PRACOVNÁ SKUPINA PRE OCHRANU ÚDAJOV ZRIADENÁ PODĽA ČLÁNKU 29

17/SK

WP 247

Stanovisko č. 1/2017
k navrhovanému nariadeniu o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES

Prijaté 4. apríla 2017

Táto pracovná skupina bola zriadená podľa článku 29 smernice 95/46/ES. Je nezávislým európskym poradným orgánom na ochranu údajov a súkromia. Jej úlohy sú definované v článku 30 smernice 95/46/ES a v článku 15 smernice 2002/58/ES.

Úlohy sekretariátu zaisťuje riaditeľstvo C (Základné práva a právny štát) Európskej komisie, Generálne riaditeľstvo pre spravodlivosť a spotrebiteľov, B-1049 Brusel, Belgicko, kancelária č. MO-59 05/035.

Webové sídlo: http://ec.europa.eu/justice/data-protection/index_sk.htm.

PRACOVNÁ SKUPINA PRE OCHRANU JEDNOTLIVCOV SO ZRETEĽOM NA SPRACOVANIE OSOBNÝCH ÚDAJOV,

ktorá bola zriadená smernicou Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995,

so zreteľom na články 29 a 30 uvedenej smernice,

so zreteľom na svoj rokovací poriadok,

PRIJALA TOTO STANOVISKO:

ZHRNUTIE

Pracovná skupina víta návrh nariadenia o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách, ktorý Európska komisia predložila 10. januára 2017. Pracovná skupina víta skutočnosť, že pre tento regulačný nástroj **bola zvolená forma nariadenia**. Vďaka tomu sa zabezpečí, že v rámci celej EÚ budú platiť jednotné pravidlá, ako aj jednoznačnosť pre dozorné orgány aj organizácie. Takisto sa tým zabezpečí aj súlad so všeobecným nariadením o ochrane údajov. Tento súlad sa podporí aj tým, že ako orgán zodpovedný za presadzovanie pravidiel o súkromí v elektronických komunikáciách bol určený ten **istý orgán, ktorý je zodpovedný za monitorovanie dodržiavania všeobecného nariadenia o ochrane údajov**.

Súčasne je pozitívny aj výber (resp. ponechanie) **doplnkového právneho nástroja**. Ochrana dôvernej komunikácie a koncových zariadení má osobitné charakteristiky, ktoré sa vo všeobecnom nariadení o ochrane údajov neriešia. Z tohto dôvodu sú potrebné doplňujúce ustanovenia týkajúce sa týchto služieb, aby sa zabezpečila primeraná ochrana základných práv na súkromie a dôvernosť komunikácie, a to aj v súvislosti s dôvernosťou koncových zariadení. Pracovná skupina v tejto súvislosti jednoznačne podporuje **principiálny prístup** zvolený v navrhovanom nariadení, ktorý spočíva v **široko formulovaných zákazoch a úzko vymedzených výnimkách**, ako aj v **cielenom uplatňovaní pojmu „súhlas“**.

Pracovná skupina víta rozšírenie rozsahu pôsobnosti navrhovaného nariadenia s cieľom zahrnúť **poskytovateľov služieb Over-The-Top (OTT)**, ktoré sú funkčne rovnocenné tradičnejším komunikačným prostriedkom a preto majú podobný potenciálny vplyv na súkromie a právo na dôvernosť komunikácie ľudí v EÚ. Takisto je pozitívne, že sa v navrhovanom nariadení jednoznačne upravuje **obsah aj súvisiace metaúdaje**, a že sa v ňom uznáva, že **metaúdaje môžu odhaliť veľmi citlivé údaje**.

Pracovná skupina však musí uviesť štyri body, ktoré vyvolávajú **vážne obavy**. Pokiaľ ide o **sledovanie polohy koncových zariadení**, **podmienky, za ktorých je povolená analýza obsahu a metaúdajov a štandardné nastavenie koncových zariadení a softvéru a napokon steny, ktoré podmieňujú prístup súhlasom so sledovaním**, treba uviesť, že navrhovaným nariadením by sa znížila úroveň ochrany, ktorú poskytuje všeobecné nariadenie o ochrane údajov. Pracovná skupina v tomto stanovisku predkladá konkrétne návrhy s cieľom zabezpečiť, aby nariadenie o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách poskytovalo rovnakú alebo vyššiu úroveň ochrany, ktorá bude zodpovedať citlivému charakteru údajov z komunikácií (obsahu aj metaúdajov).

Pokiaľ ide o **sledovanie wi-fi**, v závislosti od okolností a účelu zberu údajov, v zmysle všeobecného nariadenia o ochrane údajov takéto sledovanie podlieha povinnosti získať súhlas, resp. sa môže vykonať iba vtedy, ak sa získané osobné údaje anonymizujú. V prípade anonymizácie musia byť splnené tieto štyri podmienky: účel získavania údajov z koncových zariadení musí byť obmedzený výlučne na štatistický výpočet, sledovanie musí byť časovo a priestorovo obmedzené na rozsah nevyhnutne potrebný na tento účel, údaje sa hneď potom okamžite vymažú alebo anonymizujú, a budú k dispozícii účinné možnosti odvolania súhlasu. Európska komisia sa vyzýva, aby podporila technickú normu pre mobilné zariadenia, aby tieto zariadenia automaticky signalizovali námietku proti takémuto sledovaniu.

Pokiaľ ide o **analýzu obsahu a metaúdajov**, východiskovým bodom by malo byť to, že spracovanie údajov z komunikácií bez súhlasu všetkých koncových používateľov (odosielateľov a príjemcov) by malo byť zakázané. S cieľom umožniť poskytovateľom služieb poskytovať služby výslovne požadované používateľom, ako je napr. funkcia vyhľadávania alebo indexovania, resp. programy prevodu textu do reči, mala by sa stanoviť domáca výnimka vzťahujúca sa na spracovávanie obsahu a metaúdajov na čisto osobné účely používateľa.

Pokiaľ ide o **súhlas so sledovaním**, pracovná skupina vyzýva na zavedenie výslovného zákazu stien, ktoré podmieňujú prístup súhlasom so sledovaním, t. j. dania len možnosti, že buď bude používateľ súhlasiť so sledovaním, alebo mu nebude poskytnutý prístup („ber alebo nechaj tak“), v dôsledku čoho sú používatelia nútení súhlasiť so sledovaním, ak chcú tento prístup získať.

Pracovná skupina v neposlednom rade odporúča, aby sa stanovilo, že koncové zariadenia a softvér musia **štandardne ponúkať nastavenie ochrany súkromia** a ponúkať používateľom jasnú alternatívu, pokiaľ ide o možnosť potvrdiť alebo zmeniť toto štandardné nastavenie počas inštalácie. Toto nastavenie musí byť ľahko prístupné počas používania. Používatelia musia mať možnosť vyjadriť špecifický súhlas prostredníctvom nastavenia svojho prehliadača. Preferencie v súvislosti s ochranou súkromia by sa nemali týkať len obmedzenia zásahov tretích strán, resp. súborov cookie. Pracovná skupina výrazne odporúča, aby bola povinnosť dodržiavať štandard „Nesledovať“ stanovená ako mandatórna.

Pracovná skupina identifikovala aj ďalšie problematické body, a to napr. pokiaľ ide o rozsah pôsobnosti, ochranu koncových zariadení a priamy marketing. Napokon identifikovala aj otázky, ktoré si vyžadujú objasnenie s cieľom lepšie chrániť koncových používateľov, ako aj v záujme vyššej právnej istoty pre všetky zainteresované strany.

OBSAH

1. ÚVOD

1. Pracovná skupina zriadená podľa článku 29 (ďalej len „pracovná skupina“) víta návrh nariadenia Európskej komisie (ES) o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (ďalej len „navrhované nariadenie“) [1], ktorým by sa mala nahradiť smernica o súkromí a elektronických komunikáciách(ďalej len „smernica o súkromí a elektronických komunikáciách“)[2].

2. Mnohé aspekty navrhovaného nariadenia sú pozitívne a Európska komisia urobila prostredníctvom tohto navrhovaného nariadenia dôležitý krok. Tento návrh však možno ešte zlepšiť. To pomôže lepšie chrániť koncových používateľov, ale zároveň prinesie aj vyššiu právnu istotu pre všetky zainteresované strany.

3. Pracovná skupina preto predkladá niekoľko problematických bodov a odporúčaní na ozrejmenie, ktorými by sa mal zaoberať Európsky parlament a Rada ministrov v rámci prejednávania tohto navrhovaného nariadenia. V tomto stanovisku sa najprv posúdia pozitívne aspekty navrhovaného nariadenia a následne sa uvedú problematické aspekty a body na ozrejmenie.

2. POZITÍVNE ASPEKTY NAVRHOVANÉHO NARIADENIA

HARMONIZÁCIA NA ÚROVNI EÚ, ZLADENIE POKÚT A VÝLUČNÉ PRESADZOVANIE PRÁVA ZO STRANY ORGÁNOV PRE OCHRANU OSOBNÝCH ÚDAJOV

4. Pracovná skupina víta skutočnosť, že pre tento regulačný nástroj **bola zvolená forma nariadenia**. Takto bude zabezpečená jednotnosť pravidiel v rámci celej EÚ (s určitými výnimkami uvedenými ďalej). To bude znamenať aj jednoznačnosť pre dozorné orgány aj organizácie. Okrem toho treba uviesť, že vzhľadom na kľúčovú úlohu všeobecného nariadenia o ochrane údajov[3]v rámci navrhovaného nariadenia to napomôže zabezpečiť konzistentnosť medzi oboma nástrojmi. Súčasne je pozitívny aj výber (resp. ponechanie) **doplnkového právneho nástroja**. Ochrana dôvernej komunikácie a koncových zariadení má osobitné charakteristiky, ktoré sa vo všeobecnom nariadení o ochrane údajov nerieši. Z tohto dôvodu sú potrebné doplňujúce ustanovenia týkajúce sa týchto služieb, aby sa zabezpečila primeraná ochrana tohto základného práva. Pracovná skupina v tejto súvislosti jednoznačne **podporuje principiálny prístup zvolený v navrhovanom nariadení, ktorý spočíva v široko formulovaných zákazoch a úzko vymedzených výnimkách**, a domnieva sa, že by sa zákonodarcovia

---

1 Návrh nariadenia Európskeho parlamentu a Rady o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (nariadenie o súkromí a elektronických komunikáciách), 2017/0003 (COD), url adresa: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

2 Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. ES L 201, 31.7.2002, s. 37 – 47, url adresa: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.

3 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88, url adresa: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

mali vyvarovať stanovenia otvorených výnimiek na spôsob článku 6 všeobecného nariadenia o ochrane údajov, a najmä na spôsob článku 6 písm. f) (oprávnený záujem).

5. **Presadzovanie pravidiel o súkromí prostredníctvom toho istého orgánu, ktorý je zodpovedný za monitorovanie dodržiavania všeobecného nariadenia o ochrane údajov**, ešte viac podporí súlad medzi týmito dvoma nástrojmi. Vzhľadom na vzťah medzi ochranou osobných údajov a ochranou dôvernej komunikácie a koncových zariadení je užitočné, že presadzovanie ustanovení navrhovaného nariadenia je zverené rovnakému dozornému orgánu, ktorý presadzuje všeobecné nariadenie o ochrane údajov (odôvodnenie č. 38 a článok 18 navrhovaného nariadenia). Okrem toho sa v judikatúre Súdneho dvora Európskej únie (ďalej len „SDEÚ“)[4] potvrdzuje zásadný význam nezávislosti dozorných orgánov v zmysle článku 7 Charty. Z praktického hľadiska by uvedené však viedlo k výraznému dodatočnému nárastu pracovných povinností pre orgány pre ochranu osobných údajov, a to bez záruky ich plnenia v prípade, že nebudú aj navýšené rozpočtové prostriedky, Orgány pre ochranu osobných údajov z tohto dôvodu vítajú znenie odôvodnenia č. 38 navrhovaného nariadenia, v ktorom sa uvádza, že všetky dozorné orgány by mali dostať dodatočné finančné a ľudské zdroje, priestory a infraštruktúru potrebné na účinný výkon úloh podľa nového nariadenia. Takisto sa oceňuje aj skutočnosť, že v článku 18 ods. 2 sa stanovuje právny základ pre spoluprácu medzi dozornými orgánmi podľa navrhovaného nariadenia a vnútroštátnymi regulačnými orgánmi podľa navrhovanej smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie („EECC“)[5].

6. Vzhľadom na úzke prepojenie medzi navrhovaným nariadením a všeobecným nariadením o ochrane údajov pracovná skupina víta aj **zosúladenie pokút podľa navrhovaného nariadenia s pokutami v uvedenom všeobecnom nariadení**. Činnosti, ktoré spadajú do rozsahu pôsobnosti navrhovaného nariadenia, sú dosť citlivé, keďže okrem iného zahŕňajú zasahovanie do súkromnej komunikácie a koncových zariadení. Výška pokút by mala zodpovedať tomuto citlivému kontextu. Uvedený kontext je takisto aj dôvod, prečo je dôležitá harmonizácia v celej EÚ, aby sa zaviedla rovnako vysoká úroveň ochrany v celom regióne. V článku 23 navrhovaného nariadenia sa stanovujú účinné pokuty za porušenie tohto nariadenia, ktoré sú na podobnej úrovni ako pokuty za porušenie pravidiel všeobecného nariadenia o ochrane údajov, s výnimkou určitých prípadov (pozri poznámku č. 38).

7. Pracovná skupina víta aj **vypustenie osobitných pravidiel pre oznamovanie porušenia ochrany údajov**, aby sa zabránilo zbytočnému prekrývaniu s požiadavkami všeobecného nariadenia o ochrane údajov týkajúcimi sa takéhoto porušenia.

8. Takisto **víta aj skutočnosť, že pozornosť je teraz zameraná na poskytnutie rovnakej úrovne ochrany všetkým koncovým používateľom**, keďže v navrhovanom nariadení sa prestalo rozlišovať medzi „účastníkmi“ a inými používateľmi elektronických komunikačných služieb.

---

[4] Pozri napr. rozhodnutie SDEÚ zo 6. októbra 2015, C-362/14 (*Safe Harbour*), bod 41 a rozhodnutia SDEÚ z 21. decembra 2016, C-203/15 a C-698/15 (*Tele2/Watson*), bod. 123.

[5] Návrh smernice Európskeho parlamentu a Rady, ktorou sa stanovuje európsky kódex elektronickej komunikácie (prepracované znenie), 2016/0288 (COD), 12.10.2016, url adresa: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN.

ROZŠÍRENIE ROZSAHU PÔSOBNOSTI V POROVNANÍ SO SMERNICOU O SÚKROMÍ A ELEKTRONICKÝCH KOMUNIKÁCIÁCH

9. Pracovná skupina víta **rozšírenie rozsahu pôsobnosti navrhovaného nariadenia s cieľom zahrnúť poskytovateľov služieb Over-The-Top (OTT)**, ktoré sú funkčne rovnocenné tradičnejším komunikačným prostriedkom a preto majú podobný potenciálny vplyv na súkromie a právo na dôvernosť komunikácie občanov EÚ. Osobitne víta skutočnosť, že do rozsahu pôsobnosti nariadenia teraz patria všetky kategórie OTT – OTT0, OTT1 a niektoré subjekty OTT2)[6], keďže navrhované nariadenie upravuje nielen tradičné komunikačné prostriedky (OTT0), ale aj funkčne rovnocenné služby (OTT1), ako sa uvádza v článku 8 ods. 1 písm. c) navrhovaného nariadenia. Takisto je pozitívne, že nad rámec vymedzení pojmov v rámci EECC boli zahrnuté aj niektoré subjekty OTT2, v prípade, že poskytujú doplnkovú medziľudskú a interaktívnu komunikáciu úzko spojenú s ich službami, ako sú napr. hry, aplikácie slúžiace na zoznamovanie, resp. stránky s hodnoteniami výrobkov či služieb (článok 4 ods. 2 navrhovaného nariadenia). Takisto treba uvítať aj skutočnosť, že bolo **ozrejmené, že ochrana sa vzťahuje aj na interakciu typu stroj-stroj. V odôvodnení č. 12 sa uvádza, že na zariadenie, ktoré navzájom komunikujú, sa vzťahuje ochrana v zmysle navrhovaného nariadenia. Uvedené je vhodné, keďže táto komunikácia často obsahuje informácie chránené právom na súkromie. Bolo by však vhodné, aby sa ozrejmila uplatniteľnosť (pozri poznámku č. 40).**

10. Takisto je pozitívne, že sa v **navrhovanom nariadení sa jednoznačne upravuje obsah a súvisiace metaúdaje**. V odôvodnení č. 14 sa ozrejmuje, že účelom vymedzenia pojmu „údaje z elektronických komunikácií" uvedeného v článku 4 ods. 3 písm. a), je dostatočne široké vymedzenie, aby tento pojem zahŕňal *všetky* typy obsahu, ako aj súvisiace metaúdaje, a to bez ohľadu na prostriedky prenosu signálov. Pracovná skupina však v poznámke č. 39 uvádza ako problematickú skutočnosť, že o aktuálnom vymedzení pojmu „údaje z elektronických komunikácií" sa stále vedie diskusia. V súlade s rozšírením rozsahu pôsobnosti pracovná skupina považuje za významný doplnok, že sa **uznáva, že metaúdaje môžu odhaliť veľmi citlivé údaje** (pozri časť 2.2 dôvodovej správy, odôvodnenie č. 2). Takisto víta skutočnosť, že Európska komisia takýmto spôsobom začleňuje aspekty rozhodnutí SDEÚ vo veciach *Digital Rights Ireland* a *Tele2/Watson* Pracovná skupina takisto oceňuje, že bolo **uznané, že analýza obsahu predstavuje vysoko rizikové spracovanie**. V odôvodnení č. 19 a článku 6 ods. 3 písm. b) sa stanovuje logický právny predpoklad, že spracovanie obsahu predstavuje vysoko rizikové spracovanie v zmysle článku 35 všeobecného nariadenia o ochrane údajov, a preto si bez ohľadu na existenciu vysokého zostatkového rizika vyžaduje predchádzajúcu konzultáciu s (hlavným) orgánom pre ochranu osobných údajov. Pracovná skupina má zároveň obavy v súvislosti s rozsahom vymedzenia pojmu „metaúdaje", ako aj so skutočnosťou, že analýza metaúdajov nepodlieha rovnakému povinnému posúdeniu vplyvu na ochranu údajov (pozri poznámky č. 33 a č. 46).

---

6 Pokiaľ ide o ďalšie vysvetlenie týchto pojmov, pozri BEREC, *Report on OTT Services*, BoR (16) 35, 29. január 2016, s. 15 a 16, url adresa: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. V rámci uvedenej správy zoberte na vedomie, že tieto kategórie boli vymedzené na účely ich použitia v rámci diskusie o preskúmaní a ich účelom nie je, aby slúžili ako právne pojmy.

11. Takisto treba uvítať skutočnosť, že sa naďalej **uznáva význam anonymizácie**. Anonymizácia zohrávala dôležitú úlohu už v rámci smernice o súkromí a elektronických komunikáciách, a to pri zabezpečovaní kompatibility (napríklad článok 6 ods. 1 smernice o e-súkromí, v ktorom sa stanovuje, že prevádzkové údaje, ktoré sú uchovávané, sa musia vymazať alebo anonymizovať, ak už nie sú potrebné na prenos správy. V článku 6 ods. 2 písm. c) a článku 6 ods. 3 písm. b) navrhovaného nariadenia sa umožňuje výnimka zo zákazu spracovania metaúdajov a obsahu na základe súhlasu, pod podmienkou, že daný účel alebo účely „*nemožno dosiahnuť spracovaním anonymizovaných informácií*“. Požiadavka, aby boli uplatnené takéto opatrenia na ochranu súkromia, popri požiadavke, že používatelia musia udeliť svoj súhlas, chráni týchto používateľov pred bezdôvodným spracovaním. Pracovná skupina však má zároveň vážne obavy, že prijatie takýchto techník anonymizácie sa nebude požadovať v prípade sledovania polohy používateľov prostredníctvom ich mobilných zariadení (pozri poznámku č. 17). Okrem toho treba uviesť, že aj keď sa budú musieť anonymizačné opatrenia uplatniť, poskytovatelia by mali vždy vykonávať posúdenie vplyvu na ochranu údajov (pozri poznámky č. 33 a č. 46), a pracovná skupina vyzýva, aby bola stanovená ďalšia povinnosť, a to zverejniť spôsob, akým sú údaje anonymizované a agregované (pozri poznámku č. 42b).

12. Ďalším pozitívom je **široko formulovaná ochrana koncových zariadení**. Odôvodnenie č. 20 a článok 8 stanovujú, že technológie používané na prístup do koncových zariadení nie sú podstatné: na akýkoľvek zásah do koncového zariadenia vrátane použitia funkcie spracovania takéhoto zariadenia, je potrebný súhlas koncového používateľa (s určitými výnimkami). Európska komisia teraz užitočne potvrdila, že pod toto ustanovenie spadá aj rozpoznávanie zariadení (device fingerprinting). Pracovná skupina ďalej víta skutočnosť, že je možné **vymáhať splnenie povinnosti** v prípade, že tretia strana nevyhovie preferenciám, ktoré jednotlivec vyjadril prostredníctvom **nastavenia svojho prehliadača**, ako sa to opisuje v odôvodnení č. 22. Toto by mohlo pomôcť v situáciách, keď určitá tretia strana (napr. reklamná sieť) nerešpektuje toto nastavenie. Uvedené by sa však malo stanovovať aj v príslušných ustanoveniach navrhovaného nariadenia.

13. Napokon treba uviesť, že pracovná skupina víta, že **do rozsahu pôsobnosti navrhovaného nariadenia sú aj naďalej zaradené právnické osoby** (pozri napr. časť 2.2 dôvodovej správy, odôvodnenia č. 3, 33 a 42 a články 1 a 15 a článok 16 ods. 5). Tak je to už podľa smernice o súkromí a elektronických komunikáciách, keďže však orgány pre ochranu osobných údajov budú zodpovedné za presadzovanie týchto nových pravidiel, je vhodné, aby sa to osobitne zdôraznilo. Orgány pre ochranu osobných údajov tak budú môcť prijať opatrenia v prípadoch, keď sa právnické osoby stali obeťami porušenia právnych predpisov, ako napr. keď dostávajú spam alebo ak sa ich komunikácia tajne monitoruje. Pracovná skupina chce však ako dôvod na obavu uviesť aj skutočnosť, že nie je jasné, ako sa požiadavka súhlasu uplatňuje na právnické osoby (pozri poznámku č. 41a) ani to, čo sa myslí pod pojmom „oprávnený záujem“ pri právnických osobách v prípade priameho marketingu (pozri poznámku č. 43c).

CIELENÉ UPLATŇOVANIE POJMU „SÚHLAS“

14. Pracovná skupina víta aj ďalšiu kategóriu zlepšení, ktoré sa týkajú uplatňovania a výkladu pojmu „súhlas“. V prvom rade víta, že **bolo ozrejmené, že prístup na internet a (mobilná) telefónia sa považujú za základné služby a poskytovatelia týchto služieb nesmú svojich zákazníkov „nútiť“, aby súhlasili s akýmkoľvek spracúvaním osobných údajov, ktoré nie je nevyhnutné na poskytovanie tejto základnej služby**. Konkrétne sa v odôvodnení č. 18 konštatuje, že služby základného širokopásmového prístupu na internet a hlasovej komunikácie sa považujú za základné služby, čo znamená, že vzhľadom na závislosť ľudí, pokiaľ ide o prístup k týmto službám, nemožno ich súhlas so spracúvaním ich údajov z elektronických komunikácií na takéto ďalšie účely (napr. na spracovanie na reklamné alebo marketingové účely) považovať za platný. Pracovná skupina má zároveň obavy v súvislosti s tým, že toto ozrejmenie je príliš úzke. Služby poskytované niektorými poskytovateľmi OTT možno takisto považovať za základné služby a nariadenie o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách by malo výslovne zakázať bezalternatívne služby bez možnosti zmeny nastavenia aj za iných okolností (pozri poznámku č. 20).

15. Ďalej treba ako pozitívum uviesť, že **sa harmonizuje požiadavka súhlasu so zahrnutím osobných údajov fyzických osôb do informačných zoznamov**. V zmysle článku 15 navrhovaného nariadenia sa spracovanie osobných údajov v rámci informačných zoznamov umožňuje len v prípade súhlasu fyzických osôb a možnosti namietať v prípade právnických osôb. Uvedené je bližšie ozrejmené v odôvodnení č. 31, kde sa konštatuje, že tento súhlas musí byť konkrétny, pokiaľ ide o osobitné kategórie osobných údajov, ktoré sa majú zahrnúť do informačného zoznamu. Pracovná skupina však konštatuje ako problematický bod, že navrhované nariadenie by mohlo jasnejšie stanovovať, aby sa osobitný samostatný súhlas vyžadoval pri každom vyhľadávaní a spätnom vyhľadávaní (pozri poznámku č. 37).

16. **Takisto sa oceňuje aj nová cielená výnimka pre zasahovanie do koncového zariadenia bez narušenia súkromia**. Pracovná skupina považuje za užitočné, že v navrhovanom nariadení sa ozrejmuje, že daný zákaz sa nevzťahuje na meranie webového prenosu údajov [v rámci úzko vymedzenej výnimky stanovujúcej, že takéto meranie vykonáva poskytovateľ služby informačnej spoločnosti, ktorú požaduje koncový používateľ, pozri článok 8 ods. 1 písm. d) navrhovaného nariadenia]. Pozri ďalej odôvodnenie č. 21. Pracovná skupina však navrhuje použiť technologicky neutrálnejšie vymedzenie a ozrejmiť uplatniteľnosť tejto výnimky (pozri poznámku č. 25).

3. BODY VYVOLÁVAJÚCE VÁŽNE OBAVY

NAVRHOVANÉ NARIADENIE NARÚŠA OCHRANU PODĽA VŠEOBECNÉHO NARIADENIA O OCHRANE ÚDAJOV

Ako sa uvádza vyššie, navrhované nariadenie prináša viacero vylepšení. Sú v ňom však aj problematické body, ktoré sú rôzneho stupňa závažnosti. Pracovná skupina sa v tejto časti venuje štyrom otázkam, v súvislosti s ktorými existujú **vážne obavy**. Ide o ustanovenia, ktoré **oslabujú úroveň ochrany priznanú podľa všeobecného nariadenia o ochrane údajov:**

17. **Povinnosti obsiahnuté** v **nariadení** v **súvislosti so sledovaním polohy koncových zariadení by mali byť v súlade s požiadavkami stanovenými vo všeobecnom nariadení o ochrane údajov**. V článku 8 ods. 2 písm. b) navrhovaného nariadenia sa v prípade získavania informácií vysielaných koncovými zariadeniami vyžaduje iba zobrazenie oznámenia a zavedenie bezpečnostných opatrení. V tomto článku sa ďalej stanovuje, že osoba zodpovedná za toto získavanie musí uviesť všetky opatrenia, ktoré môžu koncoví používatelia prijať na minimalizovanie alebo zastavenie tohto získavania informácií. Z tohto dôvodu článok 8 ods. 2 písm. b) budí dojem, ako keby organizácie mohli získavať informácie vysielané koncovými zariadeniami na sledovanie fyzického pohybu jednotlivcov (ako napr. „sledovanie cez wi-fi“ alebo „sledovanie cez bluetooth“) bez súhlasu dotknutej osoby. Subjekt, ktorý získava tieto údaje, by si zjavne mohol splniť svoju povinnosť prostredníctvom oznámenia, v ktorom by informoval používateľov, aby si vypli svoje zariadenia, ak nechcú byť sledovaní. Takýto prístup by bol v rozpore so základným cieľom telekomunikačnej politiky Európskej komisie, ktorý spočíva v snahe poskytnúť vysokorýchlostné mobilné internetové pripojenie za silnej ochrany súkromia a pri nízkych nákladoch pre všetkých Európanov, a to bez ohľadu na hranice.

    Navrhované nariadenie navyše neobsahuje nijaké jasné obmedzenia, pokiaľ ide o rozsah získavania údajov alebo následného spracúvania. V tomto kontexte treba poznamenať, že tieto MAC adresy predstavujú osobné údaje, a to aj po prijatí takých bezpečnostných opatrení, ako je napríklad hašovanie. Tým, že sa v navrhovanom nariadení neustanovujú ďalšie požiadavky alebo obmedzenia, je úroveň ochrany týchto osobných údajov podľa navrhovaného nariadenia výrazne nižšia ako v rámci všeobecného nariadenia o ochrane údajov, v zmysle ktorého by takéto sledovanie muselo byť spravodlivé, zákonné a transparentné. V odôvodnení č. 25 sa ďalej nekonštruktívne uvádza, že určité funkcie sledovania cez wifi nepredstavujú veľké riziko pre ochranu súkromia, zatiaľ čo iné áno, napríklad sledovanie jednotlivcov v čase. Hoci pracovná skupina oceňuje, že sa v navrhovanom nariadení uznáva, aké veľké riziká z pohľadu ochrany súkromia predstavuje uvedené sledovanie jednotlivcov v čase, je nekonštruktívne, ak sa o určitých funkciách rozhodne vopred, že nepredstavujú riziko pre súkromie, a to bez akéhokoľvek posúdenia okolností a proporcionality spracovania. Takéto posúdenie by sa malo uskutočniť pri zohľadnení ďalej uvedených podmienok týkajúcich sa neanonymizovaného sledovania cez wifi.

    V závislosti od okolností a účelu získavania údajov môže podliehať sledovanie v zmysle všeobecného nariadenia o ochrane údajov povinnosti získať súhlas, resp. sa môže vykonať iba vtedy, ak sa získané osobné údaje anonymizujú. Túto anonymizáciu je najlepšie uskutočniť okamžite po tom, ako boli údaje získané. Ak so zreteľom na účely, na ktoré sa údaje získavajú, nie je možné tieto údaje anonymizovať okamžite, predmetné údaje možno spracovať počas obdobia, kedy tieto údaje nie sú anonymizované, len za ďalej uvedených podmienok: i) účel získavania údajov musí byť obmedzený výlučne na štatistický výpočet (pozri príklady uvedené ďalej), ii) sledovanie musí byť časovo a priestorovo obmedzené na rozsah nevyhnutne potrebný na tento účel, iii) údaje sa hneď potom okamžite vymažú alebo anonymizujú, a iv) k dispozícii musia byť účinné možnosti odvolania súhlasu.

Prevádzkovatelia sú za každých okolností povinní plniť svoju povinnosť poskytovať primerané informácie.

Pracovná skupina má obavy, že potenciálna ponuka individuálneho „opt-out“ za organizáciu, ktorá tieto údaje získava, by znamenalo neprijateľnú záťaž pre občanov, a to vzhľadom na nárast zavádzania takýchto sledovacích technológií zo strany organizácií súkromného aj verejného sektora. Pracovná skupina preto vyzýva európskeho zákonodarcu, aby podporil vytvorenie technickej normy pre zariadenia automaticky signalizujúce námietku proti takémuto sledovaniu, ako aj aby zabezpečil dodržiavanie povinnosti vyhovieť takémuto signálu.

Je pravdepodobné, že podľa všeobecného nariadenia o ochrane údajov by bolo nutné získať súhlas v prípade, že by prevádzkovateľ zhromažďoval a uchovával nepriamo identifikovateľné (prostredníctvom sledovania cez wifi alebo bluetooth) MAC adresy zariadení, a vypočítaval by polohu používateľa s cieľom sledovať jeho polohu v priebehu času, napr. vo viacerých predajniach. Uvedené osobitne platí v prípade, že by sa takéto sledovanie uskutočňovalo na verejných miestach, kde majú používatelia oprávnené očakávanie, že nebudú identifikovaní ani sledovaní, a to aj napriek zberu MAC adries okoloidúcich. Takýto súhlas by bolo možné udeliť napríklad pomocou určitej aplikácie, ktorá by používateľov vyzývala, aby umožnili sledovanie ich polohy v určitých špecifikovaných oblastiach výmenou za obchodné ponuky, resp. prostredníctvom registračných miest na špecifických miestach, alebo prostredníctvom modulu na udelenie súhlasu v rámci WiFi hotspotov.

Bez súhlasu dotknutej osoby môžu prevádzkovatelia spracúvať informácie vysielané koncovými zariadeniami na účely sledovania fyzického pohybu týchto osôb len v obmedzenom počte prípadov. Je to tak napríklad v prípade, že sa určuje počet zákazníkov prítomných v rámci určitého priestoru, resp. ak sa získavajú vysielané údaje na oboch stranách miesta bezpečnostnej kontroly s cieľom zobraziť čas čakania. V oboch týchto prípadoch by však bolo nutné údaje vymazať alebo anonymizovať hneď po získaní údajov na štatistické účely. To znamená, že MAC adresy zariadení návštevníkov na konkrétnom mieste, ako je napr. obchod, sa musia anonymizovať okamžite po tom, ako tieto údaje boli získané, bez toho, aby boli uložené natrvalo, pričom táto anonymizácia sa musí uskutočniť takým spôsobom, aby sa technicky vylúčila možnosť ich opätovná identifikovateľnosť. V prípade výpočtu času čakania by bolo nutné vymazať alebo anonymizovať MAC adresy okamžite po tom, ako tieto údaje už nie sú relevantné pre výpočet času čakania (napríklad preto, že návštevník už absolvoval bezpečnostnú kontrolu alebo opustil čakajúci rad).
Prevádzkovateľ by okrem toho musel splniť požiadavky týkajúce sa minimalizácie získavania údajov (napr. by nesmel realizovať sledovanie nonstop, ak by bol účel obmedzený na otváracie hodiny obchodu a/alebo odber vzoriek v určitých intervaloch). Prevádzkovatelia by okrem toho museli prijať aj iné opatrenia na zmiernenie, aby sa zabezpečil žiadny alebo len veľmi malý vplyv na súkromie používateľov, napr. na ochranu súkromia osôb, ktoré žijú v okolí miesta získavania údajov.

To, že v článku 8 ods. 2 bola zvolená len požiadavka oznámenia, je ešte pozoruhodnejšie vzhľadom na záver odôvodnenia č. 20, kde sa uvádza, že informácie týkajúce sa zariadenia koncového používateľa sa môžu zbierať aj vzdialene na účely

identifikácie a sledovania, a že – podľa navrhovaného nariadenia – môžu vážne ohroziť súkromie koncového používateľa. Okrem toho treba uviesť, že táto povinnosť nejde nad rámec informačnej povinnosti už stanovenej v článkoch 13 a 14 všeobecného nariadenia o ochrane údajov. S týmito vážnymi zásahmi do súkromia prostredníctvom sledovania sa spája potenciálny prístup tretích osôb k takto získaným údajom, ako napr. možnosť pre orgány presadzovania práva identifikovať koncových používateľov na základe uloženej MAC adresy či adries vysielaných ich mobilnými zariadeniami.

18. **Je nutné rozpracovať podmienky, za ktorých je povolená analýza obsahu a metaúdajov.**

V článku 6 navrhovaného nariadenia sa stanovuje rozdielna úroveň ochrany metaúdajov a obsahu. Pracovná skupina nepodporuje tento rozdiel v priznanej ochrane: obe kategórie údajov sú mimoriadne citlivé. Z tohto dôvodu by metaúdaje a obsah mali požívať rovnako vysokú úroveň ochrany. Východiskovým pravidlom by teda malo byť, že bez súhlasu všetkých koncových používateľov (t. j. vysielateľa aj príjemcu) nie je možné spracúvať metaúdaje ani obsah.

Podľa účelu by sa však určité spracovania mali povoliť aj bez tohto súhlasu, a to ak sú nevyhnutné na tieto účely:

- poskytovatelia môžu spracúvať údaje z elektronických komunikácií na účely uvedené v článku 6 ods. 1 písm. a) a b) a článku 6 ods. 2 písm. a) a b) navrhovaného nariadenia[7];
- treba ozrejmiť, že určité technológie na odhalenie a filtrovanie spamu a zmierňovanie pôsobenia botnetov môžu byť takisto považované za nevyhnutné na odhalenie a zastavenie zneužívania elektronických komunikačných služieb. Pokiaľ ide o filtrovanie spamu, koncovým používateľom by mali byť ponúkané, v prípade, že je to technicky možné, štruktúrované možnosti na opt-out;
- malo by sa objasniť, že analýza údajov z elektronických komunikácií na účely zákazníckych služieb môže tiež spadať pod výnimku – „potrebné na účely fakturácie“ – [pozri článok 6 ods. 2 písm. b)]. Príslušné metaúdaje sa môžu uchovávať až do konca obdobia, dokedy možno v súlade s predpismi napadnúť určitú faktúru, resp. dokedy je možné požadovať podľa vnútroštátneho práva jej úhradu. Príslušné údaje (ako napr rôzne url adresy) možno uchovávať len na požiadanie koncového používateľa, a to aj len na obdobie potrebné na vyriešenie sporu o faktúre (z čoho vyplýva, že by sa článok 7 ods. 3 mal zmeniť);
- mala by existovať možnosť spracovať údaje z elektronických komunikácií v záujme poskytovania služieb výslovne požadovaných používateľom, ako je funkcia vyhľadávania alebo indexovania kľúčového slova, virtuálni

[7] Pokiaľ ide o povinné požiadavky na kvalitu služieb v zmysle článku 6 ods. 2 písm. a) navrhovaného nariadenia, poskytovatelia by mali brať do úvahy podmienky opísané v nariadení (EÚ) 2015/2120, a to najmä v článku 3 a odôvodnení č. 10 a odôvodneniach č. 13 až 15; Na základe tohto ustanovenia možno požadovať od poskytovateľov, aby spracovali údaje z komunikácie s cieľom odhaliť a oddeliť malvér a špiónske programy (spyware) a takisto im môže byť povolené komprimovať údaje.

pomocníci, programy prevodu textu do reči a prekladateľské služby. Uvedené si vyžaduje, aby bola zavedená výnimka pre analýzu takýchto údajov pre výhradne osobné použitie, resp. pre použitie v určitej domácnosti, ako aj pre použitie súvisiace s prácou jednotlivca[8]. Táto možnosť by sa umožnila bez súhlasu všetkých používateľov, avšak len so súhlasom koncového používateľa, ktorý požaduje danú službu. Takýto špecifický súhlas by takisto zabránil poskytovateľovi, aby tieto údaje použil na iné účely.

To znamená, že analýza obsahu a/alebo metaúdajov na akýkoľvek iný účel, napr. z analytických dôvodov, na profilovanie, behaviorálnu reklamu alebo iné účely v záujme (komerčného) prínosu pre poskytovateľa, si vyžaduje súhlas všetkých koncových používateľov, ktorých údaje by sa mali spracúvať. Pokiaľ ide o tieto situácie, v navrhovanom nariadení by sa malo ozrejmiť, že len samotné odoslanie e-mailu alebo iného druhu osobnej správy z inej služby koncovému používateľovi, ktorý udelil osobný súhlas so spracovaním svojho obsahu a metaúdajov (napríklad pri registrácii do služby na odosielanie pošty), nepredstavuje platný súhlas odosielateľa.

Napokon treba uviesť, že spracovanie osobných údajov iných dotknutých osôb než sú koncoví používatelia (napr. obrázku alebo opisu tretej osoby v rámci komunikácie medzi dvoma ľudí) takisto musí byť v súlade so všetkými príslušnými ustanoveniami všeobecného nariadenia o ochrane údajov.

19. **Koncové zariadenia a softvér musia *štandardne* odrádzať od nezákonného zasahovania do nich, brániť mu, a zakazovať ho, a poskytovať informácie o existujúcich možnostiach**. Hoci sa v navrhovanom nariadení stanovuje poskytovateľom softvéru povinnosť, aby „ponúkali možnosť“ zabrániť obmedzenej forme zasahovania do koncového zariadenia a takisto aj povinnosť, aby pri inštalácii od koncového používateľa požadovali súhlas s nastavením (článok 10 ods. 1 a 2), tieto možnosti nepredstavujú *štandardnú ochranu súkromia*. Navyše treba uviesť, že „možnosť“ zabrániť určitým zásahom v súčasnosti už existuje, a doposiaľ neviedla k dostatočnému vyriešeniu problému neodôvodneného sledovania. A to je presne dôvod, pre ktorý sa vo všeobecnom nariadení o ochrane údajov urobilo vedomé politické rozhodnutie zaviesť zásady ochrany údajov a súkromia už v štádiu návrhu a štandardnej ochrany (článok 25 všeobecného nariadenia o ochrane údajov). V navrhovanom nariadení sa narúšajú tieto zásady, pokiaľ ide o údaje týkajúce sa komunikácie a zariadenia. Popri tom sa v smernici 2014/53/EÚ[9] o rádiových zariadeniach (uvádzanej v odôvodnení č. 10) stanovujú len veľmi obmedzené bezpečnostné povinnosti, pretože sa ukladá len povinnosť, že „rádiové zariadenie obsahuje prostriedky na zabezpečenie ochrany osobných údajov a súkromia užívateľa a účastníka“; [článok 3 ods. 3 písm. e)]. Uvedené však nedokáže nahradiť štandardné nastavenie ochrany súkromia podľa navrhovaného nariadenia. V tejto súvislosti je tiež potrebné poznamenať, že z prieskumu Eurobarometer týkajúceho sa súkromia a elektronických komunikácií, ktorý sa uskutočnil v decembri 2016 vyplýva, že

[8] Aj keď v odôvodnení č. 13 sa z rozsahu pôsobnosti navrhovaného nariadenia výslovne vynímajú podnikové siete, táto nová výnimka pre individuálne použitie by mala riešiť aj používanie služieb cloud computingu zo strany zamestnancov na pracovné použitie, ako je napríklad vyhľadávanie vo svojej elektronickej pošte.

[9] Smernica 2014/53/EÚ o rádiových zariadeniach.

takmer sedem z desiatich (69 %) respondentov úplne súhlasí s tým, že by ich štandardné nastavenie prehliadača malo zabrániť tomu, aby sa ich informácie zdieľali[10]. Pracovná skupina má osobitné obavy, pokiaľ ide o nastavenie prehliadača a vymedzenie pojmu „tretie strany“. Pozri poznámku č. 24. Okrem toho treba mať na pamäti, že toto ustanovenie sa netýka len prehliadačov používaných v počítačoch, ale vzťahuje sa aj na iné typy softvéru, ktorý umožňuje komunikáciu (vrátane operačných systémov, aplikácií a softvérových rozhraní zariadení napojených na internet vecí). Záverom je, že koncové zariadenia a softvér musia *štandardne* poskytovať nastavenie chrániace súkromie a navigovať používateľov prostredníctvom konfiguračnej ponuky k nastaveniu, ktoré sa odchyľuje od štandardných nastavení pri inštalácii. Toto konfiguračné menu by malo byť kedykoľvek ľahko prístupné počas používania. Pracovná skupina vyzýva európskeho zákonodarcu, aby upresnil rozsah pôsobnosti článku 10 na tento účel.

20. **V navrhovanom nariadení by sa mali výslovne zakázať steny, ktoré podmieňujú prístup súhlasom so sledovaním**, t. j. prax, v rámci ktorej sa prístup na webovú lokalitu alebo ku službe poskytuje len v prípade, že jednotlivci súhlasia s tým, že budú sledovaní na iných webových lokalitách alebo pri iných službách. Ako už bolo uvedené v predchádzajúcich stanoviskách pracovnej skupiny ku smernici o súkromí a elektronických komunikáciách[11], takéto bezalternatívne prístupy na spôsob „ber alebo nechaj tak“ sú len zriedka oprávnené[12]. V prípade, že využívanie funkcií koncových zariadení pre spracovávanie a uchovávanie údajov a získavanie informácií z koncových zariadení umožňuje sledovanie aktivít používateľa v priebehu času alebo v rámci niekoľkých služieb (napr. rôznych webových sídiel alebo aplikácií), tieto činnosti spracovania môžu vážne narušiť súkromie takýchto používateľov. So zreteľom na zásadný význam, ktorý má internet pre umožnenie základnej slobody prejavu vrátane práva na prístup k informáciám, by možnosť jednotlivcov získať prístup k obsahu online nemala závisieť od udelenia súhlasu so sledovaním činnosti na zariadeniach alebo na webových lokalitách či v rámci aplikácií. V budúcom nariadení o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách by sa malo stanovovať, že webové lokality a aplikácie nesmú podmieňovať prístup k nim súhlasom s takýmito rušivými činnosťami spracúvania, a to bez ohľadu na použitú technológiu sledovania, ako sú napr. súbory cookie, rozpoznávanie zariadení, vkladanie jednoznačných identifikátorov alebo iné monitorovacie techniky. Nutnosť takéhoto zákazu zdôrazňuje aj nedávny prieskum Eurobarometer týkajúci sa súkromia a elektronických komunikácií, v ktorom sa konštatuje, že takmer dve tretiny respondentov považujú za neprijateľné, aby ich aktivity online boli monitorované výmenou za neobmedzený prístup na určitú webovú lokalitu (64 %).

21. Záverom možno zhrnúť, že pokiaľ ide o vyššie uvedené štyri body, v **navrhovanom nariadení by sa mal naplniť jeho prísľub, že poskytne rovnakú alebo vyššiu**

---

10 Pozri Flash Eurobarometer 443 o súkromí a elektronických komunikáciách, uverejnený v decembri 2016, s. 5.

11 Pozri napr. stanovisko Pracovnej skupiny v súvislosti so smernicou o e-súkromí, WP 240, s. 16 a jej stanovisko WP 208 k vyňatiu z povinnosti získať súhlas, s. 5.

12 Týmto postojom nie je dotknutý článok 7 ods. 4 všeobecného nariadenia o ochrane údajov, ktorý takisto môže v iných vhodných situáciách vylučovať bezalternatívny výber na spôsob „všetko alebo nič“.

úroveň ochrany ako poskytuje všeobecné nariadenie o ochrane údajov. V odôvodnení č. 5 sa sucho konštatuje, že v navrhovanom nariadení sa neznižuje úroveň ochrany poskytovanej všeobecným nariadením o ochrane údajov. Toto však v kontexte aktuálneho znenia navrhovaného nariadenia neplatí, a to najmä pokiaľ ide o sledovanie zariadení (poznámka č. 17), chýbajúcu zásadu ochrany súkromia ako štandardného nastavenia (poznámka č. 19), a pokiaľ ide o úpravu v súvislosti so súhlasom (poznámka č. 18). Uvedené má osobitnú relevanciu vzhľadom na skutočnosť, že v tom istom odôvodnení sa uvádza, že navrhované nariadenie bude *„lex specialis"* ku všeobecnému nariadeniu o ochrane údajov a bude ho dopĺňať, pokiaľ ide o údaje z elektronických komunikácií, ktoré možno kvalifikovať ako „osobné údaje". Pracovná skupina navrhuje, aby sa v znení navrhovaného nariadenia ozrejmilo prinajmenšom to, že:

i) zákazy podľa navrhovaného nariadenia majú prednosť pred povoleniami podľa všeobecného nariadenia o ochrane údajov (napr, že zákaz zasahovania podľa článku 5 navrhovaného nariadenia má prednosť pred právami poskytovateľov elektronických komunikačných služieb na ďalšie spracúvanie osobných údajov podľa článku 5 ods. 1 písm. b) a článku 6 ods. 4 uvedeného všeobecného nariadenia;

ii) v prípade, že je spracovanie povolené podľa niektorej z výnimiek (vrátane súhlasu) zo zákazu stanovených v navrhovanom nariadení, toto spracovanie, v prípade že ide o spracovanie osobných údajov, musí byť aj tak v súlade so všetkými príslušnými ustanoveniami uvedeného všeobecného nariadenia;

iii) v prípade, že je spracovanie povolené podľa niektorej z výnimiek zo zákazu stanovených v navrhovanom nariadení, každé iné spracovanie na základe uvedeného všeobecného nariadenia je zakázané, vrátane spracovania na iný účel na základe článku 6 ods. 4 uvedeného všeobecného nariadenia. To by nemalo brániť prevádzkovateľom, aby si vyžiadali dodatočný súhlas pre nové operácie spracovania. Takisto by to zákonodarcom nemalo brániť v tom, aby stanovili ďalšie, obmedzené a špecifické výnimky v navrhovanom nariadení, ktorými by sa napríklad umožnilo spracúvanie na vedecké alebo štatistické účely podľa článku 89 všeobecného nariadenia o ochrane údajov, alebo na ochranu „životne dôležitých záujmov" jednotlivcov podľa článku 6 písm. d) uvedeného všeobecného nariadenia.

Navrhované nariadenie by sa malo navyše vykladať takým spôsobom, aby sa zabezpečilo, že bude poskytovať prinajmenšom rovnakú a prípadne aj vyššiu úroveň ochrany, ako poskytuje všeobecné nariadenie o ochrane údajov.

4. ĎALŠIE PROBLEMATICKÉ BODY

Pracovná skupina zriadená podľa článku 29 má okrem už uvedených bodov **obavy**, pokiaľ ide o tieto problematické body:

JE POTREBNÉ ROZŠÍRIŤ ÚZEMNÝ A VECNÝ ROZSAH PÔSOBNOSTI

22. **Pojem „metaúdaje" je príliš úzko vymedzený**. Predmetný pojem sa v súčasnosti vymedzuje v článku 4 ods. 3 písm. c) ako „údaje spracúvané v elektronickej komunikačnej sieti na účely prenosu, distribúcie alebo výmeny obsahu elektronických komunikácií" (podčiarknutie doplnené). Použitie slova „sieť" ako

keby naznačovalo, že len údaje generované v priebehu poskytovania služby na „nižšej“ vrstve siete sa dajú kvalifikovať ako „metaúdaje“. To by mohlo znamenať, že údaje generované v rámci poskytovania služieb kategórií OTT by boli vylúčené z uvedeného rozsahu pôsobnosti. To by bolo nežiaduce a pravdepodobne to takisto ani nie je úmysel, keďže zámerom je rozšíriť rozsah pôsobnosti navrhovaného nariadenia aj na poskytovateľov služieb kategórií OTT. Na účely vyriešenia tohto problému by sa malo vymedzenie pojmu „metaúdaje z elektronických komunikácií“ zmeniť tak, aby zahŕňalo všetky údaje spracúvané na účely prenosu, distribúcie alebo výmeny obsahu elektronických komunikácií.

23. Ďalším dôvodom na obavy je skutočnosť, že **územný rozsah pôsobnosti navrhovaného nariadenia s ohľadom na organizácie neusadené v EÚ sa vzťahuje len na poskytovateľov elektronických komunikačných služieb**. Podľa navrhovaného nariadenia je poskytovateľ elektronických komunikačných služieb, ktorý nie je usadený v EÚ, povinný písomne určiť zástupcu v Únii (článok 3 ods. 2). Okrem toho sa v odôvodnení č. 9 uvádza, že nariadenie by sa malo vzťahovať na spracúvanie zo strany poskytovateľov elektronických komunikačných služieb bez ohľadu na miesto spracovania. Pracovná skupina víta toto ozrejmenie. Keďže sa však znenie obmedzuje len na poskytovateľov elektronických komunikačných služieb, nie je jasné, v akom rozsahu sa tento územný rozsah pôsobnosti vzťahuje aj na iné subjekty (napríklad na subjekty zasahujúce do koncového zariadenia koncového používateľa alebo získavajúce informácie vysielané koncovým zariadením koncového používateľa – porovnaj článok 3 ods. 1 písm. c) v spojení s článkom 8 navrhovaného nariadenia). Pracovná skupina preto navrhuje, aby sa článok 3 ods. 2 a článok 3 ods. 5 zmenili tak, aby zahŕňali poskytovateľov verejne dostupných informačných zoznamov, poskytovateľov softvéru umožňujúceho elektronické komunikácie a osoby odosielajúce priame marketingové obchodné komunikácie či získavajúce (ďalšie) informácie súvisiace s koncovými zariadeniami koncových používateľov alebo uložené v týchto zariadeniach (porovnaj odôvodnenie č. 8 navrhovaného nariadenia)[13].

JE NUTNÉ POSILNIŤ OCHRANU KONCOVÝCH ZARIADENÍ

Ďalšia kategória obáv súvisí s nedostatočnou ochranou koncových zariadení v navrhovanom nariadení.

24. Po prvé, v **navrhovanom nariadení sa nesprávne implikuje, že platný súhlas možno poskytnúť prostredníctvom nešpecifického nastavenia prehliadača**. Pracovná skupina uznáva úvahu, že koncoví používatelia sú zaplavení žiadosťami o poskytnutie súhlasu (odôvodnenie č. 22). Nastavenie prehliadača (a porovnateľného softvéru) zohrávajú úlohu pri riešení tohto problému. Keďže však účelom

[13] Pozri článok 3 ods. 2 všeobecného nariadenia o ochrane údajov: „*Toto nariadenie sa vzťahuje na spracúvanie osobných údajov dotknutých osôb, ktoré sa nachádzajú v Únii, prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v Únii, pričom spracovateľská činnosť súvisí: a) s ponukou tovaru alebo služieb týmto dotknutým osobám v Únii bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo b) so sledovaním ich správania, pokiaľ ide o ich správanie na území Únie.*“ Takáto povinnosť by takisto mohla zahŕňať výnimky podobné článku 27 ods. 2 všeobecného nariadenia o ochrane údajov.

všeobecného nastavenia prehliadača nie je, aby sa vzťahovalo na použitie technológií sledovania v jednom jednotlivom prípade, toto nastavenie nie je vhodné na poskytnutie súhlasu podľa článku 7 a odôvodnenia č. 32 všeobecného nariadenia o ochrane údajov (keďže takýto súhlas nie je informovaný a dostatočne konkrétny).

Koncový používateľ musí mať možnosť udeliť osobitný súhlas so sledovaním, a to v prípade každej jednej webovej lokality alebo aplikácie, na rôzne účely, ako je napr. zdieľanie na sociálnych médiách alebo reklama. Prevádzkovateľ, ktorý zodpovedá za niekoľko webových sídiel alebo aplikácií, môže žiadať o poskytnutie súhlasu pre všetky ostatné lokality alebo aplikácie pod jeho kontrolou, pokiaľ sa tieto žiadosti o poskytnutie súhlasu predkladajú osobitne.

Prevádzkovateľ je navyše povinný dodržať všetky ďalšie povinnosti súvisiace s týmto súhlasom vrátane povinnosti poskytovať užívateľom primerané informácie. V prípade prehliadačov aj prevádzkovateľov údajov uvedené znamená, že by to nebol platný súhlas, ak by ponúkali len možnosť „prijať všetky súbory cookie“, pretože toto by nedávalo používateľom možnosť poskytnúť požadovaný štruktúrovaný súhlas. Prehliadače by však mali používateľom umožňovať, aby sa informovane a vedome rozhodli, že budú súhlasiť so všetkými súbormi cookie, čím sa predíde potrebe toho, aby od nich v budúcnosti navštívené webové lokality zakaždým vyžadovali udelenie súhlasu.

Pracovná skupina dôrazne odporúča, aby sa v navrhovanom nariadení ako mandatórna zaviedla povinnosť, že prehliadače musia implementovať technické mechanizmy, ako je napr. štandard Nesledovať, aby sa zabezpečilo, že používatelia budú mať skutočne na výber a budú mať pod kontrolou zasahovanie do svojich zariadení[14].

Ešte dôležitejšie je však to, aby sa v navrhovanom nariadení zabezpečilo, aby voľba používateľa, pokiaľ ide o uchovávanie informácií v zariadení, ako aj signál „Nesledovať“ (Do Not Track, DNT) z prehliadača, boli všetkými prevádzkovateľmi akceptované ako právne záväzný údaj o súhlase alebo odmietnutí poskytnutia súhlasu. Uvedeným nie sú dotknuté ďalšie usmernenia pracovnej skupiny v súvislosti s dodržiavaním štandardu Nesledovať (DNT), a presnejšie s dodržiavaním zásady obmedzenia účelu, ktoré môžu byť vydané po vypracovaní tohto štandardu (plánovaný termín ukončenia prác je koniec roka 2017).

Implicitné druhy „súhlasu“, ako je napríklad kliknutie na webovej lokalite alebo posúvanie sa na stránke, nemôže zrušiť rozhodnutia v súvislosti s uchovávaním ani signál „Nesledovať“ (DNT). Dôležitým prínosom používania tohto štandardu je to, že sa neobmedzuje len na sledovaciu technológiu súborov cookie, ale že rieši aj iné druhy sledovania, ako je napríklad rozpoznávanie zariadení.

Mandátorne stanovenie povinnosti dodržiavať tento štandard vyrieši aj ďalší problém, ktorým je pojem „tretie strany“ s ktorým sa operuje v článku 10. Webová lokalita alebo aplikácia vo všeobecnosti obsahuje mnoho prvkov, či už ide o prvky zo samotnej stránky alebo externé prvky. Externý kód môže tiež bežať v kontexte navštívenej webovej lokality a pritom komunikovať s nejakým serverom tretej strany. Trvalý súbor cookie môže prísť od prvej strany, keď používateľ navštívi napríklad

[14] Pozri URL adresu: https://www.w3.org/TR/tracking-compliance/. V odseku 7 sa vysvetľuje model výnimky a rozdiel medzi výnimkou pre určitú celú webovú lokalitu a výnimkou pre celý web. V odseku 6 sa uvádza strojovo čitateľná informácia, ktorú prevádzkovatelia môžu poskytovať, pokiaľ ide o požiadavku na informácie poskytované s cieľom získania súhlasu.

lokalitu sociálnej siete. Táto lokalita sociálnej siete by však mohla byť aj treťou stranou, a to v prípade, že používateľ navštívi inú webovú stránku, ktorá obsahuje interakciu s uvedenou lokalitou sociálnej siete. Vo všetkých týchto prípadoch, a to bez ohľadu na to, či ide o „prístup“ k informáciám v zariadení koncového používateľa alebo o ich „uchovávanie“, uvedené kroky predstavujú zásahy do zariadenia, na ktoré je potrebný súhlas (ak sa neuplatňuje niektorá z výnimiek). V rámci štandardu Nesledovať (DNT) sa toto rieši použitím pojmov „pre celú webovú lokalitu“ a „pre celú sieť“. Z tohto dôvodu by sa v záujme zvýšenia právnej istoty pre všetky zainteresované strany mal odkaz na tretie strany obsiahnutý v navrhovanom nariadení preformulovať tak, aby zahŕňal všetky subjekty, s ktorými má zariadenie interakciu (pretože tieto subjekty uchovávajú informácie v zariadení alebo k nim majú prístup).

V záujme zladenia štandardu Nesledovať (DNT) s vysokou úrovňou ochrany dôvernosti komunikácie a ochrany údajov priznanej podľa charty by sa v navrhovanom nariadení malo spresniť, že žiadosti o udelenie súhlasu so sledovaním pre celú sieť (na rozdiel od súhlasu so sledovaním pre celú webovú lokalitu) by sa mali podávať osobitne a používatelia by mali mať slobodnú možnosť akceptovať takúto žiadosť, resp. jej nevyhovieť. V navrhovanom nariadení by sa navyše v záujme ochrany používateľov pred častými žiadosťami o súhlas malo zabezpečiť, aby keď používateľ nevyhovie žiadosti určitej organizácie o súhlas so sledovaním v rámci celej siete (prostredníctvom štandardu Nesledovať „DNT“, resp. prostredníctvom samostatnej čiernej listiny) tento nesúhlas znamenal, že táto organizácia bude blokovaná a nebude môcť podať následné žiadosti o súhlas po dobu najmenej 6 mesiacov. Toto pravidlo by nemalo zbaviť príslušnú organizáciu možnosti, aby v prípade, že ju používateľ priamo navštívi (t. j. ako prvú stranu), požiadala o súhlas na svojej vlastnej webovej lokalite (t. j. možnosti žiadať o súhlas pre celú webovú lokalitu). V praxi to znamená, že napríklad webová lokalita na streaming audiovizuálneho obsahu, ktorá zasiela trvalé súbory cookie, môže o súhlas požiadať, keď ju používateľ navštívi, avšak nemôže oň žiadať opakovane po dobu 6 mesiacov v prípade, že používateľ odmietol udeliť súhlas a navštevuje iné webové lokality, ktoré obsahujú videá z danej streamingovej stránky.

25. Ďalej treba uviesť, že **výnimka pre „meranie využívania webu“ je nepresne naformulovaná**. V článku 8 ods. 1 písm. d) navrhovaného nariadenia sa stanovuje výnimka pre meranie využívania webu. Prvým problematickým bodom je, že tento pojem nie je vymedzený a možno si ho pomýliť s profilovaním používateľov. Z vymedzenia pojmu by malo jasne vyplývať, že túto výnimku nie je možné použiť na účely profilovania užívateľov. Táto výnimka by sa mala vzťahovať len na analytiku používania potrebnú na analýzu výkonnosti služby požadovanej používateľom, avšak nie na analytiku používateľa (t. j. na analýzu správania identifikovateľných používateľov webovej lokality, aplikácie alebo zariadenia). Z tohto dôvodu výnimku nemožno použiť v situácii, keď sa dajú údaje spojiť s údajmi identifikovateľného používateľa spracúvanými poskytovateľom alebo iným prevádzkovateľom. Okrem toho treba uviesť, že opis výnimky naznačuje technologicky veľmi konkrétnu aplikáciu. Pojem „meranie využívania webu“ by sa mal preto nanovo vymedziť technologicky neutrálne, aby boli zahrnuté aj podobné analytické informácie o použití získané z aplikácií, nositeľných zariadení a zariadení internetu vecí.

Pracovná skupina navrhuje, aby sa na inšpiráciu využila holandská výnimka, ktoré sa uplatňuje, ak je to nevyhnutne potrebné na získanie informácií o technickej kvalite alebo účinnosti dodávanej služby informačnej spoločnosti a nemá žiadny alebo iba malý vplyv na súkromie účastníka alebo koncového používateľa (porovnaj článok 11.7a ods. 3 písm. b) holandského zákona o telekomunikáciách). V rámci tejto výnimky sa zohľadňuje skutočnosť, že väčšina údajov zhromažďovaných prostredníctvom analytiky webovej lokality alebo aplikácie má charakter osobných údajov. Z toho vyplýva, že na spracúvanie týchto údajov sa vzťahuje všeobecné nariadenie o ochrane údajov. To implikuje, že analytiku používania by mohla vykonávať aj externá organizácia, avšak len vtedy, ak:
i) táto organizácia koná ako spracovateľ údajov;
ii) bola uzatvorená dodávateľská dohoda v súlade so všeobecným nariadením o ochrane údajov;
iii) použitá analytická technológia bráni opätovnej identifikácii, a to vrátane anonymizácie IP adries používateľov;
iv) konkrétne súbory cookie alebo iné údaje použité na analytiku možno použiť len na účely konkrétnej webovej lokality, aplikácie alebo nositeľného zariadenia a nemožno ich prepojiť s inými identifikovateľnými údajmi;
v) používatelia majú právo „opt-out“ (pozri aj poznámky č. 17 a č. 50 tohto stanoviska).

Hoci by v prípade, že by boli splnené tieto podmienky, nebolo treba získať súhlas, prevádzkovatelia musia beztak poskytnúť používateľom primerané informácie, a to napríklad prostredníctvom uvedenia statusu, pokiaľ ide sledovania, v zobrazovacom poli v rámci štandardu Nesledovať[15].

26. V navrhovanom nariadení **by sa mali stanoviť úzko a presne vymedzené výnimky z požiadavky získať súhlas**. Znenie výnimky z požiadavky získať súhlas so zasahovaním do zariadení v článku 8 ods. 1 písm. c) je takmer totožné s platným znením článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách – „*ak je to nevyhnutne potrebné, na zabezpečenie služby informačnej spoločnosti, ktorú výslovne požaduje účastník alebo užívateľ*“, pričom však bez uvedenia dôvodu bolo vypustené slovo „nevyhnutne“. Uvedené je zdrojom obáv z dvoch dôvodov. Po prvé, predmetné ustanovenie smernice o súkromí a elektronických komunikáciách už vzbudilo značnú diskusiu o rozsahu jeho pôsobnosti medzi dozornými orgánmi a organizáciami, a vypustenie slova „nevyhnutne“ poskytne ešte menej právnej istoty. Takisto je to dôvod na obavy aj preto, že pracovná skupina už poskytla usmernenie týkajúce sa výkladu pojmu „nevyhnutne“ v tomto kontexte. Pracovná skupina navrhla toto ozrejmenie v stanovisku týkajúcom sa vyňatia z povinnosti získať súhlas so súbormi cookie (WP 194):
„*Súbor cookie je nevyhnutne potrebný na zabezpečenie konkrétnej funkcionality pre používateľa (alebo účastníka): v prípade znefunkčnenia súborov cookie by táto*

[15] Pozri: Tracking Preference Expression (DNT) (vyjadrenie preferencie, pokiaľ ide o sledovanie v rámci normy Nesledovať), Editor's draft (návrh editora) 7. marec 2016.

funkcionalita nebola k dispozícii, pričom používateľ (alebo účastník) predmetnú funkcionalitu výslovne požaduje, ako súčasť služieb informačnej spoločnosti."[16]

Pracovná skupina okrem toho ozrejmila, že

súbory cookie „tretích strán" zvyčajne nie sú „nevyhnutne potrebné" pre používateľa, ktorý navštevuje určitú webovú lokalitu, keďže tieto súbory zvyčajne súvisia s inou službou, ako je tá, ktorú používateľ „výslovne požaduje"[17].
Pracovná skupina dodala, že používanie sociálnych doplňujúcich modulov zameraných na osoby, ktoré nie sú používateľmi určitej platformy alebo webovej lokality, by takisto nemalo byť považované za nevyhnutne potrebné.

Okrem toho treba uviesť, že hoci sa v článku 6 ods. 1 písm. b) navrhovaného nariadenia umožňuje spracovanie údajov z elektronických komunikácií ak je to „potrebné" na bezpečnostné účely, v odôvodnení č. 49 všeobecného nariadenia o ochrane údajov sa stanovuje, že to musí byť nevyhnutne potrebné. Vynechanie slova „nevyhnutne" nemohol byť úmysel, keďže v odôvodnení č. 21 navrhovaného nariadenia sa uvádza, že súhlas so zasahovaním by nemalo byť potrebné vyžadovať v prípade, že je „nevyhnutne potrebné". Bez ohľadu na to predstavuje navrhované nariadenie príležitosť ešte viac ozrejmiť, že táto previerka nevyhnutnosti v kontexte tohto nariadenia by sa mala vykladať reštriktívne v súvislosti so všetkými výnimkami. Pracovná skupina preto navrhuje, aby v súvislosti so všetkými výnimkami obsiahnutými v článku 6 a v článku 8 ods. 1 navrhovaného nariadenia bolo doplnené pred slovo „potrebné" slovo „nevyhnutne".

V navrhovanom nariadení by sa na druhej strane malo výslovne umožňovať vykonať zásah do zariadení s cieľom nainštalovať bezpečnostné aktualizácie. Odosielanie bezpečnostných aktualizácií prostredníctvom internetu je uprednostňovanou metódou inštalácie bezpečnostných aktualizácií v prípade väčšiny zariadení koncových používateľov. Inštalácia aktualizácie sa považuje za zásah do koncového zariadenia. Existuje oprávnený záujem na tom, aby sa zaistila aktuálnosť zabezpečenia týchto zariadení. Poskytovateľ bezpečnostných aktualizácií by vo všeobecnosti mal byť preto schopný inštalovať nevyhnutne potrebné bezpečnostné aktualizácie bez súhlasu koncového používateľa. Nie je však jasné, či takýto zásah môže využiť výnimku zo zákazu zasahovania stanovenú na účely poskytnutia služby informačnej spoločnosti v článku 8 ods. 1 písm. c). Bolo by potrebné ozrejmiť, že inštalácia bezpečnostných aktualizácií na základe tejto výnimky je možná, avšak len ak, i) sú tieto aktualizácie diskrétne zbalené a žiadnym spôsobom nemenia funkcionalitu softvéru na zariadení (vrátane interakcie s inými softvérmi alebo nastavením, ktoré si zvolil používateľ), ii) je koncový používateľ vopred informovaný zakaždým, keď sa aktualizácia inštaluje a iii) má tento koncový používateľ možnosť vypnúť automatickú inštaláciu týchto bezpečnostných aktualizácií.

---

16 Pracovná skupina zriadená podľa článku 29, WP 294, Stanovisko č. 04/2012 týkajúce sa vyňatia z povinnosti získať súhlas so súbormi cookie, prijaté 7. júna 2012, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

17 Tamtiež.

PRIAMY MARKETING

Ďalšia kategória obáv sa týka nedostatočnej ochrany pred priamym marketingom.

27. Prvým dôvodom na obavy je skutočnosť, že **vymedzenie pojmu priameho marketingu je príliš obmedzené.** V článku 4 ods. 3 písm. f) navrhovaného nariadenia sa stanovuje, že „priame marketingové komunikácie sú formou písomnej alebo ústnej reklamy, ktorá sa odosiela jednému alebo viacerým identifikovaným alebo identifikovateľným koncovým používateľom elektronických komunikačných služieb“. Použitie slova „odosiela“ naznačuje použitie technických komunikačných prostriedkov, ktoré nevyhnutne zahŕňajú údaje doručenie komunikátu, zatiaľ čo väčšina reklamy na internete (v rámci platforiem sociálnych médií alebo na webových lokalitách) nezahŕňa „odosielanie“ reklamy v užšom slova zmysle. Uvedené zdôrazňujú aj príklady, ktoré nasledujú po tomto vymedzení pojmu (SMS správa, elektronická pošta) a v odôvodnení č. 33. Všetky sa odvolávajú na dosť tradičné formy marketingovej komunikácie, a aj tak použitie naozaj dosť tradičných volacích systémov podľa všetkého nepatrí do tohto rozsahu pôsobnosti. Tento článok a odôvodnenie by sa mali zmeniť tak, aby zahŕňali všetku reklamu – *odosielanú, cielenú alebo predkladanú* – jednému alebo viacerým identifikovaným alebo identifikovateľným koncovým používateľom. Okrem toho by sa malo ďalej zabezpečiť, aby sa behaviorálna reklama (založená na profiloch koncových používateľov) tiež považovala za priame marketingové komunikácie zamerané na jedného alebo viacerých identifikovaných alebo identifikovateľných koncových používateľov (keďže táto reklama sa tiež považuje za cielenú na konkrétnych, identifikovateľných používateľov).

    Ďalej treba uviesť, že podľa navrhovaného rozsahu pôsobnosti pojmu „priame marketingové komunikácie“ by sa ochrana podľa článku 16 ods. 1 obmedzovala len na správy obsahujúce reklamný materiál, a nechránila by jednotlivcov pred inými správami odosielanými, cielenými alebo predkladanými na marketingové účely (ako sú napríklad správy zasielané potenciálnym záujemcom a žiadajúce o poskytnutie súhlasu, o podporu politických názorov alebo o vyjadrenie voličskej preferencie, o podporu pre charitatívne organizácie alebo iné neziskové organizácie, resp. akékoľvek budovanie značky určitej organizácie). Ďalej treba uviesť, že ako metóda priameho marketingu sa ďalej používajú faxy, hoci nie sú v predmetnom vymedzení uvedené. Článok 4 ods. 3 písm. f) by preto mal zahŕňať akúkoľvek formu reklamy, agitácie a propagácie, a to aj pre neziskové organizácie, pričom by mal výslovne zahŕňať popri elektronickej pošte a SMS správach aj fax [pozri tiež návrh na vysvetlenie v poznámke č. 43 písm. a)]: V odôvodnení č. 32 sa napokon uvádza, že do priameho marketingu patria aj správy, ktoré odosielajú politické strany s cieľom vlastnej propagácie. Toto odôvodnenie treba aktualizovať, aby zahŕňalo aj politikov a volebných kandidátov, ktorí propagujú vlastnú kandidatúru.

28. Po druhé treba uviesť, že **odvolanie súhlasu s priamym marketingom nie je bezplatné a ani také jednoduché ako udeliť súhlas**. Je nutné ozrejmiť možnosť odvolať súhlas podľa navrhovaného nariadenia, aby sa zabezpečila konzistentnosť a zlepšila ochrana príjemcov. V článku 16 ods. 6 navrhovaného nariadenia sa v súčasnosti stanovuje, že príjemcovia priamej reklamy musia byť informovaní

o potrebných informáciách, „aby mohli jednoduchým spôsobom uplatniť svoje právo vziať späť svoj súhlas s prijímaním ďalších marketingových komunikácií“, (podčiarknutie doplnené). To sa potvrdzuje aj v odôvodnení č. 34. Z odôvodnenia č. 70 všeobecného nariadenia o ochrane údajov však vyplýva, že dotknuté osoby majú podľa tohto nariadenia nielen právo namietať proti spracovaniu osobných údajov na účely priameho marketingu jednoduchým spôsobom, ale aj na to, aby tak mohli urobiť „bezplatne“. Tento pojem je použitý aj v článku 16 ods. 2 navrhovaného nariadenia, avšak len pokiaľ ide o možnosť „opt-out“ z priameho marketingu založeného na kontaktných údajoch získaných v súvislosti s predajom.

V článku 7 ods. 3 všeobecného nariadenia o ochrane údajov sa stanovuje, že odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie a že používatelia musia mať možnosť kedykoľvek svoj súhlas odvolať. Navyše treba uviesť, že pracovná skupina vo svojom stanovisku č. 04/2010 ku kódexu správania Federácie európskeho priameho a interaktívneho marketingu (FEDMA) – uznala význam poskytnutia „jednoduchého účinného, bezplatného, priameho a ľahko prístupného spôsobu zrušenia odberu“ priameho marketingu [18]. Tento štandard pre odvolanie súhlasu by sa mal začleniť do pravidiel upravujúcich priamy marketing v navrhovanom nariadení. To isté platí aj pre požiadavku článku 7 ods. 3 všeobecného nariadenia o ochrane údajov, kde sa stanovuje, že odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie a že sa odvolanie musí dať vykonať kedykoľvek.

29. V tejto súvislosti by sa mal objasniť **spôsob odvolania súhlasu alebo opt-out na účely priamych marketingových volaní**. Na základe článku 16 ods. 4 navrhovaného nariadenia sa členské štáty môžu rozhodnúť pre opt-out režim v prípade priamych marketingových hlasových volaní. V navrhovanom nariadení by sa mali určiť opatrenia na odvolanie súhlasu a opatrenia pre opt-out z marketingových volaní. V odôvodnení č. 36 sa uvádza, že členské štáty *by mali preto zaviesť a/alebo zachovať* vnútroštátne opt-out systémy. Na základe tohto ustanovenia by tak mohli členské štáty dokonca umožniť situáciu, keď by používateľ musel uskutočniť opt-out v prípade jednotlivých poskytovateľov komunikačných služieb. Takéto vykonanie nechráni používateľov pred obťažovaním prostredníctvom neodôvodnenej komunikácie[19] ani neposkytuje mechanizmus, ktorý by bol v súlade so všeobecným nariadením o ochrane údajov a ktorý by umožňoval odvolanie súhlasu jednoducho a kedykoľvek. Nariadenie by preto malo stanoviť, že každý členský štát *musí* vytvoriť vnútroštátny register blokovania neželaných volaní. Okrem toho by nariadenie malo stanoviť, že príjemcovia hlasových volaní by mali dostať dve možnosti svoj súhlas odvolať: pokiaľ ide o budúce volanie z danej spoločnosti alebo organizácie a možnosť sa počas týchto volaní zaregistrovať do vnútroštátneho registra blokovania neželaných volaní.

---

[18] Pracovná skupina zriadená podľa článku 29, WP174, stanovisko č. 04/2010 ku kódexu správania Federácie európskeho priameho a interaktívneho marketingu (FEDMA) pri používaní osobných údajov v rámci priameho marketingu, prijaté 13. júla 2010, url adresa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf.

[19] Napríklad v Spojenom kráľovstve telekomunikačný operátor BT zaznamenal za jeden týždeň 31 miliónov obťažujúcich volaní. Pozri: http://www.bbc.com/news/business-38635921.

30. Dôvodom na obavy je aj skutočnosť, že pri **odosielaní priamych marketingových oznámení nie je výslovne zakázané používanie falošných totožností**. V odôvodnení č. 34 sa uvádza, že „ maskovanie identity a používanie falošnej identity, falošných spiatočných adries alebo čísel pri odosielaní nevyžiadaných obchodných komunikácií na účely priameho marketingu“ je zakázané. V článku 16 ods.4 je však iba uvedené, že koncoví užívatelia musia byť informovaní o „totožnosti právnickej alebo fyzickej osoby, v mene ktorej sa komunikácia prenáša“. Táto povinnosť informovať príjemcu o totožnosti by mala byť doplnená o jasný zákaz používania maskovaných alebo falošných kontaktných adries na účely priameho marketingu.

31. Tento bod sa dotýka ďalšieho problému: **požiadavka na zobrazenie predvoľby pri priamych marketingových volaniach sa uvádza ako alternatíva požiadavky na identifikáciu kontaktnej linky**. V zmysle článku 16 ods. 3 sú priame marketingové volania povolené, ak volajúce fyzické alebo právnické osoby buď i) uvedú číslo, na ktorom ich je možné kontaktovať [článok 16 ods. 3 písm. a)], alebo ii) uvedú osobitný kód alebo predvoľbu, z ktorej vyplýva, že volanie je marketingovým volaním [článok 16 ods. 3 písm. b)]. Hoci pracovná skupina víta povinnosť používať predvoľbu podľa článku 16 ods. 3 písm. b), domnieva sa, že táto požiadavka nerieši tú istú vec, ktorú rieši povinnosť identifikácie kontaktnej linky v článku 16 ods. 3 písm. a). Kým požiadavka na zobrazenie predvoľby má umožniť príjemcovi vopred identifikovať volania ako marketingové volania (a prijať potrebné opatrenia na zablokovanie týchto volaní), požiadavka na identifikáciu kontaktnej linky má poskytnúť príjemcom (a dozorným úradom) identifikačné a kontaktné údaje iniciátora marketingu. To je osobitne dôležité pre automatizované volania, kde existuje značná nerovnováha medzi možnosťami marketérov uskutočňovať obťažujúce volania a možnosťami príjemcu, ako sa týmto volaniam vyhnúť. Uvedené požiadavky teda nemôžu byť alternatívne, ale musia sa vzájomne dopĺňať.

HARMONOGRAM

32. Pracovná skupina pozitívne hodnotí Európsku komisiu za to, že uznala potrebu nadobudnutia účinnosti navrhovaného nariadenia spoločne so všeobecným nariadením o ochrane údajov v máji 2018, aby sa zamedzilo nesúladu medzi týmito dvoma legislatívnymi aktmi. Napriek tomu je však znepokojujúce, že tento časový plán je ambiciózny, pričom si vyžaduje aj dokončenie návrhu európskeho kódexu elektronických komunikácií (EECC). Pracovná skupina z tohto dôvodu žiada, aby sa k dodržaniu termínu máj 2018 zaviazali všetky zainteresované strany zapojené do legislatívneho procesu.

ĎALŠIE OBAVY

Táto časť sa zaoberá niekoľkými ďalšími obavami.

33. Po prvé má pracovná skupina obavy v súvislosti s **návrhom, aby boli prijateľné necielené opatrenia na uchovávanie údajov**. V dôvodovej správe sa uvádza, že podľa navrhovaného nariadenia členské štáty môžu slobodne ponechať alebo vytvoriť národné rámce pre uchovávanie údajov, v rámci ktorých okrem iného stanovia opatrenia pre cielené uchovávanie údajov (bod 1.3). Po rozhodnutí vo veci

Tele2/Watson[20] je jasné, že rámce umožňujúce iné ako cielené uchovávanie nie sú podľa charty prípustné (a dokonca aj rámce pre cielené uchovávanie podliehajú dôležitým podmienkam, ako je napr. dohľad), ako aj že globálny prístup k metaúdajom bude musieť byť považovaný za porušenie podstaty článku 7, rovnako ako je to v prípade globálneho prístupu k obsahu elektronickej komunikácie (pozri rozhodnutie Súdneho dvora vo veci Schrems, bod 94). Znenie tejto vety teda naznačuje určitý priestor pre členské štáty, pokiaľ ide o opatrenia na uchovávanie údajov, ktorý však neexistuje. V tejto súvislosti treba uviesť, že v navrhovanom nariadení **nie je metaúdajom poskytovaná dostatočná úroveň ochrany**. Ako už bolo uvedené v poznámke č. 10, pracovná skupina víta, že sa uznáva, že metaúdaje môžu odhaliť veľmi citlivé údaje. Metaúdajom sa však v navrhovanom nariadení neposkytuje ochrana, ktorá by z tohto uznania mala vyplynúť. Vzhľadom na citlivosť metaúdajov by sa najmä pred vykonaním analýzy podľa čl. 6 ods. 2 písm. c)malo uskutočniť posúdenie vplyvu na ochranu údajov (pozri tiež poznámku č. 46).

34. Po druhé, **navrhovaným nariadením by sa nežiaducim spôsobom rozšírili možnosti uchovávania údajov.** V článku 11 navrhovaného nariadenia sa odkazuje na článok 23 ods. 1 písm. a) až e) všeobecného nariadenia o ochrane údajov, keď sa tam opisujú účely, na ktoré môžu členské štáty obmedziť povinnosti a práva stanovené v článkoch 5 až 8 nariadenia. Všeobecné nariadenie o ochrane údajov nestanovuje takéto obmedzenia, pokiaľ ide o osobitné kategórie údajov, v súlade s vysokými rizikami pre dotknuté osoby. Hoci článok 15 smernice o súkromí a elektronických komunikáciách v súčasnosti umožňuje podobné obmedzenia, ich účely sú menej početné. Nové navrhované nariadenie by umožnilo nové obmedzenia na účely „výkon[u] trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu“ [článok 23 ods. 1 písm. d) všeobecného nariadenia o ochrane údajov], ako aj pokiaľ ide o „iné dôležité ciele všeobecného verejného záujmu Únie alebo členského štátu, najmä predmet dôležitého hospodárskeho alebo finančného záujmu Únie alebo členského štátu vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia a sociálneho zabezpečenia“ [článok 23 ods. 1 písm. e) všeobecného nariadenia]. Tieto účely sú v porovnaní so smernicou o súkromí a elektronických komunikáciách nielen nové, ale posledný účel podľa článku 23 ods. 1 písm. d) a celý účel podľa článku 23 ods. 1 písm. e) sú formulované mimoriadne široko. Preto sa navrhuje vypustiť odkaz na článok. 23 ods. 1 písm. a) až e) všeobecného nariadenia o ochrane údajov a namiesto toho spomenúť iba účely v súčasnosti uvedené v článku 15 smernice o súkromí a elektronických komunikáciách.

35. **Povinnosť informovať používateľov o bezpečnostných rizikách má minimálny rozsah pôsobnosti.** Pracovná skupina víta skutočnosť, že poskytovatelia služieb musia informovať používateľov o bezpečnostných rizikách a opatreniach na riešenie týchto rizík, ako sú napríklad šifrovacie technológie (článok 17 a odôvodnenie č. 37). Nadpis ustanovenia však znie: „Informácie o zistených bezpečnostných rizikách“. Skutočnosť, že tento nadpis hovorí o zistených rizikách, naznačuje, že toto ustanovenie sa týka len (potenciálnych) narušení bezpečnosti, zatiaľ čo znenia ustanovenia a odôvodnenia skôr poukazujú na všeobecné vzdelávanie koncových

[20] ECLI:EU:C:2016:970, URL: http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203.

používateľov. Napríklad, ak poskytovateľ služby zistí, že zariadenie používateľa je napadnuté malvérom a stalo sa súčasťou botnetu, predmetné ustanovenie podľa všetkého ukladá priamu povinnosť poskytovateľovi informovať používateľa o vyplývajúcich rizikách. Rozsah pôsobnosti tohto ustanovenia by však mal byť ozrejmený a nemal by sa obmedzovať len na tento konkrétny scenár. Ustanovenie by malo prinajmenšom pokrývať identifikované bezpečnostné riziká všetkých zariadení, ktoré koncovému používateľovi poskytuje poskytovateľ ako súčasť predplatenej služby, ako sú napríklad smerovače a mobilné zariadenia, pričom by malo zahŕňať aj vzdelávanie o rizikách zmeny nastavenia, ktoré bolo nastavené na ochranu súkromia podľa zásady ochrany súkromia už v štádiu návrhu.

Pracovná skupina odporúča, aby sa rozsah pôsobnosti rozšíril tak, aby zahŕňal poskytovateľov softvéru, ktorý umožňuje elektronické komunikácie (pozri odôvodnenie č. 8), a pokiaľ možno aj na novú kategóriu: poskytovateľov technológií, ktoré sú zásadné pre zabezpečenie komunikácie, ktorí nie sú poskytovateľmi služieb (napr. poskytovatelia šifrovacích technológií). V prípade tohto posledného menovaného rozšírenia je tiež potrebné venovať pozornosť tomu, aby sa uvedená povinnosť neduplikovala s povinnosťami oznamovania porušení bezpečnosti v iných nástrojoch, ako sú napr. smernica o kybernetickej bezpečnosti[21] a iné právne nástroje týkajúce sa poskytovateľov certifikátu. Keďže druhá uvedená kategória poskytovateľov technológií zvyčajne nemá priamy kontakt s koncovými používateľmi, je tiež potrebné vysvetliť, ako si môžu plniť svoju informačnú povinnosť podľa tohto ustanovenia.

36. Pracovná skupina víta ustanovenia článkov 2 a 13, ktoré sa budú vzťahovať na interpersonálne komunikačné služby s číslovaním. Nie je však hneď jasné, prečo by **podobná úroveň ochrany súkromia nemala byť dostupná aj pre funkčne rovnocenné služby volania kategórie OTT.**

37. Pracovná skupina má takisto obavy v súvislosti s **nedostatočnou zrejmosťou, pokiaľ ide o štruktúrovaný súhlas so spätným vyhľadávaním v zoznamoch**. Ustanovenie článku 15 ods. 2 navrhovaného nariadenia vyžaduje, aby poskytovatelia získali súhlas od koncových používateľov predtým, než tieto funkcie vyhľadávania v súvislosti s údajmi povolia (pozri aj odôvodnenie č. 31). Pracovná skupina víta harmonizáciu požiadavky na získanie súhlasu, pokiaľ ide o zaraďovanie do zoznamov, ale vyjadruje poľutovanie nad nedostatočnou štruktúrovanosťou, pokiaľ ide o rôzne druhy vyhľadávania. Súčasný návrh smernice o súkromí a elektronických komunikáciách umožňuje členským štátom vyžadovať osobitný súhlas so spätným vyhľadávaním, a to na základe článku 12 ods. 3. V tomto článku sa uvádza, že „*Členské štáty môžu požadovať, aby pre akýkoľvek účel verejného telefónneho zoznamu, iný než je vyhľadanie kontaktných údajov osôb na základe ich mena prípadne minima ďalších identifikačných údajov, bol potrebný dodatočný súhlas účastníkov.*“ Na základe tohto ustanovenia je v mnohých členských štátoch

[21] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1 – 30), url adresa: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

vyžadovaný osobitný súhlas pre funkcie spätného vyhľadávania s prihliadnutím na rôzne úrovne identifikovateľnosti, a teda obťažujúceho charakteru oboch funkcií.

38. Z formálnejšieho pohľadu možno uviesť, že **úroveň pokút za všetky porušenia v zmysle nariadenia nie je harmonizovaná**. Podľa navrhovaného nariadenia členské štáty stanovia pravidlá týkajúce sa sankcií za porušenie článku 23 ods. 4, článku 23 ods. 6 a článku 24 navrhovaného nariadenia. Je súladnejšie uvedené stanoviť v samotnom navrhovanom nariadení.

39. V neposlednom rade treba uviesť, že **navrhované nariadenie vychádza z vymedzení pojmov, ktoré sa môžu stať „pohyblivými cieľmi“**. V rade kľúčových konceptov sa navrhované nariadenie odvoláva na iný právny nástroj, ktorý má v súčasnosti podobu len návrhu: návrh európskeho kódexu elektronických komunikácií (EECC) [pozri napríklad článok. 4 ods. 1 písm. b)]. Dvoma dôležitými príkladmi toho je vymedzenie pojmu „koncový používateľ“, ktoré v súčasnosti zahŕňa fyzické aj právnické osoby, a vymedzenia pojmov „elektronická komunikačná služba“ a „interpersonálna komunikačná služba“, ktoré sa v navrhovanom nariadení odrážajú v článku 4 ods. 1 písm. b); „interpersonálna komunikačná služba“ je ďalej podrobnejšie upravená v článku 4 ods. 2 tak, aby zahŕňala druhy služieb špecificky vylúčené z európskeho kódexu elektronických komunikácií (EECC)[22]. Toto stanovisko vychádza z vymedzení pojmov tak, ako sú v súčasnosti naformulované, avšak je celkom pravdepodobné, že navrhovaný európsky kódex elektronických komunikácií a/alebo jeho kľúčové koncepty sa zmenia. To by malo okamžitý vplyv aj na navrhované nariadenie. Ideálne všetky pojmy, ktoré vychádzajú z európskeho kódexu elektronických komunikácií, by mali byť vymedzené samostatne v navrhovanom nariadení, resp. toto nariadenie by malo prinajmenšom zahŕňať objasnenie v prípade, že existujú akékoľvek pojmy, ktorých vymedzenie sa líši od ich vymedzení uvedených v európskom kódexe elektronických komunikácií (napr. už uvádzané zahrnutie „doplnkových služieb“ do vymedzenia „interpersonálnych komunikačných služieb“). Ak to však nie je možné, pracovná skupina by chcela navrhnúť všetkým stranám zapojeným do legislatívneho procesu, aby zabezpečili, že navrhované nariadenie aj európsky kódex elektronických komunikácií budú prerokované a bude sa o nich hlasovať súčasne, aby zúčastnené strany mohli správne posúdiť rozsah pôsobnosti a dôsledky nových nástrojov.

[22] Napríklad v článku 4 ods. 2 navrhovaného nariadenia uvádza, že „interpersonálna komunikačná služba“ zahŕňa „aj služby, ktoré umožňujú interpersonálnu a interaktívnu komunikáciu len ako drobnú doplnkovú funkciu prepojenú s inou službou“, zatiaľ čo článok 2 ods. 5 európskeho kódexu elektronických komunikácií takéto služby z uvedeného vymedzenia vylučuje. (Európsky kódex elektronických komunikácií zahŕňa „interpersonálnu komunikačnú službu“ v rámci širšej kategórie „elektronické komunikačné služby“ v článku 2 ods. 4).

5. NÁVRHY NA OZREJMENIE V ZÁUJME ZABEZPEČENIA PRÁVNEJ ISTOTY

Okrem uvedených bodov by pracovná skupina takisto rada zdôraznila aj niektoré ustanovenia navrhovaného nariadenia, pre ktoré by bolo prínosom ozrejmenie. Takéto ozrejmenie je považované za potrebné pre zlepšenie právnej istoty všetkých zainteresovaných strán, pokiaľ ide o to, že bude existovať jednotné chápanie a uplatňovanie nariadenia o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách v celej EÚ.

OZREJMENIE ROZSAHU PÔSOBNOSTI

40. Pokiaľ ide o rozsah pôsobnosti navrhovaného nariadenia, pracovná skupina navrhuje toto ozrejmenie:

    a) **Pojem „koncový používateľ“ by mal zahŕňať všetkých jednotlivých používateľov**. V článku 2 ods.14 európskeho kódexu elektronických komunikácií (EECC) je „koncový používateľ“ vymedzený ako používateľ neposkytujúci verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby. Je potrebné objasniť, že jednotlivci, ktorí prispievajú do sietí – napríklad do mrežových sietí prostredníctvom svojho Wi-Fi smerovača – nie sú vylúčení z pôsobnosti ochrany navrhovaného nariadenia.
    b) **Je potrebné objasniť, že územná pôsobnosť sa vzťahuje na všetkých koncových používateľov v Únii**. V článku 3 ods. 1 písm. a) sa stanovuje, že navrhované nariadenie sa vzťahuje na poskytovanie elektronických komunikačných služieb koncovým používateľom „v Únii“, zatiaľ čo článok 3 ods. 1 písm. c) stanovuje, že sa vzťahuje na ochranu koncových zariadení koncových používateľov, „ktorí sa nachádzajú v Únii“ (podčiarknutie doplnené). Uvedené sa v rôznych prekladoch líši. Nemecký preklad neobsahuje toto rozlíšenie, zatiaľ čo iné preklady, ako napríklad preklady do francúzštiny, španielčiny a holandčiny toto rozlíšenie majú. Z odôvodnenia č. 9 je jasné, že územná pôsobnosť je chápaná široko, bez ohľadu na to, či sú služby poskytované z krajín mimo Únie, resp. či spracovaniu dochádza v Únii. Navrhuje sa teda vypustiť slová „ktorí sa nachádzajú“ v článku 3 ods. 1 písm. c) s cieľom zdôrazniť túto širokú pôsobnosť.
    c) **Zdá sa, že navrhované nariadenie chráni dôverné oznámenia iba počas *tranzitu,* nie v čase, keď sú *uložené***. Súčasný prístup v navrhovanom nariadení sa sústredí na ochranu prenosu komunikácií. Pozri napríklad odôvodnenie č. 15, v ktorom sa uvádza, že zákaz zachytávania údajov z komunikácií by sa mal uplatňovať počas prenosu údajov, t. j. až do prijatia obsahu elektronickej komunikácie určeným adresátom. Rozsah tejto ochrany vychádza z koncepčného rámca komunikácií, ktorý je zastaraný. Väčšina údajov z komunikácií zostáva uložená u poskytovateľov služby, a to aj po prijatí. Je potrebné zabezpečiť, aby dôverný charakter týchto údajov bol aj naďalej chránený. Okrem toho komunikácia medzi účastníkmi tých istých služieb založených na cloude (napríklad poskytovateľov webmailu) bude často zahŕňať len málo prenosu: odosielanie mailu sa väčšinou skôr prejaví v databáze poskytovateľa, než aby došlo k skutočnému odosielaniu oznámení medzi dvoma stranami. Argument, že

je to už zahrnuté vo všeobecnom nariadení o ochrane údajov, nie je presvedčivý: základným úmyslom navrhovaného nariadenia je chrániť všetku dôvernú komunikáciu, bez ohľadu na technické prostriedky, akými sa uskutočňuje. Je možné, že ide len o legislatívno-technickú chybu, pretože zákaz podľa článku 5 sa týka „uchovávania" a „spracovania".

d) **Do rozsahu pôsobnosti navrhovaného nariadenia by mali spadať všetky verejné bezdrôtové internetové hotspoty**. Keďže je používanie bezdrôtových hotspotov bežné, je úplne logické, že by nemali byť pochybnosti o tom, či je dôvernosť komunikácie prenášanej cez tieto hotspoty chránená. Pokus o objasnenie tejto veci v nariadení sa však nepodaril, pretože do rozsahu pôsobnosti patria len siete poskytované „nevymedzenej skupine koncových používateľov" (odôvodnenie č. 13). Pojmy „nevymedzená skupina koncových používateľov" a „uzavretá skupina koncových používateľov" treba vymedziť. Predovšetkým je potrebné ozrejmiť, že zabezpečené bezdrôtové siete (t. j. siete s heslom) takisto patria do tohto rozsahu pôsobnosti, ak je toto heslo poskytnuté teoreticky nekonečnej skupine používateľov, ktorých totožnosť nemožno vopred určiť (napr. zákazníci v kaviarni, návštevníci na letisku). Základnou zásadou v tejto súvislosti je, že v súlade s predchádzajúcim stanoviskom pracovnej skupiny WP 29 k revízii smernice o súkromí a elektronických komunikáciách, že „*len služby, ku ktorým dochádza v úradnom alebo pracovnom styku výlučne na účely spojené s prácou alebo na úradné účely, resp. technická komunikácia medzi neverejnými subjektmi alebo verejnými subjektmi výhradne na účely riadenia pracovných alebo obchodných procesov, ako aj využívanie služieb pre výlučne domáce účely, môžu byť z nástroja týkajúceho sa súkromia a elektronických komunikácií vyňaté*". (s. 8).

e) **Navrhované nariadenie by sa malo vzťahovať na údaje získané pri ponúkaní služieb digitálneho vysielania.** So zreteľom na citlivú povahu diváckych zvyklostí, pretože odhaľujú osobné záujmy a charakteristické črty divákov, by sa v navrhovanom nariadení malo stanoviť (napr. v odôvodneniach), že vylúčenie služieb poskytujúcich „obsah prenášaný prostredníctvom elektronických komunikačných sietí" z vymedzenia pojmu „elektronická komunikačná služba" neznamená, že na poskytovateľov služieb, ktorí ponúkajú elektronické komunikačné služby aj služby poskytujúce obsah, sa ustanovenia navrhovaného nariadenia, ktoré sa zameriava na poskytovateľov elektronických komunikačných služieb, nevzťahujú. Uvedené je osobitne dôležité, pretože poskytovanie služieb poskytujúcich „obsah prenášaný prostredníctvom elektronických komunikačných sietí" je vylúčený z vymedzenia pojmu „elektronické komunikačné služby" podľa navrhovaného európskeho kódexu elektronických komunikácií (článok 2 ods. 4).

f) **Údaje z komunikácií sú vo všeobecnosti osobné údaje**. V odôvodnení č. 4 sa uvádza, že údaje z elektronických komunikácií môžu obsahovať osobné údaje. Väčšina údajov z komunikácií sú však osobné údaje[23], pričom z veľkej

[23] Pozri napríklad rozhodnutie Súdneho dvora zo 6. novembra 2003, *Lindqvist*, C-101/01, ECLI: EU: C: 2003: 596, bod 24 (pokiaľ ide o telefónne číslo), rozhodnutie Súdneho dvora z 19. októbra 2016, *Breyer*, C-582/14, ECLI: EU: C: 2016: 779, bod 49 (pokiaľ ide o dynamické IP adresy), a rozhodnutia Súdneho dvora z 8. apríla 2014, *Digital Rights Ireland*, C-293/12 a C-594/12, ECLI: EU: C: 2014: 238, body 26-27 (pokiaľ ide o citlivosť metaúdajov).

časti údaje značne dôvernej a citlivej povahy, takže toto by sa malo upraviť a malo by byť uvedené, že tieto údaje sú vo všeobecnosti osobnými údajmi.

g) **Dôverná komunikácia zahŕňa správy v rámci platforiem.** V odôvodnení č. 1 je vysvetlené, že zásada dôvernosti sa vzťahuje na „súčasné aj budúce komunikačné prostriedky“. Toto odôvodnenie pokračuje zoznamom príkladov týchto prostriedkov vrátane „osobných správ odosielaných cez sociálne médiá“. To má pravdepodobne zahŕňať súkromné správy medzi užívateľmi sociálnych sietí (napr. Facebook alebo Twitter) alebo správy uverejnené na „timeline“, ktoré sú prístupné obmedzenému počtu osôb, avšak znenie nie je príliš jasné.

h) **Ako sa nariadenie o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách vzťahuje na interakcie typu stroj-stroj.** Ako je uvedené v bode 9, pracovná skupina víta, že ochrana sa vzťahuje aj na interakciu typu stroj-stroj. To je však uvedené len v odôvodnení č. 12, nie však v zodpovedajúcom článku. Táto ochrana je žiaduca, pretože takáto komunikácia často obsahuje informácie chránené na základe práva na súkromie. Na druhej strane úzka kategória komunikácie výlučne medzi strojmi by mala byť oslobodená, pokiaľ nemá žiadny vplyv na súkromie alebo dôvernosť komunikácie, napríklad v prípadoch, keď táto komunikácia prebieha pri vykonávaní protokolu na prenos dát medzi sieťovými prvkami (napr. servery, prepínače) na účely vzájomného informovania týchto prvkov o stave svojej činnosti.

   Konkrétnou súvislosťou, pri ktorej si uplatňovanie nariadenia o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách vyžaduje ozrejmenie, je oblasť inteligentných dopravných systémov. Predpokladá sa, že vozidlá budú neustále prenášať dáta obsahujúce jednoznačný identifikátor, a to rádiovo. Bez dodatočnej ochrany v nariadení o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách, pokiaľ ide o údaje z komunikácií, by to mohlo viesť k neustálemu sledovaniu jazdných návykov, trás a rýchlosti vodičov. Ustanovenie článku 2 ods. 1 európskeho kódexu elektronických komunikácií však obsahuje nové a rozšírené vymedzenie pojmu „komunikačných siete“. Patria tam prenosové systémy, ktoré nemajú centralizovanú správu a ktoré umožňujú prenos signálov rádiovo. V odôvodnení č. 14 navrhovaného nariadenia sa uvádza, že tieto údaje sú údaje z elektronických komunikácií. Podľa článku 5 navrhovaného nariadenia je akýkoľvek druh zachytávania, monitorovanie alebo uchovávanie týchto dát z komunikácií zakázané, pokiaľ sa neuplatňuje niektorá z výnimiek. Napriek tomu existuje záujem na spracovaní týchto údajov umožňujúcich, aby sa objekty, ako sú automobily bez vodiča a zariadenia bez obsluhy, vzájomne varovali o svojej blízkosti alebo o iných rizikách. Otázkou potom je, aká výnimka by sa uplatnila v takomto prípade. Súhlas koncových používateľov nie je používateľnou výnimkou, pretože sa môže stať nevyhnutnosťou, aby tieto údaje mohli byť vždy spracované. Poskytovatelia by teda mali byť schopní využiť konkrétne výnimky a umožniť objektom, ako sú automobily bez vodiča a zariadenia bez obsluhy, aby sa vzájomne varovali o svojej blízkosti alebo o iných rizikách.

41. Pokiaľ ide o koncepciu a použitie súhlasu v súčasnom navrhovanom nariadení, pracovná skupina navrhuje tieto ozrejmenia:
    a) **Ako má byť koncepcia súhlasu uplatňovaná v súvislosti s právnickými osobami.** V odôvodnení č. 3 sa uvádza, že nariadenie by malo zabezpečiť, aby sa ustanovenia všeobecného nariadenia o ochrane údajov vzťahovali aj na koncových používateľov, ktorí sú právnickými osobami. Podľa tohto odôvodnenia to zahŕňa aj vymedzenie súhlasu podľa všeobecného nariadenia o ochrane údajov (pozri aj odôvodnenie č. 18). Ako je uvedené v poznámke č. 13, pracovná skupina víta výslovné zahrnutie právnických osôb do rozsahu pôsobnosti nariadenia. Praktické použitie tejto zásady však nie je jasné. Vymedzenie súhlasu podľa všeobecného nariadenia o ochrane údajov si vyžaduje, aby bol súhlas „informovaný“ a aby mal formu „vyhlásenia alebo jednoznačného potvrdzujúceho úkonu“ (článok 4 ods. 11 všeobecného nariadenia o ochrane údajov). Je potrebné objasniť, kedy môže byť právnická osoba v skutočnosti považovaná za „informovanú“ a kedy existuje takýto prejav vôle právnickej osoby.
    b) V tejto súvislosti treba uviesť, že vo väčšine prípadov nemôže zamestnávateľ poskytnúť súhlas v mene svojich zamestnancov, pretože ak zamestnávateľ vyžaduje súhlas od zamestnanca, a vzhľadom na nevyváženosť síl existuje významná reálna alebo potenciálna zaujatosť, ktorá vyplýva z neposkytnutia súhlasu, tento súhlas nie je platný, pretože nie je poskytnutý slobodne[24]. Pokiaľ ide o **spoločnosti poskytujúce zariadenia alebo vybavenie jednotlivcom, navrhované nariadenie neobsahuje (vhodnú) výnimku** zo zákazu zasahovania. Jedným príkladom je situácia, keď chce napr. zamestnávateľ aktualizovať telefón, ktorý poskytol. Druhým príkladom je situácia, keď zamestnávateľ ponúkne zamestnancom prenajaté vozidlá a z administratívnych dôvodov umožňuje, aby tretia strana prostredníctvom palubnej jednotky vo vozidle zhromažďovala lokalizačné údaje. V oboch prípadoch má zamestnávateľ záujem do týchto zariadení zasahovať.
    Toto zasahovanie nemožno považovať za nevyhnutné na poskytovanie služby informačnej spoločnosti [článok 8 ods. 1 písm. c)] ani za potrebné na meranie návštevnosti [článok 8 ods. 1 písm. d)]. Uvedené by bolo možné riešiť zavedením novej výnimky, aby bola zahrnutá situácia, keď i) zamestnávateľ poskytne určité zariadenia v rámci pracovného pomeru, ii) zamestnanec je užívateľom tohto zariadenia a iii) zasahovanie je nevyhnutné na to, aby zamestnanec mohol so zariadením pracovať (čo znamená použitie zásad proporcionality a subsidiarity, pokiaľ ide o zber údajov). Iba ak sú splnené uvedené podmienky, by malo byť možné, aby zamestnávateľ zasahoval do zariadenia koncových používateľov.
    c) **Zlepšovanie kontrol s cieľom zastaviť automatické presmerovanie volaní**. Článok 14 ustanovuje dôležitú kontrolu pre koncových používateľov s cieľom zastaviť automatické presmerovanie volaní treťou stranou. Táto ochrana môže byť ďalej vylepšená aj tým, že súhlas koncového používateľa bude potrebný už pri spustení presmerovania volania.

[24] Pozri stanovisko č. 15/2011 k vymedzeniu súhlasu (WP 187), stanovisko č. 8/2001 o spracovaní osobných údajov v kontexte zamestnania (WP48) a nové stanovisko k spracovaniu údajov v práci (prijaté súbežne s týmto stanoviskom).

42. Pracovná skupina navrhuje ozrejmenie ďalej uvedených bodov, pokiaľ ide o lokalizačné údaje alebo iné metaúdaje:
    a) Mal by sa ozrejmiť význam slovného spojenia **„lokalizačné údaje vygenerované v inom kontexte, než je kontext poskytovania elektronických komunikačných služieb“** uvedeného v odôvodnení č. 17. Nie je jasné, či sa uvedené týka lokalizačných údajov zozbieraných napríklad prostredníctvom aplikácií, ktoré používajú údaje z funkcie GPS v inteligentných zariadeniach a/alebo generujú lokalizačné údaje na základe blízkych Wi-Fi smerovačov, a/alebo lokalizačných údajov zozbieraných palubnými navigáciami a/alebo generovania lokalizačných údajov iným spôsobom. Tieto nejasnosti vytvárajú právnu neistotu, pokiaľ ide o rozsah povinnosti. V každom prípade lokalizačné údaje koncového zariadenia fyzickej osoby sú osobnými údajmi, a preto sa na spracovanie týchto údajov vzťahujú povinnosti podľa všeobecného nariadenia o ochrane údajov.
    b) Je potrebné ozrejmiť, že **oprávnené spracovanie lokalizačných údajov a iných metaúdajov si zväčša <u>nevyžaduje</u> jednoznačný identifikátor. V odôvodnení č. 17 sa ako príklad komerčného využitia elektronických komunikačných metaúdajov zo strany poskytovateľov elektronických komunikačných služieb spomínajú teplotné mapy. Pre vytvorenie základnej teplotnej mapy však nie sú potrebné žiadne jednoznačné identifikátory, postačí iba štatistické počítanie. Ďalší príklad spomínaný v uvedenom odôvodnení – využívanie a zaťaženie infraštruktúry – možno tiež vypočítať na základe určitých meracích bodov, napríklad vytvorením súhrnnej štatistiky zo snímačov dopravy, s cieľom poskytnúť informácie o zaťažení na určitom mieste v určitý čas, bez nutnosti poznať aj totožnosť pripojených osôb.**

       Okrem toho toto odôvodnenie uvádza ako príklad zobrazenie dopravných pohybov v určitých smeroch počas daného časového obdobia, kedy by bol nevyhnutný jednoznačný identifikátor na prepojenie polôh osoby v určitých časových intervaloch. Zdá sa, že týmto príkladom uvedené odôvodnenie legitimizuje ďalšie spracovanie týchto údajov v záujme podpory analytiky zameranej na „veľké dáta“. Jedinou podmienkou podľa navrhovaného nariadenia pre tento druh spracovania je povinnosť vykonať posúdenie vplyvu na ochranu osobných údajov, ak by tento druh spracovania „*predstavoval veľké riziko pre práva a slobody fyzických osôb*“. Táto podmienka je nedostačujúca. Navyše je v rozpore s povinnosťou uvedenou v článku 6, že tento druh spracovania môže byť vykonávaný len so súhlasom používateľov a iba ak tieto údaje nemožno anonymizovať, t. j. bez akýchkoľvek jednoznačných identifikátorov. Používatelia často nemôžu odmietnuť zhromažďovanie svojich geolokalizačných údajov zo strany poskytovateľov elektronických komunikačných služieb, pokiaľ je toto zhromažďovanie technicky potrebné na prenos komunikácie k používateľovi, resp. ak je toto spracovanie nevyhnutné na poskytnutie požadovanej služby (napr. navigácia). V predchádzajúcich stanoviskách pracovná skupina dospela

k záveru, že takéto lokalizačné údaje z inteligentných zariadení sú osobnými údajmi citlivej povahy a že výhody analyzovania týchto údajov neprevažujú nad právom užívateľov na ochranu dôverného charakteru metaúdajov ich komunikácií ani nad ich všeobecným právom na ochranu údajov podľa všeobecného nariadenia o ochrane údajov. V uvedenom odôvodnení sa teda musí prinajmenšom stanoviť, že poskytovatelia musia splniť povinnosti vyplývajúce z článku 25 všeobecného nariadenia o ochrane údajov v prípade ďalšieho spracovania lokalizačných údajov alebo iných metaúdajov. To znamená, že sa musia prijať minimálne tieto opatrenia:

i) používanie dočasných pseudonymov;

ii) vymazanie akejkoľvek tabuľky na spätné vyhľadávanie medzi týmito pseudonymami a pôvodnými identifikačnými údajmi;

iii) agregácia na úroveň, keď individuálni používatelia už nemôžu byť identifikovaní prostredníctvom svojich konkrétnych trás a

iv) vymazanie odľahlých hodnôt, ktoré by umožňovali identifikáciu (všetky tieto opatrenia musia byť uplatnené kumulatívne).

V navrhovanom nariadení sa musí napokon stranám, ktoré sú zapojené do spracovania lokalizačných údajov a iných metaúdajov, uložiť povinnosť zverejňovať svoje metódy anonymizácie a ďalšej agregácie, bez toho aby bola dotknutá zákonom chránená dôvernosť. To by umožnilo dozorným orgánom aj širokej verejnosti si ľahko overiť, či je zvolená metóda primeraná.

OZREJMENIE TÝKAJÚCE SA NEVYŽIADANÝCH KOMUNIKÁCIÍ

43. Pracovná skupina navrhuje ozrejmenie ďalej uvedených bodov, pokiaľ ide o nevyžiadané komunikácie:

a) **Znenie zákazu priameho marketingu bez súhlasu.** V článku 16 ods. 1 navrhovaného nariadenia sa teraz uvádza, že elektronické komunikačné služby „môžu“ byť používané na účely zasielania priamych marketingových oznámení (so súhlasom), ale nie je tam obsiahnutý výslovný zákaz zasielania (smerovania alebo predkladania) priamych marketingových oznámení bez súhlasu. To je v rozpore s prístupom v iných ustanoveniach, kde je najskôr formulovaný zákaz, po ktorom nasledujú určité konkrétne výnimky. Súčasné znenie naznačuje zhovievavejší prístup (ktorý pravdepodobne nie je úmyselný). Pracovná skupina navrhuje mierne upravené znenie súčasného článku 13 ods. 1 smernice o súkromí a elektronických komunikáciách: „Používanie elektronických komunikačných služieb vrátane hlasových volaní, automatických volacích a komunikačných systémov, a to aj poloautomatických systémov, ktoré spájajú volaného s jednotlivcom, faxov a elektronickej pošty alebo iné používanie elektronických komunikačných služieb zo strany fyzických alebo právnických osôb na účely predkladania priamych marketingových komunikácií koncovým používateľom sa povoľuje len v súvislosti s koncovými používateľmi, ktorí vopred vyjadrili súhlas.“

b) **Rozsah pôsobnosti ustanovení o marketingových komunikáciách a volaniach existujúcim kontaktom.** V článku 16 ods. 2 sa stanovuje, že ak osoba získa od svojho súčasného zákazníka elektronické kontaktné údaje na účely elektronickej pošty, môže táto osoba využiť tieto údaje na ďalší priamy

marketing svojich vlastných výrobkov a služieb, ak je zákazníkom jasne a jednoznačne poskytnutá možnosť bezplatne a jednoduchým spôsobom proti takémuto použitiu namietať, a to v čase získavania informácií a pri každom odoslaní správy. Uvedené je v súčasnosti obmedzené len na obchodné kontakty získané „v súvislosti s predajom výrobku alebo služby“ a na účely ďalšieho obchodného marketingu vlastných podobných výrobkov alebo služieb. Vzhľadom na to, že ustanovenia o priamom marketingu sa obdobne vzťahujú na nekomerčné propagačné činnosti (napr. činnosti charít alebo politických strán), toto ustanovenie by sa malo zmeniť tak, aby sa obdobne vzťahovalo aj na nekomerčné organizácie pri kontaktovaní predchádzajúcich podporovateľov v rámci propagácie ich vlastných podobných cieľov alebo ideálov, a rovnaké právo namietať by sa malo vzťahovať na priame marketingové volania. Okrem toho by mala byť stanovená lehota platnosti „kontaktných údajov existujúcich zákazníkov“ v elektronických komunikáciách na komerčné, charitatívne alebo politické účely, pričom táto lehota by sa mala vzťahovať aj na priame marketingové volania. Ak si členské štáty zvolili systém námietky proti hlasovým marketingovým volaniam, prítomnosť relácie „kontakt existujúceho zákazníka“ má prednosť pred registráciou v registri blokovania neželaných volaní. V týchto situáciách nemajú koncoví používatelia žiadnu skutočnú možnosť zabrániť obťažujúcim volaniam od spoločností alebo organizácií, s ktorými boli kedysi v kontakte, ale už si neželajú s nimi prísť do styku. Všeobecne by teda nariadenie malo stanoviť platnosť tejto výnimky pre prípad, že ide o „kontakt existujúceho zákazníka“, a to napríklad na jeden alebo dva roky, v závislosti od oprávnených očakávaní dotknutých koncových používateľov.

c) **Použitie pravidiel priameho marketingu na právnické osoby.** V článku 16 ods. 5 navrhovaného nariadenia sa stanovuje, že členské štáty zabezpečia, aby oprávnené záujmy koncových používateľov, ktorí sú právnickými osobami, boli v prípade nevyžiadaných komunikácií dostatočne chránené. V článku 13 ods. 5 smernice o súkromí a elektronických komunikáciách sa opisujú oprávnené záujmy účastníkov, ktorí nie sú fyzickými osobami. Nie je jasné, aké sú dôsledky tejto zmeny znenia. V odôvodneniach by bolo treba ozrejmiť, že táto zmena nevyjadruje úmysel poskytnúť nižšiu úroveň ochrany. V tejto súvislosti treba uviesť, že zákaz priameho marketingu bez súhlasu sa vzťahuje na „koncových používateľov, ktorí sú fyzickými osobami a vyjadrili svoj súhlas“ (podčiarknutie doplnené). Je potrebné ozrejmiť, že to zahŕňa fyzické osoby *pracujúce pre* právnické osoby. Na druhej strane by nebolo treba získavať súhlas pri oslovení právnických osôb prostredníctvom generických kontaktných údajov, ktoré boli na tento účel zverejnené (ako je napr. „info@companyname.eu“).

d) **Použitie pravidiel priameho marketingu na osoby konajúce v postavení (politických) zástupcov:** Článok 16 v navrhovanom znení môže zabrániť niektorým komunikáciám odosielaným zvoleným zástupcom a vyjadrujúcim obavy alebo záujmy obchodného charakteru. Je potrebné ozrejmiť, že nariadenie takýmto komunikáciám nebráni.

44. Je potrebné ďalej ozrejmiť **uplatňovanie charty a EDĽP na vnútroštátne zákony o uchovávaní.** V odôvodnení č. 26 sa stanovuje, že akékoľvek opatrenia členských štátov na ochranu verejného záujmu, ako napríklad opatrenie pre zákonné zachytávanie, musí byť v súlade aj s chartou (popri súlade s EDĽP). Tento stav je žiaduci, pretože je v súlade s odôvodnením rozhodnutia vo veci *Tele2/Watson*, že akékoľvek národné výnimky z ochrany spracovania osobných údajov podľa právnych predpisov EÚ podliehajú charte (a porušenia v rámci vnútroštátnych právnych predpisov tak môžu byť predložené Súdnemu dvoru Európskej únie). V článku 11 navrhovaného nariadenia sa však len uvádza, že obmedzenia rozsahu práv a povinností uvedených v článkoch 5 až 8 navrhovaného nariadenia musia rešpektovať podstatu základných práv a slobôd, pričom tieto obmedzenia musia predstavovať potrebné a primerané opatrenia. Mal by tu byť uvedený aj výslovný odkaz na chartu a EDĽP.

45. **Skutočnosť, že dôvernosť komunikácie je takisto chránená podľa článku 8 EDĽP.** V bode 1.1 dôvodovej správy a v odôvodnení č. 1 je vysvetlené, že navrhovaným nariadením sa vykonáva článok 7 charty. To sa opakuje v odôvodnení č. 19. Základné právo na dôvernosť komunikácie je však chránené nielen v tomto ustanovení, ale tiež podľa článku 8 EDĽP. Zahrnutie výslovného odkazu do niektorého z článkov navrhovaného nariadenia by ďalej potvrdilo, že pri posudzovaní (konečného) nariadenia bude potrebné vziať do úvahy aj príslušnú judikatúru Európskeho súdu pre ľudské práva. Tento odkaz je okrem iného už zahrnutý v odôvodnení č. 20 (týkajúcom sa koncových zariadení) a v odôvodnení 26 (týkajúcom sa zákonného zachytávania) a ďalej podporený úvahami v bode 2.1 dôvodovej správy (týkajúcom sa vzťahu medzi chartou a EDĽP v súvislosti s právnickými osobami), avšak nie je v žiadnom z príslušných článkov, ako napríklad v článku 11 ods. 1.

ĎALŠIE OZREJMENIA

46. Malo by sa ozrejmiť, že **povinnosti podľa všeobecného nariadenia o ochrane údajov, napríklad pokiaľ ide o režim porušenia údajov a posúdenie vplyvu na ochranu údajov, platia ďalej**, v prípade, že strany spracúvajú osobné údaje v kontexte údajov z elektronických komunikácií. Keďže v odôvodnení č. 5 sa uvádza, že navrhované nariadenie je *lex specialis* k všeobecnému nariadeniu o ochrane údajov a že spracovanie údajov z elektronických komunikácií by malo byť povolené len v súlade s navrhovaným nariadením, možno vysloviť pochybnosti, či sa určité povinnosti podľa všeobecného nariadenia o ochrane údajov uplatňujú aj v kontexte navrhovaného nariadenia. To platí najmä v prípade, keď by sa navrhované nariadenie mohlo interpretovať tak, že stanovuje určitú povinnosť, ktorú však upravuje aj všeobecné nariadenie o ochrane údajov. Medzi názorné príklady patria:
    i) navrhované nariadenie ukladá povinnosť určitého oznamovania „zistených“ bezpečnostných rizík (článok 17) (pozri tiež poznámku č. 35), ale všeobecné nariadenie o ochrane údajov obsahuje režim oznamovania prípadov porušenia bezpečnosti údajov (články 33 a 34);

ii) v navrhovanom nariadení sa uvádza, že vykonanie posúdenia vplyvu na ochranu údajov a konzultácie s dozorným orgánom v súlade so všeobecným nariadením o ochrane údajov je za určitých okolností povinné [odôvodnenie č. 17 a odôvodnenie č. 19, článok 6 ods. 3 písm. b)], zatiaľ čo všeobecné nariadenie o ochrane údajov už stanovuje, kedy musí byť vykonané posúdenie vplyvu na ochranu údajov a kedy je vyžadovaná konzultácia (články 35 a 36);

iii) neuvádza sa, že ak sa splnia potrebné podmienky výnimky zo zákazu spracovania podľa článku 5 navrhovaného nariadenia, je napriek tomu nutné splniť všetky príslušné povinnosti podľa všeobecného nariadenia o ochrane údajov, pokiaľ je spracovanie osobných údajov a akékoľvek iné spracovanie podľa všeobecného nariadenia o ochrane údajov zakázané. Je potrebné ozrejmiť, že test zlučiteľnosti stanovený v článku 6 ods. 4 všeobecného nariadenia o ochrane údajov sa teda neuplatňuje.

iv) Navrhované nariadenie nestanovuje mechanizmus certifikácie obdobný tomu, ako sa stanovuje v článkoch 42 a 43 všeobecného nariadenia o ochrane údajov. Keďže je pôsobnosť článku 42 všeobecného nariadenia o ochrane údajov prísne vzaté obmedzená na zavedenie certifikačných mechanizmov ochrany údajov a zavedenie pečate a značky ochrany údajov na účely preukázania súladu so všeobecným nariadením o ochrane údajov, treba zvážiť, či by nemalo byť zavedené porovnateľné ustanovenie, ktoré by umožnilo vydávanie certifikátov pre operácie spracovania, štandardy, výrobky alebo služby, pokiaľ ide o ich súlad s navrhovaným nariadením.

Aby sa zabezpečilo, že tieto nejasnosti nebudú použité ako argument na zníženie úrovne ochrany podľa navrhovaného nariadenia, je potrebné ozrejmiť, že vo všetkých týchto prípadoch prevádzkovatelia musia takisto splniť aj všeobecné nariadenie o ochrane údajov.

47. Okrem toho je potrebné objasniť, že **požiadavka na odvolanie súhlasu sa použije aj v súvislosti so zasahovaním do koncových zariadení**. V článku 8 ods. 1 písm. b) navrhovaného nariadenia sa stanovuje možnosť zasahovať do koncových zariadení koncových používateľov so súhlasom. V článku 9 ods. 3 sa vyžaduje, aby koncoví používatelia mali možnosť svoj súhlas kedykoľvek odvolať, ale vzťahuje sa to len na súhlas s analýzou metaúdajov a obsahu. Je potrebné ozrejmiť, že táto povinnosť sa vzťahuje aj na zasahovanie do koncových zariadení.

48. V tejto súvislosti je potrebné ozrejmiť, že **pripomienka možnosti odvolať súhlas sa vzťahuje aj na súhlas poskytnutý prostredníctvom nastavenia prehliadača**. V článku 9 ods. 3 sa vyžaduje, aby bola koncovým používateľom v pravidelných šesťmesačných intervaloch pripomínaná možnosť svoj súhlas kedykoľvek odvolať. Keďže sa pracovná skupina domnieva, že všeobecné nastavenia prehliadačov a iného softvéru vrátane operačných systémov, aplikácií a softvérových rozhraní pre zariadenia pripojené do internetu vecí (t. j. nie na základe konkrétnych štruktúrovaných kontrol), nemôžu byť platným opatrením pre poskytovanie súhlasu, pretože všeobecné nastavenia nie sú vhodné na poskytnutie konkrétneho súhlasu s konkrétnymi scenármi (pozri poznámku č. 24), štandardné nastavenie by mala byť užívateľsky prívetivé (pozri poznámku č. 19). *Ak* sa v tomto smere navrhované nariadenie nezmení, nastavenie musí byť dostatočne štruktúrované, aby bola

zabezpečená kontrola nad každým spracovaním údajov, na ktoré používateľ poskytne svoj súhlas, a musí pokrývať každú funkciu zariadenia, ktorá by mohla viesť k spracúvaniu údajov. Okrem toho by koncovému používateľovi mala byť aspoň v pravidelnom intervale (šiestich mesiacov) pripomínaná možnosť tieto nastavenia zmeniť.

49. Je potrebné privítať, že v navrhovanom nariadení sa vyžaduje, aby softvér už uvedený na trh informoval koncového používateľa o jeho možnostiach nastavenia ochrany súkromia (článok 10). **Nie je však jasné, ako to možno účinne použiť v prípade starších produktov** a iných produktov, ktoré už nie sú podporované. Okrem toho je potrebné ďalej ozrejmiť, ako sa táto povinnosť bude vzťahovať na slobodný softvér, ktorý je vyvíjaný otvoreným a decentralizovaným spôsobom.

50. Je potrebné objasniť, že **ponuka možnosti blokovať súbory cookie (tretích strán) podľa článku 10 navrhovaného nariadenia má prednosť pred výnimkou pre meranie využívania webu** podľa článku 8 ods. 1 písm. d). Alebo inak: aj keď webová lokalita môže využívať analytiku pre meranie návštevnosti internetových stránok podľa čl. 8 ods. 1 písm. d), používatelia by napriek tomu mali mať právo tieto technológie sledovania vo svojom prehliadači blokovať.

51. Je potrebné ozrejmiť **vymedzenie (polo) automatických volacích a komunikačných systémov**. Vymedzenie tohto pojmu uvedené v článku 4 ods. 3 písm. h) navrhovaného nariadenia obsahuje odkaz na samotný pojem v druhej časti vety („vrátane volaní uskutočňovaných pomocou automatických volacích a komunikačných systémov, pri ktorých sa spája volaná osoba s inou osobou“). Navrhuje sa túto poslednú vetu z vymedzenia vypustiť a zmeniť vymedzenie v článku. 4 ods. 3 písm. g) tak, aby zahŕňalo volania s pomocou poloautomatických komunikačných systémov, ako sú napríklad volacie automaty (tzv. „dialery“), ktoré spoja volanú osobu s inou osobou.

52. Je potrebné ozrejmiť **informácie, ktoré sú „súčasťou prihlásenia sa k službe“**. V odôvodnení č. 14 sa uvádza, že metaúdaje z elektronických komunikácií „môžu zahŕňať informácie, ktoré sú súčasťou prihlásenia sa k službe, ak sa takéto informácie spracúvajú na účely prenosu, distribúcie alebo výmeny obsahu elektronických komunikácií“. Je nejasné, aký je cieľ tohto znenia.

53. Je potrebné ozrejmiť **použiteľnosť mechanizmov konzistentnosti a spolupráce**. V odôvodnení č. 38 sa uvádza, že navrhované nariadenie sa opiera o mechanizmus konzistentnosti podľa všeobecného nariadenia o ochrane údajov. Okrem toho sa v článku 18 ods. 1 stanovuje, že kapitoly VI a VII všeobecného nariadenia o ochrane údajov sa uplatňujú primerane. V článku 19 je ďalej uvedené, že Európsky výbor pre ochranu údajov vykonáva úlohy stanovené v článku 70 všeobecného nariadenia o ochrane údajov. Hoci je použitie týchto ustanovení pomerne jasné, nemožno vylúčiť, že vzniknú otázky výkladu, pokiaľ ide o kľúčové koncepty mechanizmov konzistentnosti a spolupráce podľa všeobecného nariadenia o ochrane údajov. Napríklad mechanizmus vedúceho orgánu sa uplatňuje v prípadoch, keď dochádza k „cezhraničnému spracovaniu“ (článok 56 ods. 1 všeobecného nariadenia o ochrane údajov): nie je zrejmé, ako sa toto uplatňuje v prípade zasahovania do koncových

zariadení alebo analýzy obsahu alebo metaúdajov podľa navrhovaného nariadenia. Je preto vhodné ozrejmiť použitie týchto kľúčových konceptov v niektorom z odôvodnení a zdôrazniť, že všetky zostávajúce otázky týkajúce sa uplatniteľnosti týchto kapitol všeobecného nariadenia o ochrane údajov v súvislosti s navrhovaným nariadením budú riešené výkladom ustanovení týchto kapitol v súlade s ich zámerom. Okrem toho je vhodné objasniť, že článok 70 sa v kontexte navrhovaného nariadenia uplatňuje primerane na Európsky výbor pre ochranu údajov (čo v súčasnosti v odôvodneniach chýba).

*** * ***