeba vyjasnit.

## 2. Kladné aspekty navrhovaného nařízení

*HARMONIZACE V RÁMCI CELÉ EU, SJEDNOCENÍ POKUT A VÝLUČNÉ PROSAZOVÁNÍ PRÁVA ÚŘADY PRO OCHRANU ÚDAJŮ*

4. Pracovní skupina vítá **volbu nařízení jako regulačního nástroje**. Zajistí to jednotná pravidla v rámci celé EU (s určitými výjimkami, které budou pojednány níže). Vyjasní to situaci pro dozorové úřady a obdobné organizace. S ohledem na klíčovou úlohu, kterou hraje obecné nařízení o ochraně osobních údajů<sup>3</sup> v navrhovaném nařízení, to navíc pomůže zajistit soudržnost mezi oběma nástroji. Zároveň je pozitivní **volba (zachování) doplňkového právního nástroje**. Ochrana důvěrné komunikace a koncových zařízení má zvláštní charakteristiky, které obecné nařízení o ochraně osobních údajů neupravuje. Pokud jde o tyto druhy služeb, jsou tedy

---

<sup>1</sup> Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), 2017/0003 (COD), viz internetové stránky ([http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41241](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241)).

<sup>2</sup> Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. L 201, 31.7.2002, s. 37–47, viz internetové stránky (<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058>).

<sup>3</sup> 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 (obecné nařízení o ochraně osobních údajů), Úř. věst. L 119/1, 4.5.2016, s. 1–88, viz internetové stránky (<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>).

zapotřebí doplňková ustanovení, aby se zajistila odpovídající ochrana tohoto základního práva. V této souvislosti pracovní skupina rovněž **podporuje zásadový přístup zvolený v navrhovaném nařízení, jenž spočívá v obecných zákazech a omezených výjimkách**, a domnívá se, že je zapotřebí se vyhnout zavedení otevřených výjimek v souladu s článkem 6 obecného nařízení o ochraně osobních údajů, a zejména čl. 6 písm. f) uvedeného nařízení (z důvodu oprávněných zájmů).

5. **Prosazování těchto pravidel stejným orgánem, který odpovídá za monitorování souladu s obecným nařízením o ochraně osobních údajů**, dále podpoří soudržnost mezi oběma nástroji. S ohledem na vztah mezi ochranou osobních údajů a ochranou důvěrné komunikace a koncových zařízení je užitečné, aby prosazování ustanovení navrhovaného nařízení bylo svěřeno stejnému dozorovému úřadu, který prosazuje obecné nařízení o ochraně osobních údajů (38. bod odůvodnění a článek 18 navrhovaného nařízení). Kromě toho judikatura Soudního dvora Evropské unie (SDEU)<sup>4</sup> potvrzuje, že je zásadní, aby dozorový úřad byl nezávislý, jak stanoví článek 7 Listiny. Z praktického hlediska by to však vedlo k významnému navýšení práce úřadů pro ochranu údajů bez jakékoli záruky splnění úkolu, pokud nebude navýšen rozpočet. Úřady pro ochranu údajů tedy vítají 38. bod odůvodnění navrhovaného nařízení, který zdůrazňuje, že každému dozorovému úřadu by měly být poskytnuty dodatečné finanční a lidské zdroje, prostory a infrastruktura potřebné pro účinné plnění jeho úkolů podle nového nařízení. Rovněž vítají, že čl. 18 odst. 2 stanoví právní základ pro spolupráci mezi dozorovými úřady zřízenými podle navrhovaného nařízení a vnitrostátními regulačními orgány zřízenými podle navrhované směrnice, kterou se stanoví evropský kodex pro elektronické komunikace (dále jen „evropský kodex pro elektronické komunikace“)<sup>5</sup>.
6. Vzhledem k úzkému vztahu mezi navrhovaným nařízením a obecným nařízením o ochraně osobních údajů je **sjednocení pokut podle navrhovaného nařízení s obecným nařízením o ochraně údajů** také vítáno. Činnosti, které spadají do oblasti působnosti navrhovaného nařízení, jsou dosti citlivé a zahrnují mimo jiné zasahování do důvěrných sdělení a koncových zařízení. Výše pokut by měla být přiměřená těmto citlivým souvislostem. Tyto souvislosti jsou také důvodem, proč je harmonizace v rámci EU důležitá, aby byla zajištěna stejná vysoká úroveň ochrany napříč celým regionem. Článek 23 navrhovaného nařízení stanoví účinné pokuty za porušování nařízení, v obdobné výši jako pokuty stanovené pro porušování pravidel podle obecného nařízení o ochraně osobních údajů, s výjimkou některých bodů (viz poznámka 38).
7. **Vyjmutí konkrétních pravidel, jak oznamovat porušení zabezpečení údajů z těchto právních předpisů**, je třeba také uvítat, neboť zamezí zbytečnému překrývání s

---

<sup>4</sup> Viz např. rozsudek Soudního dvora ze dne 6. října 2015, Safe Harbour, C-362/14, ECLI:EU:C:2015:650, bod 41, a rozsudek Soudního dvora ze dne 21. prosince 2016, Tele2/Watson, C-203/15 a C-698/15, ECLI:EU:C:2016:970, bod 123.

<sup>5</sup> Návrh směrnice Evropského parlamentu a Rady, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění), 2016/0288 (COD), 12.10.2016, viz internetové stránky ([http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN)).

požadavky týkajícími se narušování údajů podle obecného nařízení o ochraně osobních údajů.

8. Rovněž je vítáno, že **pozornost je nyní zaměřena na poskytování rovnocenné úrovně ochrany všem koncovým uživatelům**, neboť navrhované nařízení již nerozlišuje mezi „účastníky“ a jinými uživateli služeb elektronických komunikací.

#### *ROZŠÍŘENÍ OBLASTI PŮSOBNOSTI V POROVNÁNÍ SE SMĚNICÍ O SOUKROMÍ A ELEKTRONICKÝCH KOMUNIKACÍCH*

9. Pracovní skupina vítá **rozšíření oblasti působnosti navrhovaného nařízení s cílem zahrnout poskytovatele služeb „Over-The-Top“ (OTT)**, služeb, které jsou funkčně rovnocenné tradičnějším komunikačním prostředkům, a mají tedy obdobný potenciál dopadu na soukromí občanů EU a na jejich právo na důvěrnost sdělení. Pracovní skupina zvláště vítá, že do oblasti působnosti nařízení nyní spadají všechny kategorie OTT (OTT0, OTT1 a některé OTT2)<sup>6</sup>, neboť nařízení se nevztahuje pouze na tradiční komunikační prostředky (OTT0), ale také na funkčně rovnocenné služby (OTT1), jak je uvedeno v čl. 8 odst. 1 písm. c) navrhovaného nařízení. Je také pozitivní, že kromě definic podle evropského kodexu pro elektronické komunikace jsou zahrnuty některé OTT2, pokud zajišťují pomocnou interpersonální a interaktivní komunikaci, která je ze své podstaty spjata s jejich službami, například v rámci her, seznamovacích aplikací nebo recenzních stránek (čl. 4 odst. 2 navrhovaného nařízení). Obdobně je třeba uvítat **vysvětlení, že ochrana zahrnuje také interakci mezi stroji**. Ve 12. bodě odůvodnění je vyjasněno, že na zařízení, která vzájemně komunikují, se vztahuje ochrana poskytovaná podle navrhovaného nařízení. To je žádoucí, neboť tyto komunikace často obsahují informace chráněné na základě práv na soukromí. Měla by však být vyjasněna použitelnost (viz poznámka 40h).
10. Je rovněž pozitivní, že se **navrhované nařízení jasně vztahuje na obsah a související metadata**. Ve 14. bodě odůvodnění je vyjasněno, že definice „data elektronických komunikací“ uvedená v čl. 4 odst. 3 písm. a) má být dostatečně široká, aby zahrnovala *veškerý* obsah, jakož i související metadata, bez ohledu na například prostředky přenosu signálů. Pracovní skupina však v poznámce 39 uvádí jako problematický bod, že o této stávající definici „dat elektronických komunikací“ se stále ještě jedná. V souladu s tímto rozšířením oblasti působnosti pracovní skupina považuje **uznání skutečnosti, že metadata mohou odhalit velmi citlivé údaje** (viz odstavec 2.2 důvodové zprávy, 2. bod odůvodnění), za nezbytný doplněk. Pracovní skupina vítá skutečnost, že Evropská komise tímto krokem začleňuje názory Evropského soudního dvora obsažené v rozsudcích ve věcech Digital Rights Ireland a Tele2/Watson. Pracovní skupina zřízená podle článku 29 také oceňuje **uznání, že**

---

<sup>6</sup> Další vysvětlení těchto pojmů viz BEREC, *Report on OTT Services* (Zpráva o službách OTT), BoR (16) 35, 29. ledna 2016, s. 15 a 16, viz internetové stránky: ([http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services)). Upozorňujeme také na komentář ve zprávě, že uvedené kategorie mají být považovány za koncepty, které mají být použity v debatě o přezkumu, a nejsou zamýšleny jako právní koncepty.



**analýza obsahu je vysoce rizikovým zpracováním.** V 19. bodě odůvodnění a v čl. 6 odst. 3 písm. b) se stanoví logický právní předpoklad, že skenování obsahu je vysoce rizikovým zpracováním podle článku 35 obecného nařízení o ochraně osobních údajů a zřejmě bez ohledu na existenci zbytkového vysokého rizika vždy vyžaduje předchozí konzultaci s (hlavním) úřadem pro ochranu údajů. Zároveň má pracovní skupina výhrady k rozsahu definice „metadat“ a ke skutečnosti, že na analýzu metadat se nevztahuje stejný povinný požadavek týkající se posouzení vlivu na ochranu osobních údajů (viz poznámky 33 a 46).

11. Je rovněž třeba uvítat, že i nadále je **uznávána důležitost anonymizace**. Ve směrnici o soukromí a elektronických komunikacích již hrála opatření v oblasti anonymizace úlohu při zajišťování slučitelnosti (např. čl. 6 odst. 1 směrnice o soukromí a elektronických komunikacích, který stanoví, že provozní údaje musí být vymazány nebo anonymizovány, jakmile již nejsou potřebné pro přenos sdělení). V čl. 6 odst. 2 písm. c) a čl. 6 odst. 3 písm. b) navrhovaného nařízení je přípustná výjimka ze zákazu zpracování metadat a obsahu na základě souhlasu a za předpokladu, že dotčený účel(y) „nelze splnit zpracováním anonymizovaných informací“. Vyžadování takovýchto opatření na ochranu soukromí vedle žádosti o souhlas uživatelů chrání tyto uživatele před neodůvodněným zpracováním. Pracovní skupina však má zároveň vážné obavy, že přijetí těchto anonymizačních metod by nebylo vyžadováno při sledování polohy uživatelů prostřednictvím jejich mobilních zařízení (viz poznámka 17). Kromě toho, i když mají být použita anonymizační opatření, měli by poskytovatelé vždy provádět posouzení vlivu na ochranu osobních údajů (viz poznámky 33 a 46) a pracovní skupina žádá o doplnění povinnosti zveřejnit, jak jsou data anonymizována a slučována (viz poznámka 42b).
12. Dalším pozitivním bodem je **široká formulace ochrany koncových zařízení**. Ve 20. bodě odůvodnění a v článku 8 se uvádí, že není důležité, jaké technologie se používají pro přístup ke koncovým zařízením: jakékoli zasahování do koncového zařízení, včetně používání jeho funkcí zpracování, vyžaduje souhlas koncového uživatele (s určitými výjimkami). Evropská komise nyní užitečně potvrdila, že toto ustanovení se vztahuje na vytváření digitálních otisků konkrétního zařízení (*device fingerprinting*). Kromě toho pracovní skupina vítá, že pokud třetí strana nedodrží předvolby **nastavené v prohlížeči** konkrétní osoby, jsou tyto předvolby **vynutitelné**, jak je popsáno ve 22. bodě odůvodnění. Je to užitečné v situacích, kdy třetí strana (např. inzertní síť) tato nastavení nerespektuje. Mělo by to však být uvedeno i v příslušném ustanovení navrhovaného nařízení.
13. V neposlední řadě je třeba uvítat, že i nadále jsou **právnícké osoby zahrnuty do působnosti navrhovaného nařízení** (viz odstavec 2.2 důvodové zprávy; 3., 33. a 42 bod odůvodnění; články 1 a 15 a čl. 16 odst. 5). Tak je tomu již ve směrnici o soukromí a elektronických komunikacích, jelikož však úkolem úřadů pro ochranu údajů bude prosazování nových pravidel, je užitečné to konkrétně zdůraznit. Úřady pro ochranu údajů tak mohou podniknout kroky v případech, kdy jsou právnícké osoby obětí porušení ochrany údajů, například pokud společnosti dostávají spamy nebo jsou jejich komunikace tajně sledovány. Pracovní skupina však také jako problematický bod uvádí, že uplatňování souhlasu v případě právníckých osob je

nejasné (viz poznámka 41a) a není jasné, co se rozumí pojmem „oprávněný zájem“ právnických osob v případě přímého marketingu (viz poznámka 43c).

#### *CÍLENÉ UPLATŇOVÁNÍ KONCEPTU SOUHLASU*

14. Pracovní skupina vítá další kategorii vylepšení související s uplatňováním a výkladem konceptu souhlasu. Zaprvé je vítáno **vysvětlení, že přístup k internetu a (mobilnímu) telefonnímu volání jsou základní služby a poskytovatelé těchto služeb nemohou „nutit“ své zákazníky, aby souhlasili s jakýmkoli zpracováním údajů, které není nezbytné pro poskytnutí samotné základní služby**. V 18. bodě odůvodnění se zejména uvádí, že základní širokopásmový přístup k internetu a hlasové komunikační služby se mají považovat za základní služby, což vzhledem k závislosti lidí na přístupu k těmto službám znamená, že souhlas se zpracováním dat komunikací pro tyto doplňkové účely (tj. zpracování pro účely reklamy nebo marketingu) nemůže být platný. Zároveň se pracovní skupina obává, zda toto vysvětlení není příliš omezené. Služby určitých poskytovatelů služeb OTT mohou být rovněž považovány za základní služby a nařízení o soukromí a elektronických komunikacích by mělo volbu „ber nebo nech být“ výslovně zakázat i v jiných situacích (viz poznámka 20).
15. Kromě toho je pozitivní, že **požadavek na souhlas se zahrnutím osobních údajů fyzických osob do seznamů je harmonizovaný**. Podle článku 15 navrhovaného nařízení je zpracování údajů ve veřejných seznamech možné pouze se souhlasem fyzických osob a s možností vznést námitku v případě právnických osob. Toto je dále upřesněno ve 31. bodě odůvodnění, který uvádí, že tento souhlas musí být konkrétní, pokud jde o konkrétní kategorie osobních údajů, které mají být do seznamu zahrnuty. Pracovní skupina však poznamenává, že navrhované nařízení by mohlo být jasněji uvádět že pro vyhledávání a zpětné vyhledávání bude zapotřebí konkrétní samostatný souhlas (viz poznámka 37).
16. Oceňována je také **nová cílená výjimka pro nerušivý zásah do koncových zařízení**. Pracovní skupina zřízená podle článku 29 považuje za užitečné, že navrhované nařízení vyjasňuje, že zákaz se nevztahuje na měření návštěvnosti internetových stránek (s omezenou výjimkou, kdy toto měření provádí poskytovatel služby informační společnosti požadované koncovým uživatelem; viz čl. 8 odst. 1 písm. d) navrhovaného nařízení). Viz dále 21. bod odůvodnění. Pracovní skupina však navrhuje použít definici, která bude z technologického hlediska neutrálnější, a vyjasnit použitelnost této výjimky (viz poznámka 25).

### **3. BODY, K NIMŽ JSOU VÁŽNÉ VÝHRADY**

#### *OCHRANA PODLE OBECNÉHO NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ JE NAVRHOVANÝM NAŘÍZENÍM OSLABENA*

Jak je uvedeno výše, navrhované nařízení zahrnuje řadu klíčových vylepšení. K některým bodům má však pracovní skupina výhrady s různou mírou závažnosti. V tomto oddíle pracovní skupina probere čtyři otázky, k nimž má **vážné výhrady**. Jedná se o ustanovení,

kteřa snižují úroveň ochrany poskytované obecným nařízením o ochraně osobních údajů:

**17. Povinnosti uvedené v nařízení, jež se týkají sledování umístění koncových zařízení, by měly být v souladu s požadavky obecného nařízení o ochraně osobních údajů.** Ustanovení čl. 8 odst. 2 písm. b) navrhovaného nařízení pouze vyžaduje, aby bylo zobrazeno oznámení a provedena bezpečnostní opatření pro účely shromažďování informací vysílaných koncovými zařízeními. Ustanovení čl. 8 odst. 2 písm. b) dále uvádí, že osoba odpovědná za toto shromažďování musí uvést případná opatření, která mohou koncoví uživatelé učinit, aby shromažďování minimalizovali nebo je zastavili. Přitom čl. 8 odst. 2 písm. b) vyvolává dojem, že organizace mohou shromažďovat informace vysílané koncovým zařízením pro sledování fyzického pohybu osob (např. „sledování pomocí Wi-Fi“ nebo „sledování pomocí Bluetooth“) bez souhlasu dotyčné osoby. Strana shromažďující tyto údaje by mohla zdánlivě splňovat požadavky tak, že prostřednictvím oznámení informuje uživatele, aby vypnuli svá zařízení, pokud nechtějí být sledováni. Tento přístup by byl v rozporu se základním cílem telekomunikační politiky Evropské komise poskytovat vysokorychlostní mobilní připojení k internetu se silnou ochranou soukromí za nízkou cenou všem Evropanům, a to přes hranice.

Kromě toho navrhované nařízení nestanoví žádná jasná omezení, pokud jde o rozsah shromažďování údajů nebo činnosti následného zpracovávání. V této souvislosti je třeba uvést, že adresy MAC jsou osobními údaji i poté, co byla přijata bezpečnostní opatření jako hašování. Tím, že nejsou stanoveny další požadavky nebo omezení, je úroveň ochrany těchto osobních údajů podle navrhovaného nařízení významně nižší než podle obecného nařízení o ochraně osobních údajů, podle kterého by takovéto sledování muselo být korektní a zákonné a rovněž transparentní. Ve 25. bodě odůvodnění se dále zbytečně uvádí, že některé z funkcí sledování prostřednictvím Wi-Fi nepředstavují vysoké riziko z hlediska soukromí, zatímco jiné – např. sledování osob v průběhu času – toto riziko představují. Přestože pracovní skupina oceňuje uznání, že sledování osob v průběhu času představuje vysoká rizika z hlediska soukromí, není účelné již předem rozhodnout, že určité jiné funkce rizika nepředstavují, bez dalšího posouzení okolností a přiměřenosti zpracování. Toto posouzení by mělo být provedeno s přihlédnutím k níže uvedeným podmínkám, které se týkají neanonymizovaného sledování prostřednictvím Wi-Fi.

V závislosti na okolnostech a účelu shromažďování údajů bude sledování podle obecného nařízení o ochraně osobních údajů pravděpodobně buď podléhat souhlasu, nebo může být prováděno pouze v případě, že budou shromážděné osobní údaje anonymizovány. Tato anonymizace se přednostně provádí neprodleně po shromáždění. Pokud není okamžitá anonymizace možná s ohledem na účely, pro které jsou údaje shromažďovány, mohou být tyto údaje zpracovávány po dobu, kdy nejsou anonymizovány, pouze za níže uvedených podmínek: i) účel shromažďování údajů musí být omezen na čistě statistické počítání (viz níže uvedené příklady), ii) sledování je omezeno v čase a prostoru na rozsah nezbytně nutný pro daný účel, iii) údaje jsou neprodleně poté vymazány nebo anonymizovány a iv) existuje účinná

možnost se shromažďování údajů neúčastnit. Za všech okolností musí správci údajů samozřejmě splnit požadavek na poskytování odpovídajících informací.

Pracovní skupina se obává, že potenciální nabídka individuální neúčasti pro organizaci, která tyto údaje shromažďuje, by představovala nepřijatelnou zátěž pro občany s ohledem na stále častější využívání takovýchto technologií sledování organizacemi soukromého i veřejného sektoru. Pracovní skupina tedy vyzývá evropské zákonodárce k podpoře vývoje technických norem, aby zařízení mohla automaticky signalizovat námitku vůči takovému sledování, a k zajištění vynutitelnosti respektování tohoto signálu.

Například souhlas podle obecného nařízení o ochraně osobních údajů by byl pravděpodobně vyžadován, pokud správce údajů shromažďuje a uchovává nepřímo identifikovatelné (prostřednictvím Wi-Fi nebo Bluetooth) adresy MAC zařízení a vypočítává umístění uživatele, aby bylo možné sledovat umístění uživatele v průběhu času, například v rámci více obchodů. To platí zejména v případě, kdy toto sledování probíhá na veřejných místech, kde uživatelé oprávněně očekávají, že nebudou identifikováni nebo sledováni, ale přesto jsou zde adresy MAC kolemjdoucích shromažďovány. Takovýto souhlas lze například získat za pomoci aplikace, která vyzývá uživatele, aby umožnili sledování své polohy ve vymezených oblastech výměnou za komerční nabídky nebo nabízením přihlašovacích bodů v rámci vymezených lokalit nebo prostřednictvím modulu pro poskytování souhlasu ve Wi-Fi hotspotech.

Pouze v omezeném počtu případů by mohlo být správcům údajů dovoleno zpracovávat informace vysílané koncovými zařízeními pro účely sledování jejich fyzického pohybu bez souhlasu dotčené osoby. Mohlo by tomu tak být například při počítání počtu zákazníků v rámci konkrétního místa nebo při shromažďování údajů vysílaných na obou stranách stanoviště bezpečnostní kontroly pro zobrazení doby čekání. V obou případech by však údaje musely být vymazány nebo anonymizovány, jakmile bude naplněn statistický účel. To znamená, že adresy MAC zařízení návštěvníků v rámci konkrétního místa, jako např. obchod, musí být anonymizovány okamžitě po shromáždění bez trvalého ukládání adres MAC a způsobem technicky vylučujícím zpětnou identifikovatelnost. V případě výpočtu čekací doby by adresy MAC musely být vymazány nebo anonymizovány, jakmile přestanou být údaje pro výpočet čekací doby zapotřebí (například z toho důvodu, že návštěvník se již přemístil na druhou stranu bezpečnostní kontroly nebo opustil frontu).

Kromě toho by správce údajů musel splnit požadavky na minimalizaci údajů (například neprovádět nepřetržité sledování, pokud je účel omezen na otevírací dobu obchodu, a/nebo provádět náhodný výběr v určitých intervalech). Správci údajů musí také přijmout další opatření ke zmírnění rizik, aby zajistili nulový nebo velmi malý dopad na práva uživatelů na soukromí, například pro ochranu soukromí osob žijících vedle sběrného místa.

Volba požadavku pouhého oznámení podle čl. 8 odst. 2 navrhovaného nařízení je ještě zajímavější s ohledem na závěr 20. bodu odůvodnění, že informace související se zařízením koncových uživatelů mohou být rovněž shromažďovány dálkově, a to za

účelem identifikace a sledování, a že toto zpracování – podle navrhovaného nařízení – může vážně zasahovat do soukromí těchto koncových uživatelů. Kromě toho uvedená povinnost nepřesahuje informační povinnost již stanovenou v článcích 13 a 14 obecného nařízení o ochraně osobních údajů. Vážné narušení soukromí sledováním je dále znásobeno potenciálním přístupem jiných osob ke shromážděným údajům, jako například možnost identifikace koncových uživatelů na základě uložených adres MAC vysílaných jejich mobilními zařízeními pro účely prosazování práva.

**18. Podmínky, za kterých je analýza obsahu a metadat přípustná, musí být dále upřesněny.**

V článku 6 navrhovaného nařízení jsou metadatům a obsahu poskytnuty různé úrovně ochrany. Pracovní skupina zřízená podle článku 29 toto rozlišení nepodporuje: obě kategorie dat jsou vysoce citlivé. Metadata a obsah by tedy měly mít stejně vysokou úroveň ochrany. Výchozím bodem by tak měl být zákaz zpracovávat metadata i obsah bez souhlasu všech koncových uživatelů (tj. odesílatele i příjemce).

V závislosti na účelu však může být určité zpracování přípustné bez souhlasu, pokud je nezbytně nutné pro daný účel:

- Poskytovatelé mohou zpracovávat data elektronických komunikací pro účely uvedené v čl. 6 odst. 1 písm. a) a b) a čl. 6 odst. 2 písm. a) a b) navrhovaného nařízení<sup>7</sup>.
- Je třeba vyjasnit, že určité metody odhalování/filtrování spamu a zmírňování dopadu botnetů mohou být rovněž považovány za nezbytně nutné pro odhalení nebo zastavení zneužívání služeb elektronických komunikací (čl. 6 odst. 2 písm. b)). Pokud jde o filtrování spamu, koncovým uživatelům, kteří dostávají spam, by měla být nabídnuta, pokud je to technicky možné, strukturovaná volba vyjádření nesouhlasu.
- Mělo by být vyjasněno, že analýza dat elektronických komunikací pro účely služeb zákazníkům může rovněž spadat pod výjimku „nezbytné pro vyúčtování“ (viz čl. 6 odst. 2 písm. b)). Příslušná metadata mohou být uchovávána do konce období, v němž lze v souladu s vnitrostátním právem vyúčtování právně napadnout nebo uplatňovat nárok na platbu. Příslušné údaje (např. internetová adresa) mohou být uchovávány pouze na žádost koncového uživatele a pouze na dobu nezbytně nutnou k vyřešení sporu týkajícího se vyúčtování (což znamená, že čl. 7 odst. 3 by měl být pozměněn).
- Mělo by být umožněno zpracovávat data elektronických komunikací pro účely poskytování služeb výslovně požadovaných koncovým uživatelem,

<sup>7</sup> Pokud jde o nezbytnost splnění povinných požadavků na kvalitu služby, jak je uvedeno v čl. 6 odst. 2 písm. a) navrhovaného nařízení, poskytovatelé by také měli přihlídnout k podmínkám popsaným v nařízení (EU) 2015/2120, zejména v článku 3 a v 10. a 13. až 15. bodě odůvodnění. Na základě tohoto ustanovení může být od poskytovatelů vyžadováno, aby zpracovávali data komunikací k odhalování a filtrování malwaru a tzv. špionážního softwaru („spyware“) a může jim být umožněno data komprimovat.

jako například funkce vyhledávání nebo indexování klíčových slov, virtuální asistenti, moduly pro převod textu na řeč a překladatelské služby. To vyžaduje zavedení výjimky pro analýzu těchto údajů pro čistě individuální (domácí) použití, jakož i pro individuální použití související s prací<sup>8</sup>. Toto by tak bylo možné bez souhlasu všech koncových uživatelů, ale mohlo by k tomu docházet pouze se souhlasem koncového uživatele požadujícího danou službu. Tento konkrétní souhlas by rovněž zabraňoval poskytovateli v používání těchto údajů pro jiné účely.

To znamená, že analýza obsahu a/nebo metadat pro veškeré jiné účely, jako např. analytika, profilování, behaviorální reklama nebo jiné účely v (komerční) prospěch poskytovatele, vyžaduje souhlas všech koncových uživatelů, jejichž údaje by byly zpracovávány. Pokud jde o tyto situace, navrhované nařízení by mělo vysvětlit, že pouhý akt odeslání e-mailu nebo jiného druhu osobní komunikace z jiné služby koncovému uživateli, který osobně souhlasil se zpracováním svého obsahu a metadat (např. během registrace ke službě elektronické pošty), nepředstavuje platný souhlas odesílatele.

V neposlední řadě je třeba vyjasnit, že zpracování údajů jiných osob než dotčených koncových uživatelů (např. fotografie nebo popis třetí osoby vyměřované mezi dvěma osobami) musí rovněž splňovat všechna příslušná ustanovení obecného nařízení o ochraně osobních údajů.

19. **Koncová zařízení a software musí *standardně* odrazovat od protiprávních zásahů do těchto zařízení a softwaru, těmto zásahům předcházet a zakazovat je a poskytovat informace o možnostech.** Ačkoli navrhované nařízení ukládá povinnost poskytovatelům softwaru, který umožňuje elektronické komunikace, „nabízet možnost“ zabránit omezené formě zásahu do koncového zařízení a při instalaci ukládá povinnost poskytovatelům softwaru od koncových uživatelů vyžadovat souhlas s nastavením (čl. 10 odst. 1 a 2), tato možnost není rovnocenná *standardnímu nastavení ochrany soukromí*. Kromě toho „možnost“ zabránit určitému zásahu již v současné době existuje, avšak doposud nedokázala dostatečně řešit problém neodůvodněného sledování. Přesně z tohoto důvodu bylo v obecném nařízení o ochraně osobních údajů přijato vědomé politické rozhodnutí zavést zásady záměrné a standardní ochrany údajů a soukromí (článek 25 obecného nařízení o ochraně osobních údajů). Navrhované nařízení podrývá tyto zásady, pokud jde o data komunikací a zařízení. Naopak směrnice o rádiových zařízeních 2014/53/EU<sup>9</sup> (zmíněná v 10. bodě odůvodnění) stanoví pouze velmi omezenou bezpečnostní povinnost vyžadující, aby rádiová zařízení byla vybavena „bezpečnostním zařízením, které zajišťuje ochranu osobních údajů a soukromí uživatele a účastníka“ (čl. 3 odst. 3 písm. e)). Toto nemůže nahradit konkrétní standardní nastavení ochrany

<sup>8</sup> Přestože 13. bod odůvodnění navrhovaného nařízení výslovně vylučuje korporátní síť z oblasti působnosti nařízení, tato nová výjimka týkající se individuálního použití by se měla vztahovat také na používání cloudových služeb zaměstnanci pro účely související s prací, jako například vyhledávání ve své elektronické poště.

<sup>9</sup> Směrnice o rádiových zařízeních 2014/53/EU.

soukromí podle navrhovaného nařízení. V tomto ohledu stojí za to také uvést, že průzkum Eurobarometr o soukromí a elektronických komunikacích zveřejněný v prosinci 2016 uvádí, že „[t]éměř sedm z deseti (69 %) respondentů zcela souhlasí s tím, že by standardní nastavení jejich prohlížeče mělo zamezit sdílení jejich informací“<sup>10</sup>. Pracovní skupina má vedle toho obavy, pokud jde o nastavení prohlížeče a vymezení „třetích stran“ (viz poznámka 24). Kromě toho je třeba mít na paměti, že toto ustanovení se týká nejen prohlížečů používaných v počítačích, ale vztahuje se také na jiné druhy softwaru, který umožňuje komunikaci (včetně operačních systémů, aplikací a softwarových rozhraní pro zařízení připojená díky internetu věcí). Stručně řečeno koncové zařízení a software musí standardně nabízet nastavení ochrany soukromí a provést uživatele konfiguračním menu, aby se mohli při instalaci od těchto standardních nastavení odchýlit. Tato konfigurační menu by měla být během používání vždy snadno přístupná. Pracovní skupina vyzývá evropské zákonodárce, aby v tomto smyslu vyjasnili oblast působnosti článku 10.

20. **Nařízení o soukromí a elektronických komunikacích výslovně zakazuje tzv. „tracking walls“**, tj. praxi, kdy je přístup na internetové stránky nebo k službě odepřen, pokud osoba nesouhlasí s tím, že bude sledována na jiných internetových stránkách nebo službách. Jak již bylo uvedeno v předchozích stanoviscích pracovní skupiny týkajících se směrnice o soukromí a elektronických komunikacích<sup>11</sup>, přístupy jako „ber nebo nech být“ jsou zřídka legitimní<sup>12</sup>. Pokud využití funkcí koncového zařízení pro zpracování a uchovávání, nebo shromažďování informací z koncových zařízení koncových uživatelů umožňují sledovat činnost uživatele v průběhu času nebo v rámci několika služeb (např. různé internetové stránky nebo aplikace), mohou tyto činnosti zpracování vážně zasahovat do soukromí těchto uživatelů. S ohledem na zásadní význam internetu při umožňování základního práva na svobodu vyjadřování, včetně práva na přístup k informacím, by možnost osob získat přístup k obsahu on-line neměla záviset na souhlasu se sledováním činností na různých zařízeních a na různých internetových stránkách / v různých aplikacích. Budoucí nařízení o soukromí a elektronických komunikacích by tedy mělo stanovit, že přístup k obsahu například na internetových stránkách a v aplikacích nemůže být podmíněn souhlasem k takto obtěžujícími činnostmi zpracování bez ohledu na použitou metodu sledování, například cookies, vytváření digitálních otisků zařízení, vkládání jedinečných identifikátorů nebo jiné monitorovací techniky. Nezbytnost tohoto zákazu zdůraznil nedávný průzkum Eurobarometr o soukromí a elektronických komunikacích, podle něhož „[t]éměř dvě třetiny respondentů uvádějí, že je nepřijatelné, aby byly jejich on-line činnosti monitorovány výměnou za neomezený přístup na určitou internetovou stránku (64 %)“.

---

<sup>10</sup> Viz bleskový průzkum Eurobarometr 443, *Report e-Privacy* (Zpráva o soukromí a elektronických komunikacích) (zveřejněný v prosinci 2016), s. 5.

<sup>11</sup> Viz např. WP240 (přezkum směrnice o soukromí a elektronických komunikacích), s. 16; WP208 (výjimka ze souhlasu), s. 5.

<sup>12</sup> Tímto postojem není dotčen čl. 7 odst. 4 obecného nařízení o ochraně osobních údajů, který může rovněž vyloučit volbu „ber nebo nech být“ v jiných situacích, pokud je to na místě.

21. Stručně řečeno, pokud jde o čtyři výše uvedené body, **navrhované nařízení by mělo naplnit svůj příslib poskytnout rovnocennou nebo vyšší úroveň ochrany než obecné nařízení o ochraně osobních údajů**. V 5. bodě odůvodnění se skutečně uvádí, že navrhované nařízení nesnižuje úroveň ochrany poskytované podle obecného nařízení o ochraně osobních údajů. V současné podobě navrhovaného nařízení je to však nesprávné, zejména pokud jde o sledování zařízení (poznámka 17), chybějící zásadu standardního nastavení ochrany soukromí (poznámka 19) a souhlas (poznámka 18). Toto je obzvláště důležité, neboť ve stejném bodě odůvodnění se uvádí, že navrhované nařízení představuje „*lex specialis* k obecnému nařízení o ochraně osobních údajů; upřesní jej a doplní, pokud jde o data elektronických komunikací, která lze považovat za osobní údaje“. Pracovní skupina navrhuje, aby text nařízení o soukromí a elektronických komunikacích alespoň vyjasnil, že:

- i) zákazy podle nařízení o soukromí a elektronických komunikacích mají přednost před povoleními podle obecného nařízení o ochraně osobních údajů (např. zákaz zasahování podle článku 5 nařízení o soukromí a elektronických komunikacích má přednost před právy poskytovatelů služeb elektronických komunikací dále zpracovávat osobní údaje podle čl. 5 odst. 1 písm. b) a čl. 6 odst. 4 obecného nařízení o ochraně osobních údajů);
- ii) pokud je zpracování přípustné podle jakékoli výjimky (včetně souhlasu) ze zákazů podle nařízení o soukromí a elektronických komunikacích, toto zpracování, pokud se týká osobních údajů, přesto vyžaduje, aby byla dodržena všechna příslušná ustanovení obecného nařízení o ochraně osobních údajů;
- iii) pokud je zpracování přípustné podle jakékoli výjimky ze zákazů podle nařízení o soukromí a elektronických komunikacích, jakékoli jiné zpracování na základě obecného nařízení o ochraně osobních údajů je zakázáno, včetně zpracování pro jiné účely na základě čl. 6 odst. 4 obecného nařízení o ochraně osobních údajů. To by nebránilo správcům požadovat další souhlas pro nové operace zpracování. Nebránilo by to ani zákonodárcům povolit další, omezené a konkrétní výjimky z nařízení o soukromí a elektronických komunikacích, například umožnit zpracování pro vědecké nebo statistické účely podle článku 89 obecného nařízení o ochraně osobních údajů nebo chránit „životně důležité zájmy“ osob podle čl. 6 odst. 1 písm. d) obecného nařízení o ochraně osobních údajů.

Kromě toho by nařízení o soukromí a elektronických komunikacích mělo být vykládáno tak, aby bylo zajištěno, že poskytuje alespoň stejnou, případně vyšší úroveň ochrany v porovnání s obecným nařízením o ochraně osobních údajů.

#### **4. DALŠÍ BODY, K NIMŽ JSOU VÝHRADY**

Kromě výše uvedených bodů je pracovní skupina zřízená podle článku 29 **znepokojena** ohledně těchto záležitostí.

*ÚZEMNÍ A VĚCNOU OBLAST PŮSOBNOSTI JE TŘEBA ROZŠÍŘIT*

22. **Pojem „metadata“ je vymezen příliš úzce**. Tento pojem je nyní vymezen v čl. 4 odst. 2 písm. c) jako „údaje zpracovávané v síti elektronických komunikací pro účely



přenášení, šíření nebo výměny obsahu elektronických komunikací“ (zdůraznění přidáno). Použití slova „sítě“ naznačuje, že pouze údaje získané během poskytování služeb ve „spodní“ vrstvě sítě lze považovat za „metadata“. To by mohlo znamenat, že údaje získané během poskytování služby OTT by byly z této působnosti vyloučeny. To by bylo nežádoucí a pravděpodobně nechtěné vzhledem k záměru rozšířit oblast působnosti navrhovaného nařízení na poskytovatele služeb OTT. Aby bylo možné tuto otázku řešit, definice „metadat elektronických komunikací“ by měla být pozměněna tak, aby zahrnovala všechna data zpracovávaná pro účely přenášení, šíření nebo výměny obsahu elektronických komunikací.

23. Kromě toho je znepokojující, že **územní působnost navrhovaného nařízení, pokud jde o organizace, které nejsou usazené v EU, se vztahuje pouze k poskytovatelům služeb elektronických komunikací**. Podle navrhovaného nařízení poskytovatel služeb elektronických komunikací, který není usazen v EU, určí písemně zástupce v Unii (čl. 3 odst. 2). V 9. bodě odůvodnění je také uvedeno, že nařízení by se vztahovalo na zpracování poskytovateli služeb elektronických komunikací bez ohledu na místo zpracování. Pracovní skupina toto vyjasnění vítá. Jelikož je však znění omezeno na poskytovatele služeb elektronických komunikací, je nejisté, do jaké míry se tato územní působnost vztahuje na jiné typy stran (například strany zasahující do koncových zařízení koncových uživatelů nebo shromažďující informace vysílané těmito zařízeními, viz čl. 3 odst. 1 písm. c) nebo článek 8 navrhovaného nařízení). Pracovní skupina proto navrhuje změnit čl. 3 odst. 2 a čl. 3 odst. 5 tak, aby zahrnovaly poskytovatele veřejně dostupných seznamů, poskytovatele softwaru umožňujícího elektronické komunikace a osoby zasílající přímá marketingová obchodní sdělení nebo shromažďující (jiné) informace související s koncovými zařízeními koncových uživatelů nebo uložené v těchto zařízeních, kdykoli jsou jejich činnosti zacíleny na uživatele v EU (viz 8. bod odůvodnění navrhovaného nařízení)<sup>13</sup>.

#### *OCHRANA KONCOVÝCH ZAŘÍZENÍ MUSÍ BÝT POSÍLENA*

Další kategorie výhrad se týká nedostatečné ochrany koncových zařízení v navrhovaném nařízení.

24. Zprvée **navrhované nařízení nesprávně navrhuje, aby platný souhlas mohl být poskytnut prostřednictvím nespécifického nastavení prohlížeče**. Pracovní skupina souhlasí s úvahou, že koncoví uživatelé jsou v současné době přetíženi žádostmi o poskytnutí souhlasu (22. bod odůvodnění). Při řešení tohoto problému je důležité nastavení prohlížeče (a srovnatelného softwaru). Jelikož se však obecná nastavení prohlížeče nemají vztahovat na použití sledovací technologie v jednom konkrétním

<sup>13</sup> Viz čl. 3 odst. 2 obecného nařízení o ochraně osobních údajů: „*Toto nařízení se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí: a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba, nebo b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie.*“ Tato povinnost by také mohla zahrnovat výjimky v souladu s čl. 27 odst. 2 obecného nařízení o ochraně osobních údajů.

případě, jsou nevhodná pro poskytnutí souhlasu podle článku 7 a 32. bodu odůvodnění obecného nařízení o ochraně osobních údajů (jelikož souhlas není informovaný a dostatečně konkrétní).

Koncový uživatel musí mít možnost poskytnout samostatný souhlas pro internetové stránky nebo aplikaci pro sledování pro různé účely (například sdílení v rámci sociálních médií nebo reklama). Správce údajů odpovědný za více internetových stránek nebo aplikací může také požádat o souhlas pro všechny ostatní stránky nebo aplikace, které má na starosti, pokud je tato žádost o souhlas předložena samostatně.

Kromě toho musí správce splnit všechny ostatní povinnosti spojené se souhlasem, včetně povinnosti poskytnout uživatelům odpovídající informace. V případě prohlížečů i správců údajů to znamená, že by bylo neplatné, pokud by nabídli pouze možnost „přijímat všechna cookies“, neboť to by uživatelům neumožnilo poskytnout požadovaný strukturovaný souhlas. Prohlížeče by však měly dávat uživatelům možnost učinit informované a vědomé rozhodnutí přijmout všechna cookies, a tím zabránit jakýmkoli budoucím specifickým žádostem o souhlas z internetových stránek, které navštíví.

Pracovní skupina velmi doporučuje, aby nařízení o soukromí a elektronických komunikacích uložilo prohlížečům povinnost zavést technické mechanismy, například normu *Do Not Track*, aby se zajistilo, že uživatelé skutečně budou mít možnost volby a kontrolu nad zasahováním do svých zařízení<sup>14</sup>.

Především by toto nařízení mělo zajistit, že volba, pokud jde o ukládání informací v zařízení a signál *Do Not Track* z prohlížeče, bude přijímána jako právně závazné vyjádření souhlasu nebo odmítnutí všemi správci údajů. Tím nejsou nijak dotčeny další pokyny pracovní skupiny, pokud jde o soulad normy *Do Not Track*, mimo jiné se zásadou omezení účelu, jakmile bude norma dokončena (plánováno na konec roku 2017).

Nepřímé druhy „souhlasu“, jako například kliknutí na internetové stránky nebo posouvání stránky, nemohou převážit volby, pokud jde o ukládání a signál *Do Not Track*. Důležitou výhodou používání této normy je, že není omezena na sledovací technologie cookies, ale vztahuje se také na jiné druhy sledování, jako je například digitální vytváření otisků.

Stane-li se dodržování této normy právně závazné, vyřeší to i další problém, a to stávající použití pojmu „třetí strany“ v článku 10. Internetová stránka nebo aplikace obvykle obsahuje mnoho prvků, jak ze samotné internetové stránky, tak vnějších prvků. A vnější kód může rovněž fungovat v souvislosti s navštívenou internetovou stránkou, neboť podává zprávy zpět na server třetí strany. Sledovací cookie může být obsluhováno první stranou, pokud uživatel navštíví například stránky některé sociální sítě. Tato stránka sociální sítě by také mohla být třetí stranou, pokud tento uživatel navštíví jinou internetovou stránku, která funguje v součinnosti se stránkou uvedené sociální sítě. Ve všech těchto případech, bez ohledu na to, zda se jedná o „přístup“ k informacím v zařízení koncového uživatele, nebo o „ukládání“ informací do tohoto zařízení, to představuje zasahování do zařízení, které vyžaduje souhlas (pokud se nepoužije jedna z výjimek). V normě *Do Not Track* se v této souvislosti používá

---

<sup>14</sup> Viz internetové stránky (<https://www.w3.org/TR/tracking-compliance/>). Bod 7 vysvětluje model výjimky a rozlišování mezi výjimkami platnými pro určitou internetovou stránku a pro celý internet. Bod 6 se týká strojově čitelných informací, které správci údajů mohou poskytnout, pokud jde o žádosti o informace pro získání souhlasu.

pojem „site-wide“ (pro určitou internetovou stránku) a „internet-wide“ (pro celý internet). Pro zlepšení právní jistoty všech zúčastněných stran by tedy odkaz na „třetí strany“ v nařízení o soukromí a elektronických komunikacích měl být přeformulován tak, aby zahrnoval všechny subjekty, s nimiž je zařízení v součinnosti (protože ukládají informace do zařízení nebo mají k informacím v zařízení přístup).

Aby byla norma *Do Not Track* kompatibilní s vysokou úrovní ochrany důvěrného charakteru sdělení a ochrany údajů poskytovanou podle Listiny, mělo by nařízení o soukromí a elektronických komunikacích by stanovit, že požadavky na sledování pro celý internet na rozdíl od sledování pro určitou internetovou stránku musí být předloženy samostatně a uživatelé by měli mít možnost tyto žádosti přijmout nebo odmítnout. Kromě toho by pro ochranu uživatelů před častými žádostmi o souhlas mělo nařízení o soukromí a elektronických komunikacích zajistit, že odmítnutí přijmout sledování v rámci celého internetu od určité organizace (prostřednictvím normy *Do Not Track* nebo prostřednictvím samostatné černé listiny) této organizaci zabráni v předkládání budoucích žádostí o souhlas, a to po dobu nejméně šesti měsíců. Toto pravidlo uvedené organizaci nebrání, pokud uživatel její stránky přímo navštíví (tj. jako první strana), požádat o souhlas na svých vlastních internetových stránkách (tj. žádost o souhlas platný pro určitou internetovou stránku). V praxi to znamená, že například internetová stránka nabízející audiovizuální přenos prostřednictvím internetu (tzv. video streaming), která používá sledovací cookies, může požádat o souhlas, pokud daný uživatel tuto video streamingovou stránku navštíví, ale nemůže o souhlas znovu požádat po dobu šesti měsíců, pokud tento uživatel souhlas odepřel a navštíví jiné internetové stránky, které obsahují videa poskytovaná z uvedené streamingové internetové stránky.

25. Dále platí, že **výjimka pro „měření návštěvnosti internetových stránek“ je nepřesně formulovaná.** Navrhované nařízení v čl. 8 odst. 1 písm. d) stanoví výjimku pro měření návštěvnosti internetových stránek. Prvním bodem, který vyvolává obavy, je skutečnost, že tento pojem není definován a může být zaměněn s profilováním uživatele. Definice by měla jasně vymezit, že tuto výjimku nelze použít pro účely profilování. Výjimka by se měla vztahovat pouze na analytiku využití nezbytnou pro analýzu výkonnosti služby požadované uživatelem, ale nikoli na analytiku uživatele (tj. analýzu chování identifikovatelných uživatelů internetové stránky, aplikace nebo zařízení). Výjimku tedy nelze použít v situacích, kdy mohou být údaje propojeny s identifikovatelnými údaji o uživateli zpracovávanými poskytovatelem nebo jinými správci údajů. Kromě toho její popis naznačuje technologicky velmi specifickou aplikaci. Definice pojmu „měření návštěvnosti internetových stránek“ by tedy měla být přeformulována tak, aby byla technologicky neutrální a zahrnovala i obdobné analytické využití informací získávaných z aplikací, nositelné elektroniky a zařízení internetu věcí.

Pracovní skupina navrhuje čerpat inspiraci z nizozemské výjimky, která se uplatní, pokud je to nezbytně nutné za účelem získání informací o technické kvalitě nebo účinnosti poskytovaných služeb informační společnosti a má nulový nebo malý dopad na soukromí dotyčného účastníka a/nebo uživatele (viz čl. 11.7a odst. 3 písm. b) nizozemského zákona o telekomunikacích). Tato výjimka přihlíží ke skutečnosti, že většina údajů shromážděných prostřednictvím webové nebo aplikační

analytiky jsou stále osobní údaje. To znamená, že obecné nařízení o ochraně osobních údajů se vztahuje i na zpracování těchto údajů. Naznačuje to například, že analytiku využití by mohla provádět také externí organizace, avšak pouze v případě, že:

- i) uvedená organizace vystupuje jako zpracovatel údajů;
- ii) je uzavřena dohoda se zpracovatelem, která je v souladu s obecným nařízením o ochraně osobních údajů;
- iii) použitá technologie analytiky zabraňuje opakované identifikaci a zahrnuje mimo jiné anonymizaci IP adres od uživatelů;
- iv) specifická cookie(s) nebo jiné údaje použité pro analytiku lze použít pouze pro danou specifickou internetovou stránku, aplikaci nebo nositelnou elektroniku a nelze je propojit s jinými identifikovatelnými údaji;
- v) uživatelé mají právo vyjádřit nesouhlas (viz také poznámky 17 a 50 tohoto stanoviska).

I kdyby souhlas nebyl vyžadován, pokud budou tyto podmínky splněny, správci údajů musí přesto uživatelům poskytnout odpovídající informace, například prostřednictvím polí představujících stav sledování v normě *Do Not Track*<sup>15</sup>.

26. Nařízení o soukromí a elektronických komunikacích **by mělo zajistit úzce a přesně formulované výjimky z požadavků na souhlas**. Znění výjimky z požadavku na souhlas týkající se zasahování do zařízení podle čl. 8 odst. 1 písm. c) je téměř totožné se stávajícím zněním ve směrnici o soukromí a elektronických komunikacích (čl. 5 odst. 3): „*nezbytně nutné pro poskytování služeb informační společnosti, které si účastník nebo uživatel výslovně vyžádal*“. Bez jakéhokoli vysvětlení je však vypuštěno kritické slovo „nezbytně“. Důvody k obavám jsou dva. Zaprvé toto ustanovení směrnice o soukromí a elektronických komunikacích již vyvolalo rozsáhlou diskusi o jeho oblasti působnosti mezi dozorovými úřady a organizacemi a odstranění slova „nezbytně“ poskytne ještě méně právní jistoty. Toto je také znepokojující, protože pracovní skupina v této souvislosti již poskytla pokyny k výkladu pojmu „nezbytně“. Pracovní skupina navrhla následující vyjasnění ve stanovisku k výjimce z požadavku na souhlas s cookies (WP194): „*cookie je nezbytně nutná k tomu, aby bylo možné uživateli (nebo účastníkovi) poskytnout konkrétní funkci: nejsou-li cookies povoleny, funkce nebude dostupná a tuto funkci si uživatel (nebo účastník) výslovně vyžádal jako součást služby informační společnosti*“.<sup>16</sup>

Kromě toho pracovní skupina vyjasnila, že:

---

<sup>15</sup> Viz: *Tracking Preference Expression (DNT)* (Vyjádření předvolby sledování (*Do Not Track*)), autorův návrh ze dne 7. března 2016.

<sup>16</sup> Pracovní skupina zřízená podle článku 29, WP 294, stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies, přijaté dne 7. června 2012, viz internetové stránky ([http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_cs.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf)).

*cookies „třetích stran“ dále obvykle nejsou „nezbytně nutné“ pro uživatele, který internetovou stránku navštíví, jelikož tyto cookies se obvykle pojí se službou, která je odlišná od té, která byla uživatelem „výslovně vyžádána“<sup>17</sup>.*

Pracovní skupina dodala, že používání modulů plug-in pro sociální sítě zaměřené na neuživatele platformy nebo internetové stránky by stejně tak nebylo považováno za nezbytně nutné.

Dále platí, že zatímco čl. 6 odst. 1 písm. b) navrhovaného nařízení umožňuje zpracování dat elektronických komunikací, pokud je to „nezbytné“ z bezpečnostních důvodů, 49. bod odůvodnění obecného nařízení o ochraně osobních údajů vyžaduje, aby to bylo nezbytně nutné. Vypuštění slova „nezbytně“ mohlo být neúmyslné, neboť 21. bod odůvodnění navrhovaného nařízení zmiňuje, že by souhlas pro zasahování neměl být vyžadován, pokud je to „nezbytně“ nutné. Nicméně navrhované nařízení poskytuje příležitost dále vyjasnit, že test nezbytnosti v souvislosti s tímto nařízením by měl být s ohledem na všechny výjimky vykládán úzce. Pracovní skupina tedy navrhuje, že pokud jde o všechny výjimky uvedené v článku 6 a čl. 8 odst. 1 navrhovaného nařízení, mělo by být slovo „nezbytně“ nahrazeno slovy „nezbytně nutné“.

Na druhé straně by nařízení o soukromí a elektronických komunikacích mělo výslovně umožňovat zasahování do zařízení za účelem instalace aktualizací zabezpečení. Odesílání aktualizací zabezpečení přes internet je upřednostňovanou metodou pro instalaci aktualizací zabezpečení na většině zařízení koncových uživatelů. Instalace aktualizací je považována za zasahování do koncových zařízení. Existuje oprávněný zájem zajistit, aby zabezpečení těchto zařízení bylo vždy aktuální. Poskytovatel bezpečnostních balíčků by tedy obecně měl být schopen instalovat nezbytně nutné aktualizace zabezpečení bez souhlasu koncového uživatele. Je však nejisté, zda lze na toto zasahování vztáhnout výjimku ze zákazu zasahování týkající se „informační společnosti“ (čl. 8 odst. 1 písm. c)). Mělo by být vyjasněno, že instalace aktualizací zabezpečení je podle této výjimky přípustná, ale pouze v případě, že i) aktualizace zabezpečení tvoří samostatný balíček a žádným způsobem nemění funkce softwaru na daném zařízení (včetně interakce s jiným softwarem nebo nastavení zvolených uživatelem), ii) koncový uživatel je informován předem při každé instalaci aktualizace a iii) koncový uživatel má možnost vypnout automatickou instalaci těchto aktualizací.

## *PŘÍMÝ MARKETING*

Další kategorie výhrad se týká nedostatečné ochrany před přímým marketingem.

27. Zaprvé je znepokojující, že **rozsah přímého marketingu je příliš omezený**. V čl. 4 odst. 3 písm. f) navrhovaného nařízení je „přímé marketingové sdělení“ definováno jako „jakákoli forma reklamy, ať už písemná nebo ústní, která je zaslána jednomu nebo více identifikovaným nebo identifikovatelným koncovým uživatelům služeb

---

<sup>17</sup> Tamtéž.

elektronických komunikací“. Použití slova „zaslána“ naznačuje použití technologických komunikačních prostředků, které nezbytně zahrnují přenos sdělení, zatímco většina reklamy na internetu (prostřednictvím platform sociálních médií nebo na internetových stránkách) nezahrnuje „zasílání“ reklam v pravém slova smyslu. To je dále zdůrazněno příklady, které následují v uvedené definici (SMS, e-mail) a ve 33. bodě odůvodnění. Všechny příklady se týkají spíše tradičních forem marketingové komunikace, a ani tak použití – vcelku tradičních – volacích systémů pravděpodobně nespádá do této oblasti působnosti. Uvedený článek a bod odůvodnění by měly být pozměněny tak, aby zahrnovaly veškerou reklamu, která je *zaslána, směřována nebo prezentována* jednomu nebo více identifikovaným nebo identifikovatelným koncovým uživatelům. Kromě toho by mělo být dále zajištěno, aby behaviorální reklama (na základě profilů koncových uživatelů) byla také považována za přímé marketingové sdělení směřované „jednomu nebo více identifikovaným nebo identifikovatelným koncovým uživatelům“ (neboť tyto reklamy jsou zacíleny na konkrétní, identifikovatelné uživatele).

Dále pak v rámci navrhovaného rozsahu „přímých marketingových sdělení“ by ochrana podle čl. 16 odst. 1 byla omezena na sdělení obsahující reklamní materiál a nechránila by jednotlivce před jinými sděleními zasílanými, směřovanými nebo prezentovanými pro marketingové účely (např. sdělení zaměřená na získávání kontaktů na potenciální klienty (tzv. lead generation) žádající o souhlas, propagace politických názorů nebo volebních preferencí, propagace charitativních nebo jiných neziskových organizací nebo propagace značky určité organizace). Jako přímá marketingová metoda se navíc stále používají i faxové přístroje, ačkoli nejsou v definici zmíněny. Ustanovení čl. 4 odst. 3 písm. f) by tedy mělo zahrnovat jakoukoli formu reklamy, získávání zákazníků nebo propagace, rovněž pro neziskové organizace, a mělo by společně s elektronickou poštou a SMS výslovně zahrnovat faxové přístroje (viz také návrh na vyjasnění v poznámce 43 písm. a)). V neposlední řadě 32. bod odůvodnění uvádí, že přímý marketing zahrnuje sdělení zasílaná politickými stranami za účelem své propagace. Toto by mělo být změněno tak, aby byli zahrnuti i politici a kandidáti do voleb, kteří propagují svou kandidaturu.

28. Zadruté **odvolání souhlasu s přímým marketingem není bezplatné ani stejně snadné jako poskytnutí souhlasu.** Možnost odvolat souhlas podle navrhovaného nařízení je nutné vyjasnit, aby se zajistila soudržnost a zlepšila ochrana příjemců. V čl. 16 odst. 6 navrhovaného nařízení se v současné době stanoví, že příjemcům přímého marketingu musí být poskytnuty „informace nezbytné pro to, aby mohli jednoduchým způsobem uplatnit své právo odvolat svůj souhlas s přijímáním dalších marketingových sdělení“ (zdůraznění přidáno). To potvrzuje 34. bod odůvodnění. Ze 70. bodu odůvodnění obecného nařízení o ochraně osobních údajů však vyplývá, že subjekty údajů by podle obecného nařízení o ochraně osobních údajů měly mít právo vznést námitku proti zpracování pro účely přímého marketingu nejen jednoduchým způsobem, ale také „bezplatně“. Tento pojem se rovněž používá v čl. 16 odst. 2 navrhovaného nařízení, ale pouze pokud jde o vyjádření nesouhlasu s přímým marketingem na základě kontaktních údajů získaných v souvislosti s prodejem.

V čl. 7 odst. 3 obecného nařízení o ochraně osobních údajů se stanoví, že odvolat souhlas musí být stejně snadné jako jej poskytnout a že jednotlivci by měli mít právo

souhlas kdykoli odvolat. Kromě toho již ve svém stanovisku č. 4/2010 týkajícím se Federace evropského přímého marketingu (FEDMA) (WP174) pracovní skupina uznala, že je důležité nabídnout „jednoduchý, účinný, bezplatný, přímý a snadno dostupný způsob odhlášení odběru“ přímého marketingu<sup>18</sup>. Tato norma pro odvolání souhlasu by měla být zahrnuta do pravidel přímého marketingu v navrhovaném nařízení. Totéž se týká požadavku uvedeného v čl. 7 odst. 3 obecného nařízení o ochraně osobních údajů, že odvolat souhlas kdykoli by mělo být stejně snadné jako jej poskytnout.

29. V této souvislosti by **měl být vyjasněn způsob odvolání souhlasu nebo vyjádření nesouhlasu pro účely přímých marketingových volání**. Na základě čl. 16 odst. 4 navrhovaného nařízení se mohou členské státy rozhodnout nepovolit hlasová volání pro účely marketingu. Nařízení o soukromí a elektronických komunikacích by mělo stanovit opatření pro odvolání souhlasu a vyjádření nesouhlasu pro účely marketingových volání. Ve 36. bodě odůvodnění se stanoví, že členské státy *by měly mít možnost* zavést a/nebo zachovat vnitrostátní systémy pro vyjádření nesouhlasu. Na základě tohoto ustanovení by tak členské státy mohly dokonce umožnit situaci, kdy by uživatel musel vyjádřit nesouhlas pro jednotlivé poskytovatele komunikačních služeb. Toto provedení nechrání uživatele před obtěžováním neodůvodněnou komunikací<sup>19</sup> ani neposkytuje mechanismus, který by byl v souladu s obecným nařízením o ochraně osobních údajů a umožňoval odvolání souhlasu snadno a kdykoli. Nařízení by proto mělo stanovit, že každý členský stát *musí* vytvořit vnitrostátní rejstřík kontaktů, jejichž uživatelé si nepřejí přijímat nevyžádaná sdělení (*Do Not Call Register*). Kromě toho by nařízení mělo stanovit, že příjemci hlasových volání by měly mít dvě možnosti: možnost odvolat svůj souhlas k budoucímu volání z dané společnosti nebo organizace a možnost se během těchto volání zaregistrovat do vnitrostátního rejstříku kontaktů, jejichž uživatelé si nepřejí přijímat nevyžádaná sdělení (*Do Not Call Register*).

30. Znepokojující je také skutečnost, že **při odesílání přímých marketingových sdělení není výslovně zakázáno používání falešných totožností**. Ve 34. bodě odůvodnění se uvádí, že je nezbytné zakázat „maskování totožnosti a používání falešných totožností a falešných zpátečních adres nebo čísel při zasílání nevyžádaných obchodních sdělení pro účely přímého marketingu“. V čl. 16 odst. 6 je však pouze uvedeno, že koncoví uživatelé musí být informováni o „totožnosti právnické nebo fyzické osoby, jejímž jménem je sdělení přenášeno“. Tato povinnost informovat příjemce o totožnosti by měla být doplněna o jasný zákaz používání maskovaných nebo falešných kontaktních adres pro účely přímého marketingu.

---

18 Pracovní skupina zřízená podle článku 29, WP174, stanovisko č. 4/2010 k evropskému kodexu chování FEDMA pro používání osobních údajů v přímém marketingu, přijaté dne 13. července 2010, viz internetové stránky ([http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf)).

19 Například ve Spojeném království telekomunikační operátor BT zaznamenal 31 milionů obtěžujících volání v jednom týdnu. Viz internetové stránky (<http://www.bbc.com/news/business-38635921>).

31. Tento bod souvisí s další výhradou: **požadavek na předčísli pro přímá marketingová volání je uváděn jako alternativa požadavku na identifikaci kontaktní linky**. Podle čl. 16 odst. 3 jsou přímá marketingová volání přípustná, pokud volající bud' i) uvede identitu linky, na které lze kontaktovat fyzickou nebo právnickou osobu uskutečňující volání (čl. 16 odst. 3 písm. a)), nebo ii) používá konkrétní kód/předčísli identifikující skutečnost, že se jedná o marketingové volání (čl. 16 odst. 3 písm. b)). Ačkoli pracovní skupina vítá povinnost používat předčísli uvedenou čl. 16 odst. 3 písm. b), domnívá se, že tento požadavek neřeší tutéž věc, kterou řeší povinnost identifikace kontaktní linky v čl. 16 odst. 3 písm. a). Zatímco požadavek na předčísli má příjemci umožnit předem identifikovat volání jako marketingové volání (a přijmout opatření k zablokování těchto hovorů), požadavek na identifikaci kontaktní linky má poskytnout příjemcům (a dozorovým úřadům) prostředky, jak identifikovat a kontaktovat iniciátora marketingu. To je zvláště důležité pro automatizovaná volání, kde existuje značná nerovnováha mezi možnostmi obchodníků uskutečňovat obtěžující volání a možnostmi příjemce se těmto voláním vyhnout. Uvedené požadavky tedy nemohou být alternativami, ale musí se vzájemně doplňovat.

#### ČASOVÝ HARMONOGRAM

32. Pracovní skupina zřízená podle článku 29 chválí Evropskou komisi za to, že uznala potřebnost vstupu navrhovaného nařízení v platnost společně s obecným nařízením o ochraně osobních údajů v květnu 2018, aby se zamezilo nesoudržnosti mezi oběma legislativními akty. Přesto je však znepokojující, že se jedná o ambiciózní harmonogram, který rovněž vyžaduje dokončení návrhu evropského kodexu pro elektronické komunikace. Pracovní skupina zřízená podle článku 29 tedy požaduje, aby se všechny strany zapojené do legislativního procesu zavázaly k termínu květen 2018.

#### DALŠÍ VÝHRADY

Tento oddíl se zabývá řadou dalších výhrad.

33. Zaprvé je pracovní skupina zřízená podle článku 29 znepokojena **návrhem, aby byla přijatelná necílená opatření pro uchovávání údajů**. Důvodová zpráva uvádí, že podle navrhovaného nařízení členské státy mohou zachovat nebo vytvořit vnitrostátní rámce pro uchovávání údajů, které mimo jiné stanoví cílená opatření pro uchovávání údajů (bod 1.3). Po rozsudku ve věci Tele2/Watson<sup>20</sup> je jasné, že rámce umožňující jiné než cílené uchovávání nejsou přípustné podle Listiny (a i rámce pro cílené uchovávání podléhají důležitým podmínkám, jako je dohled) a že globální přístup k metadatům bude muset být považován za porušení podstaty článku 7, stejně jako je tomu v případě globálního přístupu k obsahu elektronických komunikací (viz rozsudek Soudního dvora ve věci Schrems, bod 94). Formulace této věty tedy

<sup>20</sup> ECLI:EU:C:2016:970, viz internetové stránky (<http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>).



naznačuje určitý prostor pro členské státy, pokud jde o opatření pro uchovávání údajů, který však neexistuje. V souvislosti s tím **není** v navrhovaném nařízení **metadatům poskytována dostatečná úroveň ochrany**. Jak je uvedeno v poznámce 10, pracovní skupina zřízená podle článku 29 vítá uznání, že metadata mohou odhalit velmi citlivé údaje. Metadatům se však v navrhovaném nařízení nedostává ochrany, která by z tohoto uznání měla vyplynout. Vzhledem k jejich citlivosti by zejména před analýzou podle čl. 6 odst. 2 písm. c) mělo být provedeno posouzení vlivu na ochranu osobních údajů (viz také poznámka 46).

34. Zadruhé **navrhované nařízení by nežádoucím způsobem rozšířilo možnosti uchovávání údajů**. Článek 11 navrhovaného nařízení odkazuje na čl. 23 odst. 1 písm. a) až e) obecného nařízení o ochraně osobních údajů, když popisuje účely, pro které mohou členské státy omezit povinnosti a práva stanovená v článcích 5 až 8 nařízení. Vzhledem k vysokým rizikům pro subjekty údajů obecné nařízení o ochraně osobních údajů takováto omezení u zvláštních kategorií údajů nestanoví. Článek 15 směrnice o soukromí a elektronických komunikacích v současné době sice obdobné omezení umožňuje, ale za účely vymezenými účely. Nově navrhované nařízení by umožnilo nová omezení pro účely „výkon[u] trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení“ (čl. 23 odst. 1 písm. d) obecného nařízení o ochraně osobních údajů) a „jiné důležité cíle obecného veřejného zájmu Unie nebo členského státu, zejména důležitý hospodářský nebo finanční zájem Unie nebo členského státu, včetně peněžních, rozpočtových a daňových záležitostí, veřejného zdraví a sociálního zabezpečení“ (čl. 23 odst. 1 písm. e) obecného nařízení o ochraně osobních údajů). Tyto účely jsou v porovnání se směrnicí o soukromí a elektronických komunikacích nejen nové, ale poslední účel podle čl. 23 odst. 1 písm. d) a celý účel podle čl. 23 odst. 1 písm. e) jsou formulovány mimořádně široce. Navrhuje se tedy vypustit odkaz na čl. 23 odst. 1 písm. a) až e) obecného nařízení o ochraně osobních údajů a namísto toho zmínit pouze účely v současné době uvedené v článku 15 směrnice o soukromí a elektronických komunikacích.

35. **Povinnost informovat uživatele o bezpečnostních rizicích má minimální rozsah**. Pracovní skupina vítá skutečnost, že poskytovatelé služeb musí informovat uživatele o bezpečnostních rizicích a opatřeních k řešení těchto rizik, jako například šifrování (článek 17 a 37. bod odůvodnění). Název ustanovení však zní: „Informace o zjištěných bezpečnostních rizicích“. Skutečnost, že název mluví o zjištěných rizicích, naznačuje, že toto ustanovení se týká pouze (potenciálních) porušení bezpečnosti, zatímco znění ustanovení a bodu odůvodnění spíše ukazují na obecnou osvětu koncových uživatelů. Například pokud poskytovatel služby zjistí, že zařízení uživatele je napadeno malwarem a stalo se součástí botnetu, toto ustanovení podle všeho ukládá poskytovateli přímou povinnost informovat uživatele o výsledných rizicích. Oblast působnosti tohoto ustanovení by však měla být vyjasněna a neměla by být omezena na tento konkrétní scénář. Uvedené ustanovení by mělo přinejmenším pokrývat zjištěná bezpečnostní rizika ve všech zařízeních, která poskytovatel dodává koncovému uživateli jako součást přihlášení se k užívání služby, například směrovače a mobilní zařízení, a zahrnovat osvětu o rizicích změny nastavení, které bylo v souladu se zásadou záměrné ochrany soukromí nastaveno k ochraně soukromí.

Pracovní skupina doporučuje, aby byla působnost ustanovení rozšířena tak, aby zahrnovalo poskytovatele softwaru umožňujícího elektronické komunikace (viz 8. bod odůvodnění), a pokud možno také novou kategorii: poskytovatelé technologie zásadní pro zajištění komunikace, kteří nejsou poskytovateli služeb (např. poskytovatelé šifrovacích technologií). V případě rozšíření na tuto novou kategorii je třeba rovněž věnovat pozornost tomu, aby se uvedená povinnost nepřekrývala s povinnostmi oznamovat porušení bezpečnosti v jiných nástrojích, jako jsou směrnice o bezpečnosti sítí a informací<sup>21</sup> a jiné právní nástroje týkající se poskytovatelů certifikátu. Jelikož druhá uvedená kategorie poskytovatelů technologie obvykle nemá přímý kontakt s koncovými uživateli, je také třeba vysvětlit, jak mohou splnit svou informační povinnost podle tohoto ustanovení.

36. Pracovní skupina vítá ustanovení článků 2 a 13, které se budou vztahovat na interpersonální komunikační služby založené na číslech. Není však hned jasné, proč **by obdobná úroveň ochrany soukromí neměla být dostupná také pro funkčně rovnocenné služby volání OTT.**
37. Pracovní skupina je rovněž znepokojena **nevyjasněností strukturovaného souhlasu pro zpětné vyhledávání v seznamech.** Ustanovení čl. 15 odst. 2 navrhovaného nařízení vyžaduje, aby poskytovatelé získali souhlas od koncových uživatelů předtím, než tyto vyhledávací funkce související s údaji povolí (viz také 31. bod odůvodnění). Pracovní skupina vítá harmonizaci požadavku na obsah, pokud jde o zařazování do seznamů, ale má výhrady k nedostatečné strukturovanosti, pokud jde o různé druhy vyhledávání. Stávající návrh směrnice o soukromí a elektronických komunikacích umožňuje členským státům vyžadovat samostatný souhlas se zpětným vyhledáváním, a to na základě čl. 12 odst. 3. Tento článek uvádí, že „*členské státy mohou vyžadovat, aby byli účastníci požádáni o dodatečný souhlas, bude-li účel veřejného účastnického seznamu jiný, než je vyhledávání podrobností pro kontaktování osoby na základě jejího jména a případně nutnosti i minimálního množství dalších identifikátorů*“. Na základě tohoto ustanovení je v mnoha členských státech vyžadován samostatný souhlas pro funkce zpětného vyhledávání s přihlédnutím k různým úrovním identifikovatelnosti, a tedy rušivosti obou funkcí.
38. Z formálnějšího hlediska **není výše pokut harmonizována u všech porušení nařízení.** Podle navrhovaného nařízení členské státy stanoví pravidla pro sankce za porušení čl. 23 odst. 4, čl. 23 odst. 6 a článku 24 navrhovaného nařízení. Je logičtější zajistit to také v samotném nařízení o soukromí a elektronických komunikacích.
39. A v neposlední řadě **navrhované nařízení vychází z definic, které se mohou stát „pohyblivými cíli“.** V řadě klíčových konceptů se navrhované nařízení odvolává k jinému právnímu nástroji, který má v současné době podobu návrhu: návrh směrnice, kterou se stanoví evropský kodex pro elektronické komunikace (viz například čl. 4

<sup>21</sup> Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, Úř. věst. L 194, 19.7.2016, s. 1–30, viz internetové stránky ([http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:OJ.L\\_.2016.194.01.0001.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:OJ.L_.2016.194.01.0001.01.ENG)).

odst. 1 písm. b)). Dvěma důležitými příklady jsou v tomto případě definice „koncového uživatele“, která v současné době zahrnuje fyzické i právnické osoby, a definice „služeb elektronických komunikací“ a „interpersonálních komunikačních služeb“, které jsou v navrhovaném nařízení uvedeny ve zmíněném čl. 4 odst. 1 písm. b). Interpersonální komunikační služby jsou dále podrobněji rozvedeny v čl. 4 odst. 2, přičemž zahrnují druhy služeb specificky vyloučené z evropského kodexu pro elektronické komunikace.<sup>22</sup> Toto stanovisko vychází z definic tak, jak jsou v současné době nastaveny, avšak je celkem pravděpodobné, že navrhovaný evropský kodex pro elektronické komunikace a/nebo jeho klíčové koncepty se změní. To by mělo okamžitý dopad rovněž na nařízení o soukromí a elektronických komunikacích. Ideálně by všechny pojmy, které vycházejí z evropského kodexu pro elektronické komunikace, měly být nezávisle definovány v nařízení o soukromí a elektronických komunikacích; nebo minimálně by navrhované nařízení mělo vyjasnit případné pojmy, jejichž definice se odchylují od definic uvedených v evropském kodexu pro elektronické komunikace (např. výše uvedené zahrnutí „doplňkových služeb“ do definice „interpersonálních komunikačních služeb“). Pokud to však není možné, pracovní skupina by ráda navrhla všem stranám zapojeným do legislativního procesu, aby zajistily, že navrhované nařízení i evropský kodex pro elektronické komunikace budou projednány a bude se o nich hlasovat souběžně, aby zúčastněné strany mohly správně posoudit působnost a důsledky nových nástrojů.

## 5. NÁVRHY NA VYJASNĚNÍ PRO ZAJIŠTĚNÍ PRÁVNÍ JISTOTY

Kromě výše uvedených bodů by pracovní skupina také ráda upozornila na některá ustanovení navrhovaného nařízení, pro která by vyjasnění bylo přínosem. Tato vyjasnění jsou považována za potřebná pro zlepšení právní jistoty všech zúčastněných stran, že nařízení o soukromí a elektronických komunikacích bude jednotně chápáno a uplatňováno v celé EU.

### *VYJASNĚNÍ PŮSOBNOSTI*

40. Pokud jde o působnost navrhovaného nařízení, pracovní skupina zřízená podle článku 29 navrhuje toto vyjasnění:

- a. **Pojem „koncový uživatel“ by měl zahrnovat všechny jednotlivé uživatele.** V čl. 2 odst. 14 evropského kodexu pro elektronické komunikace je „koncový uživatel“ definován jako uživatel, který nezajišťuje veřejné komunikační sítě ani neposkytuje veřejně přístupné služby elektronických komunikací. Je třeba vyjasnit, že jednotlivci, kteří přispívají do sítě – například do sítě typu „mesh“ se svým Wi-Fi směrovačem – nejsou vyloučeni z působnosti ochrany navrhovaného nařízení.

---

<sup>22</sup> Například čl. 4 odst. 2 navrhovaného nařízení uvádí, že interpersonální komunikační služba „zahrnuje služby, které umožňují interpersonální a interaktivní komunikaci pouze jako nepodstatnou pomocnou funkci, která je ze své podstaty spjata s jinou službou“, zatímco čl. 2 odst. 5 evropského kodexu pro elektronické komunikace takovéto služby z uvedené definice vylučuje. (Evropský kodex pro elektronické komunikace zahrnuje „interpersonální komunikační službu“ do širší kategorie „služby elektronických komunikací“ v čl. 2 odst. 4.)

- b. **Je třeba vyjasnit, že územní působnost se vztahuje na všechny koncové uživatele v Unii.** V čl. 3 odst. 1 písm. a) se stanoví, že navrhované nařízení se vztahuje na poskytování služeb elektronických komunikací koncovým uživatelům „v Unii“, zatímco čl. 3 odst. 1 písm. c) stanoví, že se vztahuje na ochranu koncových zařízení koncových uživatelů „nacházejících se v Unii“ (zdůraznění přidáno). To se v různých překladech liší. Německý překlad neobsahuje toto rozlišení, zatímco jiné překlady, jako například francouzština, španělština a nizozemština, toto rozlišení mají. Z 9. bodu odůvodnění je jasné, že územní působnost je chápána ze široka bez ohledu na to, zda jsou služby poskytovány ze zemí mimo Unii nebo zda ke zpracování dochází v Unii. Navrhuje se tedy vypustit slova „nacházejících se“ v čl. 3 odst. 1 písm. c) s cílem zdůraznit tuto širokou oblast působnosti.
- c. **Zdá se, že navrhované nařízení chrání pouze důvěrná sdělení během tranzitu, nikoli v době, kdy jsou uložena.** Stávající přístup v navrhovaném nařízení se soustředí na ochranu přenosu komunikací. Viz například 15. bod odůvodnění, který uvádí, že během přenosu, tj. do doby, než obsah komunikace obdrží zamýšlený adresát, by měl platit zákaz zachycování dat komunikací. Rozsah této ochrany vychází z koncepčního rámce komunikací, který je zastaralý. Většina dat komunikací zůstává uložena u poskytovatelů služby, a to i po obdržení. Je třeba zajistit, aby důvěrný charakter těchto dat byl i nadále chráněn. Kromě toho komunikace mezi účastníky těchto služeb založených na cloudu (například poskytovatelů webové pošty) budou často zahrnovat pouze málo přenosu: odesílání mailu se většinou spíše projeví v databázi poskytovatele, než aby šlo o skutečné odesílání sdělení mezi dvěma stranami. Argument, že tato situace je již zahrnuta v obecném nařízení o ochraně osobních údajů, není přesvědčivý: základním úmyslem navrhovaného nařízení je chránit veškerou důvěrnou komunikaci bez ohledu na technické prostředky takovéto komunikace. Je možné, že se jedná pouze o redakční chybu, neboť zákaz podle článku 5 se týká „uchovávání“ a „zpracování“.
- d. **Všechny veřejné bezdrátové internetové hotspoty by měly spadat do oblasti působnosti navrhovaného nařízení.** Jelikož je používání bezdrátových hotspotů běžné, je naprosto logické, že by neměly být pochybnosti o tom, zda je důvěrný charakter sdělení přenášených přes tyto hotspoty chráněn. Pokus o vyjasnění této věci v nařízení se však nezdařil, neboť oblast působnosti je rozšířena pouze na síť poskytované „nedefinované skupině koncových uživatelů“ (13. bod odůvodnění). Pojmy „nedefinovaná skupina koncových uživatelů“ a „uzavřená skupina koncových uživatelů“ je třeba definovat. Zejména je třeba vyjasnit, že do působnosti nařízení spadají také bezpečné bezdrátové sítě (tj. s heslem), pokud je heslo poskytnuto teoreticky neurčené skupině uživatelů, jejichž totožnost nelze předem určit (např. zákazníci v kavárně, návštěvníci na letišti). Základní zásadou v této souvislosti je, že v souladu s předchozím stanoviskem pracovní skupiny zřízené podle článku 29 k přezkumu směrnice o soukromí a elektronických komunikacích „*pouze služby, k nimž dochází v úředním nebo pracovním kontextu výhradně pro účely spojené s prací nebo pro úřední účely, nebo technická komunikace mezi neveřejnými subjekty nebo veřejnými subjekty výhradně za účelem řízení pracovních nebo obchodních procesů,*

*jakož i využívání služeb pro výlučně domácí účely mohou být z nástroje týkajícího se soukromí a elektronických komunikací vyňaty“ (str. 8).*

- e. **Navrhované nařízení by se mělo vztahovat na data shromážděná při nabízení služeb digitálního vysílání.** S ohledem na citlivou povahu diváckých zvyklostí, jež odhalují osobní zájmy a charakteristické rysy diváků, by nařízení o soukromí a elektronických komunikacích mělo stanovit (možná v podobě bodu odůvodnění), že vyloučení služeb poskytujících „obsah přenášený prostřednictvím sítí elektronických komunikací“ z definice „služby elektronických komunikací“ neznamená, že poskytovatelé služeb, kteří nabízejí služby elektronických komunikací i služby poskytující obsah nespádají do působnosti ustanovení nařízení o soukromí a elektronických komunikacích, které se zaměřuje na poskytovatele služeb elektronických komunikací. Toto je zvláště důležité, neboť poskytování služeb poskytujících „obsah přenášený prostřednictvím sítí elektronických komunikací“ je vyloučeno z definice „služby elektronických komunikací“ podle navrhovaného evropského kodexu pro elektronické komunikace (čl. 2 odst. 4).
- f. **Data komunikací jsou obvykle osobními údaji.** Ve 4. bodě odůvodnění se uvádí, že data komunikací mohou obsahovat osobní údaje. Osobními údaji je však většina dat komunikací<sup>23</sup> a z velké části se jedná o data poněkud důvěrné a citlivé povahy, takže toto by mělo být pozměněno a mělo by být uvedeno, že obvykle jsou osobními údaji.
- g. **Důvěrná komunikace zahrnuje zprávy v rámci platformy.** V 1. bodě odůvodnění je vysvětleno, že zásada důvěrnosti se vztahuje na „stávající a budoucí komunikační prostředky“. Tento bod odůvodnění pokračuje seznamem příkladů těchto prostředků, včetně „zasílání osobních zpráv prostřednictvím sociálních médií“. To má pravděpodobně zahrnovat soukromé zprávy mezi uživateli sociální sítě (např. Facebook nebo Twitter) nebo zprávy zveřejněné na Facebooku pomocí funkce Timeline, které jsou přístupné omezenému počtu osob, avšak znění tohoto bodu není příliš jasné.
- h. **Jak se nařízení o soukromí a elektronických komunikacích vztahuje na interakce mezi stroji.** Jak je uvedeno v bodě 9, pracovní skupina vítá rozšíření ochrany na interakci mezi stroji. To je však zmíněno pouze ve 12. bodě odůvodnění, nikoli v odpovídajícím článku. Tato ochrana je žádoucí, neboť takovéto komunikace často obsahují informace chráněné na základě práv na soukromí. Na druhé straně úzká kategorie komunikace čistě mezi stroji by měla být vyjmuta, pokud nemá žádný dopad na soukromí nebo důvěrný charakter sdělení, například v případech, kdy tato komunikace probíhá při provádění protokolu pro přenos dat mezi síťovými prvky (např. servery, přepínače) za účelem vzájemného informování o stavu své činnosti.

---

<sup>23</sup> Viz například rozsudek Soudního dvora ze dne 6. listopadu 2003, Lindqvist, C-101/01, ECLI:EU:C:2003:596, bod 24 (pokud jde o telefonní číslo), rozsudek Soudního dvora ze dne 19. října 2016, Breyer, C-582/14, ECLI:EU:C:2016:779, bod 49 (pokud jde o dynamické IP adresy), a rozsudek Soudního dvora ze dne 8. dubna 2014, C-293/12 a C-594/12 (Digital Rights Ireland), ECLI:EU:C:2014:238, body 26–27 (pokud jde o citlivost metadat).

Jednou konkrétní oblastí, v níž použití nařízení o soukromí a elektronických komunikacích vyžaduje vyjasnění, jsou inteligentní dopravní systémy. Předpokládá se, že vozidla budou neustále přenášet data obsahující jedinečný identifikátor, a to rádiově. Bez dodatečné ochrany dat komunikací v nařízení o soukromí a elektronických komunikacích by to mohlo vést k neustálému sledování jízdních návyků, tras a rychlosti řidičů. Ustanovení čl. 2 odst. 1 evropského kodexu pro elektronické komunikace obsahuje novou a rozšířenou definici komunikačních sítí. Tyto sítě zahrnují přenosové systémy, které nemají centralizovanou správu a které umožňují přenos signálů rádiově. Ve 14. bodě odůvodnění nařízení o soukromí a elektronických komunikacích se stanoví, že tato data jsou data elektronických komunikací. Podle článku 5 navrhovaného nařízení je jakýkoli druh zachycování, monitorování nebo uchovávání těchto dat komunikací zakázán, pokud se nepoužije jedna z výjimek. Přesto je zájem na zpracovávání těchto údajů, které umožňují, aby se objekty jako automobily bez řidiče a zařízení bez obsluhy vzájemně varovaly o své blízkosti nebo o jiných rizicích. Otázkou pak je, jaká výjimka by se použila v tomto případě. Souhlas koncových uživatelů není proveditelnou výjimkou, neboť se vždy může stát, že zpracování těchto údajů bude nezbytné. Poskytovatelé by tedy měli být schopni využít konkrétní výjimky a umožnit objektům, jako jsou automobily bez řidiče a zařízení bez obsluhy, aby se vzájemně varovaly o své blízkosti nebo o jiných rizicích.

#### *VYJASNĚNÍ KONCEPTU A POUŽITÍ SOUHLASU*

41. Pokud jde o koncept a použití souhlasu ve stávajícím navrhovaném nařízení, pracovní skupina zřízená podle článku 29 navrhuje tato vyjasnění:
- a. **Jak má být koncept souhlasu uplatňován v případě právnických osob.** Ve 3. bodě odůvodnění se uvádí, že nařízení by mělo zajistit, aby se ustanovení obecného nařízení o ochraně osobních údajů vztahovala rovněž na koncové uživatele, kteří jsou právnickými osobami. Podle uvedeného bodu odůvodnění to zahrnuje definici souhlasu podle obecného nařízení o ochraně osobních údajů (viz také 18. bod odůvodnění). Jak je uvedeno v poznámce 13, pracovní skupina vítá výslovné zahrnutí právnických osob do působnosti nařízení. Praktické použití této zásady však není jasné. Definice souhlasu podle obecného nařízení o ochraně osobních údajů vyžaduje, aby byl souhlas „informovaný“ a projevem vůle, kterým subjekt údajů dává „prohlášením či jiným zjevným potvrzením své svolení“ (čl. 4 odst. 11 obecného nařízení o ochraně osobních údajů). Je třeba vyjasnit, kdy může být právnická osoba opravdu považována za „informovanou“ a kdy existuje takovýto projev vůle právnické osoby.
  - b. V této souvislosti stojí za to uvést, že ve většině případů nemůže zaměstnavatel poskytnout souhlas jménem svých zaměstnanců, protože pokud zaměstnavatel vyžaduje souhlas od zaměstnance, a s ohledem na nevyváženost sil existuje významná reálná nebo potenciální podjatost, která vyplývá z neposkytnutí souhlasu, tento souhlas není platný, neboť není

poskytnut svobodně<sup>24</sup>. Pokud jde o **společnosti poskytující zařízení nebo vybavení jednotlivcům, navrhované nařízení neobsahuje (vhodnou) výjimku** ze zákazu zasahování. Jedním příkladem je situace, kdy zaměstnavatel chce aktualizovat společností poskytnutý telefon. Druhým příkladem je situace, kdy zaměstnavatel nabídne zaměstnancům pronájem vozidel a z administrativních důvodů nechává lokalizační údaje shromažďovat třetí stranu prostřednictvím palubní jednotky ve vozidle. V obou případech má zaměstnavatel zájem do těchto zařízení zasahovat.

Toto zasahování nelze považovat za nezbytné pro poskytování služby informační společnosti (čl. 8 odst. 1 písm. c)) ani za nezbytné pro měření návštěvnosti internetových stránek (čl. 8 odst. 1 písm. d)). Řešením by mohlo být zavedení nové výjimky, aby byla zahrnuta situace, kdy i) zaměstnavatel poskytne určité zařízení v rámci pracovního poměru, ii) zaměstnanec je uživatelem tohoto zařízení a iii) zasahování je nezbytně nutné pro to, aby zaměstnanec mohl se zařízením pracovat (což znamená použití zásad proporcionality a subsidiarity, pokud jde o shromažďování údajů). Zaměstnavatel by mohl zasahovat do zařízení koncových uživatelů pouze při splnění uvedených podmínek.

- c. **Zlepšování kontrol s cílem zastavit automatické přesměrování hovorů.** Článek 14 stanoví důležitou kontrolu pro koncové uživatele umožňující zastavit automatické přesměrování třetí stranou. Tato ochrana může být ještě vylepšena tím, že souhlas se zahájením přesměrování hovoru bude rovněž vyžadován nejprve od koncového uživatele.

#### *VYJASNĚNÍ LOKALIZAČNÍCH ÚDAJŮ A JINÝCH METADAT*

42. Pracovní skupina navrhuje vyjasnění níže uvedených bodů, pokud jde o lokalizační údaje a jiná metadata:

- a. Význam výrazu „**lokalizační údaje, které jsou generovány v jiném kontextu, než je poskytování služeb elektronických komunikací**“ v 17. bodě odůvodnění by měl být vyjasněn. Je nejasné, zda se tento výraz týká lokalizačních údajů shromažďovaných například prostřednictvím aplikací, které používají údaje z funkce GPS v chytrých zařízeních a/nebo generují lokalizační údaje na základě blízkých Wi-Fi směrovačů, a/nebo lokalizačních údajů shromažďovaných palubními navigacemi a/nebo jiných způsobů generování lokalizačních údajů. Tyto nejasnosti vytvářejí právní nejistotu, pokud jde o rozsah povinností. V každém případě jsou lokalizační údaje koncového zařízení fyzické osoby osobními údaji, a proto se na zpracování těchto údajů vztahují povinnosti podle obecného nařízení o ochraně osobních údajů.
- b. Je třeba vyjasnit, že **oprávněné zpracování lokalizačních údajů a jiných metadat většinou nevyžaduje jedinečný identifikátor**. V 17. bodě

<sup>24</sup> Viz stanovisko č. 15/2011 k definici souhlasu (WP 187), stanovisko č. 8/2001 ke zpracování osobních údajů v kontextu zaměstnání (WP48) a nové stanovisko ke zpracování údajů v zaměstnání (přijaté souběžně s tímto stanoviskem).

odůvodnění se zmiňují teplotní mapy jako příklad, jak mohou poskytovatelé služeb elektronických komunikací komerčně využívat metadata elektronických komunikací. Pro vytvoření základní teplotní mapy však nejsou zapotřebí žádné jedinečné identifikátory, postačí pouhé statistické počítání. Další příklad zmíněný v uvedeném bodu odůvodnění: využití infrastruktury a tlak na ni lze také počítat podle určitých měřicích bodů, například vytváření souhrnné statistiky využívání dopravních věží umožní poskytovat informace o tlaku v určitém místě v určitý čas bez nutnosti znát také totožnost připojených osob.

Kromě toho tento bod odůvodnění zmiňuje jako příklad zobrazení dopravních pohybů v určitých směrech během určitého časového období, kdy by byl nezbytný jedinečný identifikátor, aby bylo možné v určitých časových intervalech spojit pozice osob. Tímto příkladem uvedený bod odůvodnění podle všeho legitimizuje další zpracování těchto údajů na podporu analytiky „dat velkého objemu“. Podle navrhovaného nařízení je jedinou podmínkou pro tento druh zpracování povinnost provést posouzení vlivu na ochranu osobních údajů, pokud zpracování *bude mít za následek velké riziko pro práva a svobody fyzických osob*. Tato podmínka je nedostačující. Je také v rozporu s povinností uvedenou v článku 6, že tento druh zpracování může být prováděn pouze se souhlasem uživatelů, a pouze pokud data nelze anonymizovat, tj. bez jakýchkoli jedinečných identifikátorů. Uživatelé často nemohou odmítnout shromažďování svých geolokalizačních údajů poskytovateli služeb elektronických komunikací, pokud je toto shromažďování technicky nezbytné pro přenos komunikace k uživateli nebo pokud je toto zpracování nezbytné k poskytnutí požadované služby (např. navigace). V předchozích stanoviscích pracovní skupina dospěla k závěru, že takovéto lokalizační údaje z chytrých zařízení jsou osobními údaji citlivé povahy a že výhody analyzování těchto údajů nepřevažují nad právem uživatelů na ochranu důvěrného charakteru metadat jejich komunikací, ani nepřevažují nad jejich obecným právem na ochranu údajů podle obecného nařízení o ochraně osobních údajů. Uvedený bod odůvodnění tedy musí přinejmenším stanovit, že poskytovatelé musí splnit povinnosti vyplývající z článku 25 obecného nařízení o ochraně osobních údajů v případě dalšího zpracování lokalizačních údajů nebo jiných metadat. To znamená, že musí být přijata přinejmenším tato opatření:

- i) používání dočasných pseudonymů;
- ii) vymazání jakékoli tabulky zpětného vyhledávání mezi těmito pseudonymy a původními identifikačními údaji;
- iii) agregace na úroveň, kdy individuální uživatelé již nemohou být identifikováni prostřednictvím svých konkrétních itinerářů a
- iv) vymazání odlehklých hodnot, které by umožňovaly identifikaci (všechna tato opatření musí být provedena společně).

V neposlední řadě nařízení o soukromí a elektronických komunikacích musí stranám, které jsou zapojeny do zpracování lokalizačních údajů a jiných metadat, ukládat povinnost zveřejňovat své metody anonymizace a další agregace, aniž by byla dotčena právem chráněná důvěrnost. To by umožnilo



jak dozorovým úřadům, tak široké veřejnosti snadno ověřovat, zda je zvolená metoda přiměřená.

#### *VYJASNĚNÍ TÝKAJÍCÍ SE NEVYŽÁDANÝCH SDĚLENÍ*

43. Pracovní skupina navrhuje vyjasnění níže uvedených bodů, pokud jde o nevyžádaná sdělení:

- a. **Znění zákazu přímého marketingu bez souhlasu.** Ustanovení čl. 16 odst. 1 navrhovaného nařízení nyní uvádí, že služby elektronických komunikací „mohou“ být používány pro účely zasílání přímých marketingových sdělení (se souhlasem), ale neobsahuje výslovný zákaz zasílání (směrování nebo předávání) přímých marketingových sdělení bez souhlasu. To je v rozporu s přístupem v jiných ustanoveních, kde je nejdříve formulován zákaz, za nímž pak následují určité konkrétní výjimky. Stávající znění naznačuje shovívavější přístup (který pravděpodobně není úmyslný). Pracovní skupina navrhuje mírně upravené znění stávajícího čl. 13 odst. 1 směrnice o soukromí a elektronických komunikacích: „Používání služeb elektronických komunikací fyzickými nebo právními osobami, včetně hlasových volání, automatických volacích a komunikačních systémů, včetně poloautomatických systémů, které propojují volanou osobu s danou osobou, faxů, elektronické pošty nebo jiného využívání služeb elektronických komunikací pro účely předávání přímých marketingových sdělení koncovým uživatelům je možné pouze v případě koncových uživatelů, kteří k tomu dali předchozí souhlas.“
- b. **Oblast působnosti ustanovení o marketingových sděleních a voláních stávajícím kontaktům.** V čl. 16 odst. 2 se stanoví, že pokud osoba získá od svého stávajícího zákazníka jeho elektronické kontaktní údaje pro elektronickou poštu, může tato osoba využít tyto údaje pro účely dalšího přímého marketingu svých vlastních výrobků a služeb, pokud je poskytnuta jasná, bezplatná a snadná příležitost vznést námitku v době, kdy jsou údaje shromážděny, a při každé zprávě. To je v současné době omezeno na obchodní kontakty získané „v souvislosti s prodejem výrobku nebo služby“ a pro účely dalšího obchodního marketingu svých vlastních obdobných výrobků nebo služeb. Vzhledem k tomu že ustanovení o přímém marketingu se obdobně vztahují na nekomerční propagační činnosti (např. charit nebo politických stran), toto ustanovení by mělo být pozměněno tak, aby se obdobně vztahovalo na nekomerční organizace při kontaktování předchozích podporovatelů v rámci propagace jejich vlastních obdobných cílů nebo ideálů, a stejné právo vznést námitku by se mělo vztahovat na přímá marketingová volání. Kromě toho by měla být stanovena lhůta pro platnost „kontaktů stávajících zákazníků“ v elektronických komunikacích pro komerční, charitativní nebo politický účel a tato lhůta by se měla vztahovat i na přímá marketingová volání. Pokud si členské státy zvolily systém námítky proti hlasovým marketingovým voláním, přítomnost relace „kontakt stávajícího zákazníka“ převažuje nad registrací v rejstříku „Nevolejte“. V těchto situacích nemají koncoví uživatelé žádnou skutečnou možnost zabránit obtěžujícím voláním od společností nebo organizací, s nimiž byli jednou v

kontaktu, ale už si nepřejí s nimi jednat. Obecně by tedy nařízení mělo stanovit platnost této výjimky „stávající zákazník“, například na jeden nebo dva roky, ve vztahu k legitimním očekáváním dotýčným koncových uživatelů.

- c. **Použití pravidel přímého marketingu na právnické osoby.** V čl. 16 odst. 5 navrhovaného nařízení se stanoví, že členské státy zajistí, že oprávněné zájmy koncových uživatelů, kteří jsou právnickými osobami, jsou v případě nevyžádaných sdělení dostatečně chráněny. Ustanovení čl. 13 odst. 5 směrnice o soukromí a elektronických komunikacích popisuje oprávněné zájmy účastníků, kteří nejsou fyzickými osobami. Není jasné, jaké jsou důsledky této změny znění. V bodech odůvodnění je třeba vyjasnit, že tato změna nevyjadřuje úmysl poskytnout nižší úroveň ochrany. V této souvislosti se zákaz přímého marketingu bez souhlasu vztahuje na „koncové uživatele, kterí jsou fyzickými osobami a udělili svůj souhlas“ (zdůraznění přidáno). Je třeba vyjasnit, že to zahrnuje fyzické osoby *pracující pro* právnické osoby. Na druhé straně by souhlas nebyl vyžadován pro přístup k právnickým osobám prostřednictvím obecných kontaktních údajů, které byly pro tento účel zveřejněny (např. „info@companyname.eu“).
- d. **Použití pravidel přímého marketingu na osoby jednající v postavení (politických) zástupců:** Článek 16 v navrhovaném znění může zabránit tomu, aby zvoleným zástupcům byla odesílána některá sdělení obsahující obchodní obavy nebo zájmy. Je třeba vyjasnit, že nařízení takovýmto sdělením nebrání.

#### vyjasnění týkající se použití nástrojů v oblasti základních práv

- 44. **Použití Listiny a EÚLP na vnitrostátní předpisy v oblasti uchovávání údajů** je třeba dále vyjasnit. Ve 26. bodě odůvodnění se stanoví, že jakákoli opatření členských států pro ochranu veřejného zájmu, jako například opatření pro zákonné zachycování, musí být (vedle EÚLP) v souladu také s Listinou. Tento stav je žádoucí, neboť je v souladu s odůvodněním rozsudku ve věci Tele2/Watson, že jakékoli vnitrostátní výjimky z ochrany zpracování údajů podle právních předpisů EU podléhají Listině (a porušení prostřednictvím vnitrostátních právních předpisů tak mohou být předložena Soudnímu dvoru Evropské unie). Článek 11 navrhovaného nařízení však pouze uvádí, že omezení oblasti působnosti článků 5 až 8 navrhovaného nařízení musí respektovat podstatu základních práv a svobod a představovat nezbytné a přiměřené opatření. Měl by zde být uveden i výslovný odkaz na Listinu a EÚLP.
- 45. **Skutečnost, že důvěrný charakter sdělení je také chráněn podle článku 8 EÚLP.** V bodě 1.1 důvodové zprávy a v 1. bodě odůvodnění je vysvětleno, že navrhované nařízení provádí článek 7 Listiny. To je zopakováno v 19. bodě odůvodnění. Základní právo na důvěrná sdělení je však chráněno nejen v tomto ustanovení, ale také podle článku 8 EÚLP. Zahrnutí výslovného odkazu v některém z článků navrhovaného nařízení by dále potvrdilo, že při posuzování (konečného) nařízení bude třeba vzít v úvahu také příslušnou judikaturu Evropského soudu pro lidská práva. Tento odkaz je mimo jiné již zahrnut ve 20. bodě odůvodnění (týkajícím se koncových zařízení) a ve

26. bodě odůvodnění (týkajícím se zákonného zachycování) a dále podpořen úvahami v bodě 2.1 důvodové zprávy (týkajícím se vztahu mezi Listinou a EÚLP v souvislosti s právníky osobami), nikoli však v kterémkoli z příslušných článků, jako například v čl. 11 odst. 1.

#### DALŠÍ VYJASNĚNÍ

46. Je třeba vyjasnit, že **povinnosti podle obecného nařízení o ochraně osobních údajů, například pokud jde o režim porušení zabezpečení údajů a posouzení vlivu na ochranu osobních údajů, zůstávají v platnosti**, pokud strany zpracovávají osobní údaje v kontextu údajů elektronických komunikací. Jelikož v 5. bodě odůvodnění je uvedeno, že navrhované nařízení je *lex specialis* k obecnému nařízení o ochraně osobních údajů a že zpracování dat elektronických komunikací by mělo být povoleno pouze v souladu s navrhovaným nařízením, lze vyslovit pochybnosti, zda se určité povinnosti podle obecného nařízení o ochraně osobních údajů použijí také v kontextu navrhovaného nařízení. To platí zejména v případě, kdy by navrhované nařízení mohlo být vykládáno tak, že stanovuje určitou povinnost, kterou upravuje i obecné nařízení o ochraně osobních údajů. Mezi ilustrativní příklady patří:

- (i) Navrhované nařízení ukládá povinnost určitého ohlašování „zjištěných“ bezpečnostních rizik (článek 17) (viz také poznámka 35), ale obecné nařízení o ochraně osobních údajů obsahuje režim ohlašování případů porušení zabezpečení údajů (články 33 a 34).
- (ii) Navrhované nařízení zmiňuje, že provedení posouzení vlivu na ochranu osobních údajů a konzultace s dozorovým úřadem v souladu s obecným nařízením o ochraně osobních údajů je za určitých okolností povinné (17. a 19. bod odůvodnění a čl. 6 odst. 3 písm. b)), zatímco obecné nařízení o ochraně osobních údajů již stanoví, kdy musí být provedeno posouzení vlivu na ochranu osobních údajů a kdy je vyžadována konzultace (články 35 a 36).
- (iii) Není vyjasněno, že pokud se splní nezbytné podmínky výjimky ze zákazu zpracování podle článku 5 navrhovaného nařízení, je přesto nutné splnit všechny příslušné povinnosti podle obecného nařízení o ochraně osobních údajů, pokud je zpracování osobních údajů a jakékoli jiné zpracování podle obecného nařízení o ochraně osobních údajů zakázáno. Je třeba vyjasnit, že test slučitelnosti stanovený v čl. 6 odst. 4 obecného nařízení o ochraně osobních údajů se tedy nepoužije.
- (iv) Navrhované nařízení o soukromí a elektronických komunikacích nestanoví mechanismus pro vydávání osvědčení obdobný jako články 42 a 43 obecného nařízení o ochraně osobních údajů. Jelikož je oblast působnosti článku 42 obecného nařízení o ochraně osobních údajů přísně vzato omezena na zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečeti a známek dokládajících ochranu údajů pro účely prokázání souladu s obecným nařízením o ochraně osobních údajů, je třeba uvážit, zda by nemělo být zavedeno srovnatelné ustanovení, které by umožnilo vydávání osvědčení pro operace zpracování, normy, výrobky nebo služby k zajištění jejich souladu s nařízením o soukromí a elektronických komunikacích.

Aby bylo zajištěno, že tyto nejasnosti nebudou použity jako argument ke snížení úrovně ochrany podle navrhovaného nařízení, je třeba vyjasnit, že ve všech těchto případech správci rovněž musí dodržovat obecné nařízení o ochraně osobních údajů.

47. Kromě toho je třeba vyjasnit, že **požadavek na odvolání souhlasu se použije také v souvislosti se zasahováním do koncových zařízení**. V čl. 8 odst. 1 písm. b) navrhovaného nařízení se stanoví možnost zasahovat do koncových zařízení koncových uživatelů s jejich souhlasem. Ustanovení čl. 9 odst. 3 vyžaduje, aby koncoví uživatelé měli možnost svůj souhlas kdykoli odvolat, což se však vztahuje pouze na souhlas s analýzou metadat a obsahu. Je třeba vyjasnit, že tato povinnost se vztahuje i na zasahování do koncových zařízení.
48. V této souvislosti je třeba vyjasnit, že **připomínka možnosti souhlas odvolat se vztahuje také na souhlas udělený prostřednictvím nastavení prohlížeče**. Ustanovení čl. 9 odst. 3 vyžaduje, aby byla koncovým uživatelům v pravidelném intervalu šesti měsíců připomínána možnost jejich souhlas kdykoli odvolat. Jelikož se pracovní skupina domnívá, že obecná nastavení prohlížečů a jiného softwaru, včetně operačních systémů, aplikací a softwarových rozhraní pro zařízení připojená díky internetu věcí (tj. nikoli na základě konkrétních strukturovaných kontrol), nemohou být platným opatřením pro poskytování souhlasu, neboť obecná nastavení nejsou vhodná k poskytnutí konkrétního souhlasu s konkrétními scénáři (viz poznámka 24), standardní nastavení by měla být uživatelsky přívětivá (viz poznámka 19). *Pokud* se v tomto ohledu navrhované nařízení nezmění, nastavení musí být dostatečně strukturovaná, aby byla zajištěna kontrola nad zpracováním všech údajů, k němuž uživatel poskytne souhlas, a musí pokrývat každou funkci zařízení, která by mohla ke zpracovávání údajů vést. Kromě toho by koncovému uživateli měla být alespoň v pravidelném intervalu (šesti měsíců) připomínána možnost tato nastavení změnit.
49. Je třeba uvítat, že navrhované nařízení vyžaduje, aby software již uvedený na trh informoval koncového uživatele o jeho možnostech nastavení ochrany soukromí (článek 10). **Je však nejisté, jak to lze účinně použít v případě starších produktů** a jiných produktů, které již nejsou podporovány. Kromě toho je třeba dále vyjasnit, jak se tato povinnost bude vztahovat na software s otevřeným zdrojovým kódem, který je vyvíjen otevřeným a decentralizovaným způsobem.
50. Je třeba vyjasnit, že **nabídka možnosti blokovat cookies (třetích stran) podle článku 10 navrhovaného nařízení převažuje nad výjimkou pro měření návštěvnosti internetových stránek** podle čl. 8 odst. 1 písm. d). Neboli jinými slovy: i když internetová stránka může využívat analytiku pro měření návštěvnosti internetových stránek podle čl. 8 odst. 1 písm. d), uživatelé by přesto měli mít právo tyto technologie sledování ve svém prohlížeči blokovat.
51. **Je třeba vyjasnit definici (polo)automatických volacích a komunikačních systémů**. Definice tohoto pojmu uvedená v čl. 4 odst. 3 písm. h) navrhovaného nařízení obsahuje odkaz na samotný pojem ve druhé části věty („včetně volání uskutečněných za použití automatických volacích a komunikačních systémů, které spojí volanou osobu s jinou osobou“). Navrhuje se tuto poslední větu z definice vypustit a změnit definici v čl. 4 odst. 3 písm. g) tak, aby zahrnovala volání s pomocí

poloautomatických komunikačních systémů, jako jsou například volací automaty (tzv. „dialer“), které spojí volanou osobu s jinou osobou.

**52. Je třeba vyjasnit informace, které jsou „součástí přihlášení se k užívání služby“.**

Ve 14. bodě odůvodnění je uvedeno, že metadata elektronických komunikací „mohou zahrnovat informace, které jsou součástí přihlášení se k užívání služby, jsou-li tyto informace zpracovávány pro účely přenášení, šíření nebo výměny obsahu elektronických komunikací“. Je nejasné, jaký je záměr tohoto znění.

**53. Je třeba vyjasnit použitelnost mechanismů jednotnosti a spolupráce.** V 38. bodě odůvodnění je uvedeno, že navrhované nařízení se opírá o mechanismus jednotnosti podle obecného nařízení o ochraně osobních údajů. Kromě toho čl. 18 odst. 1 stanoví, že kapitoly VI a VII obecného nařízení o ochraně osobních údajů se použijí obdobně. V článku 19 je dále uvedeno, že Evropský sbor pro ochranu osobních údajů plní úkoly stanovené v článku 70 obecného nařízení o ochraně osobních údajů. Ačkoli je použití těchto ustanovení relativně jasné, nelze vyloučit, že vyvstanou otázky výkladu, pokud jde o klíčové koncepty mechanismů jednotnosti a spolupráce podle obecného nařízení o ochraně osobních údajů. Například mechanismus vedoucího úřadu se použije v případech, kdy dochází k „přeshraničnímu zpracování“ (čl. 56 odst. 1 obecného nařízení o ochraně osobních údajů): není jisté, jak se toto použije v případě zasahování do koncových zařízení nebo analýzy obsahu nebo metadat podle navrhovaného nařízení. Je proto vhodné vyjasnit použití těchto klíčových konceptů v některém bodě odůvodnění a zdůraznit, že veškeré zbývající otázky týkající se použitelnosti těchto kapitol obecného nařízení o ochraně osobních údajů v souvislosti s navrhovaným nařízením budou řešeny výkladem ustanovení těchto kapitol v souladu s jejich záměrem. Kromě toho je vhodné vyjasnit, že článek 70 se v kontextu navrhovaného nařízení použije obdobně na Evropský sbor pro ochranu osobních údajů (to nyní v bodech odůvodnění chybí).

\* \* \*