



**Spoločné stanovisko  
EDPB – EDPS 4/2022,  
k návrhu nariadenia  
Európskeho parlamentu a  
Rady, ktorým sa stanovujú  
pravidlá predchádzania  
sexuálnemu zneužívaniu detí  
a boja proti nemu**

**Prijaté 28. júla 2022**

## OBSAH

1.	Kontext.....	7
2.	Rozsah stanoviska .....	9
3.	Všeobecné pripomienky k právu na dôvernosť komunikácie a k ochrane osobných údajov .....	9
4.	Konkrétne pripomienky .....	12
4.1	Vzťah k existujúcim právnym predpisom .....	12
4.1.1	Vzťah k všeobecnému nariadeniu o ochrane údajov a smernici o súkromí a elektronických komunikáciách.....	12
4.1.2	Vzťah k nariadeniu (EÚ) 2021/1232 a vplyv na dobrovoľné odhaľovanie online sexuálneho zneužívania detí .....	12
4.2	Právny základ podľa všeobecného nariadenia o ochrane údajov .....	13
4.3	Povinnosti týkajúce sa posudzovania a zmierňovania rizík.....	13
4.4	Podmienky vydávania príkazov na zistenie.....	15
4.5	Analýza nevyhnutnosti a primeranosti plánovaných opatrení .....	16
4.5.1	Účinnosť zisťovania .....	17
4.5.2	Žiadne menej rušivé opatrenie .....	18
4.5.3	Proporcionalita v užšom zmysle .....	19
4.5.4	Zisťovanie známeho materiálu obsahujúceho sexuálne zneužívanie detí .....	21
4.5.5	Zisťovanie doteraz neznámeho materiálu obsahujúceho sexuálne zneužívanie detí ..	21
4.5.6	Zisťovanie kontaktovania detí („grooming“).....	22
4.5.7	Záver o nevyhnutnosti a proporcionality plánovaných opatrení .....	23
4.6	Oznamovacie povinnosti .....	24
4.7	Povinnosti týkajúce sa odstraňovania a blokovania .....	24
4.8	Príslušné technológie a záruky .....	25
4.8.1	Špecificky navrhnutá a štandardná ochrana údajov .....	25
4.8.2	Spoľahlivosť technológií .....	25
4.8.3	Skenovanie zvukovej komunikácie .....	26
4.8.4	Overovanie veku .....	27
4.9	Uchovávanie informácií.....	27
4.10	Vplyv na šifrovanie .....	27
4.11	Dohľad, presadzovanie práva a spolupráca .....	29
4.11.1	Úloha vnútroštátnych dozorných orgánov podľa všeobecného nariadenia o ochrane údajov	29

4.11.2	Úloha EDPB.....	30
4.11.3	Úloha Európskeho centra pre prevenciu sexuálneho zneužívania detí a boj proti nemu 31	
4.11.4	Úloha Europolu.....	33
5.	Záver.....	37

## Zhrnutie

Európska komisia 11. mája 2022 zverejnila návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu.

Návrhom by sa poskytovateľom hostingových služieb, interpersonálnych komunikačných služieb a iných služieb uložili kvalifikované povinnosti týkajúce sa zisťovania, oznamovania, odstraňovania a blokovania známeho a nového online materiálu obsahujúceho sexuálne zneužívanie detí, ako aj kontaktovania detí. V návrhu sa takisto ustanovuje zriadenie novej decentralizovanej agentúry EÚ (ďalej len „centrum EÚ“) a siete vnútroštátnych koordinačných orgánov pre otázky sexuálneho zneužívania detí s cieľom umožniť vykonávanie navrhovaného nariadenia. Ako sa uvádza v dôvodovej správe k návrhu, opatrenia obsiahnuté v návrhu by mali vplyv na výkon základných práv používateľov predmetných služieb.

Sexuálne zneužívanie detí je obzvlášť závažnou a ohavnou trestnou činnosťou a umožnenie účinných opatrení na boj proti nemu je cieľom všeobecného záujmu uznaného Úniou, ktorým je cieľom je ochrana práv a slobôd obetí. EDPB a EDPS zároveň pripomínajú, že akékoľvek obmedzenia základných práv, ako sú tie, ktoré sa predpokladajú v návrhu, musia byť v súlade s požiadavkami stanovenými v článku 52 ods. 1 Charty základných práv Európskej Únie.

EDPB a EDPS zdôrazňujú, že návrh vyvoláva vážne obavy, pokiaľ ide o primeranosť plánovaných zásahov a obmedzení ochrany základných práv na súkromie a ochranu osobných údajov. V tejto súvislosti by EDPB a EDPS chceli zdôrazniť, že procesné záruky nikdy nemôžu v plnej miere nahradiť vecné záruky. Komplexný systém eskalácie od posúdenia rizika a zmierňujúcich opatrení k príkazu na zistenie [detection order] nemôže nahradiť požadovanú jednoznačnosť hmotnoprávných povinností.

EDPB a EDPS sa domnievajú, že návrh nie je dostatočne jasný, pokiaľ ide o kľúčové prvky, ako sú pojmy „významné riziko“. Okrem toho subjekty zodpovedné za uplatňovanie týchto záruk, počnúc súkromnými operátormi a končiace správnymi a/alebo súdnymi orgánmi, majú veľmi široký priestor na voľnú úvahu, čo vedie k právnej neistote, pokiaľ ide o vyváženie dotknutých práv v každom jednotlivom prípade. EDPB a EDPS zdôrazňujú, že zákonodarcia musí pri povoľovaní obzvlášť závažných zásahov do základných práv zabezpečiť právnu jasnosť, pokiaľ ide o to, kedy a kde sú zásahy povolené. Hoci EDPB a EDPS uznávajú, že legislatívne opatrenia nemôžu byť príliš normatívne a musia ponechať určitú flexibilitu pri ich praktickom uplatňovaní, EDPB a EDPS sa domnievajú, že návrh ponecháva príliš veľký priestor na potenciálne zneužívanie z dôvodu neexistencie jasných hmotnoprávných noriem.

Pokiaľ ide o nevyhnutnosť a primeranosť plánovaných opatrení na zisťovanie, EDPB a EDPS sú znepokojení najmä v súvislosti s opatreniami plánovanými na zisťovanie neznámeho materiálu obsahujúceho sexuálne zneužívanie detí („CSAM“) a kontaktovania detí („grooming“) v rámci interpersonálnych komunikačných služieb. EDPB a EDPS sa domnievajú, že vzhľadom na ich rušivý vplyv, ich pravdepodobnostný charakter a mieru chybovosti spojenú s takýmito technológiami, zásahy spôsobené týmito opatreniami presahujú rámec toho, čo je nevyhnutné a primerané. Okrem toho opatrenia umožňujúce orgánom verejnej moci všeobecný prístup k obsahu komunikácie s cieľom zistiť kontaktovanie detí môžu s väčšou pravdepodobnosťou ovplyvniť podstatu práv zaručených v článkoch 7 a 8 Charty. Príslušné ustanovenia týkajúce sa groomingu by sa preto mali z návrhu vypustiť. Okrem toho sa v návrhu z rozsahu pôsobnosti nevylučuje využívanie skenovania zvukovej komunikácie. EDPB a EDPS sa domnievajú, že skenovanie zvukovej komunikácie je obzvlášť rušivé a ako také musí zostať mimo rozsahu povinností zisťovania stanovených v navrhovanom nariadení, a to pokiaľ ide o hlasové správy aj komunikáciu naživo.

EDPB a EDPS takisto vyjadrujú pochybnosti o účinnosti blokovacích opatrení a domnievajú sa, že by bolo neprimerané vyžadovať od poskytovateľov internetových služieb dešifrovanie online komunikácií s cieľom zablokovať komunikáciu týkajúcu sa materiálu obsahujúceho sexuálne zneužívanie detí.

EDPB a EDPS okrem toho poukazujú na to, že šifrovacie technológie zásadným spôsobom prispievajú k rešpektovaniu súkromného života a dôvernosti komunikácií, slobode prejavu, ako aj k inováciám a rastu digitálneho hospodárstva, ktoré sa opiera o vysokú úroveň dôvery, ktorú takéto technológie poskytujú. V odôvodnení 26 návrhu sa nielen pri výbere technológií na zisťovanie, ale aj pri technických opatreniach na ochranu dôvernosti komunikácií, ako je šifrovanie, uvádza výhrada, že tento výber technológie musí spĺňať požiadavky navrhovaného nariadenia, t. j. musí umožňovať zistenie. Podporuje sa tým myšlienka vyplývajúca z článku 8 ods. 3 a článku 10 ods. 2 návrhu, že poskytovateľ nemôže odmietnuť vykonanie príkazu na zistenie na základe technickej nemožnosti. EDPB a EDPS sa domnievajú, že by mala existovať lepšia rovnováha medzi potrebou spoločnosti mať bezpečné a súkromné komunikačné kanály a bojom proti ich zneužívaniu. V návrhu by sa malo jasne uviesť, že žiadne ustanovenie navrhovaného nariadenia by sa nemalo vykladať ako zákaz alebo oslabenie šifrovania.

Hoci EDPB a EDPS vítajú tvrdenie v návrhu, v ktorom sa stanovuje, že návrh nemá vplyv na právomoci a kompetencie orgánov na ochranu osobných údajov podľa všeobecného nariadenia o ochrane údajov, EDPB a EDPS zastávajú názor, že vzťah medzi úlohami koordinačných orgánov a úlohami orgánov na ochranu údajov by sa mal napriek tomu lepšie upraviť. EDPB a EDPS v tejto súvislosti oceňujú úlohu, ktorú návrh prisudzuje EDPB tým, že požaduje jeho zapojenie do praktického vykonávania návrhu, najmä potrebu, aby EDPB vydal stanovisko k technológiám, ktoré by centrum EÚ sprístupnilo na vykonávanie príkazov na zisťovanie. Malo by sa však objasniť, aký účel by stanovisko slúžilo v tomto procese a ako by centrum EÚ konalo po získaní stanoviska od EDPB.

EDPB a EDPS napokon poznamenávajú, že v návrhu sa predpokladá úzka spolupráca medzi centrom EÚ a Europolom, ktoré by si mali navzájom poskytovať „čo najširší prístup k relevantným informačným systémom“. Hoci EDPB a EDPS v zásade podporujú spoluprácu týchto dvoch agentúr, vzhľadom na to, že centrum EÚ nie je orgánom presadzovania práva, EDPB a EDPS stále poskytnú viacero odporúčaní na zlepšenie príslušných ustanovení vrátane toho, že poskytnutie osobných údajov medzi centrom EÚ a Europolom sa uskutočňuje len na individuálnom základe na základe riadne posúdenej žiadosti, a to prostredníctvom zabezpečeného komunikačného nástroja na výmenu informácií, ako je sieť SIENA.

## Európsky výbor pre ochranu údajov a Európsky dozorný úradník pre ochranu údajov

so zreteľom na článok 42 ods. 2 nariadenia 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (ďalej len „nariadenie o ochrane údajov inštitúciami EÚ“),<sup>1</sup>

so zreteľom na Dohodu o EHP, a najmä na jej prílohu XI a protokol 37, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018,<sup>2</sup>

So zreteľom na žiadosť Európskej komisie o spoločné stanovisko Európskeho výboru pre ochranu údajov a Európskeho dozorného úradníka pre ochranu údajov z 12. mája 2022 k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu,<sup>3</sup>

### PRIJALI TOTO SPOLOČNÉ STANOVISKO

## 1. KONTEXT

1. Európska komisia (ďalej len „Komisia“) 11. mája 2022 zverejnila návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu („návrh“ alebo „navrhované nariadenie“).<sup>4</sup>
2. Návrh bol vydaný po prijatí nariadenia (EÚ) 2021/1232 o dočasnej výnimke z určitých ustanovení smernice 2002/58/ES, pokiaľ ide o používanie technológií poskytovateľmi interpersonálnych komunikačných služieb nezávislých od číslovania na spracúvanie osobných a iných údajov na účely boja online proti sexuálnemu zneužívaniu detí (ďalej len „dočasné nariadenie“).<sup>5</sup> V dočasnom nariadení sa od príslušných poskytovateľov služieb nevyžaduje, aby zaviedli opatrenia na zisťovanie materiálu zobrazujúceho sexuálne zneužívanie detí (napr. obrázky, videá atď.) alebo kontaktovanie detí (známe aj ako „grooming“) v rámci svojich služieb, ale umožňuje týmto poskytovateľom dobrovoľné vykonávanie týchto činností v súlade s podmienkami stanovenými v uvedenom nariadení.<sup>6</sup>
3. Návrh pozostáva z dvoch hlavných prvkov. Po prvé, poskytovateľom hostingových služieb, interpersonálnych komunikačných služieb a iných služieb sa ukladajú kvalifikované povinnosti týkajúce

---

<sup>1</sup> Ú. v. EÚ L 295, 21.11.2018, s. 39.

<sup>2</sup> Odkazy na „členské štáty“ uvedené v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.

<sup>3</sup> Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu, COM(2022) 209 final.

<sup>4</sup> Tamže.

<sup>5</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1232 zo 14. júla 2021 o dočasnej výnimke z určitých ustanovení smernice 2002/58/ES, pokiaľ ide o používanie technológií poskytovateľmi interpersonálnych komunikačných služieb nezávislých od číslovania na spracúvanie osobných a iných údajov na účely boja proti online sexuálnemu zneužívaniu detí, Ú. v. EÚ L 274, 2021, s. 41.

<sup>6</sup> Pozri tiež stanovisko EDPS 7/2020 k návrhu dočasných výnimiek zo smernice 2002/58/ES na účely boja proti sexuálnemu zneužívaniu detí online (10. novembra 2020).

sa zisťovania, oznamovania, odstraňovania a blokovania známeho a nového online materiálu obsahujúceho sexuálne zneužívanie detí, ako aj kontaktovania detí. Po druhé, v návrhu sa stanovuje zriadenie novej decentralizovanej agentúry EÚ (Európske centrum pre prevenciu sexuálneho zneužívania detí a boj proti nemu, ďalej len „centrum EÚ“) a siete vnútroštátnych koordinačných orgánov pre otázky sexuálneho zneužívania detí s cieľom umožniť vykonávanie navrhovaného nariadenia.<sup>7</sup>

4. Ako sa uvádza v dôvodovej správe k návrhu, opatrenia obsiahnuté v návrhu by mali vplyv na výkon základných práv používateľov predmetných služieb. Tieto práva zahŕňajú najmä základné práva na rešpektovanie súkromia (vrátane dôvernosti komunikácií ako súčasť širšieho práva na rešpektovanie súkromného a rodinného života), ochranu osobných údajov a slobodu prejavu a informácií.<sup>8</sup>
5. Takéto navrhované opatrenia majú navyše vychádzať z existujúcich právnych predpisov EÚ v oblasti ochrany údajov a súkromia a do určitej miery ich dopĺňať. V tejto súvislosti sa v dôvodovej správe uvádza, že:

„Tento návrh nadväzuje na všeobecné nariadenie o ochrane údajov. Poskytovatelia sa v praxi pri spracúvaní stanovenom vo všeobecnom nariadení o ochrane údajov zvyčajne odvolávajú na rôzne dôvody, na základe ktorých spracúvajú osobné údaje nevyhnutne získané v rámci dobrovoľného zisťovania a oznamovania online sexuálneho zneužívania detí. V návrhu sa stanovuje systém cielených príkazov na zistenie a uvádzajú sa v ňom podmienky zisťovania, vďaka čomu sa pri týchto činnostiach poskytuje väčšia právna istota. Pokiaľ ide o činnosti týkajúce sa povinného zisťovania, ktoré zahŕňajú spracúvanie osobných údajov, návrhom sa najmä v prípade príkazov na zistenie vydávaných na jeho základe, tak stanovuje dôvod na takéto spracúvanie uvedený v článku 6 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov, v ktorom sa stanovuje spracúvanie osobných údajov nevyhnutné na splnenie právnej povinnosti podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha.

Návrh sa okrem iného vzťahuje na poskytovateľov, ktorí ponúkajú interpersonálne elektronické komunikačné služby, a preto podliehajú vnútroštátnym ustanoveniam, ktorými sa transponuje smernica o súkromí a elektronických komunikáciách a jej navrhovaná revízia, ktorá je v súčasnosti predmetom rokovaní. Opatreniami uvedenými v návrhu sa v niektorých ohľadoch obmedzuje rozsah práv a povinností podľa príslušných ustanovení uvedenej smernice, konkrétne vo vzťahu k činnostiam, ktoré sú nevyhnutne potrebné na vykonanie príkazov na zistenie. Návrh sa v tejto súvislosti týka analogického uplatňovania článku 15 ods. 1 uvedenej smernice.“<sup>9</sup>

6. Vzhľadom na závažnosť predpokladaných zásahov do základných práv má návrh osobitný význam pre ochranu práv a slobôd fyzických osôb, pokiaľ ide o spracúvanie osobných údajov. Komisia sa preto 12. mája 2022 rozhodla konzultovať s Európskym výborom pre ochranu údajov (ďalej len „EDPB“) a Európskym dozorným úradníkom pre ochranu údajov (ďalej len „EDPS“) v súlade s článkom 42 ods. 2 nariadenia o ochrane údajov inštitúciami EÚ.

---

<sup>7</sup> COM(2022)209 final, s. 17.

<sup>8</sup> COM(2022)209 final, s. 12.

<sup>9</sup> COM(2022)209 final, s. 4 – 5.

## 2. ROZSAH STANOVISKA

7. V tomto spoločnom stanovisku sa uvádzajú spoločné názory EDPB a EDPS na návrh. Obmedzuje sa na aspekty návrhu týkajúce sa ochrany súkromia a osobných údajov. V spoločnom stanovisku sa poukazuje najmä na oblasti, v ktorých návrh nezabezpečuje dostatočnú ochranu základných práv na súkromie a ochranu údajov alebo si vyžaduje ďalšie zosúladenie s právnym rámcom EÚ v oblasti ochrany súkromia a osobných údajov.
8. Ako sa ďalej vysvetľuje v tomto spoločnom stanovisku, návrh vyvoláva vážne obavy, pokiaľ ide o nevyhnutnosť a primeranosť plánovaných zásahov a obmedzení ochrany základných práv na súkromie a ochranu osobných údajov. Cieľom tohto spoločného stanoviska však nie je poskytnúť vyčerpávajúci zoznam všetkých otázok týkajúcich sa ochrany súkromia a údajov, ktoré návrh vyvoláva, ani poskytnúť konkrétne návrhy na zlepšenie znenia návrhu. Namiesto toho sa v tomto spoločnom stanovisku uvádzajú pripomienky na vysokej úrovni k hlavným otázkam nastoleným v návrhu, ktoré identifikovali EDPB a EDPS. EDPB a EDPS však zostávajú k dispozícii na poskytnutie ďalších pripomienok a odporúčaní spoluzákonodarcom počas legislatívneho procesu k návrhu.

## 3. VŠEOBECNÉ PRIPOMIENKY K PRÁVU NA DÔVERNOSŤ KOMUNIKÁCIE A K OCHRANE OSOBNÝCH ÚDAJOV

9. Dôvernosť komunikácie je základným prvkom základného práva na rešpektovanie súkromného a rodinného života zakotveného v článku 7 Charty základných práv Európskej únie (ďalej len „Charta“).<sup>10</sup> Okrem toho sa v článku 8 Charty uznáva základné právo na ochranu osobných údajov. Právo na dôvernosť komunikácie a právo na súkromný a rodinný život sú zaručené aj v článku 8 Európskeho dohovoru o ľudských právach (ďalej len „EDLP“) a sú súčasťou ústavných tradícií spoločných pre členské štáty.<sup>11</sup>
10. EDPB a EDPS pripomínajú, že práva zakotvené v článku 7 a 8 Charty však nie sú absolútnymi právami, ale musia sa posudzovať so zreteľom na ich funkciu v spoločnosti.<sup>12</sup> Sexuálne zneužívanie detí je obzvlášť závažnou a ohavnou trestnou činnosťou a umožnenie účinných opatrení na boj proti nemu je cieľom všeobecného záujmu uznaného Úniou, ktorým je cieľom je ochrana práv a slobôd obetí. Pokiaľ ide o účinné opatrenie na boj proti trestným činom páchaným na maloletých a iných zraniteľných osobách, Súdny dvor Európskej únie (ďalej len „SDEÚ“) poukázal na to, že pozitívne povinnosti môžu vyplývať z článku 7 Charty, v ktorom sa od orgánov verejnej moci vyžaduje, aby prijali právne opatrenia na ochranu súkromného a rodinného života, obydli a komunikácie. Takéto povinnosti môžu vyplývať

---

<sup>10</sup> Pozri napr. Vyhlásenie EDPB o preskúmaní nariadenia o súkromí v elektronických komunikáciách a jeho vplyvu na ochranu jednotlivcovs ohľadom na súkromie a dôvernosť ich komunikácie (25. mája 2018).

<sup>11</sup> Takmer všetky európske ústavy zahŕňajú právo na ochranu dôvernosti komunikácie. Pozri napr. článok 15 ústavy Talianskej republiky; článok 10 základného zákona Spolkovej republiky Nemecko, článok 22 belgickej ústavy; a článok 13 ústavy Holandského kráľovstva.

<sup>12</sup> Pozri okrem iného rozsudok SDEÚ, vec C-311/18, Facebook Ireland a Schrems, bod 172 a tam citovanú judikatúru. Pozri tiež odôvodnenie 4 všeobecného nariadenia o ochrane údajov.



ajz článkov 3 a 4 Charty, pokiaľ ide o ochranu telesnej a duševnej integrity jednotlivca a zákaz mučenia a neľudského a ponižujúceho zaobchádzania.<sup>13</sup>

11. Akékoľvek obmedzenia práv zaručených Chartou, ako sú tie, ktoré sa predpokladajú v návrhu<sup>14</sup>, musia byť zároveň v súlade s požiadavkami stanovenými v článku 52 ods. 1 Charty. Každé opatrenie zasahujúce do práva na dôvernosť komunikácie a práva na súkromný a rodinný život musí v prvom rade rešpektovať podstatu daných práv.<sup>15</sup> Podstata práva je narušená, ak právo stratí svoj základný obsah a jednotlivec ho nemôže uplatniť.<sup>16</sup> Zásah vo vzťahu k sledovanému cieľu nemôže predstavovať neprimeraný a neúnosný zásah, ktorým by bola zasiahnutá samotná podstata takto zaručeného práva.<sup>17</sup> To znamená, že aj základné právo, ktoré nie je absolútnej povahy, ako je právo na dôvernosť komunikácie a právo na ochranu osobných údajov, má niektoré základné prvky, ktoré nesmú byť obmedzené.
12. SDEÚ pri viacerých príležitostiach uplatnil kritérium „podstaty práva“ [essence of the right] v oblasti súkromia elektronických komunikácií. V rozsudku Tele2 Sverige a Watson Súdny dvor rozhodol, že právna úprava, ktorá neumožňuje uchovávanie obsahu komunikácie, nemôže mať nepriaznivý vplyv na podstatu práv na súkromný život a na ochranu osobných údajov.<sup>18</sup> V rozsudku vo veci Schrems Súdny dvor konštatoval, že právnu úpravu umožňujúcu orgánom verejnej moci všeobecný prístup k obsahu elektronických komunikácií treba považovať za právnu úpravu, ktorá zasahuje do podstaty obsahu základného práva na rešpektovanie súkromného života, ako je zaručené článkom 7 Charty.<sup>19</sup> V rozsudku vo veci Digital Rights Ireland a Seitlinger a i. Súdny dvor konštatoval, že hoci uchovávanie údajov požadované smernicou 2006/24 predstavovalo obzvlášť závažný zásah do základného práva na súkromie a ostatných práv stanovených v článku 7 Charty, nemôže mať nepriaznivý vplyv na podstatu týchto práv, keďže smernica neumožňuje získanie vedomostí o obsahu elektronických komunikácií ako takých.<sup>20</sup> Z tejto judikatúry možno vyvodiť, že opatrenia umožňujúce orgánom verejnej moci mať všeobecný prístup k obsahu komunikácie môžu s väčšou pravdepodobnosťou ovplyvniť podstatu práv zaručených v článkoch 7 a 8 Charty. Tieto úvahy sú rovnako relevantné aj v súvislosti s opatreniami na zisťovanie materiálu obsahujúceho sexuálne zneužívanie detí a kontaktovania detí, ako sú tie, ktoré sa predpokladajú v návrhu.
13. SDEÚ okrem toho zistil, že opatrenia v oblasti bezpečnosti údajov zohrávajú kľúčovú úlohu pri zabezpečovaní toho, aby nebola nepriaznivo ovplyvnená podstata základného práva na ochranu osobných údajov uvedeného v článku 8 Charty.<sup>21</sup> Pri zabezpečovaní uplatňovania všetkých základných práv sú v digitálnom veku kľúčové technické riešenia na zabezpečenie a ochranu dôvernosti

---

<sup>13</sup> SDEÚ, spojené veci C-511/18, C-512/18 a C-520/18, La Quadrature du Net a i., body 126 – 128. Pozri aj stanovisko EDPS 7/2020 k návrhu dočasných výnimiek zo smernice 2002/58/ES na účely boja proti sexuálnemu zneužívaniu detí online (10. novembra 2020) bod 12.

<sup>14</sup> Pozri COM(2022)209 final, s. 12 – 13.

<sup>15</sup> Článok 52 ods. 1 Charty.

<sup>16</sup> Pozri Usmernenia EDPS o posudzovaní primeranosti opatrení, ktoré obmedzujú základné práva na súkromie a na ochranu osobných údajov (19. decembra 2019), s. 8. Dostupné na: [https://edps.europa.eu/sites/default/files/publication/19-12-19\\_edps\\_proportionality\\_guidelines2\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf).

<sup>17</sup> SDEÚ, vec C-393/19, OM, bod 53.

<sup>18</sup> SDEÚ, spojené veci C-203/15 a C-698/15, Tele2 Sverige a Watson, bod 101.

<sup>19</sup> SDEÚ, vec C-362/14, Schrems, bod 94.

<sup>20</sup> SDEÚ, spojené veci C-293/12 a C-594/12, Digital Rights Ireland a Seitlinger a i., bod 39.

<sup>21</sup> Tamže, bod 40.

elektronických komunikácií vrátane opatrení na šifrovanie.<sup>22</sup> Toto je potrebné náležite zohľadniť pri posudzovaní opatrení na povinné zisťovanie materiálu obsahujúceho sexuálne zneužívanie detí alebo kontaktovania detí, najmä ak by viedli k oslabeniu alebo zhoršeniu šifrovania.<sup>23</sup>

14. V článku 52 ods. 1 Charty sa tiež stanovuje, že akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto Charte musí byť ustanovené zákonom [law]. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.<sup>24</sup> Na splnenie požiadavky proporcionality sa musia v právnej úprave stanoviť jasné a presné pravidlá upravujúce rozsah a uplatňovanie predmetných opatrení a stanoviť minimálne záruky, aby osoby, ktorých osobné údaje sú dotknuté, mali dostatočné záruky, že ich údaje budú účinne chránené pred rizikom zneužitia.<sup>25</sup> Táto právna úprava musí vymedziť okolnosti a podmienky, za akých možno prijať opatrenie upravujúce spracúvanie takýchto údajov, čím zaručí, aby zásah nešiel nad rámec toho, čo je striktné nevyhnutné.<sup>26</sup> Ako objasnil SDEÚ, potreba takýchto záruk je o to väčšia, ak sa osobné údaje spracúvajú automatizovaným spôsobom a ak ide o ochranu konkrétnej kategórie osobných údajov, ktoré sú citlivými údajmi.<sup>27</sup>
15. Návrhom by sa obmedzil výkon práv a povinností stanovených v článku 5 ods. 1 a 3 a článku 6 ods. 1 smernice 2002/58/ES („smernica o súkromí a elektronických komunikáciách“)<sup>28</sup>, pokiaľ je to potrebné na vykonanie príkazov na zistenie vydaných v súlade s kapitolou 1 oddielom 2 návrhu. EDPB a EDPS sa preto domnievajú, že návrh je potrebné posúdiť nielen z hľadiska Charty a všeobecného nariadenia o ochrane údajov, ale aj z hľadiska článkov 5, 6 a článku 15 ods. 1 smernice o súkromí a elektronických komunikáciách.

---

<sup>22</sup> Pozri rezolúciu Rady pre ľudské práva č. 47/16 o presadzovaní, ochrane a uplatňovaní ľudských práv na internete, dokument OSNA/HRC/RES/47/16 (26. júla 2021).

<sup>23</sup> Pozri aj odôvodnenie 25 dočasného nariadenia.

<sup>24</sup> Pozri „Posúdenie nevyhnutnosti opatrení, ktoré obmedzujú základné právo na ochranu osobných údajov: Súbor nástrojov“, 11. apríla 2019, dostupné na: [https://edps.europa.eu/sites/default/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf).

<sup>25</sup> SDEÚ, spojené veci C-511/18, C-512/18 a C-520/18, La Quadrature du Net a i., bod 132.

<sup>26</sup> Tamže.

<sup>27</sup> Tamže.

<sup>28</sup> Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávanía osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zmenená smernicou 2006/24/ES a smernicou 2009/136/ES.

## 4. KONKRÉTNE PRIPOMIENKY

### 4.1 Vzťah k existujúcim právnym predpisom

#### 4.1.1 Vzťah kvšeobecnému nariadeniu o ochrane údajov a smernici o súkromí a elektronických komunikáciách

16. V návrhu sa uvádza, že ním nie sú dotknuté pravidlá vyplývajúce z iných aktov Únie, najmä zo všeobecného nariadenia o ochrane údajov<sup>29</sup> a zo smernice o súkromí a elektronických komunikáciách. Na rozdiel od dočasného nariadenia sa v návrhu nestanovuje výslovná dočasná výnimka, ale obmedzenie výkonu práv a povinností stanovených v článku 5 ods. 1, článku 5 ods. 3 a článku 6 ods. 1 smernice o súkromí a elektronických komunikáciách. Ďalej treba poznamenať, že v dočasnom nariadení sa stanovuje výnimka výlučne z ustanovení článku 5 ods. 1 a článku 6 ods. 1, a nie z článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.
17. V návrhu sa ďalej odkazuje na článok 15 ods. 1 smernice o súkromí a elektronických komunikáciách, ktorým sa umožňuje členským štátom prijať legislatívne opatrenia na obmedzenie rozsahu práv a povinností špecifikovaných v článkoch 5 a 6 uvedenej smernice, ak takéto obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti okrem iného na zabránenie trestným činom, ich vyšetrovanie, zisťovanie a stíhanie. Podľa návrhu sa článok 15 ods. 1 smernice o súkromí a elektronických komunikáciách uplatňuje analogicky, ak návrh obmedzuje výkon práv a povinností stanovených v článku 5 ods. 1, článku 5 ods. 3 a článku 6 ods. 1 smernice o súkromí a elektronických komunikáciách.
18. EDPB a EDPS pripomínajú, že SDEÚ jasne uviedol, že článok 15 ods. 1 smernice o súkromí a elektronických komunikáciách sa má vykladať reštriktívne, čo znamená, že výnimka zo zásady dôvernosti komunikácie, ktorú umožňuje článok 15 ods. 1, musí zostať výnimkou a nesmie sa stať pravidlom.<sup>30</sup> Ako sa uvádza v tomto spoločnom stanovisku, EDPB a EDPS sa domnievajú, že návrh nespĺňa požiadavky (prísnej) nevyhnutnosti, účinnosti a primeranosti. EDPB a EDPS okrem toho dospeli k záveru, že návrh by znamenal, že zásah do dôvernosti komunikácie by sa v skutočnosti mohol stať pravidlom, a nezostal by výnimkou.

#### 4.1.2 Vzťah k nariadeniu (EÚ) 2021/1232 a vplyv na dobrovoľné odhaľovanie online sexuálneho zneužívania detí

19. Podľa článku 88 návrhu by sa týmto nariadením zrušilo dočasné nariadenie, v ktorom sa stanovuje dočasná výnimka z určitých ustanovení smernice o súkromí a elektronických komunikáciách s cieľom umožniť dobrovoľné používanie technológií na odhaľovanie materiálu obsahujúceho sexuálne zneužívanie detí a kontaktovania detí poskytovateľmi interpersonálnych komunikačných služieb nezávislých od číslovania. Od dátumu začatia uplatňovania navrhovaného nariadenia by teda neexistovala žiadna výnimka zo smernice o súkromí a elektronických komunikáciách, ktorá by umožňovala dobrovoľné odhaľovanie online sexuálneho zneužívania detí takýmito poskytovateľmi.

---

<sup>29</sup> 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) (Text s významom pre EHP) (Ú. v. EÚ L 119, 4.5.2016, s. 1–88).

<sup>30</sup> Rozsudok z 21. decembra 2016, spojené veci C-203/15 a C-698/15, Tele2 Sverige AB a Watson, bod 89.

20. Vzhľadom na to, že povinnosti zisťovania zavedené v návrhu by sa vzťahovali len na príjemcov príkazov na zisťovanie, bolo by dôležité v znení navrhovaného nariadenia jasne uviesť, že dobrovoľné používanie technológií na odhaľovanie materiálu obsahujúceho sexuálne zneužívanie detí a kontaktovania detí zostáva povolené len v rozsahu povolenom podľa smernice o súkromí a elektronických komunikáciách a všeobecného nariadenia o ochrane údajov. Znamenalo by to napríklad, že poskytovateľom interpersonálnych komunikačných služieb nezávislých od číslovania by sa zabránilo používať takéto technológie na dobrovoľnom základe, pokiaľ by to nebolo povolené podľa vnútroštátnych právnych predpisov, ktorými sa transponuje smernica o súkromí a elektronických komunikáciách, v súlade s článkom 15 ods. 1 smernice o súkromí a elektronických komunikáciách a Chartou.
21. Vo všeobecnosti by navrhovanému nariadeniu prospela väčšia jasnosť, pokiaľ ide o status dobrovoľného zisťovania online sexuálneho zneužívania detí po dátume začatia uplatňovania navrhovaného nariadenia, a prechod od režimu dobrovoľného zisťovania stanoveného v dočasnom nariadení k povinnostiam zisťovania stanoveným v navrhovanom nariadení. EDPB a EDPS napríklad odporúčajú objasniť, že navrhované nariadenie by neposkytovalo právny základ pre spracúvanie osobných údajov výlučne na účely dobrovoľného zisťovania online sexuálneho zneužívania detí.

#### 4.2 Právny základ podľa všeobecného nariadenia o ochrane údajov

22. Cieľom návrhu je stanoviť právny základ v zmysle všeobecného nariadenia o ochrane údajov pre spracúvanie osobných údajov na účely odhaľovania materiálu obsahujúceho sexuálne zneužívanie detí a groomingu. V dôvodovej správe sa preto uvádza: „Pokiaľ ide o činnosti týkajúce sa povinného zisťovania, ktoré zahŕňajú spracúvanie osobných údajov, návrhom sa najmä v prípade príkazov na zistenie vydávaných na jeho základe, sa tak stanovuje dôvod na takéto spracúvanie uvedený v článku 6 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov, v ktorom sa stanovuje spracúvanie osobných údajov nevyhnutné na splnenie právnej povinnosti podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha.“<sup>31</sup>
23. EDPB a EDPS vítajú rozhodnutie Komisie odstrániť právnu neistotu, pokiaľ ide o právny základ spracúvania osobných údajov, ktorá vznikla na základe dočasného nariadenia. EDPB a EDPS takisto súhlasia so záverom Komisie, že dôsledky zavedenia opatrení na zisťovanie sú príliš ďalekosiahle a závažné na to, aby sa rozhodnutie o tom, či vykonať takéto opatrenia, ponechalo na poskytovateľov služieb.<sup>32</sup> EDPB a EDPS zároveň poznamenávajú, že akýkoľvek právny základ, ktorý poskytovateľom služieb ukladá povinnosť zasahovať do základných práv na ochranu údajov a súkromia, bude platný len vtedy, ak je v súlade s podmienkami stanovenými v článku 52 ods. 1 Charty, ako sa analyzuje v ďalšom texte.

#### 4.3 Povinnosti týkajúce sa posudzovania a zmierňovania rizík

24. Podľa kapitoly II oddielu 1 návrhu sa od poskytovateľov hostingových služieb a poskytovateľov interpersonálnych komunikačných služieb vyžaduje, aby v prípade každej takejto služby, ktorú ponúkajú, identifikovali, analyzovali a posúdili riziko využívania služby na účely online sexuálneho zneužívania detí a potom sa pokúsili minimalizovať zistené riziko uplatnením „primeraných zmierňujúcich opatrení prispôsobených identifikovanému riziku“.

---

<sup>31</sup> Tamže, s. 4.

<sup>32</sup> Pozri návrh, COM(2022) 209 final, s. 14.

25. EDPB a EDPS poznamenávajú, že pri vykonávaní posúdenia rizika by mal poskytovateľ zohľadniť najmä prvky uvedené v článku 3 ods. 2 písm. a) až e) návrhu vrátane: zákazov a obmedzení stanovených v obchodných podmienkach; spôsobu, akým používatelia využívajú službu, a jeho vplyv na toto riziko; spôsobu, akým poskytovateľ navrhol a prevádzkuje službu vrátane obchodného modelu, správy a príslušných systémov a procesov, ako aj jeho vplyv na toto riziko. Pokiaľ ide o riziko kontaktovania detí, navrhované prvky, ktoré treba zvážiť sú: rozsah, v akom službu využívajú alebo pravdepodobne využívajú deti; vekové skupiny a riziko kontaktovania podľa vekovej skupiny; dostupnosť funkcií umožňujúcich vyhľadávanie používateľov, funkcie umožňujúcich používateľom nadviazať priamy kontakt s inými používateľmi, najmä prostredníctvom súkromnej komunikácie a funkcie umožňujúcich používateľom vymieňať si snímky alebo videá s inými používateľmi.
26. Hoci EDPB a EDPS uznávajú, že tieto kritériá sa zdajú byť relevantné, napriek tomu sa obávajú, že takéto kritériá ponechávajú pomerne široký priestor na výklad a posúdenie. Niekoľko kritérií je opísaných príliš všeobecne (napr. „spôsob, akým používatelia využívajú službu, a jeho vplyv na toto riziko“) alebo sa týkajú základných funkcií, ktoré sú spoločné pre mnohé online služby (napr. „umožňujú používateľom vymieňať si snímky alebo videá s inými používateľmi“). Tieto kritériá ako také podľa všetkého môžu viesť k subjektívnemu (a nie objektívnemu) posúdeniu.
27. Podľa názoru EDPB a EDPS to isté platí aj pre opatrenia na zmiernenie rizika, ktoré sa majú prijať podľa článku 4 návrhu. Opatrenia, ako je prispôbenie moderovania obsahu alebo odporúčacích systémov poskytovateľa prostredníctvom vhodných technických a prevádzkových opatrení a personálu, sú podľa všetkého relevantné pri znižovaní identifikovaného rizika. Ak sa však tieto kritériá uplatňujú v rámci komplexného procesu posudzovania rizika a v kombinácii s abstraktnými a vágnymi výrazmi opisujúcimi prijateľnú mieru rizika (napr. „v značnej miere“), nespĺňajú kritériá právnej istoty a predvídateľnosti potrebné na odôvodnenie zásahu do dôvernosti komunikácie medzi súkromnými osobami, čo predstavuje jasný zásah do základných práv na súkromie a slobodu prejavu.
28. Hoci poskytovatelia nie sú oprávnení zasahovať do dôvernosti komunikácie v rámci svojich stratégií posudzovania rizika a zmierňovania rizika pred prijatím príkazu na zistenie, existuje priame prepojenie medzi povinnosťami posudzovania a zmierňovania rizika a následnými povinnosťami týkajúcimi sa zisťovania. Podľa článku 7 ods. 4 návrhu závisí vydanie príkazu na zistenie od existencie dôkazov o významnom riziku, že by sa relevantná služba mohla využívať na účely online sexuálneho zneužívania detí. Pred vydaním príkazu na zistenie sa musí dodržať zložitý proces zahŕňajúci poskytovateľov, koordinačný orgán a súdny alebo iný nezávislý správny orgán zodpovedný za vydanie príkazu. Po prvé, poskytovatelia musia posúdiť riziko využívania svojich služieb na účely online sexuálneho zneužívania detí (článok 3 návrhu) a vyhodnotiť možné opatrenia na zmiernenie rizika (článok 4 návrhu) na zníženie tohto rizika. Výsledky tohto postupu sa potom oznámia príslušnému koordinačnému orgánu (článok 5 návrhu). Ak z posúdenia rizika vyplynie, že napriek úsiliu o jeho zmiernenie pretrváva významné riziko, koordinačný orgán vypočuje poskytovateľa v súvislosti s návrhom žiadosti o vydanie príkazu na zistenie a poskytne poskytovateľovi možnosť predložiť pripomienky. Poskytovateľ je ďalej povinný predložiť plán vykonávania vrátane stanoviska príslušného orgánu na ochranu údajov v prípade zistenia groomingu. Ak sa koordinačný orgán vecou zaoberá, požiada o príkaz na zistenie, ktorý vydá súd alebo iný nezávislý správny orgán. Preto počiatočné posúdenie rizika a opatrenia zvolené na zníženie zisteného rizika sú rozhodujúcim základom pre posúdenie koordinačného orgánu, ako aj príslušného súdneho alebo správneho orgánu, pokiaľ ide o to, či je príkaz na zistenie potrebný.
29. EDPB a EDPS berú na vedomie zložité kroky vedúce k vydaniu príkazu na zistenie, ktoré zahŕňajú počiatočné posúdenie rizika zo strany poskytovateľa a jeho návrh opatrení na zmiernenie rizika, ako aj ďalšiu interakciu poskytovateľa s príslušným koordinačným orgánom. EDPB a EDPS sa domnievajú, že poskytovateľ má značnú možnosť ovplyvniť výsledok tohto procesu. EDPB a EDPS v tejto súvislosti

poznávajú, že v odôvodnení 17 návrhu sa stanovuje, že poskytovatelia by mali byť schopní v rámci podávania správ o rizikách „uviesť ochotu a pripravenosť“ prijať v prípade potreby príkaz na zistenie. Preto nemožno predpokladať, že každý poskytovateľ sa bude snažiť vyhnúť vydaniu príkazu na zistenie s cieľom zachovať dôvernosť komunikácie svojich používateľov uplatňovaním najúčinnjších, ale najmenej rušivých zmierňujúcich opatrení, najmä ak takéto zmierňujúce opatrenia zasahujú do slobody poskytovateľa podnikat' podľa článku 16 Charty.

30. EDPS a EDPB by chceli zdôrazniť, že procesné záruky nikdy nemôžu v plnej miere nahradiť hmotnoprávne záruky. Zložitý proces vedúci k možnému vydaniu príkazu na zistenie, ktorý je opísaný vyššie, by preto mal byť sprevádzaný jasnými hmotnoprávnymi povinnosťami. EDPB a EDPS sa domnievajú, že v návrhu nie je jasných niekoľko kľúčových prvkov (napr. pojmy „významné riziko“, „v značnej miere“ atď.), čo nemožno napraviť prítomnosťou viacerých vrstiev procesných záruk. Je to ešte dôležitejšie vzhľadom na skutočnosť, že subjekty zodpovedné za uplatňovanie týchto záruk (napr. poskytovatelia, súdne orgány atď.) majú široký priestor na voľnú úvahu, pokiaľ ide o to, ako dané práva vyvážiť v každom jednotlivom prípade. Vzhľadom na rozsiahle zásahy do základných práv, ktoré by vyplynuli z prijatia návrhu, by zákonodarca mal zabezpečiť, aby bol návrh jednoznačnejší, pokiaľ ide o to, kedy a kde sú takéto zásahy povolené. Hoci EDPB a EDPS uznávajú, že legislatívne opatrenia nemôžu byť príliš normatívne a musia ponechať určitú flexibilitu pri ich praktickom uplatňovaní, domnievajú sa, že súčasné znenie návrhu ponecháva príliš veľký priestor na potenciálne zneužívanie z dôvodu neexistencie jasných hmotnoprávných noriem.
31. Vzhľadom na potenciálny významný vplyv na veľmi veľký počet dotknutých osôb (t. j. potenciálne na všetkých používateľov interpersonálnych komunikačných služieb), EDPB a EDPS zdôrazňujú potrebu vysokej úrovne právnej istoty, jasnosti a predvídateľnosti právnych predpisov s cieľom zabezpečiť, aby navrhované opatrenia boli skutočne účinné pri dosahovaní cieľa, ktorý sledujú, a zároveň čo najmenej poškodzovali dotknuté základné práva.

#### 4.4 Podmienky vydávania príkazov na zistenie

32. V článku 7 návrhu sa stanovuje, že koordinačný orgán v krajine usadenia má právomoc požiadať príslušný súdny orgán členského štátu, alebo iný nezávislý správny orgán tohto členského štátu, aby vydal príkaz na zistenie, na základe ktorého sa od poskytovateľa hostingových služieb alebo poskytovateľa interpersonálnych komunikačných služieb, na ktorého sa vzťahuje právomoc daného členského štátu, vyžaduje prijatie opatrení uvedených v článku 10 na zistenie online sexuálneho zneužívania detí v rámci konkrétnej služby.
33. EDPB a EDPS náležite zohľadňujú tieto prvky, ktoré je potrebné splniť pred vydaním príkazu na zistenie:
- existujú dôkazy o významnom riziku, že služba sa použije na účely online sexuálneho zneužívania detí v zmysle článku 7 ods. 5, 6 alebo 7, podľa toho, ktorý je uplatniteľný;
  - dôvody vydania príkazu na zistenie prevažujú nad negatívnymi dôsledkami pre práva a oprávnené záujmy všetkých dotknutých strán, najmä so zreteľom na potrebu zabezpečiť spravodlivú rovnováhu medzi základnými právami týchto strán.
34. Význam významného rizika je špecifikovaný v ods. 5 a nasl. článku 7, v závislosti od druhu predmetného príkazu na zistenie. Významné riziko sa v prípade príkazov na zistenie týkajúcich sa šírenia známeho materiálu obsahujúceho sexuálne zneužívanie detí predpokladá, ak sú splnené tieto podmienky:

- a. napriek akýmkoľvek zmiernujúcim opatreniam, ktoré poskytovateľ mohol prijať alebo prijme, sa služba pravdepodobne v značnej miere využíva na šírenie známeho materiálu obsahujúceho sexuálne zneužívanie detí; a
  - b. existujú dôkazy o tom, že táto služba alebo porovnateľná služba, ak táto služba ešte nebola v Únii ponúkaná k dátumu žiadosti o vydanie príkazu na zistenie, sa za posledných 12 mesiacov v značnej miere využívala na šírenie známeho materiálu obsahujúceho sexuálne zneužívanie detí.
35. Aby bolo možné vydať príkaz na zistenie neznámeho materiálu obsahujúceho sexuálne zneužívanie detí, musí sa pravdepodobnosť a faktické dôkazy vzťahovať na neznámy materiál obsahujúci sexuálne zneužívanie detí a musí byť vydaný predbežný príkaz na zistenie pre známy materiál obsahujúci sexuálne zneužívanie detí, ktorý viedol k významnému počtu oznámení poskytovateľom súvisiacich so známym materiálom obsahujúcim sexuálne zneužívanie detí (článok 7 ods. 6 návrhu). V prípade príkazu na zisťovanie groomingu sa významné riziko považuje za existujúce, ak sa poskytovateľ považuje za poskytovateľa interpersonálnych komunikačných služieb, služba sa pravdepodobne v značnej miere využíva na kontaktovanie detí, a existujú dôkazy o tom, že služba bola v značnej miere využitá na kontaktovanie detí (článok 7 ods. 7 návrhu).
36. EDPB a EDPS poznamenávajú, že aj napriek špecifikáciám v článku 7 ods. 5 až 7 návrhu prevládajú v podmienkach vydania príkazu na zistenie nejasné právne pojmy, ako napríklad „v značnej miere“, „významný počet“, a čiastočne sa opakujú, keďže dôkazy o predchádzajúcom zneužívaní často prispievajú k stanoveniu pravdepodobnosti budúceho zneužívania.
37. V návrhu sa predpokladá systém, v rámci ktorého sa pri rozhodovaní o tom, či je príkaz na zistenie potrebný, musí prijať predbežné rozhodnutie o budúcom využívaní služby na účely online sexuálneho zneužívania detí. Je preto pochopiteľné, že prvky uvedené v článku 7 majú charakter prognózy. Použitie vágnych pojmov v návrhu však sťažuje poskytovateľom, ako aj príslušnému súdnemu alebo inému splnomocnenému nezávislému správnomu orgánu uplatňovanie právnych požiadaviek zavedených v návrhu predvídateľným a nesvojvoľným spôsobom. EDPB a EDPS sa obávajú, že tieto všeobecné a nejasné pojmy povedú k nedostatočnej právnej istote a k značným rozdielom v konkrétnom vykonávaní návrhu v rámci Únie v závislosti od výkladu pojmov, ako sú „pravdepodobnosť“ a „v značnej miere“ zo strany súdnych alebo iných nezávislých správnych orgánov v členských štátoch. Takýto výsledok by nebol prijateľný vzhľadom na skutočnosť, že ustanovenia o príkazoch na zistenie pre poskytovateľov interpersonálnych komunikačných služieb budú predstavovať „obmedzenia“ zásady dôvernosti komunikácie stanovenej v článku 5 smernice o súkromí a elektronických komunikáciách a ich jasnosť a predvídateľnosť sú preto mimoriadne dôležité na zabezpečenie jednotného uplatňovania týchto obmedzení v celej Únii.

#### 4.5 Analýza nevyhnutnosti a primeranosti plánovaných opatrení<sup>33</sup>

38. Ako už bolo uvedené, je možné vydať tri druhy príkazov na zistenie: príkazy na zistenie týkajúce sa šírenia známeho materiálu obsahujúceho sexuálne zneužívanie detí (článok 7 ods. 5 návrhu), príkazy na zistenie týkajúce sa šírenia nového materiálu obsahujúceho sexuálne zneužívanie detí (článok 7 ods. 6 návrhu) a príkazy na zistenie týkajúce sa kontaktovania detí (článok 7 ods. 7 návrhu). Každý príkaz na zistenie by si zvyčajne vyžadoval inú technológiu na jeho praktické vykonávanie. V dôsledku

---

<sup>33</sup> Pozri tiež „Stručnú príručku EDPS k nevyhnutnosti a primeranosti“, dostupná na: [https://edps.europa.eu/sites/default/files/publication/20-01-28\\_edps\\_quickguide\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf).

toho majú rôznu úroveň rušivého vplyvu, a teda rôzny vplyv na práva na súkromie a ochranu osobných údajov.

39. Technológie na odhaľovanie známeho materiálu obsahujúceho sexuálne zneužívanie detí sú zvyčajne porovnávacie technológie v tom zmysle, že sa spoliehajú na existujúcu databázu známych materiálov obsahujúcich sexuálne zneužívanie detí, s ktorou môžu porovnávať obrázky (vrátane snímok z videí). Aby sa umožnilo porovnanie, obrázky, ktoré poskytovateľ spracúva, ako aj obrázky v databáze musia byť digitálne, zvyčajne sa to deje ich konverziou na hašovacie hodnoty. Tento druh technológie hašovania má odhadovanú mieru falošných pozitívnych výsledkov maximálne 1 z 50 miliárd (t. j. 0,000000002 % miera falošných pozitívnych výsledkov).<sup>34</sup>
40. Na zisťovanie nového materiálu obsahujúceho sexuálne zneužívanie detí sa zvyčajne používa iný typ technológie vrátane klasifikátorov a umelej inteligencie.<sup>35</sup> Ich chybovosť je však vo všeobecnosti výrazne vyššia. V správe o posúdení vplyvu sa napríklad uvádza, že existujú technológie na zisťovanie nového materiálu obsahujúceho sexuálne zneužívanie detí, ktorých miera presnosti môže byť stanovená na 99,9 % (t. j. 0,1 % miery falošných pozitívnych výsledkov), ale s touto mierou presnosti sú schopné identifikovať v príslušnom súbore údajov len 80 % celkového materiálu obsahujúceho sexuálne zneužívanie detí.<sup>36</sup>
41. Pokiaľ ide o zisťovanie kontaktovania detí v textovej komunikácii, v správe o posúdení vplyvu sa vysvetľuje, že sa to zvyčajne zakladá na rozpoznávaní vzorcov. V správe o posúdení vplyvu sa uvádza, že niektoré z existujúcich technológií na zisťovanie groomingu majú „mieru presnosti“ 88 %.<sup>37</sup> Podľa Komisie to znamená, že „zo 100 rozhovorov, ktoré boli označené ako možné kriminálne kontaktovanie detí, môže byť 12 vylúčených po preskúmaní [podľa návrhu zo strany centra EÚ] a nebudú sa oznamovať orgánom presadzovania práva“.<sup>38</sup> Hoci by sa mal návrh na rozdiel od dočasného nariadenia vzťahovať aj na zvukovú komunikáciu, v správe o posúdení vplyvu sa neuvádzajú technologické riešenia, ktoré by sa mohli použiť na zisťovanie groomingu v takomto kontexte.

#### 4.5.1 Účinnosť zisťovania

42. Nevyhnutnosť znamená potrebu posúdenia účinnosti plánovaných opatrení na dosiahnutie sledovaného cieľa na základe faktických skutočností a toho, či sú menej rušivé než iné možnosti na dosiahnutie toho istého cieľa.<sup>39</sup> Ďalším faktorom, ktorý treba zohľadniť pri posudzovaní primeranosti navrhovaného opatrenia, je účinnosť existujúcich opatrení nad rámec navrhovaného opatrenia.<sup>40</sup> Ak už existujú opatrenia na rovnaký alebo podobný účel, ich účinnosť by sa mala posúdiť v rámci posúdenia proporcionality. Bez takéhoto posúdenia účinnosti existujúcich opatrení sledujúcich

---

<sup>34</sup> Pozri Európska komisia, pracovný dokument útvarov Komisie, Správa o posúdení vplyvu – Sprievodný dokument k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu, SWD(2022) 209 final [ďalej len „správa o posúdení vplyvu“ alebo „SWD(2022) 209 final“], s. 281, poznámka pod čiarou 511.

<sup>35</sup> Správa o posúdení vplyvu, s. 281.

<sup>36</sup> Tamže, s. 282.

<sup>37</sup> Tamže, s. 283.

<sup>38</sup> Návrh, COM(2022)209 final, s. 14., poznámka pod čiarou 32.

<sup>39</sup> EDPS, Posúdenie nevyhnutnosti opatrení, ktoré obmedzujú základné právo na ochranu osobných údajov: Súbor nástrojov, 11. apríla 2017, s. 5; Usmernenia EDPS o posudzovaní primeranosti opatrení, ktoré obmedzujú základné práva na súkromie a na ochranu osobných údajov (19. decembra 2019), s. 8.

<sup>40</sup> EDPS, Usmernenia EDPS o posudzovaní primeranosti opatrení, ktoré obmedzujú základné práva na súkromie a na ochranu osobných údajov (19. decembra 2019), s. 11.



rovnaký alebo podobný účel nemožno test proporcionality nového opatrenia považovať za riadne vykonaný.

43. Zisťovanie materiálu obsahujúceho sexuálne zneužívanie detí alebo groomingu poskytovateľmi hostingových služieb a poskytovateľmi interpersonálnych komunikačných služieb môže prispieť k celkovému cieľu, ktorým je predchádzanie sexuálnemu zneužívaniu detí a online šíreniu materiálu obsahujúceho sexuálne zneužívanie detí a boj proti nim. V tomto kontexte, pri potrebe posúdiť účinnosť opatrení stanovených v návrhu zároveň vznikajú tri kľúčové otázky:
  - Možno opatrenia na zisťovanie online sexuálneho zneužívania detí ľahko obísť?
  - Aký vplyv budú mať činnosti zisťovania na opatrenia prijímané orgánmi presadzovania práva?<sup>41</sup>
  - Ako by mohol návrh znížiť právnu neistotu?
44. Nie je úlohou EDPB a EDPS podrobne odpovedať na tieto otázky. EDPB a EDPS však poznamenávajú, že ani v správe o posúdení vplyvu, ani v návrhu sa tieto otázky v plnej miere neriešia.
45. Pokiaľ ide o možnosť obchádzania zisťovania materiálu obsahujúceho sexuálne zneužívanie detí, treba poznamenať, že v súčasnosti sa zdá, že neexistuje žiadne technologické riešenie na zisťovanie materiálu obsahujúceho sexuálne zneužívanie detí, ktorý je poskytovaný v zašifrovanej forme. Akúkoľvek činnosť zisťovania – dokonca aj skenovanie na strane klienta zamerané na obchádzanie šifrovania medzi koncovými bodmi, ktoré ponúka poskytovateľ<sup>42</sup> – preto možno ľahko obísť šifrovaním obsahu pomocou samostatnej aplikácie pred jeho odoslaním alebo nahraním. Opatrenia na zisťovanie uvedené v návrhu by preto mohli mať menší vplyv na šírenie materiálu obsahujúceho sexuálne zneužívanie detí na internete, než by sa dalo očakávať.
46. Komisia ďalej očakáva vzhľadom na prijatie povinností týkajúcich sa zisťovania, ktoré sa zavádzajú v návrhu, zvýšenie počtu oznámení o sexuálnom zneužívaní detí orgánom presadzovania práva.<sup>43</sup> V návrhu ani v správe o posúdení vplyvu sa však nevysvetľuje, ako sa tým vyriešia nedostatky súčasného stavu. Vzhľadom na obmedzené zdroje orgánov presadzovania práva sa zdá byť potrebné lepšie pochopiť, či by zvýšenie počtu oznámení malo významný vplyv na činnosti presadzovania práva v boji proti sexuálnemu zneužívaniu detí. EDPB a EDPS by v každom prípade chceli zdôrazniť, že takéto oznámenia by sa mali posudzovať včas, aby sa zabezpečilo, že rozhodnutie o trestnoprávnej relevantnosti oznámeného materiálu sa prijme čo najskôr, a aby sa čo najviac obmedzilo uchovávanie nerelevantných údajov.

#### 4.5.2 Žiadne menej rušivé opatrenie

47. Za predpokladu, že by sa mohli prejaviť pozitívne účinky odhaľovania materiálu obsahujúceho sexuálne zneužívanie detí a groomingu, ktoré predpokladá Komisia, zisťovanie musí byť najmenej rušivým opatrením spomedzi rovnako účinných opatrení. V článku 4 návrhu sa stanovuje, že ako prvý krok by poskytovatelia mali zvážiť prijatie zmierňujúcich opatrení na zníženie rizika využívania ich služieb na účely online sexuálneho zneužívania detí pod úroveň, ktorá oprávňuje na vydanie príkazu

---

<sup>41</sup> Podľa správy o posúdení vplyvu, príloha II, s. 132, 85,71 % respondentov z prieskumu orgánov presadzovania práva vyjadrilo obavy v súvislosti so zvýšeným objemom materiálu obsahujúceho sexuálne zneužívanie detí v poslednom desaťročí a nedostatkom zdrojov (t. j. ľudských, technických).

<sup>42</sup> Pozri oddiel 4.10 ďalej.

<sup>43</sup> Pozri okrem iného správu o posúdení vplyvu, príloha 3, SWD(2022)209 final, s. 176.

na zistenie. Ak existujú zmiernujúce opatrenia, ktoré by mohli viesť k podstatnému zníženiu množstva groomingu alebo materiálu obsahujúceho sexuálne zneužívanie detí, ktorý sa vymieňa v rámci príslušnej služby, tieto opatrenia by často predstavovali menej rušivé opatrenia v porovnaní s príkazom na zistenie.<sup>44</sup> Preto ak príslušný poskytovateľ neprijme takéto opatrenia dobrovoľne, príslušný nezávislý správny orgán alebo súdny orgán by mal mať možnosť namiesto vydania príkazu na zistenie stanoviť povinné a vymáhateľné vykonávanie zmiernujúcich opatrení. Podľa názoru EDPB a EDPS skutočnosť, že článok 5 ods. 4 návrhu umožňuje koordináčnemu orgánu „požadovať“ od poskytovateľa, aby zaviedol, preskúmal, zrušil prípadne rozšíril zmiernujúce opatrenia, nie je dostatočná, keďže takáto požiadavka by nebola nezávisle vymožitelná; nedodržanie by sa „sankcionovalo“ len nariadením príkazu na zistenie.

48. EDPB a EDPS sa preto domnievajú, že koordináčny orgán alebo príslušný nezávislý správny alebo súdny orgán by mali mať výslovnú právomoc ukladať menej rušivé zmiernujúce opatrenia pred vydaním príkazu na zistenie alebo namiesto neho.

#### 4.5.3 Proporcionalita v užšom zmysle

49. Na to, aby opatrenie rešpektovalo zásadu proporcionality zakotvenú v článku 52 ods. 1 Charty, výhody vyplývajúce z opatrenia by nemali byť prevážené nevýhodami, ktoré opatrenie spôsobuje, pokiaľ ide o výkon základných práv. Zásada proporcionality preto „obmedzuje orgány pri výkone ich právomocí tým, že vyžaduje, aby prostriedky boli primerané na dosiahnutie cieľov a nešli nad rámec toho, čo je potrebné na ich dosiahnutie (alebo dosiahnutie výsledku)“.<sup>45</sup>
50. Na to, aby bolo možné posúdiť vplyv opatrenia na základné práva na súkromie a ochranu osobných údajov, je mimoriadne dôležité presne určiť:<sup>46</sup>
- **rozsah pôsobnosti opatrenia** vrátane počtu dotknutých osôb a toho, či pri ňom dochádza k „vedľajším narušeniam súkromia“ (t. j. zasahovanie do súkromia iných osôb ako subjektov opatrenia);
  - **rozsah opatrenia** vrátane množstva zhromaždených informácií; na ako dlho; či si skúmané opatrenie vyžaduje zber a spracúvanie osobitných kategórií údajov;
  - **úroveň rušivého vplyvu** s prihliadnutím na: povahu činnosti, ktorá je predmetom opatrenia (či má vplyv na činnosti, na ktoré sa vzťahuje povinnosť dôvernosti, alebo nie, vzťah medzi advokátom a klientom; lekárska činnosť); kontext; či ide o profilovanie dotknutých osôb, alebo nie; či spracúvanie zahŕňa použitie (čiastočne alebo úplne) automatizovaného systému rozhodovania s „chybovou odchýlkou“;

---

<sup>44</sup> Mohli by sa napríklad zväziť opatrenia, ako je blokovanie poskytovania materiálu obsahujúceho sexuálne zneužívanie detí na strane klienta tým, že sa zabráni nahrávaniu a odosielaniu obsahu elektronickej komunikácie, keďže by to za určitých okolností mohlo pomôcť zabrániť obehu známeho materiálu obsahujúceho sexuálne zneužívanie detí.

<sup>45</sup> Pozri vec C-343/09, Afton Chemical, bod 45; spojené veci C-92/09 a C-93/09, Volker und Markus Schecke a Hartmut Eifert, bod 74; veci C-581/10 a C-629/10, Nelson a i. bod 71; vec C-283/11, Sky Österreich, bod 50; a vec C-101/12, Schaible, bod 29. Pozri aj EDPS, Posúdenie nevyhnutnosti opatrení, ktoré obmedzujú základné právo na ochranu osobných údajov: Súbor nástrojov (11. apríla 2017).

<sup>46</sup> EDPS, Usmernenia o posudzovaní primeranosti opatrení, ktoré obmedzujú základné práva na súkromie a na ochranu osobných údajov (19. decembra 2019), s. 23.

- či sa týka **zraniteľných osôb** alebo nie;
  - či má vplyv aj na **iné základné práva** (napríklad právo na slobodu prejavu, ako vo veciach Digital Rights Ireland a Seitlinger a i. a Tele2 Sverige a Watson).<sup>47</sup>
51. V tejto súvislosti je tiež dôležité poznamenať, že vplyv môže byť malý, pokiaľ ide o dotknutého jednotlivca, ale napriek tomu môže byť významný alebo veľmi významný kolektívne/pre spoločnosť ako celok.<sup>48</sup>
  52. Vo všetkých troch typoch príkazov na zistenie (zistenie známeho materiálu obsahujúceho sexuálne zneužívanie detí, nového materiálu obsahujúceho sexuálne zneužívanie detí a groomingu) sa v súčasnosti dostupné technológie spoliehajú na automatizované spracúvanie údajov o obsahu všetkých dotknutých používateľov. Technológie používané na analýzu obsahu sú často zložité a zvyčajne zahŕňajú používanie umelej inteligencie. V dôsledku toho nemusí byť fungovanie tejto technológie pre používateľa služby úplne zrozumiteľné. Okrem toho je známe, že technológie, ktoré sú v súčasnosti k dispozícii, najmä technológie na odhaľovanie nového materiálu obsahujúceho sexuálne zneužívanie detí alebo groomingu, majú pomerne vysokú mieru chybovosti.<sup>49</sup> Okrem toho existuje riziko oznámenia centru EÚ v súlade s článkom 12 ods. 1 a článkom 48 ods. 1 návrhu, a to na základe zistenia „potenciálneho“ materiálu obsahujúceho sexuálne zneužívanie detí.
  53. Navyše všeobecné podmienky vydania príkazu na zistenie podľa návrhu, t. j. vzťahuje sa na celú službu, a nielen na vybranú komunikáciu<sup>50</sup>, trvanie do 24 mesiacov v prípade známeho alebo nového materiálu obsahujúceho sexuálne zneužívanie detí a až 12 mesiacov v prípade groomingu<sup>51</sup> atď. môžu v praxi viesť k veľmi širokému rozsahu pôsobnosti príkazu. V dôsledku toho by monitorovanie bolo v skutočnosti všeobecné a nediferencované a v praxi by nebolo cielené.
  54. Vzhľadom na uvedené skutočnosti sú EDPB a EDPS znepokojení aj možnými odstrašujúcimi účinkami na uplatňovanie slobody prejavu. EDPB a EDPS pripomínajú, že takýto odstrašujúci účinok sa považuje za pravdepodobnejší, čím sú právne predpisy nejasnejšie.
  55. Vzhľadom na nedostatočnú špecifickosť, presnosť a jasnosť, ktoré sú potrebné na splnenie požiadavky právnej istoty<sup>52</sup>, a vzhľadom na jeho široký rozsah pôsobnosti, t. j. všetci poskytovatelia príslušných služieb informačnej spoločnosti, ktorí takéto služby ponúkajú v Únii<sup>53</sup>, sa v návrhu nezabezpečuje, aby sa účinne uplatňoval len cielený prístup k zisťovaniu materiálu obsahujúceho sexuálne zneužívanie detí a groomingu. EDPB a EDPS sa preto domnievajú, že v praxi by sa návrh mohol stať základom *de facto* všeobecného a nediferencovaného skenovania obsahu prakticky všetkých druhov elektronických komunikácií všetkých používateľov v EÚ/EHP. V dôsledku toho môžu právne predpisy viesť ľudí k tomu, že nebudú zdieľať zákonný obsah v obave, že by mohli byť cieľom na základe tohto ich konania.
  56. EDPB a EDPS však uznávajú, že rôzne opatrenia na boj proti online sexuálnemu zneužívaniu detí sa môžu vyznačovať rôznymi úrovňami rušivého vplyvu. EDPB a EDPS na úvod poznamenávajú, že

---

<sup>47</sup> Pozri tiež stanovisko EDPS 7/2020 k návrhu dočasných výnimiek zo smernice 2002/58/ES na účely boja proti sexuálnemu zneužívaniu detí online (10. novembra 2020), s. 9 a nasl.

<sup>48</sup> EDPS, Usmernenia o posudzovaní primeranosti opatrení, ktoré obmedzujú základné práva na súkromie a na ochranu osobných údajov (19. decembra 2019), s. 20.

<sup>49</sup> Pozri podrobnosti uvedené vyššie, oddiel 4.5 a ďalej, pododdiel 4.8.2.

<sup>50</sup> Pozri článok 7 ods. 1 návrhu.

<sup>51</sup> Pozri článok 7 ods. 9 tretí pododsek návrhu.

<sup>52</sup> Pozri SDEÚ, vec C-197/96, Komisia Európskych spoločenstiev/Francúzska republika, bod 15.

<sup>53</sup> Pozri článok 1 ods. 2 návrhu.

automatizovaná analýza reči alebo textu s cieľom identifikovať možné prípady kontaktovania detí bude pravdepodobne predstavovať výraznejší zásah ako porovnanie obrázkov alebo videí na základe predtým potvrdených prípadov výskytu materiálu obsahujúceho sexuálne zneužívanie detí s cieľom odhaliť šírenie materiálu obsahujúceho sexuálne zneužívanie detí. Okrem toho by sa malo rozlišovať medzi zisťovaním „známeho materiálu obsahujúceho sexuálne zneužívanie detí“ a „nového materiálu obsahujúceho sexuálne zneužívanie detí“. Okrem toho by sa mal vplyv ďalej rozlišovať medzi opatreniami určenými poskytovateľom hostingových služieb a opatreniami uloženými poskytovateľom interpersonálnych komunikačných služieb.

#### 4.5.4 Zisťovanie známeho materiálu obsahujúceho sexuálne zneužívanie detí

57. Zatiaľ čo podľa odôvodnenia 4 by bol návrh „technologicky neutrálny“, účinnosť navrhovaných opatrení na zisťovanie a ich vplyv na jednotlivcov bude vo veľkej miere závisieť od výberu použitej technológie a od vybraných ukazovateľov. Komisia túto skutočnosť uznáva v prílohe 8<sup>54</sup> správy o posúdení vplyvu a potvrdzuje ju aj iné štúdie, ako napríklad ciele náhradné posúdenie vplyvu návrhu Komisie o dočasnej výnimke zo smernice o súkromí a elektronických komunikáciách na účely boja proti online sexuálnemu zneužívaniu detí z februára 2021.<sup>55</sup>
58. V článku 10 návrhu sa stanovuje niekoľko požiadaviek na technológie, ktoré sa majú používať na účely zisťovania, najmä pokiaľ ide o ich účinnosť, spoľahlivosť a najmenej rušivý charakter, pokiaľ ide o vplyv na práva používateľov na súkromný a rodinný život vrátane dôvernosti komunikácií a na ochranu osobných údajov.
59. EDPB a EDPS v tejto súvislosti poznamenávajú, že v súčasnosti sú jedinými technológiami, ktoré sa vo všeobecnosti považujú za schopné splniť tieto štandardy, tie, ktoré sa používajú na zisťovanie známeho materiálu obsahujúceho sexuálne zneužívanie detí, t. j. porovnávacie technológie, ktoré sa opierajú o databázu hašov ako o referenciu.

#### 4.5.5 Zisťovanie doteraz neznámeho materiálu obsahujúceho sexuálne zneužívanie detí

60. Posúdenie opatrení zameraných na zisťovanie doteraz neznámeho (nového) materiálu obsahujúceho sexuálne zneužívanie detí vedie k odlišným záverom, pokiaľ ide o ich účinnosť, spoľahlivosť a obmedzenie vplyvu na základné práva na súkromie a ochranu údajov.
61. Po prvé, ako sa vysvetľuje v správe o posúdení vplyvu k návrhu, technológie, ktoré sa v súčasnosti používajú na zisťovanie doteraz neznámeho materiálu obsahujúceho sexuálne zneužívanie detí, zahŕňajú klasifikátory a umelú inteligenciu. Klasifikátor je akýkoľvek algoritmus, ktorý prostredníctvom rozpoznávania vzorov triedi údaje do označených tried alebo kategórií informácií.<sup>56</sup> Tieto technológie majú teda rôzne výsledky a vplyv z hľadiska presnosti, účinnosti a úrovne rušivého vplyvu. Zároveň sú náchyľnejšie na chyby.
62. Techniky používané na zisťovanie doteraz neznámeho materiálu obsahujúceho sexuálne zneužívanie detí sú podobné tým, ktoré sa používajú na zisťovanie kontaktovania detí, keďže obe metódy nie sú založené na jednoduchých porovnávacích technológiách, ale na prediktívnych modeloch využívajúcich

---

<sup>54</sup> Pozri informácie o miere falšných pozitívnych výsledkov v správe o posúdení vplyvu, príloha 8, s. 279 a nasl.

<sup>55</sup> Pozri návrh Komisie o dočasnej výnimke zo smernice o súkromí a elektronických komunikáciách na účely boja proti sexuálnemu zneužívaniu detí online: Ciele náhradné posúdenie vplyvu (Výskumná služba Európskeho parlamentu, február 2021), s. 14 a nasl.

<sup>56</sup> Správa o posúdení vplyvu, príloha 8, s. 281.

technológie umelej inteligencie. EDPB a EDPS sa domnievajú, že pri odhaľovaní doteraz neznámeho materiálu obsahujúceho sexuálne zneužívanie detí by sa mala uplatňovať vysoká miera obozretnosti, keďže chyba systému by mala vážne dôsledky pre dotknuté osoby, ktoré by boli automaticky označené ako osoby, ktoré sa pravdepodobne dopustili veľmi závažného trestného činu, a mali by sa oznámiť ich osobné údaje a podrobnosti o ich komunikácii.

63. Po druhé, ukazovatele výkonnosti uvedené v literatúre, z ktorých niektoré sú zdôraznené v správe o posúdení vplyvu priloženej k návrhu,<sup>57</sup> poskytujú veľmi málo informácií o podmienkach, ktoré sa použili pri ich výpočte, a ich primeranosti pokiaľ ide o podmienky v reálnom živote, čo znamená, že ich reálna výkonnosť by mohla byť výrazne nižšia, než sa očakáva, čo by viedlo k menšej presnosti a vyššiemu percentu „falošných pozitívnych výsledkov“.
64. Po tretie, ukazovatele výkonnosti by sa mali zväžiť v špecifickom kontexte používania príslušných nástrojov na zisťovanie a mali by poskytovať úplný prehľad o správaní týchto nástrojov. Pri používaní algoritmov umelej inteligencie pri obrázkoch alebo textoch je dobre zdokumentované, že k zaujatosti a diskriminácii môže dôjsť v dôsledku nedostatočnej reprezentatívnej skupiny obyvateľstva v údajoch používaných na tréning algoritmu. Tieto skreslenia by sa mali identifikovať, merať a znižovať na prijateľnú úroveň, aby boli systémy na zisťovanie skutočne prínosom pre spoločnosť ako celok.
65. Hoci bola vykonaná štúdia technológií používaných na zisťovanie,<sup>58</sup> EDPB a EDPS sa domnievajú, že na posúdenie spoľahlivosti existujúcich nástrojov je potrebná ďalšia analýza. Táto analýza by sa mala opierať o vyčerpávajúce ukazovatele výkonnosti a posúdiť vplyv potenciálnych chýb v reálnych podmienkach na všetky dotknuté osoby, ktorých sa návrh týka.
66. Ako už bolo uvedené, EDPB a EDPS majú vážne pochybnosti o tom, do akej miery sú procesné záruky stanovené v článku 7 ods. 6 návrhu dostatočné na kompenzáciu týchto rizík. Okrem toho, ako už bolo uvedené, poznamenávajú, že v návrhu sa na opis prijateľnej miery rizika používajú pomerne abstraktné a vágne pojmy (napr. „v značnej miere“).
67. EDPB a EDPS sa obávajú, že tieto všeobecné a nejasné pojmy povedú k nedostatočnej právnej istote a výrazným rozdielom v konkrétnom vykonávaní návrhu v rámci Únie v závislosti od výkladu pojmov, ako sú „pravdepodobnosť“ a „v značnej miere“ zo strany súdnych alebo iných nezávislých správnych orgánov v členských štátoch. Je to znepokojujúce aj vzhľadom na skutočnosť, že ustanovenia o príkazoch na zistenie budú predstavovať „obmedzenie“ zásady dôvernosti stanovenej v článku 5 smernice o súkromí a elektronických komunikáciách. Preto je potrebné zlepšiť ich jednoznačnosť a predvídateľnosť v navrhovanom nariadení.

#### 4.5.6 Zisťovanie kontaktovania detí („grooming“)

68. EDPB a EDPS poznamenávajú, že navrhované opatrenia týkajúce sa zisťovania kontaktovania detí („grooming“), ktoré zahŕňajú automatizovanú analýzu reči alebo textu, pravdepodobne predstavujú najvýznamnejší zásah do práv používateľov na súkromný a rodinný život vrátane dôvernosti komunikácie a na ochranu osobných údajov.
69. Zatiaľ čo zisťovanie známeho a dokonca aj nového materiálu obsahujúceho sexuálne obťažovanie detí môže byť rozsahom obmedzené na analýzu obrázkov a videí, zisťovanie groomingu by sa vo svojej

---

<sup>57</sup> Správa o posúdení vplyvu, príloha 8, s. 281 – 283.

<sup>58</sup> Správa o posúdení vplyvu, s. 279 a nasl.

podstate rozšírilo na všetky textové (a prípadne zvukové) komunikácie, ktoré patria do rozsahu pôsobnosti príkazu na zistenie. Intenzita zásahu do dôvernosti dotknutých komunikácií je preto oveľa väčšia.

70. EDPB a EDPS sa domnievajú, že *de facto* všeobecná a nediferencovaná automatizovaná analýza textovej komunikácie prenášanej prostredníctvom interpersonálnych komunikačných služieb s cieľom identifikovať potenciálne kontaktovanie detí nerešpektuje požiadavky nevyhnutnosti a proporcionality. Aj keď sa používaná technológia obmedzuje na používanie ukazovateľov, EDPB a EDPS sa domnievajú, že zavedenie takejto všeobecnej a nediferencovanej analýzy je neprimerané a môže dokonca ovplyvniť samotnú podstatu základného práva na súkromie zakotveného v článku 7 Charty.
71. Ako už bolo uvedené, chýbajúce vecné záruky v súvislosti s opatreniami na zisťovanie kontaktovania detí nemôže byť kompenzovaný len procesnými zárukami. Okrem toho je problém nedostatočnej právnej jasnosti a istoty (napr. používanie vágneho právneho jazyka ako „významný rozsah“) ešte závažnejší v prípade automatizovanej analýzy textovej osobnej komunikácie oproti porovnávaní fotografií na základe technológie hašovania.
72. EDPB a EDPS sa okrem toho domnievajú, že „odstrašujúci účinok“ na slobodu prejavu je obzvlášť významný, keď sa textová (alebo zvuková) komunikácia jednotlivcov skenuje a analyzuje vo veľkom rozsahu. EDPB a EDPS pripomínajú, že takýto odstrašujúci účinok je tým závažnejší, čím sú právne predpisy nejasnejšie.
73. Okrem toho, ako sa uvádza v správe o posúdení vplyvu<sup>59</sup> a v štúdií výskumnej služby Európskeho parlamentu<sup>60</sup>, miera presnosti technológií na zisťovanie textového groomingu je oveľa nižšia ako miera presnosti technológií na zisťovanie známeho materiálu obsahujúceho sexuálne zneužívanie detí<sup>61</sup>. Techniky zisťovania groomingu sú navrhnuté tak, aby analyzovali a priradzovali hodnotenia pravdepodobnosti každému aspektu konverzácie, a preto ich EDPB a EDPS taktiež považujú za náchylné na chyby a zraniteľné voči zneužitiu.

#### 4.5.7 Záver o nevyhnutnosti a proporcionality plánovaných opatrení

74. Pokiaľ ide o nevyhnutnosť a proporcionality plánovaných opatrení na zisťovanie, EDPB a EDPS sú obzvlášť znepokojení, pokiaľ ide o opatrenia plánované na zisťovanie neznámeho materiálu obsahujúceho sexuálne zneužívanie detí a kontaktovania detí (grooming) vzhľadom na ich rušivý vplyv z dôvodu možného umožnenia všeobecného prístupu k obsahu komunikácie, ich pravdepodobnostný charakter a mieru chybovosti spojenú s takýmito technológiami.
75. Okrem toho z judikatúry SDEÚ možno vyvodiť, že opatrenia umožňujúce orgánom verejnej moci mať všeobecný prístup k obsahu komunikácie môžu s väčšou pravdepodobnosťou ovplyvniť podstatu práv zaručených v článkoch 7 a 8 Charty. Tieto úvahy sú osobitne relevantné v súvislosti s opatreniami na zisťovanie kontaktovania detí, ktoré sa predpokladajú v návrhu.
76. EDPB a EDPS sa v každom prípade domnievajú, že zásahy spôsobené najmä opatreniami na zisťovanie kontaktovania detí presahujú rámec toho, čo je nevyhnutne potrebné a proporcionálne. Tieto opatrenia by sa preto mali z návrhu vypustiť.

---

<sup>59</sup> Správa o posúdení vplyvu, príloha 8, s. 281 – 283.

<sup>60</sup> s. 15 – 18.

<sup>61</sup> Pozri vyššie, bod 40.

#### 4.6 Oznamovacie povinnosti

77. EDPB a EDPS odporúčajú doplniť zoznam osobitných požiadaviek na oznamovanie v článku 13 návrhu o požiadavku zahrnúť do správy informácie o konkrétnej technológii, ktorá poskytovateľovi umožnila oboznámiť sa s príslušným zneužívajúcim obsahom v prípade, že sa poskytovateľ dozvedel o potenciálnom sexuálnom zneužívaní detí na základe opatrení prijatých na vykonanie príkazu na zisťovanie vydaného v súlade s článkom 7 návrhu.

#### 4.7 Povinnosti týkajúce sa odstraňovania a blokovania

78. Jedným z opatrení plánovaných v návrhu na zmiernenie rizík šírenia materiálu obsahujúceho sexuálne zneužívanie detí je vydávanie príkazov na odstránenie a blokovanie [removal and blocking orders], ktoré by poskytovateľom uložili povinnosť odstrániť alebo znemožniť prístup k materiálu zobrazujúcemu online sexuálne zneužívanie detí alebo ho zablokovať.<sup>62</sup>
79. Hoci vplyv príkazov na odstránenie na ochranu údajov a súkromia komunikácie je pomerne obmedzený, EDPB a EDPS vo všeobecnosti pripomínajú všeobecnú zásadu, ktorá sa má dodržiavať, že každé takéto opatrenie by malo byť čo najcielenejšie.
80. EDPB a EDPS zároveň upozorňujú na skutočnosť, že poskytovatelia služieb prístupu na internet majú prístup k presnej URL adrese obsahu len vtedy, ak je tento obsah sprístupnený v čistej textovej podobe [in clear text]. Vždy, keď sa obsah sprístupní prostredníctvom HTTPS, poskytovateľ služieb prístupu na internet nebude mať prístup k presnému URL, pokiaľ nenaruší šifrovanie komunikácie. EDPB a EDPS preto majú pochybnosti o účinnosti blokovacích opatrení a domnievajú sa, že by bolo neprimerané vyžadovať od poskytovateľov služieb internetového prístupu dešifrovanie online komunikácií s cieľom zablokovať komunikáciu týkajúcu sa materiálu obsahujúceho sexuálne zneužívanie detí.
81. Okrem toho a všeobecnejšie treba poznamenať, že blokovanie (alebo znemožnenie) prístupu k digitálnej položke je operácia, ktorá sa uskutočňuje na úrovni siete a jej vykonávanie sa môže ukázať ako neúčinné v prípade viacnásobných (prípadne podobných a nie identických) kópií tej istej položky. Takáto operácia sa tiež môže ukázať ako neprimeraná, ak blokovanie ovplyvňuje iné, nie nezákonné, digitálne položky, ak sú uložené na tom istom serveri, ktorý je zneprístupnený pomocou sieťových príkazov (napr. zaradenie IP adresy alebo zaradenie čiernu listinu DNS). Navyše nie všetky prístupy k blokovaniu na úrovni siete sú rovnako účinné a niektoré z nich možno ľahko obísť s pomerne základnými technickými zručnosťami.
82. Napokon by sa v navrhovanom nariadení mali objasniť právomoci koordinačných orgánov, pokiaľ ide o vydávanie príkazov na zablokovanie. Napríklad zo súčasného znenia článku 16 ods. 1 a článku 17 ods. 1 nie je jasné, či sú koordinačné orgány oprávnené vydávať príkazy na zablokovanie alebo len žiadať o ich vydanie.<sup>63</sup>

---

<sup>62</sup> Návrh, články 14 a 16.

<sup>63</sup> V článku 16 ods. 1 návrhu sa uvádza: „Koordinačný orgán v krajine usadenia má právomoc požiadať príslušný súdny orgán členského štátu, ktorý ho určil, alebo nezávislý správny orgán tohto členského štátu, aby vydal príkaz na zablokovanie [...]“, pričom v článku 17 ods. 1 sa uvádza „príkazy na zablokovanie uvedené v článku 16 vydáva koordinačný orgán v krajine usadenia [...]“ (zvýraznenie doplnené).

## 4.8 Príslušné technológie a záruky

### 4.8.1 Špecificky navrhnutá a štandardná ochrana údajov

83. Požiadavky návrhu, ktoré sa vzťahujú na technológie, ktoré sa majú zaviesť na zisťovanie materiálu obsahujúceho sexuálne zneužívanie detí a kontaktovania detí, sa nezdájú dostatočne prísne. EDPB a EDPS predovšetkým poznamenávajú, že – na rozdiel od analogických ustanovení dočasného nariadenia<sup>64</sup> – návrh neobsahuje žiadny výslovný odkaz na zásadu špecificky navrhutej a štandardnej ochrany údajov a nestanovuje, že technológie, ktoré sa používajú na skenovanie textu v komunikácii, nesmú byť schopné odvodiť podstatu obsahu komunikácie. V článku 10 ods. 3 písm. b) návrhu sa jednoducho stanovuje, že technológie nesmú byť schopné „získať“ žiadne iné informácie z príslušnej komunikácie, než sú informácie, ktoré sú nevyhnutne potrebné na zisťovanie. Zdá sa však, že tento štandard nie je dostatočne prísny, pretože by bolo možné *odvodiť* z podstaty obsahu oznámenia iné informácie bez toho, aby sa z neho *získavali* informácie ako také.
84. EDPS a EDPB preto odporúčajú, aby sa do návrhu vložilo odôvodnenie, v ktorom sa stanovuje, že zásada špecificky navrhutej a štandardnej ochrany údajov stanovená v článku 25 nariadenia (EÚ) 2016/679 sa uplatňuje na technológie upravené v článku 10 návrhu na základe právnych predpisov, a preto sa v právnom texte nemusela opakovať. Okrem toho by sa mal zmeniť článok 10 ods. 3 písm. b), aby sa zabezpečilo, že nielenže sa nezískajú žiadne iné informácie, ale ani sa neodvodnia, ako sa v súčasnosti stanovuje v článku 3 ods. 1 písm. b) dočasného nariadenia.

### 4.8.2 Spoľahlivosť technológií

85. V návrhu sa predpokladá, že poskytovatelia služieb môžu na vykonávanie príkazov na zisťovanie použiť viacero druhov technologických riešení. V návrhu sa predovšetkým predpokladá, že systémy umelej inteligencie sú k dispozícii a podieľajú sa na zisťovaní neznámeho materiálu obsahujúceho sexuálne zneužívanie detí a na zisťovaní kontaktovania detí<sup>65</sup> a niektoré koordinačné orgány ich môžu považovať za najmodernejšie [state of the art]. Hoci účinnosť návrhu závisí od spoľahlivosti týchto technologických riešení, je k dispozícii veľmi málo informácií o všeobecnom a systematickom používaní týchto techník, čo si vyžaduje starostlivé zváženie.
86. Okrem toho, hoci ich EDPB a EDPS museli použiť pri posudzovaní proporcionality z dôvodu nedostatku alternatív, treba poznamenať, že ukazovatele výkonnosti technológií na zisťovanie uvedené v správe o posúdení vplyvu, ktorá bola pripojená k návrhu, poskytujú veľmi málo informácií o tom, ako boli posúdené a či odrážajú reálnu výkonnosť príslušných technológií. Neexistujú žiadne informácie o testoch alebo referenčných hodnotách, ktoré predajcovia technológií používajú na meranie týchto výkonov. Bez takýchto informácií nie je možné zopakovať testy ani vyhodnotiť platnosť tvrdení o výkonnosti. V tejto súvislosti treba poznamenať, že hoci by sa ukazovatele výkonnosti mohli vykladať tak, že naznačujú, že niektoré nástroje na zisťovanie majú vysokú úroveň presnosti (napríklad presnosť určitých nástrojov na zisťovanie groomingu je 88 %),<sup>66</sup> tieto ukazovatele by sa mali posudzovať vzhľadom na predpokladané praktické použitie nástrojov na zisťovanie a závažnosť rizík, ktoré by pre príslušné dotknuté osoby predstavovalo nesprávne posúdenie daného materiálu. EDPB a EDPS sa okrem toho domnievajú, že pri takomto spracúvaní s vysokým rizikom predstavuje 12 % miera zlyhania vysoké riziko pre dotknuté osoby, ktoré by boli vystavené falošným pozitívnym výsledkom, a to aj

---

<sup>64</sup> Dočasné nariadenie, článok 3 ods. 1 písm. b).

<sup>65</sup> Pozri správu o posúdení vplyvu, s. 281 – 282.

<sup>66</sup> Tamže, s. 283.



vtedy, keď sú zavedené záruky na zabránenie falošným oznámeniam orgánom presadzovania práva. Je veľmi nepravdepodobné, že by poskytovatelia služieb mohli vyčleniť dostatočné zdroje na preskúmanie takéhoto percentuálneho podielu falošne pozitívnych výsledkov.

87. Ako už bolo uvedené,<sup>67</sup> ukazovatele výkonnosti by mali poskytovať úplný prehľad o správaní nástrojov na zisťovanie. Pri používaní algoritmov umelej inteligencie pri obrázkoch alebo textoch je dobre zdokumentované, že k zaujatosti a diskriminácii môže dôjsť v dôsledku nedostatočnej reprezentatívности určitých skupín obyvateľstva v údajoch používaných na tréning algoritmu. Tieto skreslenia by sa mali identifikovať, merať a znižovať na prijateľnú úroveň, aby boli systémy na zisťovanie skutočne prínosné pre spoločnosť ako celok.
88. Hoci bola vykonaná štúdia technológií používaných na zisťovanie,<sup>68</sup> EDPB a EDPS sa domnievajú, že na nezávislé posúdenie spoľahlivosti existujúcich nástrojov v reálnych prípadoch je potrebná ďalšia analýza. Táto analýza by sa mala opierať o vyčerpávajúce ukazovatele výkonnosti a posúdiť vplyv potenciálnych chýb v reálnych podmienkach na všetky dotknuté osoby, ktorých sa návrh týka. Keďže tieto technológie sú základom, z ktorého návrh vychádza, EDPB a EDPS považujú túto analýzu za mimoriadne dôležitú pre posúdenie primeranosti návrhu.
89. EDPB a EDPS takisto poznamenávajú, že v návrhu sa nevymedzujú požiadavky špecifické pre jednotlivé technológie, či už pokiaľ ide o mieru chybovosti, používanie klasifikátorov a ich validáciu alebo iné obmedzenia. Tým sa vytvorenie takýchto kritérií ponecháva na prax pri posudzovaní proporcionality používania konkrétnej technológie, čo ďalej prispieva k nedostatočnej presnosti a jasnosti.
90. Vzhľadom na význam dôsledkov pre dotknuté osoby v prípadoch falošne pozitívnych výsledkov sa EDPB a EDPS domnievajú, že miera falošných pozitívnych výsledkov sa musí znížiť na minimum a že tieto systémy sa musia navrhovať so zohľadnením skutočnosti, že prevažná väčšina elektronických komunikácií nezahŕňa žiadny materiál obsahujúci sexuálne zneužívanie detí ani kontaktovanie detí a že dokonca aj veľmi nízka miera falošných pozitívnych výsledkov bude znamenať veľmi vysoký počet falošných pozitívnych výsledkov vzhľadom na objem údajov, ktoré budú predmetom zisťovania. Všeobecnejšie sú EDPB a EDPS takisto znepokojení skutočnosťou, že výkonnosť dostupných nástrojov uvedených v správe o posúdení vplyvu nezodpovedá presným a porovnateľným ukazovateľom týkajúcim sa mier falošne pozitívnych a falošne negatívnych výsledkov, a domnievajú sa, že by sa mali vydať porovnateľné a zmysluplné ukazovatele výkonnosti pre tieto technológie predtým, než sa budú považovať za dostupné a účinné.

#### 4.8.3 Skenovanie zvukovej komunikácie

91. Na rozdiel od dočasného nariadenia<sup>69</sup> návrh nevyklučuje z rozsahu svojho uplatňovania skenovanie zvukovej komunikácie v súvislosti so zisťovaním groomingu.<sup>70</sup> EDPB a EDPS sa domnievajú, že skenovanie zvukovej komunikácie je obzvlášť rušivé, pretože by si za normálnych okolností vyžadovalo aktívne, nepretržité odpočúvanie „naživo“. Okrem toho v niektorých členských štátoch podlieha súkromie hovoreného slova osobitnej ochrane.<sup>71</sup> Okrem toho vzhľadom na skutočnosť, že v zásade by bolo potrebné analyzovať všetok obsah zvukovej komunikácie, toto opatrenie pravdepodobne

---

<sup>67</sup> Pozri body 63 – 64 vyššie.

<sup>68</sup> Pozri správu o posúdení vplyvu, s. 279 a nasl.

<sup>69</sup> Pozri dočasné nariadenie, článok 1 ods. 2.

<sup>70</sup> Pozri návrh, článok 1.

<sup>71</sup> Pozri napr. nemecký trestný zákonník, § 201.

ovplyvní podstatu práv zaručených v článkoch 7 a 8 Charty. Táto metóda zisťovania by preto mala zostať mimo rozsahu povinností týkajúcich sa zisťovania stanovených v navrhovanom nariadení, a to tak pokiaľ ide o hlasové správy, ako aj komunikáciu naživo, navyše vzhľadom na skutočnosť, že v správe o posúdení vplyvu, ktorá bola pripojená k návrhu, sa neidentifikovali žiadne konkrétne riziká alebo zmeny v rozsahu hrozieb, ktoré by si vyžadovali jej použitie.<sup>72</sup>

#### 4.8.4 Overovanie veku

92. V návrhu sa poskytovatelia nabádajú, aby na identifikáciu detských používateľov v rámci svojich služieb využívali opatrenia na overovanie veku a posúdenie veku.<sup>73</sup> EDPB a EDPS v tejto súvislosti poznamenávajú, že v súčasnosti neexistuje technologické riešenie, ktoré by bolo schopné s istotou posúdiť vek používateľa v online prostredí bez toho, aby sa spoliehalo na oficiálnu digitálnu identitu, ktorá v tejto fáze nie je dostupná každému európskemu občanovi.<sup>74</sup> Plánované použitie opatrení na overovanie veku v návrhu by preto mohlo viesť k vylúčeniu mlado vyzerajúcich dospelých z prístupu k online službám alebo k zavedeniu veľmi rušivých nástrojov na overovanie veku, čo by mohlo brániť legitímnemu využívaniu dotknutých služieb alebo od neho odrádzať.
93. V tejto súvislosti a aj keď sa v odôvodnení 16 návrhu odkazuje na nástroje rodičovskej kontroly ako možné zmierňujúce opatrenia, EDPB a EDPS odporúčajú, aby sa navrhované nariadenie zmenilo tak, aby sa poskytovateľom výslovne umožnilo, aby sa okrem overovania veku alebo ako alternatívu k overovaniu veku spoliehali na mechanizmy rodičovskej kontroly.

#### 4.9 Uchovávanie informácií

94. V článku 22 návrhu sa obmedzujú účely, na ktoré môžu poskytovatelia, na ktorých sa návrh vzťahuje, uchovávať obsahové údaje a iné údaje spracúvané v súvislosti s opatreniami prijatými na splnenie povinností stanovených v návrhu. V návrhu sa však uvádza, že poskytovatelia môžu tieto informácie uchovávať aj na účely zlepšenia účinnosti a presnosti technológií na zisťovanie sexuálneho zneužívania detí online s cieľom vykonať príkaz na zistenie, ale na tento účel neuchovávajú žiadne osobné údaje.<sup>75</sup>
95. EDPB a EDPS sa domnievajú, že len tí poskytovatelia, ktorí používajú svoje vlastné technológie na zistenie, by mali mať možnosť uchovávať údaje na zlepšenie účinnosti a presnosti technológií, zatiaľ čo tí, ktorí používajú technológie poskytované centrom EÚ, by z tejto možnosti nemali mať prospech. EDPB a EDPS okrem toho poznamenávajú, že v praxi môže byť ťažké zabezpečiť, aby sa na tento účel neuchovávali žiadne osobné údaje, keďže väčšina obsahových údajov a iných údajov spracúvaných na účely zisťovania sa pravdepodobne považuje za osobné údaje.

#### 4.10 Vplyv na šifrovanie

96. Európske orgány pre ochranu údajov sa dôsledne zasadujú za všeobecnú dostupnosť silných šifrovacích nástrojov a proti akémukoľvek typu zadných dvierok.<sup>76</sup> Dôvodom je, že šifrovanie je

---

<sup>72</sup> Pozri správu o posúdení vplyvu.

<sup>73</sup> Pozri návrh, článok 4 ods. 3, článok 6 ods. 1 písm. c) a odôvodnenie 16.

<sup>74</sup> Pozri napr. CNIL, Odporúčanie 7: Kontrola veku dieťaťa a súhlas rodiča pri rešpektovaní súkromia dieťaťa (9. augusta 2021).

<sup>75</sup> Návrh, článok 22 ods. 1.

<sup>76</sup> Pozri napr. vyhlásenie pracovnej skupiny zriadenej podľa článku 29 o šifrovaní a jeho vplyve na ochranu fyzických osôb pri spracúvaní osobných údajov v EÚ (11. apríla 2018).

dôležité na zabezpečenie uplatňovania všetkých ľudských práv offline a online.<sup>77</sup> Okrem toho, šifrovacie technológie zásadným spôsobom prispievajú k rešpektovaniu súkromného života a dôvernosti komunikácií, ako aj k inováciám a rastu digitálneho hospodárstva, ktoré sa opiera o vysokú úroveň dôvery, ktorú takéto technológie poskytujú.

97. V kontexte interpersonálnej komunikácie je šifrovanie medzi koncovými bodmi (ďalej len „E2EE“) kľúčovým nástrojom na zabezpečenie dôvernosti elektronických komunikácií, keďže poskytuje silné technické záruky proti prístupu k obsahu komunikácie pre kohokoľvek okrem odosielateľa a príjemcu (príjemcov), a to aj zo strany poskytovateľa. Zabránenie používaniu E2EE alebo akékoľvek odrádzanie od jeho používania, uloženie povinnosti poskytovateľom služieb spracúvať údaje z elektronickej komunikácie na iné účely, než je poskytovanie ich služieb, alebo uloženie povinnosti proaktívne zasielať elektronické komunikácie tretím stranám, by znamenalo riziko, že poskytovatelia ponúknu menej šifrované služby s cieľom lepšie plniť povinnosti, čím by sa oslabil úloha šifrovania vo všeobecnosti a oslabilo by sa dodržiavanie základných práv európskych občanov. Je potrebné poznamenať, že zatiaľ čo E2EE je jedným z najbežnejšie používaných bezpečnostných opatrení v kontexte elektronických komunikácií, iné technické riešenia (napr. používanie iných kryptografických schém) môžu byť alebo sa môžu stať rovnako dôležité na zabezpečenie a ochranu dôvernosti digitálnych komunikácií. Ich používaniu by sa preto nemalo brániť ani by sa nemalo odrádzať od ich používania.
98. Zavádzanie nástrojov na odpočúvanie a analýzu interpersonálnych elektronických komunikácií je v zásade v rozpore s E2EE, keďže cieľom E2EE je technicky zaručiť, že komunikácia medzi odosielateľom a príjemcom zostane dôverná.
99. Preto aj keď sa v návrhu nestanovuje povinnosť poskytovateľov systematicky realizovať odpočúvania, je pravdepodobné, že samotná možnosť, že by mohol byť vydaný príkaz na zistenie výrazne ovplyvní technické rozhodnutia poskytovateľov, najmä vzhľadom na obmedzený časový rámec, ktorý budú musieť dodržať pri plnení príkazu, a vysoké sankcie, ktorým by čelili pri jeho nesplnení.<sup>78</sup> V praxi by to mohlo viesť určitých poskytovateľov k tomu, aby prestali používať E2EE.
100. Vplyv zhoršovania používania E2EE alebo odrádzania od jeho používania, ktorý môže z návrhu vyplývať, sa musí riadne posúdiť. Každou z techník obchádzania ochrany súkromia, ktorú poskytuje E2EE, a ktoré sa uvádzajú v správe o posúdení vplyvu pripojenej k návrhu, by sa zaviedli bezpečnostné medzery.<sup>79</sup> Napríklad skenovanie na strane klienta<sup>80</sup> by pravdepodobne viedlo k značnému, necielenému prístupu a spracúvaniu nezašifrovaného obsahu na zariadeniach koncového používateľa. Takéto podstatné zhoršenie dôvernosti by malo vplyv najmä na deti, keďže je pravdepodobnejšie, že na služby, ktoré používajú, sa budú vzťahovať príkazy na zisťovanie, v dôsledku čoho budú zraniteľné voči monitorovaniu alebo odpočúvaniu. Skenovanie *na strane servera* je tiež zo svojej podstaty

---

<sup>77</sup> Pozri rezolúciu Rady pre ľudské práva č. 47/16 o presadzovaní, ochrane a uplatňovaní ľudských práv na internete, dokument OSN A/HRC/RES/47/16 (26. júla 2021).

<sup>78</sup> Pozri návrh, článok 35.

<sup>79</sup> Pozri oddiel 4.2 v Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague a Carmela Troncoso, „Bugs in our Pockets: The Risks of Client-Side Scanning“, ArXiv abs/2110.07450 (2021).

<sup>80</sup> Skenovanie na strane klienta vo všeobecnosti znamená systémy, ktoré skenujú obsah správ na základe zhody s databázou sporného obsahu pred odoslaním správy určenému príjemcovi.

nezlučiteľné s paradigmou E2EE, keďže komunikačný kanál so šifrovaním peer-to-peer, by musel byť prerušený, čo by viedlo k hromadnému spracúvaniu osobných údajov na serveroch poskytovateľov.

101. Hoci sa v návrhu uvádza, že „ponecháva na dotknutom poskytovateľovi výber technológií, ktoré bude prevádzkovať v záujme účinného plnenia príkazov na zistenie, pričom by sa to nemalo chápať ako navádzanie na používanie alebo odrádzanie od používania akejkoľvek technológie“, <sup>81</sup> štrukturálna nezlučiteľnosť niektorých príkazov na zistenie s E2EE sa v skutočnosti stáva výraznou prekážkou používania E2EE. Nemožnosť prístupu k službám využívajúcim E2EE a ich využívanie (ktoré v súčasnosti predstavujú najmodernejšiu [state of the art] technológiu z hľadiska technickej záruky dôvernosti) by mohla mať odstrašujúci účinok na slobodu prejavu a legitímne súkromné využívanie elektronických komunikačných služieb. Komisia uznáva aj nepriaznivý vzťah medzi zisťovaním materiálu obsahujúceho sexuálne zneužívanie detí alebo groomingu a E2EE, keď v správe o posúdení vplyvu <sup>82</sup> konštatuje, že je pravdepodobné, že zavedenie E2EE spoločnosťou Facebook v roku 2023 by ukončilo dobrovoľné skenovanie uskutočňované Facebookom.
102. S cieľom zabezpečiť, aby navrhované nariadenie neohrozovalo bezpečnosť alebo dôvernosť elektronických komunikácií európskych občanov, EDPB a EDPS sa domnievajú, že v normatívnych ustanoveniach návrhu by sa malo jasne uvádzať, že nič v navrhovanom nariadení by sa nemalo vykladať ako zákaz alebo oslabenie šifrovania v súlade s tým, čo sa uvádza v odôvodnení 25 dočasného nariadenia.

#### 4.11 Dohľad, presadzovanie práva a spolupráca

##### 4.11.1 Úloha vnútroštátnych dozorných orgánov podľa všeobecného nariadenia o ochrane údajov

103. V návrhu sa ustanovuje zriadenie siete vnútroštátnych koordinačných orgánov, ktoré budú zodpovedné za uplatňovanie a presadzovanie navrhovaného nariadenia. <sup>83</sup> Zatiaľ čo v odôvodnení 54 návrhu sa uvádza, že „pravidlá v oblasti dohľadu a presadzovania vyplývajúce z tohto nariadenia by sa nemali chápať tak, že majú vplyv na právomoci a kompetencie orgánov na ochranu osobných údajov podľa nariadenia (EÚ) 2016/679.“, EDPB a EDPS zastávajú názor, že vzťah medzi úlohami koordinačných orgánov a úlohami orgánov pre ochranu údajov by sa mal lepšie regulovať a že orgánom pre ochranu údajov by sa mala v rámci navrhovaného nariadenia prideliť významnejšia úloha.
104. Od poskytovateľov by sa predovšetkým malo vyžadovať, aby konzultovali orgány pre ochranu osobných údajov prostredníctvom postupu predchádzajúcej konzultácie, ako sa uvádza v článku 36 všeobecného nariadenia o ochrane údajov, pred zavedením akýchkoľvek opatrení na odhaľovanie materiálu obsahujúceho sexuálne zneužívanie detí alebo groomingu, a nie výlučne v súvislosti s používaním opatrení na zisťovanie kontaktovania detí, ako sa v súčasnosti predpokladá v návrhu. <sup>84</sup> Všetky opatrenia na zistenie by sa mali považovať za opatrenia, ktoré štandardne vedú k „vysokému riziku“, a preto by mali byť predmetom predchádzajúcej konzultácie bez ohľadu na to, či sa týkajú groomingu alebo materiálu obsahujúceho sexuálne zneužívanie detí, ako sa to už deje v prípade

---

<sup>81</sup> Návrh, odôvodnenie 26.

<sup>82</sup> Správa o posúdení vplyvu, s 27.

<sup>83</sup> Návrh, článok 25.

<sup>84</sup> Návrh, článok 7 ods. 3 druhá zarážka písm. b).

dočasného nariadenia.<sup>85</sup> Okrem toho by príslušné orgány na ochranu osobných údajov určené podľa všeobecného nariadenia o ochrane údajov mali mať vždy právomoc poskytovať svoje stanoviská k plánovaným opatreniam na zistenie, a to nielen za osobitných okolností.<sup>86</sup>

105. Okrem toho by sa navrhovaným nariadením mal zriadiť systém na riešenie a vyriešenie sporov medzi príslušnými orgánmi a orgánmi na ochranu údajov, pokiaľ ide o príkazy na zistenie. Orgány na ochranu údajov by mali mať najmä právo napadnúť príkaz na zistenie na súdoch členského štátu príslušného súdneho orgánu alebo nezávislého správneho orgánu, ktorý vydal príkaz na zistenie. EDPB a EDPS v tejto súvislosti konštatujú, že podľa súčasnej verzie návrhu môže príslušný orgán pri vydávaní príkazu na zistenie zamietnuť stanovisko príslušných orgánov na ochranu údajov. To môže potenciálne viesť k protichodným rozhodnutiam, keďže orgány na ochranu údajov by si, ako to potvrdzuje článok 36 ods. 2 všeobecného nariadenia o ochrane údajov, zachovali celú škálu svojich nápravných právomocí podľa článku 58 všeobecného nariadenia o ochrane údajov vrátane právomoci nariadiť zákaz spracúvania.

#### 4.11.2 Úloha EDPB

106. EDPB a EDPS poznamenávajú, že v článku 50 ods. 1 tretej vete návrhu sa stanovuje, že „centrum EÚ si vyžiada stanovisko svojho poradného výboru pre technológie a Európskeho výboru pre ochranu údajov“ predtým, ako do zoznamu technológií, ktoré môžu poskytovatelia hostingových služieb a poskytovatelia interpersonálnych komunikačných služieb zväžiť na použitie pri vykonávaní príkazov na zistenie, pridá konkrétnu technológiu. Ďalej sa v ňom stanovuje, že EDPB vydá svoje stanoviská do ôsmich týždňov, ktoré sa môžu v prípade potreby predĺžiť o ďalších šesť týždňov, pričom sa prihliada na zložitost' danej záležitosti. Napokon to vyžaduje, aby EDPB informovala centrum EÚ o každom takomto predĺžení lehoty do jedného mesiaca od prijatia žiadosti o konzultáciu spolu s odôvodnením omeškania.
107. Existujúce úlohy EDPB sú stanovené v článku 70 všeobecného nariadenia o ochrane údajov a článku 51 smernice (EÚ) 2016/680.<sup>87</sup> Pri týchto úlohách sa stanovuje, že EDPB poskytuje poradenstvo Komisii a vydáva stanoviská na žiadosť Komisie, vnútroštátneho dozorného orgánu alebo jeho predsedu. Zatiaľ čo v článku 1 ods. 3 písm. d) návrhu sa uvádza, že návrh nemá vplyv na pravidlá stanovené vo všeobecnom nariadení o ochrane údajov a v smernici (EÚ) 2016/680, splnomocnenie centra EÚ na podávanie žiadostí o stanoviská od EDPB presahuje úlohy zverené EDPB podľa všeobecného nariadenia o ochrane údajov a smernice (EÚ) 2016/680. Preto by sa malo v navrhovanom nariadení – aspoň v odôvodnení – jasne uviesť, že návrhom sa rozširujú úlohy EDPB. EDPB a EDPS v tejto súvislosti oceňujú dôležitú úlohu, ktorú návrh prisudzuje EDPB požadovaním jeho zapojenia do praktického vykonávania navrhovaného nariadenia. V praxi zohráva sekretariát EDPB zásadnú úlohu pri poskytovaní analytickej, administratívnej a logistickej podpory potrebnej na prijatie stanovísk EDPB. Na zabezpečenie toho, aby EDPB a jeho členovia mohli plniť svoje úlohy, je preto nevyhnutné prideliť EDPB dostatočný rozpočet a zamestnancov. V legislatívnom finančnom výkaze návrhu sa však, žiaľ,

---

<sup>85</sup> Dočasné nariadenie, článok 3 ods. 1 písm. c).

<sup>86</sup> Pozri návrh, článok 7 ods. 3 druhá zarážka písm. c).

<sup>87</sup> Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 4.5.2016, s. 89 – 131).

neuvádza, že by na vykonávanie dodatočných úloh, ktoré sa v návrhu pridelujú EDPB, boli k dispozícii akékoľvek dodatočné zdroje.<sup>88</sup>

108. EDPB a EDPS ďalej poznamenávajú, že v článku 50 návrhu sa neuvádza, ako bude centrum EÚ postupovať po prijatí stanoviska EDPB.<sup>89</sup> V odôvodnení 27 návrhu sa len uvádza, že centrum EÚ a Európska komisia by mali zohľadniť odporúčania EDPB. Malo by sa však objasniť, akému účelu by požadované stanovisko slúžilo v postupe podľa článku 50 návrhu a ako by centrum EÚ malo postupovať po získaní stanoviska od EDPB.
109. EDPB a EDPS sa okrem toho domnievajú, že zatiaľ čo akékoľvek usmernenia EDPB alebo prípadné stanovisko k používaniu technológií na zisťovanie posúdia používanie takýchto technológií na všeobecnej úrovni, v prípade predchádzajúcej konzultácie podľa článku 36 všeobecného nariadenia o ochrane údajov bude musieť vnútroštátny dozorný orgán zohľadniť osobitné okolnosti a vykonať individuálne posúdenie zamýšľaného spracúvania príslušným prevádzkovateľom. EDPB a EDPS poznamenávajú, že dozorné orgány budú a mali by uplatňovať kritériá stanovené v článku 36 všeobecného nariadenia o ochrane údajov, aby rozhodli, či je potrebné predĺžiť lehotu stanovenú vo všeobecnom nariadení o ochrane údajov na poskytnutie svojich stanovísk v reakcii na predchádzajúcu konzultáciu, pričom nie je potrebné uplatňovať odlišný prístup, ak sa predchádzajúca konzultácia týka používania technológie na zisťovanie.<sup>90</sup>
110. Napokon pri uplatňovaní článku 11 („Usmernenia o povinnostiach týkajúcich sa zisťovania“) sa v návrhu stanovuje, že Komisia môže vydať usmernenia o uplatňovaní článkov 7 až 10 návrhu. Článok 11 návrhu by sa mal zmeniť tak, aby sa objasnilo, že okrem koordinačných orgánov a centra EÚ by Komisia mala konzultovať s EDPB o návrhu usmernení mimo plánovaného procesu verejných konzultácií pred vydaním usmernení týkajúcich sa povinností týkajúcich sa zisťovania.
111. Táto úloha EDPB, ako aj jeho úloha v právnom rámci, ktorý by sa zaviedol návrhom, si preto vyžadujú ďalšie posúdenie zo strany zákonodarcu.

#### 4.11.3 Úloha Európskeho centra pre prevenciu sexuálneho zneužívania detí a boj proti nemu

112. V kapitole IV návrhu by sa zriadilo centrum EÚ ako nová decentralizovaná agentúra, ktorá by umožnila vykonávanie návrhu. Medzi úlohy centra EÚ by malo patriť aj uľahčovanie prístupu poskytovateľov k spoľahlivým technológiám na zisťovanie; sprístupňovanie ukazovateľov vytvorených na základe online sexuálneho zneužívania detí, ktoré overili súdy alebo nezávislé správne orgány členských štátov, na účely zistenia; na požiadanie poskytovanie určitej pomoci v súvislosti s vykonávaním posúdení rizík a poskytovanie podpory pri komunikácii s príslušnými vnútroštátnymi orgánmi.<sup>91</sup>
113. EDPB a EDPS v tejto súvislosti vítajú článok 77 ods. 1 návrhu, v ktorom sa potvrdzuje, že spracúvanie osobných údajov centrom EÚ podlieha nariadeniu o ochrane údajov inštitúciami EÚ, a stanovuje sa v ňom, že opatrenia na uplatňovanie uvedeného nariadenia centrom EÚ vrátane opatrení týkajúcich sa vymenovania zodpovednej osoby centra EÚ sa stanovia po porade s EDPS. EDPB a EDPS však zastávajú názor, že niekoľko ustanovení tejto kapitoly si zasluhuje dôkladnejšie preskúmanie.

---

<sup>88</sup> Pozri návrh, s. 105 a nasl.

<sup>89</sup> Pozri na porovnanie článok 51 ods. 4 smernice (EÚ) 2016/680.

<sup>90</sup> Pozri návrh, odôvodnenie 24.

<sup>91</sup> Pozri COM(2022) 209 final, s. 7.

114. EDPB a EDPS v prvom rade poznamenávajú, že v článku 48 návrhu sa stanovuje postupovanie všetkých oznámení, ktoré „nie sú zjavne neopodstatnené“<sup>92</sup>, vnútroštátnym orgánom presadzovania práva a Europolu. Táto minimálna úroveň pre centrum EÚ na zasielanie oznámení vnútroštátnym orgánom presadzovania práva a Europolu („nie zjavne neopodstatnené“) sa zdá byť príliš nízka, najmä vzhľadom na to, že účelom zriadenia centra EÚ, ako sa uvádza v správe Komisie o posúdení vplyvu<sup>93</sup>, je zmierniť zaťaženie orgánov presadzovania práva a Europolu filtrovaním obsahu, ktorý bol omylom označený ako materiál obsahujúci sexuálne obťažovanie detí. V tejto súvislosti nie je jasné, prečo by centrum EÚ ako centrum odborných znalostí nemohlo vykonať dôkladnejšie právne a faktické posúdenie s cieľom obmedziť riziko prenosu údajov nevinných osôb orgánom presadzovania práva.
115. Po druhé, ustanovenie týkajúce sa dĺžky uchovávaní osobných údajov centrom EÚ sa zdá byť pomerne otvorené vzhľadom na citlivosť príslušných údajov. Aj keby nebolo možné stanoviť maximálnu lehotu uchovávaní týchto údajov, EDPB a EDPS odporúčajú, aby sa v návrhu stanovila aspoň maximálna lehota na preskúmanie potreby ďalšieho uchovávaní údajov a požadovanie odôvodnenia predĺženia uchovávaní po uplynutí tohto obdobia.
116. Okrem toho vzhľadom na veľmi vysokú citlivosť osobných údajov, ktoré má centrum EÚ spracúvať, EDPB a EDPS zastávajú názor, že spracúvanie by malo podliehať dodatočným zárukám, najmä s cieľom zabezpečiť účinný dohľad. Mohlo by to zahŕňať povinnosť centra EÚ uchovávať logy o spracovateľských operáciách v systémoch automatizovaného spracúvania týkajúcich sa údajov (t. j. podobne ako v prípade požiadavky na operatívne osobné údaje podľa kapitoly IX nariadenia o ochrane údajov inštitúciami EÚ) vrátane logovania vkladania, upravenia, prístupu, konzultovania, sprístupňovania, spájania a vymazania osobných údajov. Na základe logov o vyhľadávaní a sprístupňovaní musí byť možné určiť dôvod, dátum a čas takýchto operácií, identifikovať osobu, ktorá vyhľadávala alebo sprístupnila operatívne osobné údaje, a pokiaľ je to možné, totožnosť príjemcov. Tieto logy by sa použili na overenie zákonnosti spracúvania, vlastné monitorovanie a zaistenie jeho integrity a bezpečnosti a na požiadanie by sa sprístupnili zodpovednej osobe centra EÚ a EDPS.
117. Okrem toho sa v návrhu odkazuje na povinnosť poskytovateľov informovať používateľov o zistení materiálu obsahujúceho sexuálne zneužívanie detí prostredníctvom príkazov na zistenie, ako aj na právo podať sťažnosť koordináčnemu orgánu.<sup>94</sup> V návrhu sa však nestanovujú postupy na výkon práv dotknutých osôb, aj vzhľadom na viaceré miesta, kam sa osobné údaje môžu poskytovať a kde sa môžu uchovávať podľa návrhu (centrum EÚ, Europol, vnútroštátne orgány presadzovania práva). Požiadavka informovať používateľov by mala zahŕňať povinnosť informovať jednotlivcov o tom, že ich údaje boli postúpené a v prípade potreby spracúvané rôznymi subjektmi (napr. vnútroštátnymi orgánmi presadzovania práva a Europolom). Okrem toho by mal existovať centralizovaný postup prijímania a koordinácie žiadostí o právo na prístup, opravu a vymazanie alebo prípadne povinnosť, aby subjekt, ktorému bola doručená žiadosť dotknutej osoby, koordinoval svoju činnosť s ostatnými dotknutými subjektmi.
118. EDPB a EDPS poznamenávajú, že podľa článku 50 návrhu má centrum EÚ za úlohu špecifikovať zoznam technológií, ktoré sa môžu použiť na vykonávanie príkazov na zistenie. Podľa článku 12 ods. 1 návrhu sú však poskytovatelia povinní oznamovať všetky informácie o možnom online sexuálnom zneužívaní

---

<sup>92</sup> Pojem „zjavne neopodstatnené“ je opísaný v odôvodnení 65 návrhu ako „ak je bez akejkoľvek vecnej právnej alebo fakтической analýzy okamžite zrejmé, že oznámené činnosti nepredstavujú sexuálne zneužívanie detí online“.

<sup>93</sup> Pozri napríklad stranu 349 správy o posúdení vplyvu.

<sup>94</sup> Pozri článok 10 ods. 6 a po predložení správy centru EÚ aj článok 12 ods. 2 návrhu.

detí v rámci svojich služieb, nielen tie, ktoré pochádzajú z vykonania príkazu na zistenie. Je veľmi pravdepodobné, že značné množstvo takýchto informácií by pochádzalo z uplatňovania zmierňujúcich opatrení poskytovateľov v súlade s článkom 4 návrhu. Preto sa zdá byť zásadné určiť, aké by mohli byť tieto opatrenia, ich účinnosť, miera chybovosti pri oznamovaní potenciálneho sexuálneho zneužívania detí a aký je ich vplyv na práva a slobody jednotlivcov. Napriek skutočnosti, že v článku 4 ods. 5 návrhu sa uvádza, že Komisia v spolupráci s koordinačnými orgánmi a centrom EÚ a po uskutočnení verejnej konzultácie môže vydať príslušné usmernenia, EDPB a EDPS považujú za dôležité, aby zákonodarca do článku 50 zahrnul aj úlohu centra EÚ poskytnúť aj zoznam odporúčaných zmierňujúcich opatrení a príslušných najlepších postupov, ktoré sú účinné najmä pri identifikácii potenciálneho online sexuálneho zneužívania detí. Keďže takéto opatrenia môžu zasahovať do základných práv na ochranu údajov a súkromia, odporúča sa, aby centrum EÚ pred vydaním takéhoto zoznamu požiadalo EDPB o stanovisko.

119. Napokon, bezpečnostné požiadavky stanovené v článku 51 ods. 4 návrhu by mali byť konkrétnejšie. V tejto súvislosti sa možno inšpirovať bezpečnostnými požiadavkami stanovenými v iných nariadeniach týkajúcich sa rozsiahlych systémov zahŕňajúcich spracúvanie s vysokým rizikom, ako je nariadenie 767/2008<sup>95</sup> (pozri článok 32), nariadenie 1987/2006<sup>96</sup> (pozri článok 16), nariadenie 2018/1862<sup>97</sup> (pozri článok 16) a nariadenie č. 603/2013<sup>98</sup> (pozri článok 34).

#### 4.11.4 Úloha Europolu

120. V návrhu sa stanovuje úzka spolupráca medzi centrom EÚ a Europolom. Podľa kapitoly IV návrhu centrum EÚ po prijatí oznámení poskytovateľov o podozreniach na materiál obsahujúci sexuálne zneužívanie detí vykoná kontrolu s cieľom posúdiť, ktoré oznámenia sú využiteľné (nie sú zjavne neopodstatnené) a postúpi ich Europolu, ako aj vnútroštátnym orgánom presadzovania práva.<sup>99</sup> Centrum EÚ poskytne Europolu prístup do svojich databáz ukazovateľov a databáz oznámení s cieľom pomôcť Europolu pri vyšetrowaní podozrení z trestných činov sexuálneho zneužívania detí.<sup>100</sup> Okrem

---

<sup>95</sup> Nariadenie Európskeho parlamentu a Rady (ES) č. 767/2008 z 9. júla 2008 o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi, Ú. v. EÚ L 218, 13.8.2008, s. 60 – 81.

<sup>96</sup> Nariadenie Európskeho parlamentu a Rady (ES) č. 1987/2006 z 20. decembra 2006 o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II) (Ú. v. EÚ L 381, 28.12.2006, s. 4 – 23).

<sup>97</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1862 z 28. novembra 2018 o zriadení, prevádzke a využívaní Schengenského informačného systému (SIS) v oblasti policajnej spolupráce a justičnej spolupráce v trestných veciach, o zmene a zrušení rozhodnutia Rady 2007/533/SVV a o zrušení nariadenia Európskeho parlamentu a Rady (ES) č. 1986/2006 a rozhodnutia Komisie 2010/261/EÚ (Ú. v. EÚ L 312, 7.12.2018, s. 56 – 106).

<sup>98</sup> Nariadenie Európskeho Parlamentu a Rady (EÚ) č. 603/2013 z 26. júna 2013 o zriadení systému Eurodac na porovnávanie odtlačkov prstov pre účinné uplatňovanie nariadenia (EÚ) č. 604/2013, ktorým sa ustanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov, a o žiadostiach orgánov členských štátov na presadzovanie práva a Europolu o porovnanie s údajmi v systéme Eurodac na účely presadzovania práva a o zmene nariadenia (EÚ) č. 1077/2011, ktorým sa zriaďuje Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti (Ú. v. EÚ L 180, 29.6.2013, s. 1 – 30).

<sup>99</sup> Pozri článok 48 návrhu.

<sup>100</sup> Pozri článok 46 ods. 4 až 5 návrhu.



toho by sa centru EÚ poskytol „čo najširší“ prístup k informačným systémom Europolu.<sup>101</sup> Obe agentúry budú tiež spoločne využívať priestory a určitú (neprevádzkovú) infraštruktúru.<sup>102</sup>

121. EDPB a EDPS poznamenávajú, že viaceré aspekty týkajúce sa spolupráce medzi navrhovaným centrom EÚ a Europolom vyvolávajú obavy alebo si vyžadujú ďalšie spresnenie.

O postupovaní oznámení centrom EÚ Europolu (článok 48)

122. V článku 48 navrhovaného nariadenia sa vyžaduje, aby centrum EÚ postupovalo oznámenia, ktoré nie sú zjavne neopodstatnené, spolu so všetkými ďalšími relevantnými informáciami, ktoré má k dispozícii, Europolu a príslušnému orgánu alebo orgánom presadzovania práva členského štátu/členských štátov, ktoré pravdepodobne majú právomoc vyšetrovať alebo stíhať potenciálne sexuálne zneužívanie detí. Hoci tento článok priznáva Europolu úlohu identifikovať príslušný orgán presadzovania práva, ak je dotknutý členský štát nejednoznačný, v tomto ustanovení sa v skutočnosti stanovuje, že všetky oznámenia sa Europolu zasielajú bez ohľadu na to, či centrum EÚ identifikovalo a už zaslalo oznámenie vnútroštátnemu orgánu.
123. V návrhu sa však neobjasňuje, aká by bola pridaná hodnota zapojenia Europolu alebo jeho očakávaná úloha po prijatí oznámení, najmä v tých prípadoch, keď bol súčasne identifikovaný a informovaný vnútroštátny orgán presadzovania práva.<sup>103</sup>
124. EDPB a EDPS pripomínajú, že mandát Europolu sa obmedzuje na podporu opatrení príslušných orgánov členských štátov a ich vzájomnú spoluprácu pri predchádzaní závažnej trestnej činnosti, ktorá sa týka dvoch alebo viacerých členských štátov, a boji proti nej.<sup>104</sup> V článku 19 nariadenia (EÚ) 2016/794<sup>105</sup> zmeneného nariadením (EÚ) 2022/991<sup>106</sup> (ďalej len „zmenené nariadenie o Europole“) sa stanovuje, že orgán Únie, ktorý poskytuje informácie Europolu, je povinný určiť účel alebo účely, na ktoré má Europol spracúvať informácie, ako aj podmienky ich spracúvania. Zodpovedá aj za zabezpečenie správnosti prenášaných osobných údajov.<sup>107</sup>
125. Plošné postupovanie oznámení Europolu by preto bolo v rozpore so zmeneným nariadením o Europole a predstavovalo by niekoľko rizík v oblasti ochrany údajov. Duplicita spracúvania osobných údajov by mohla viesť k paralelnému uchovávaniu viacerých kópií tých istých vysoko citlivých osobných údajov (napr. centrom EÚ, Europolom, vnútroštátnym orgánom presadzovania práva), čo by mohlo ohroziť správnosť údajov v dôsledku potenciálnej desynchronizácie databáz, ako aj

---

<sup>101</sup> Pozri článok 53 ods. 2 návrhu.

<sup>102</sup> Najmä pokiaľ ide o riadenie ľudských zdrojov, informačné technológie (IT) vrátane kybernetickej bezpečnosti, budov a komunikácií.

<sup>103</sup> V odôvodnení 71 návrhu sa len všeobecne odkazuje na skúsenosti Europolu s identifikáciou príslušných vnútroštátnych orgánov v nejasných situáciách a na jeho databázu spravodajských informácií o trestnej činnosti, ktoré môžu prispieť k identifikácii prepojení na vyšetrovania v iných členských štátoch.

<sup>104</sup> Pozri článok 3 zmeneného nariadenia o Europole.

<sup>105</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/794 z 11. mája 2016 o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol), ktorým sa nahrádzajú a zrušujú rozhodnutia Rady 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Ú. v. EÚ L 135, 24.5.2016, s. 53 – 114).

<sup>106</sup> Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/991 z 8. júna 2022, ktorým sa mení nariadenie (EÚ) 2016/794, pokiaľ ide o spoluprácu Europolu so súkromnými subjektmi, spracúvanie osobných údajov Europolom na podporu vyšetrovania trestných činov a úlohu Europolu v oblasti výskumu a inovácií (Ú. v. EÚ L 169, 27.6.2022, s. 1 – 42).

<sup>107</sup> Článok 38 ods. 2 písm. a) zmeneného nariadenia o Europole.

uplatňovanie práv dotknutých osôb. Okrem toho, v návrhu stanovená nízka hranica na výmenu oznámení s orgánmi presadzovania práva (tie, ktoré „nie sú zjavne neopodstatnené“) znamená vysokú pravdepodobnosť, že falošné pozitívne výsledky (t. j. obsah omylom označený ako sexuálne zneužívanie detí) sa budú uchovávať v informačných systémoch Europolu, a to potenciálne na dlhšie obdobia.<sup>108</sup>

126. EDPB a EDPS preto odporúčajú, aby sa v návrhu špecifikovali a obmedzili okolnosti a účely, za ktorých by centrum EÚ mohlo zasielať oznámenia Europolu v súlade so zmeneným nariadením o Europole. Tým by sa mali výslovne vylúčiť tie okolnosti, keď boli oznámenia zaslané príslušnému orgánu presadzovania práva členského štátu, čo znamená, že nemajú cezhraničný rozmer. Návrh by mal okrem toho obsahovať požiadavku, aby centrum EÚ zasielalo Europolu len také osobné údaje, ktoré sú primerané, relevantné a obmedzené na to, čo je nevyhnutne potrebné. Musia sa stanoviť aj osobitné záruky na zabezpečenie kvality a spoľahlivosti údajov.

---

<sup>108</sup> Podľa správy Komisie o posúdení vplyvu bol Europol schopný preskúmať len 20% z 50 miliónov jedinečných obrázkov a videí materiálu obsahujúceho sexuálne zneužívanie detí vo svojej databáze, čo vypovedá o nedostatku zdrojov na reakciu na príspevky s materiálom obsahujúcim sexuálne zneužívanie detí, ktoré v súčasnosti dostáva. Pozri správu o posúdení vplyvu, ktorá je sprievodným dokumentom k návrhu nariadenia, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu, SWD(2022) 209, s. 47–48.

Článok 53 ods. 2 o spolupráci medzi centrom EÚ a Europolom

127. V článku 53 ods. 2 návrhu sa vyžaduje, aby si Europol a centrum EÚ navzájom poskytovali „čo najširší prístup k relevantným informáciám a informačným systémom, ak je to potrebné na plnenie príslušných úloh a v súlade s právnymi aktmi Únie upravujúcimi takýto prístup“.
128. V článku 46 ods. 4 a 5 návrhu sa ďalej uvádza, že Europol má prístup do databázy ukazovateľov centra EÚ a do databázy oznámení, a v článku 46 ods. 6 sa stanovuje postup udeľovania tohto prístupu: Europol predloží žiadosť, v ktorej uvedie účel a stupeň prístupu potrebného na dosiahnutie uvedeného účelu, ktorú centrum EÚ náležite posúdi.
129. Kritériá a záruky, ktoré podmieňujú prístup Europolu k údajom získaným z informačných systémov centra EÚ a ich následné použitie, nie sú špecifikované. Okrem toho nie je vysvetlené, prečo je potrebné poskytnúť Europolu priamy prístup k informačným systémom orgánu, ktorý nie je orgánom presadzovania práva a ktoré obsahujú veľmi citlivé osobné údaje, ktorých súvis s trestnou činnosťou a predchádzaním trestnej činnosti nemusel byť preukázaný. Na zabezpečenie vysokej úrovne ochrany údajov a dodržiavanie zásady obmedzenia účelu EDPB a EDPS odporúčajú, aby sa osobné údaje z centra EÚ Europolu zasielali len na individuálnom základe [case-by-case basis] a na základe riadne posúdenej žiadosti, a to prostredníctvom zabezpečeného komunikačného nástroja na výmenu informácií, akým je SIENA.<sup>109</sup>
130. V článku 53 ods. 2 sa uvádza jediný odkaz v návrhu na prístup centra EÚ k informačným systémom Europolu. Nie je teda jasné, na aké účely a podľa akých osobitných záruk by sa takýto prístup uskutočnil.
131. EDPB a EDPS pripomínajú, že Europol je orgánom presadzovania práva zriadeným podľa zmlúv EÚ, ktorého hlavným mandátom je predchádzanie závažnej trestnej činnosti a boj proti nej. Operatívne osobné údaje spracúvané Europolom preto podliehajú prísnyh pravidlám spracúvania údajov a zárukám. Navrhované centrum EÚ nie je orgánom presadzovania práva a za žiadnych okolností by mu nemal byť poskytnutý priamy prístup do informačných systémov Europolu.
132. EDPB a EDPS ďalej poznamenávajú, že veľká časť informácií, ktoré sú predmetom spoločného záujmu centra EÚ a Europolu, sa bude týkať osobných údajov týkajúcich sa obetí údajných trestných činov, osobných údajov maloletých a osobných údajov týkajúcich sa sexuálneho života, ktoré sa podľa zmeneného nariadenia o Europole považujú za osobitné kategórie osobných údajov. V zmenenom nariadení o Europole sa stanovujú prísne podmienky týkajúce sa prístupu k osobitným kategóriám osobných údajov. V článku 30 ods. 3 zmeneného nariadenia o Europole sa stanovuje, že priamy prístup k takýmto osobným údajom má len Europol, konkrétne len obmedzený počet úradníkov Europolu, ktorým výkonný riaditeľ riadne udelil oprávnenie.<sup>110</sup>
133. EDPB a EDPS preto odporúčajú objasniť znenie článku 53 ods. 2 návrhu s cieľom náležite zohľadniť obmedzenia zavedené podľa zmeneného nariadenia o Europole a spresniť spôsoby prístupu centra EÚ. Najmä akýkoľvek prístup k osobným údajom spracúvaným v informačných systémoch Europolu, ak sa považuje za nevyhnutne potrebný na plnenie úloh centra EÚ, by sa mal udeliť len na individuálnom základe [case-by-case basis], a to na základe výslovnej žiadosti, ktorá dokumentuje konkrétny účel a odôvodnenie. Od Europolu by sa malo vyžadovať, aby tieto žiadosti dôsledne

---

<sup>109</sup> Sieťová aplikácia na zabezpečenú výmenu informácií (SIENA).

<sup>110</sup> Podľa zmeneného nariadenia o Europole sa výnimky z tohto zákazu stanovujú pre agentúry Únie zriadené podľa hlavy V ZFEÚ. Vzhľadom na právny základ návrhu (14 ZFEÚ, ktorý sa týka harmonizácie vnútorného trhu) by však táto výnimka nezahrňala navrhované centrum EÚ.

posudzoval a zasielal osobné údaje centru EÚ len vtedy, ak je to nevyhnutne potrebné a proporcionálne požadovanému účelu.

Článok 10 ods. 6 o úlohe Europolu pri informovaní používateľov po vykonaní príkazu na zistenie

134. EDPB a EDPS vítajú požiadavku stanovenú v článku 10 ods. 6 návrhu, aby poskytovatelia informovali používateľov, ktorých osobné údaje môžu byť dotknuté vykonaním príkazu na zistenie. Tieto informácie sa majú používateľom poskytnúť až po získaní potvrdenia od Europolu alebo vnútroštátneho orgánu presadzovania práva členského štátu, ktorý prijal oznámenie podľa článku 48 návrhu, že poskytovanie informácií používateľom by nezasahovalo do činností v oblasti prevencie, zisťovania, vyšetrovania a stíhania trestných činov sexuálneho zneužívania detí.
135. V súvislosti s praktickým vykonávaním tohto ustanovenia však chýba špecifickosť. Ak sa správy zasielajú Europolu aj orgánu presadzovania práva členského štátu, v návrhu sa nestanovuje, či sa vyžaduje potvrdenie od jedného alebo oboch príjemcov, a ani postupy/spôsoby na získanie tohto potvrdenia nie sú v návrhu uvedené (napr. či sa potvrdenia majú zasielať prostredníctvom centra EÚ). Vzhľadom na vysoký objem materiálu obsahujúceho sexuálne zneužívanie detí, ktorý by Europol a vnútroštátne orgány presadzovania práva mohli byť povinné spracúvať, a na chýbajúcu presnú lehotu na poskytnutie potvrdenia („bez zbytočného odkladu“) EDPB a EDPS odporúčajú objasniť uplatniteľné postupy s cieľom zabezpečiť vykonávanie tejto záruky v praxi. Okrem toho by povinnosť informovať používateľov mala zahŕňať aj informácie o príjemcoch príslušných osobných údajov.

O zbere údajov a podávaní správ o transparentnosti (článok 83)

136. V článku 83 ods. 3 návrhu sa stanovuje, že centrum EÚ zbiera údaje a generuje štatistiky týkajúce sa viacerých jeho úloh podľa navrhovaného nariadenia. Na účely monitorovania EDPB a EDPS odporúčajú doplniť do tohto zoznamu štatistické údaje o počte oznámení postúpených Europolu v súlade s článkom 48, ako aj o počte žiadostí o prístup prijatých Europolom podľa článku 46 ods. 4 a článku 46 ods. 5 vrátane počtu žiadostí, ktoré centrum EÚ schválilo a zamietlo.

## 5. ZÁVER

137. Hoci EDPB a EDPS vítajú úsilie Komisie o zabezpečenie účinných opatrení proti online sexuálnemu zneužívaniu detí, domnievajú sa, že návrh vyvoláva vážne obavy týkajúce sa ochrany údajov a súkromia. EDPB a EDPS by preto vyzvali spoluzákonodarcov, aby zmenili navrhované nariadenie, najmä s cieľom zabezpečiť, aby plánované povinnosti zisťovania spĺňali platné štandardy nevyhnutnosti a primeranosti a neviedli k oslabeniu alebo zhoršeniu šifrovania na všeobecnej úrovni. EDPB a EDPS sú naďalej pripravený ponúknuť svoju podporu počas legislatívneho procesu, ak by sa ich príspevky považovali za potrebné na riešenie obáv zdôraznených v tomto spoločnom stanovisku.

Za Európskeho dozorného úradníka pre ochranu údajov

Európsky dozorný úradník pre ochranu údajov

(Wojciech Wiewiorowski)

Za Európsky výbor pre ochranu údajov

predsedníčka

(Andrea Jelinek)