

EDPB-EIOÚ

**Společné stanovisko 4/2022
k návrhu nařízení Evropského
parlamentu a Rady, kterým se
stanoví pravidla pro
předcházení pohlavnímu
zneužívání dětí a boj proti
němu**

Přijato dne 28. července 2022

OBSAH

1.	Souvislosti	7
2.	Oblast působnosti stanoviska	8
3.	Obecné připomínky k právu na důvěrnost komunikace a na ochranu osobních údajů	9
4.	Konkrétní připomínky	12
4.1	Vztah ke stávajícím právním předpisům	12
4.1.1	Vztah k obecnému nařízení o ochraně osobních údajů a směrnici o soukromí a elektronických komunikacích	12
4.1.2	Vztah k nařízení (EU) 2021/1232 a dopad na dobrovolné odhalování pohlavního zneužívání dětí on-line	12
4.2	Právní základ podle obecného nařízení o ochraně osobních údajů	13
4.3	Povinnosti týkající se posuzování a zmírňování rizik	13
4.4	Podmínky pro vydávání detekčních příkazů	15
4.5	Analýza nezbytnosti a proporcionality plánovaných opatření	16
4.5.1	Účinnost odhalování	17
4.5.2	Neexistuje žádné opatření, které by méně zasahovalo do práv	18
4.5.3	Proporcionalita v užším slova smyslu	19
4.5.4	Odhalování známých materiálů pohlavního zneužívání dětí	20
4.5.5	Odhalování dříve neznámých materiálů pohlavního zneužívání dětí	21
4.5.6	Odhalování navazování kontaktu s dětmi („grooming“)	22
4.5.7	Závěr o nezbytnosti a proporcionality plánovaných opatření	23
4.6	Oznamovací povinnosti	23
4.7	Povinnost týkající se odstranění a povinnost provést blokování	23
4.8	Relevantní technologie a záruky	24
4.8.1	Záměrná a standardní ochrana osobních údajů	24
4.8.2	Spolehlivost technologií	25
4.8.3	Skenování zvukové komunikace	26
4.8.4	Ověřování věku	26
4.9	Uchovávání informací	27
4.10	Dopad na šifrování	27
4.11	Dohled, prosazování práva a spolupráce	29
4.11.1	Úloha vnitrostátních dozorových úřadů podle obecného nařízení o ochraně osobních údajů	29

4.11.2	Úloha EDPB.....	29
4.11.3	Úloha Střediska EU proti pohlavnímu zneužívání dětí	31
4.11.4	Úloha Europolu.....	33
5.	Závěr.....	36

Shrnutí

Dne 11. května 2022 zveřejnila Evropská komise návrh nařízení Evropského parlamentu a Rady, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu.

Návrh by poskytovatelům hostingových služeb, interpersonálních komunikačních služeb a dalších služeb uložil podmíněné povinnosti týkající se odhalování, oznamování, odstraňování a blokování známého a nového materiálu pohlavního zneužívání dětí, jakož i navazování kontaktu s dětmi. Návrh rovněž stanoví zřízení nové decentralizované agentury EU (dále jen „středisko EU“) a sítě vnitrostátních koordinačních orgánů pro otázky pohlavního zneužívání dětí s cílem umožnit provádění navrhovaného nařízení. Jak bylo uznáno v důvodové zprávě návrhu, opatření obsažená v návrhu by ovlivnila výkon základních práv uživatelů dotčených služeb.

Pohlavní zneužívání dětí je obzvláště závažným a ohavným trestným činem a cíl umožnit účinný boj proti němu představuje cíl obecného zájmu, který je uznáván Uníí a je veden snahou o ochranu práv a svobod obětí. EDPB a EIOÚ zároveň připomínají, že veškerá omezení základních práv, jako jsou ta, která stanoví návrh, musí být v souladu s požadavky stanovenými v čl. 52 odst. 1 Listiny základních práv Evropské unie.

EDPB a EIOÚ zdůrazňují, že návrh vzbuzuje vážné obavy, pokud jde o proporcionalitu zamýšleného zasahování do základních práv na soukromí a ochranu osobních údajů a omezení ochrany těchto práv. V tomto ohledu EDPB a EIOÚ zdůrazňují, že procesní záruky nemohou nikdy zcela nahradit hmotněprávní záruky. Složitý systém eskalace počínaje opatřeními týkajícími se posouzení a zmírnění rizik až po detekční příkaz nemůže nahradit nezbytnou jasnost hmotněprávních povinností.

EDPB a EIOÚ se domnívají, že návrh není dostatečně jasný, pokud jde o klíčové prvky, jako jsou například pojmy „významné riziko“. Kromě toho subjekty pověřené uplatňováním těchto záruk, počínaje soukromými subjekty a konče správními a/nebo soudními orgány, mají velmi široký prostor pro vlastní uvážení, což vede k právní nejistotě ohledně toho, jak vyvážit dotčená práva v každém jednotlivém případě. EDPB a EIOÚ zdůrazňují, že normotvůrce musí při povolování zvláště závažného zasahování do základních práv poskytnout právní jistotu ohledně toho, kdy a kde je zasahování povoleno. Ačkoli EDPB a EIOÚ uznávají, že právní předpisy nemohou být příliš preskriptivní a musí ponechat určitou flexibilitu pro praktické uplatňování, domnívají se, že návrh ponechává příliš velký prostor pro možné zneužití z důvodu neexistence jasných hmotněprávních norem.

Pokud jde o nezbytnost a proporcionalitu plánovaných opatření pro odhalování, EDPB a EIOÚ jsou znepokojeni zejména opatřeními stanovenými pro odhalování neznámého materiálu pohlavního zneužívání dětí a navazování kontaktu s dětmi („grooming“) v interpersonálních komunikačních službách. Vzhledem k míře, v jaké zasahují do základních práv, pravděpodobnostní povaze a míře chyb spojených s těmito technologiemi se EDPB a EIOÚ domnívají, že zasahování do práv způsobené těmito opatřeními přesahuje rámec toho, co je nezbytné a přiměřené. Kromě toho opatření, která umožňují veřejným orgánům mít všeobecný přístup k obsahu sdělení za účelem odhalování navazování kontaktu s dětmi, mohou s větší pravděpodobností ovlivnit podstatu práv zaručených v člancích 7 a 8 Listiny. Příslušná ustanovení týkající se groomingu by proto měla být z návrhu odstraněna. Kromě toho návrh nevylučuje ze své oblasti působnosti skenování zvukové komunikace. EDPB a EIOÚ se domnívají, že skenování zvukové komunikace obzvláště zasahuje do práv a jako takové musí zůstat mimo oblast působnosti povinností týkajících se odhalování stanovených v navrhovaném nařízení, jak co se týče hlasových zpráv, tak komunikace naživo.

EDPB a EIOÚ rovněž vyjadřují pochybnosti ohledně účinnosti blokovacích opatření a domnívají se, že požadavek, aby poskytovatelé internetových služeb dešifrovali on-line komunikaci s cílem blokovat komunikaci týkající se materiálu pohlavního zneužívání dětí, by byl nepřiměřený.

EDPB a EIOÚ dále zdůrazňují, že šifrovací technologie zásadním způsobem přispívají k respektování soukromého života a důvěrnosti komunikace, svobodě projevu, jakož i k inovacím a růstu digitální ekonomiky, která závisí na vysoké úrovni důvěry, kterou tyto technologie zajišťují. 26. bod odůvodnění návrhu stanoví výhradu nejen pro volbu detekčních technologií, ale také pro technická opatření na ochranu důvěrnosti komunikace, jako je šifrování, a sice že tato volba technologií musí splňovat požadavky navrhovaného nařízení, tj. musí umožňovat odhalování. To podporuje myšlenku vyplývající z čl. 8 odst. 3 a čl. 10 odst. 2 návrhu, že poskytovatel nemůže odmítnout provedení detekčního příkazu na základě technické nemožnosti. EDPB a EIOÚ se domnívají, že by měla existovat lepší rovnováha mezi společenskou potřebou mít zabezpečené a soukromé komunikační kanály a bojovat proti jejich zneužívání. V návrhu by mělo být jasně uvedeno, že žádné ustanovení navrhovaného nařízení by nemělo být vykládáno tak, že zakazuje nebo oslabuje šifrování.

EDPB a EIOÚ sice vítají, že součástí návrhu je prohlášení, že návrhem nejsou dotčeny pravomoci a příslušnost úřadů pro ochranu údajů podle obecného nařízení o ochraně osobních údajů, EDPB a EIOÚ jsou však toho názoru, že vztah mezi úkoly koordinačních orgánů a úkoly úřadů pro ochranu údajů by měl být lépe upraven. V tomto ohledu EDPB a EIOÚ oceňují úlohu, kterou návrh svěřuje EDPB, jelikož požaduje jeho zapojení do praktického provádění návrhu, zejména nutný požadavek, aby EDPB vydal stanovisko k technologiím, které by středisko EU zpřístupnilo za účelem výkonu detekčních příkazů. Mělo by však být vyjasněno, jakému účelu by stanovisko v tomto procesu sloužilo a jak bude středisko EU postupovat poté, co stanovisko od EDPB obdrží.

EDPB a EIOÚ rovněž konstatují, že návrh stanoví úzkou spolupráci mezi střediskem EU a Europolem, které by si měly vzájemně poskytovat „co nejširší přístup k relevantním informačním systémům“. Ačkoliv EDPB a EIOÚ v zásadě podporují spolupráci obou agentur, vzhledem k tomu, že středisko EU není donucovacím orgánem, EDPB a EIOÚ přesto předkládají několik doporučení ke zlepšení příslušných ustanovení, včetně toho, že předávání osobních údajů mezi střediskem EU a Europolem má probíhat pouze v jednotlivých případech na základě řádně posouzené žádosti, a to prostřednictvím komunikačního nástroje pro zabezpečenou výměnu informací, jako je síť SIENA.

Evropský sbor pro ochranu osobních údajů a evropský inspektor ochrany údajů

s ohledem na čl. 42 odst. 2 nařízení 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (dále jen „nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie“),¹

s ohledem na Dohodu o EHP a zejména přílohu XI a protokol 37 k uvedené dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018,²

s ohledem na žádost Evropské komise o společné stanovisko Evropského sboru pro ochranu osobních údajů a evropského inspektora ochrany údajů ze dne 12. května 2022 k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu,³

PŘIJALI TOTO SPOLEČNÉ STANOVISKO

1. SOUVISLOSTI

1. Dne 11. května 2022 zveřejnila Evropská komise (dále jen „Komise“) návrh nařízení Evropského parlamentu a Rady, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu (dále jen „návrh“ nebo „navrhované nařízení“).⁴
2. Návrh byl vydán v návaznosti na přijetí nařízení (EU) 2021/1232 o dočasné odchylce od některých ustanovení směrnice 2002/58/ES, pokud jde o používání technologií poskytovateli interpersonálních komunikačních služeb nezávislých na číslech ke zpracování osobních a jiných údajů pro účely boje proti pohlavnímu zneužívání dětí on-line (dále jen „prozatímní nařízení“).⁵ Prozatímní nařízení nevyžaduje, aby příslušní poskytovatelé služeb zavedli opatření k odhalování materiálů pohlavního zneužívání dětí (např. fotografií, videí atd.) nebo navazování kontaktu s dětmi (známé také jako „grooming“) na jejich službách, ale umožňuje těmto poskytovatelům, aby tak činili dobrovolně v souladu s podmínkami stanovenými v uvedeném nařízení.⁶
3. Návrh se skládá ze dvou hlavních stavebních kamenů. Zaprvé ukládá poskytovatelům hostingových služeb, interpersonálních komunikačních služeb a dalších služeb podmíněné povinnosti týkající se

¹ Úř. věst. L 295, 21.11.2018, s. 39.

² Pokud se v tomto dokumentu hovoří o „členských státech“, rozumějí se tím „členské státy EHP“.

³ Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu, COM(2022) 209 final.

⁴ Tamtéž.

⁵ Nařízení Evropského parlamentu a Rady (EU) 2021/1232 ze dne 14. července 2021 o dočasné odchylce od některých ustanovení směrnice 2002/58/ES, pokud jde o používání technologií poskytovateli interpersonálních komunikačních služeb nezávislých na číslech ke zpracování osobních a jiných údajů pro účely boje proti pohlavnímu zneužívání dětí on-line, Úř. věst. [2021] L 274/41.

⁶ Viz také EIOÚ, stanovisko č. 7/2020 k návrhu dočasných odchylek od směrnice 2002/58/ES pro účely boje proti pohlavnímu zneužívání dětí on-line (10. listopadu 2020).

odhalování, oznamování, odstraňování a blokování známých a nových materiálů pohlavního zneužívání dětí, jakož i navazování kontaktu s dětmi. Zadruhé návrh stanoví zřízení nové decentralizované agentury EU (dále jen „středisko EU proti pohlavnímu zneužívání dětí“ nebo „středisko EU“) a síť vnitrostátních koordinačních orgánů pro otázky pohlavního zneužívání dětí s cílem umožnit provádění navrhovaného nařízení.⁷

4. Jak bylo uznáno v důvodové zprávě návrhu, opatření obsažená v návrhu by ovlivnila výkon základních práv uživatelů dotčených služeb. Tato práva zahrnují zejména základní práva na respektování soukromí (včetně důvěrnosti komunikace jako součásti širšího práva na respektování soukromého a rodinného života), ochranu osobních údajů a svobodu projevu a informací.⁸
5. Tato navrhovaná opatření mají navíc vycházet ze stávajících právních předpisů EU v oblasti ochrany údajů a soukromí a do určité míry je doplňovat. V této souvislosti se v důvodové zprávě uvádí, že:

„Návrh vychází z obecného nařízení o ochraně osobních údajů. V praxi mají poskytovatelé tendenci při zpracování osobních údajů, které jsou součástí dobrovolného odhalování a oznamování pohlavního zneužívání dětí on-line, uplatňovat různé důvody pro zpracování, které jsou stanovené v obecném nařízení o ochraně osobních údajů. Návrh stanoví systém cílených detekčních příkazů a upřesňuje podmínky pro odhalení, čímž pro tyto činnosti poskytuje větší právní jistotu. Pokud jde o povinné činnosti týkající se odhalení, mezi které patří zpracování osobních údajů, návrh (zejména detekční příkazy vydané na jeho základě) tímto způsobem určuje důvod pro toto zpracování podle čl. 6 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů, který stanoví zpracování osobních údajů jako nezbytné pro splnění právní povinnosti podle práva Unie nebo členského státu, které se vztahuje na správce údajů.

Návrh se vztahuje mimo jiné na poskytovatele, kteří nabízejí interpersonální elektronické komunikační služby, a proto pro ně platí vnitrostátní předpisy provádějící směrnici o soukromí a elektronických komunikacích a její navrhovanou revizi, která je v současné době předmětem jednání. Opatření stanovená v návrhu omezují v některých ohledech rozsah práv a povinností podle příslušných ustanovení uvedené směrnice, zejména pokud jde o činnosti, které jsou nezbytně nutné k provedení detekčních příkazů. V tomto ohledu návrh zahrnuje analogické použití čl. 15 odst. 1 uvedené směrnice.“⁹

6. Vzhledem k závažnosti zamýšleného zasahování do základních práv má návrh zvláštní význam pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů. Dne 12. května 2022 se proto Komise v souladu s čl. 42 odst. 2 nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie rozhodla konzultovat Evropský sbor pro ochranu osobních údajů (dále jen „EDPB“) a evropského inspektora ochrany údajů (dále jen „EIOÚ“).

2. OBLAST PŮSOBNOSTI STANOVISKA

7. Toto společné stanovisko uvádí společné názory EDPB a EIOÚ na předmětný návrh. Omezuje se na ty aspekty návrhu, které se týkají ochrany soukromí a osobních údajů. Společné stanovisko zejména

⁷ COM(2022)209 final, s. 17.

⁸ COM(2022)209 final, s. 12.

⁹ COM(2022)209 final, s. 4–5.

poukazuje na oblasti, v nichž návrh nezajišťuje dostatečnou ochranu základních práv na soukromí a na ochranu údajů nebo které vyžaduje další sladění s právním rámcem EU týkajícím se ochrany soukromí a osobních údajů.

8. Jak je dále vysvětleno v tomto společném stanovisku, návrh vzbuzuje vážné obavy, pokud jde o nezbytnost a proporcionalitu zamýšlených zásahů a omezení ochrany základních práv na soukromí a na ochranu osobních údajů. Cílem tohoto společného stanoviska však není poskytnout vyčerpávající seznam všech otázek týkajících se ochrany soukromí a údajů, které návrh vyvolává, ani předložit konkrétní návrhy na zlepšení znění návrhu. Místo toho obsahuje toto společné stanovisko připomínky na vysoké úrovni k hlavním problémům návrhu, které identifikovali EDPB a EIOÚ. EDPB a EIOÚ jsou však i nadále připraveni předkládat spolunormotvůrcům během legislativního procesu týkajícího se návrhu další připomínky a doporučení.

3. OBECNÉ PŘIPOMÍNKY K PRÁVU NA DŮVĚRNOST KOMUNIKACE A NA OCHRANU OSOBNÍCH ÚDAJŮ

9. Důvěrnost komunikace je zásadním prvkem základního práva na respektování soukromého a rodinného života, jak je zakotveno v článku 7 Listiny základních práv Evropské unie (dále jen „Listina“).¹⁰ Kromě toho článek 8 Listiny uznává základní právo na ochranu osobních údajů. Právo na důvěrnost komunikace a právo na soukromý a rodinný život jsou rovněž zaručeny v článku 8 Evropské úmluvy o lidských právech (dále jen „EÚLP“) a jsou součástí ústavních tradic, které mají členské státy společné.¹¹
10. EDPB a EIOÚ připomínají, že práva zakotvená v článcích 7 a 8 Listiny se však neprojevují jako absolutní výsady, ale musí být nahlížena ve vztahu k jejich společenské funkci.¹² Pohlavní zneužívání dětí je obzvláště závažným a ohavným trestným činem a cíl umožnit účinný boj proti němu představuje cíl obecného zájmu, který uznává Unie, a je veden snahou o ochranu práv a svobod obětí. Pokud jde o účinná opatření v boji proti trestným činům páchaným na nezletilých a jiných zranitelných osobách, Soudní dvůr Evropské unie (dále jen „SDEU“) poukázal na to, že z článku 7 Listiny mohou vyplývat pozitivní povinnosti veřejných orgánů za účelem přijetí právních opatření na ochranu soukromého a rodinného života, obydlí a komunikace. Takové povinnosti mohou rovněž vyplývat z článků 3 a 4 Listiny, pokud jde o ochranu fyzické a duševní nedotknutelnosti jednotlivce a zákaz mučení a nelidského a ponižujícího zacházení.¹³
11. Veškerá omezení práv zaručených Listinou, jako jsou ta, která stanoví návrh,¹⁴ musí být zároveň v souladu s požadavky stanovenými v čl. 52 odst. 1 Listiny. Každé opatření, které zasahuje do práva na

¹⁰ Viz např. prohlášení EDPB o revizi nařízení o soukromí a elektronických komunikacích a jeho dopadu na ochranu fyzických osob, pokud jde o soukromí a důvěrnost jejich komunikace (25. května 2018).

¹¹ Téměř všechny evropské ústavy zahrnují právo na ochranu důvěrnosti komunikace. Viz např. článek 15 Ústavy Italské republiky, článek 10 Základního zákona Spolkové republiky Německo, článek 22 belgické ústavy a článek 13 Ústavy Nizozemského království.

¹² Viz mimo jiné rozsudek SDEU, věc C-311/18, *Facebook Ireland a Schrems*, bod 172 a zde citovaná judikatura. Viz též 4. bod odůvodnění obecného nařízení o ochraně osobních údajů.

¹³ SDEU, spojené věci C-511/18, C-512/18 a C-520/18, *La Quadrature du Net* a další, body 126–128. Viz také EIOÚ, stanovisko č. 7/2020 k návrhu dočasných odchylek od směrnice 2002/58/ES pro účely boje proti pohlavnímu zneužívání dětí on-line (10. listopadu 2020), bod 12.

¹⁴ Srov. COM(2022) 209 final, s. 12–13.

důvěrnost komunikace a práva na soukromý a rodinný život, musí především respektovat podstatu těchto práv.¹⁵ Podstata práva je dotčena, pokud je toto právo zbaveno svého základního obsahu a jednotlivec je nemůže uplatnit¹⁶. Zásah nemůže ve vztahu ke sledovanému cíli představovat takový nepřiměřený a neúnosný zásah do samotné podstaty takto zaručeného práva.¹⁷ To znamená, že i základní právo, které nemá absolutní povahu, jako je právo na důvěrnost komunikace a právo na ochranu osobních údajů, má některé základní složky, které nesmí být omezeny.

12. SDEU několikrát uplatnil v oblasti soukromí elektronických komunikací test zásahu do „podstaty práva“. Ve věci *Tele2 Sverige a Watson* Soudní dvůr rozhodl, že právní úprava, která neopravňuje k uchovávání obsahu sdělení, není způsobilá zasáhnout do podstaty práva na soukromý život a na ochranu osobních údajů.¹⁸ Ve věci *Schrems* Soudní dvůr rozhodl, že právní úprava, která veřejným orgánům umožňuje globální přístup k obsahu elektronických komunikací, musí být považována za zasahující do podstaty základního práva na respektování soukromého života zaručeného článkem 7 Listiny.¹⁹ Ve věci *Digital Rights Ireland a Seitlinger a další* Soudní dvůr rozhodl, že i když uchovávání údajů uložené směrnicí 2006/24 představuje zvlášť závažný zásah do základního práva na soukromí a jiných práv stanovených v článku 7 Listiny, nemůže zasáhnout do podstaty těchto práv, neboť tato směrnice neumožňuje seznámit se s obsahem elektronických sdělení jako takovým.²⁰ Z této judikatury lze vyvodit, že opatření, která veřejným orgánům umožňují všeobecný přístup k obsahu sdělení, mohou s větší pravděpodobností zasáhnout do podstaty práv zaručených v článcích 7 a 8 Listiny. Tyto úvahy jsou stejně relevantní i pro opatření na odhalování materiálu pohlavního zneužívání dětí a navazování kontaktu s dětmi, jako jsou ta, která stanoví návrh.
13. SDEU dále rozhodl, že opatření v oblasti bezpečnosti údajů hrají klíčovou úlohu při zajišťování toho, aby nebylo zasahováno do podstaty základního práva na ochranu osobních údajů podle článku 8 Listiny.²¹ V digitálním věku jsou technická řešení pro zajištění a ochranu důvěrnosti elektronických komunikací, včetně opatření pro šifrování, klíčová pro zajištění požívání všech základních práv.²² Tato skutečnost by měla být náležitě zohledněna při posuzování opatření pro povinné odhalování materiálů pohlavního zneužívání dětí nebo navazování kontaktu s dětmi, zejména pokud by to vedlo k oslabení nebo zhoršení šifrování.²³
14. Článek 52 odst. 1 Listiny rovněž stanoví, že každé omezení výkonu základního práva zaručeného Listinou musí být stanoveno zákonem. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.²⁴ Za účelem splnění požadavku

¹⁵ Viz čl. 52 odst. 1 Listiny.

¹⁶ Viz Pokyny EIOÚ k posuzování přiměřenosti opatření, která omezují základní práva na soukromí a ochranu osobních údajů (19. prosince 2019), s. 8, k dispozici na adrese https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

¹⁷ SDEU, věc C-393/19, *OM*, bod 53.

¹⁸ SDEU, spojené věci C-203/15 a C-698/15, *Tele2 Sverige a Watson*, bod 101.

¹⁹ SDEU, věc C-362/14, *Schrems*, bod 94.

²⁰ SDEU, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland a Seitlinger a další*, bod 39.

²¹ Tamtéž, bod 40.

²² Viz Rada pro lidská práva, rezoluce 47/16 o prosazování, ochraně a požívání lidských práv na internetu, dokument OSN A/HRC/RES/47/16 (26. července 2021).

²³ Viz též 25. bod odůvodnění obecného nařízení o ochraně osobních údajů.

²⁴ Viz „Posuzování nezbytnosti opatření omezujících základní právo na ochranu osobních údajů: soubor nástrojů“, 11. dubna 2019, k dispozici na adrese: https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

proporcionality musí právní úprava stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a uložit minimální požadavky, tak aby osoby, o jejichž osobní údaje jde, měly dostatečné záruky umožňující účinně chránit tyto údaje před rizikem zneužití.²⁵ Tato právní úprava musí zejména vymezit okolnosti a podmínky, za nichž může být přijato opatření týkající se zpracovávání takových údajů, čímž zaručí, že se zásah omezí na to, co je nezbytně nutné.²⁶ Jak objasnil SDEU, potřeba takových záruk je o to významnější v případě, kdy jsou osobní údaje zpracovávány automaticky a jedná-li se o ochranu oné konkrétní kategorie osobních údajů, již tvoří citlivé údaje.²⁷

15. Návrh by omezil výkon práv a povinností stanovených v čl. 5 odst. 1 a 3 a čl. 6 odst. 1 směrnice 2002/58/ES („směrnice o soukromí a elektronických komunikacích“)²⁸ v rozsahu nezbytném pro výkon detekčních příkazů vydaných v souladu s oddílem 2 kapitoly 1 tohoto návrhu. EDPB a EIOÚ se domnívají, že je proto nezbytné posoudit návrh nejen s ohledem na Listinu a obecné nařízení o ochraně osobních údajů, ale také s ohledem na články 5 a 6 a čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích.

²⁵ Viz SDEU, spojené věci C-511/18, C-512/18 a C-520/18, *La Quadrature du Net a další*, bod 132.

²⁶ Tamtéž.

²⁷ Tamtéž.

²⁸ Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) ve znění směrnice 2006/24/ES a směrnice 2009/136/ES.

4. KONKRÉTNÍ PŘIPOMÍNKY

4.1 Vztah ke stávajícím právním předpisům

4.1.1 Vztah k obecnému nařízení o ochraně osobních údajů a směrnici o soukromí a elektronických komunikacích

16. V návrhu se uvádí, že jím nejsou dotčena pravidla vyplývající z jiných aktů Unie, zejména z obecného nařízení o ochraně osobních údajů²⁹ a směrnice o soukromí a elektronických komunikacích. Na rozdíl od prozatímního nařízení návrh nestanoví výslovnou dočasnou odchylku, nýbrž omezení uplatňování práv a povinností stanovených v čl. 5 odst. 1, čl. 5 odst. 3 a čl. 6 odst. 1 směrnice o soukromí a elektronických komunikacích. Dále je třeba poznamenat, že prozatímní nařízení stanoví odchylku výlučně od ustanovení čl. 5 odst. 1 a čl. 6 odst. 1, a nikoli od čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.
17. Návrh dále odkazuje na čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích, který členským státům umožňuje přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5 a 6 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, přiměřené a úměrné opatření kromě jiného pro prevenci, vyšetřování, odhalování a stíhání trestných činů. Podle návrhu se čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích použije analogicky, pokud návrh omezuje výkon práv a povinností stanovených v čl. 5 odst. 1, čl. 5 odst. 3 a čl. 6 odst. 1 směrnice o soukromí a elektronických komunikacích.
18. EDPB a EIOÚ připomínají, že SDEU objasnil, že čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích je třeba vykládat striktně, což znamená, že výjimka ze zásady důvěrnosti komunikace, kterou čl. 15 odst. 1 připouští, musí zůstat výjimkou a nesmí se stát pravidlem.³⁰ Jak je dále uvedeno v tomto společném stanovisku, EDPB a EIOÚ se domnívají, že návrh nesplňuje požadavky na (striktní) nezbytnost, účinnost a úměrnost. EDPB a EIOÚ navíc dospěli k závěru, že návrh by znamenal, že zásah do důvěrnosti komunikace se ve skutečnosti může stát pravidlem, a nikoli zůstat výjimkou.

4.1.2 Vztah k nařízení (EU) 2021/1232 a dopad na dobrovolné odhalování pohlavního zneužívání dětí on-line

19. Podle článku 88 návrhu by se návrhem zrušilo prozatímní nařízení, které stanoví dočasnou odchylku od některých ustanovení směrnice o soukromí a elektronických komunikacích, aby poskytovatelé interpersonálních komunikačních služeb nezávislých na číslech mohli dobrovolně využívat technologie pro odhalování materiálu pohlavního zneužívání dětí a navazování kontaktu s dětmi. Ode dne použitelnosti navrhovaného nařízení by tedy neexistovala žádná odchylka od směrnice o soukromí a elektronických komunikacích, která by umožnila dobrovolné odhalování pohlavního zneužívání dětí on-line těmito poskytovateli.
20. Vzhledem k tomu, že povinnosti v oblasti odhalování zavedené tímto návrhem by se vztahovaly pouze na příjemce detekčních příkazů, bylo by důležité ve znění navrhovaného nařízení jasně stanovit, že dobrovolné používání technologií pro odhalování materiálů pohlavního zneužívání dětí a navazování

²⁹ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP) (Úř. věst. L 119, 4.5.2016, s. 1–88).

³⁰ Rozsudek ze dne 21. prosince 2016, spojené věci C-203/15 a C-698/15 *Tele2 Sverige AB a Watson*, bod 89.

kontaktem s dětmi zůstává povoleno pouze v rozsahu, v jakém to povoluje směrnice o soukromí a elektronických komunikacích a obecné nařízení o ochraně osobních údajů. To by například znamenalo, že poskytovatelům interpersonálních komunikačních služeb nezávislých na číslech by bylo zabráněno v dobrovolném používání těchto technologií, pokud by to nebylo povoleno vnitrostátními právními předpisy provádějícími směrnici o soukromí a elektronických komunikacích v souladu s čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích a Listinou.

21. Obecněji by navrhovanému nařízení prospěla větší jasnost, pokud jde o status dobrovolného odhalování pohlavního zneužívání dětí on-line po dni použitelnosti navrhovaného nařízení a pokud jde o přechod od režimu dobrovolného odhalování stanoveného v prozatímním nařízení k povinnostem v oblasti odhalování stanoveným v navrhovaném nařízení. EDPB a EIOÚ například doporučují vyjasnit, že navrhované nařízení nebude představovat právní základ pro zpracování osobních údajů výhradně za účelem dobrovolného odhalování pohlavního zneužívání dětí on-line.

4.2 Právní základ podle obecného nařízení o ochraně osobních údajů

22. Cílem návrhu je stanovit právní základ ve smyslu obecného nařízení o ochraně osobních údajů pro zpracování osobních údajů pro účely odhalování materiálů pohlavního zneužívání dětí a groomingu. V důvodové zprávě se proto uvádí: „Pokud jde o povinné činnosti týkající se odhalení, mezi které patří zpracování osobních údajů, návrh (zejména detekční příkazy vydané na jeho základě) tímto způsobem určuje důvod pro toto zpracování podle čl. 6 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů, který stanoví zpracování osobních údajů jako nezbytné pro splnění právní povinnosti podle práva Unie nebo členského státu, které se vztahuje na správce údajů.“³¹
23. EDPB a EIOÚ vítají rozhodnutí Komise odstranit právní nejistotu, pokud jde o právní základ zpracování osobních údajů, ke které docházelo v souvislosti s prozatímním nařízením. EDPB a EIOÚ rovněž souhlasí se závěrem Komise, že důsledky zavedení opatření pro odhalování jsou příliš dalekosáhlé a závažné na to, aby rozhodnutí o tom, zda tato opatření provést, byla ponechána na poskytovatelích služeb.³² EDPB a EIOÚ zároveň konstatují, že jakýkoli právní základ ukládající poskytovatelům služeb povinnost zasahovat do základních práv na ochranu údajů a soukromí bude platný pouze tehdy, pokud bude v souladu s podmínkami stanovenými v čl. 52 odst. 1 Listiny, jak je analyzováno v následujících oddílech.

4.3 Povinnosti týkající se posuzování a zmírňování rizik

24. Podle kapitoly II oddílu 1 návrhu jsou poskytovatelé hostingových služeb a poskytovatelé interpersonálních komunikačních služeb povinni u každé takové služby, kterou nabízejí, zjistit, analyzovat a posoudit riziko využívání služby pro účely pohlavního zneužívání dětí on-line a poté se snažit zjištěné riziko minimalizovat tím, že přijmou „přiměřená zmírňující opatření přizpůsobená zjištěnému riziku“.
25. EDPB a EIOÚ konstatují, že při provádění posouzení rizik by poskytovatel měl zohlednit zejména prvky uvedené v čl. 3 odst. 2 písm. a) až e) návrhu, včetně: zákazů a omezení stanovených v podmínkách poskytovatele, způsobu, jakým uživatelé využívají službu, a jeho dopadu na toto riziko, způsobu, jakým poskytovatel službu navrhl a provozuje, včetně obchodního modelu, správy a řízení a příslušných systémů a postupů, a jejich dopadu na toto riziko. Pokud jde o riziko navazování kontaktu s dětmi, je třeba zohlednit tyto navrhované prvky: rozsah, v jakém je nebo pravděpodobně bude služba využívána

³¹ Tamtéž, s. 4.

³² Srov. návrh, COM(2022) 209 final, s. 14.

děti, věkové skupiny a riziko navazování kontaktu s dětmi podle těchto věkových skupin, dostupnost funkcí umožňujících vyhledávání uživatelů, funkcí umožňujících uživatelům navázat kontakt přímo s jinými uživateli, zejména prostřednictvím soukromých komunikací, a funkcí umožňujících uživatelům sdílet obrázky nebo videa s jinými uživateli.

26. EDPB a EIOÚ sice uznávají, že tato kritéria se zdají relevantní, EDPB a EIOÚ jsou však znepokojeni tím, že tato kritéria ponechávají poměrně široký prostor pro vlastní výklad a posouzení. Několik kritérií je popsáno velmi obecně (např. „způsob, jakým uživatelé využívají službu, a jeho dopad na toto riziko“) nebo se týká základních funkcí, které jsou běžné v mnoha on-line službách (např. „možnost, aby uživatelé sdíleli obrázky nebo videa s jinými uživateli“). Kritéria jako taková vykazují tendenci k subjektivnímu (spíše než objektivnímu) posouzení.
27. Podle názoru EDPB a EIOÚ totéž platí pro opatření ke zmírnění rizika, která mají být přijata podle článku 4 návrhu. Opatření, jako je přizpůsobení systémů moderování obsahu nebo doporučovacích systémů poskytovatele prostřednictvím vhodných technických a provozních opatření a náboru zaměstnanců, se zdají být relevantní pro snížení zjištěného rizika. Pokud se však tato kritéria použijí v rámci složitého procesu posuzování rizik a v kombinaci s abstraktními a vágními pojmy popisujícími přijatelnou výši rizika (např. „do značné míry“), nesplňují kritéria právní jistoty a předvídatelnosti potřebná k odůvodnění zasahování do důvěrnosti komunikace mezi soukromými osobami, což představuje jasný zásah do základních práv na soukromí a na svobodu projevu.
28. Ačkoliv poskytovatelé nejsou oprávněni zasahovat do důvěrnosti komunikace v rámci svých strategií posuzování a zmírňování rizik před obdržení detekčního příkazu, existuje přímá souvislost mezi povinnostmi v oblasti posuzování a zmírňování rizik a následnými povinnostmi v oblasti odhalování. Podle čl. 7 odst. 4 návrhu závisí vydání detekčního příkazu na existenci důkazů o významném riziku, že by příslušná služba mohla být využívána pro účely pohlavního zneužívání dětí on-line. Před vydáním detekčního příkazu je třeba dodržet složitý proces zahrnující poskytovatele, koordinační orgán a soudní nebo jiný nezávislý správní orgán odpovědný za vydání příkazu. Zprvu, poskytovatelé musí posoudit riziko využívání svých služeb pro účely pohlavního zneužívání dětí on-line (článek 3 návrhu) a vyhodnotit možná opatření ke zmírnění rizika (článek 4 návrhu) s cílem toto riziko snížit. Výsledky tohoto postupu se poté oznámí příslušnému koordinačnímu orgánu (článek 5 návrhu). Pokud z posouzení rizik vyplývá, že přetrvává významné riziko navzdory úsilí o jeho zmírnění, koordinační orgán vyslechne poskytovatele ohledně návrhu žádosti o vydání detekčního příkazu a dá poskytovateli možnost předložit připomínky. Poskytovatel je dále povinen předložit prováděcí plán, včetně stanoviska příslušného úřadu pro ochranu údajů v případě odhalování groomingu. Pokud se případem zabývá koordinační orgán, žádá soud nebo jiný nezávislý správní orgán o vydání detekčního příkazu. Počáteční posouzení rizik a opatření zvolená ke snížení zjištěného rizika jsou proto rozhodujícím základem pro posouzení provedené koordinačním orgánem, jakož i příslušným soudním nebo správním orgánem, zda je detekční příkaz nezbytný.
29. EDPB a EIOÚ berou na vědomí složité kroky vedoucí k vydání detekčního příkazu, jež zahrnují počáteční posouzení rizik poskytovatelem a návrh opatření ke zmírnění rizik předložený poskytovatelem, jakož i další komunikaci poskytovatele s příslušným koordinačním orgánem. EDPB a EIOÚ se domnívají, že poskytovatel má zásadní možnost ovlivnit výsledek procesu. V tomto ohledu EDPB a EIOÚ konstatují, že 17. bod odůvodnění návrhu stanoví, že poskytovatelé by měli mít možnost uvést v rámci hlášení rizik, že nakonec „jsou ochotni a připraveni“ na vydání detekčního příkazu. Proto nelze předpokládat, že se jeden každý poskytovatel bude snažit vyhnout vydání detekčního příkazu, aby byla zachována důvěrnost komunikace uživatelů, a to použitím nejúčinnějších zmírňujících opatření, které co nejméně zasáhnou do práv, zejména pokud tato zmírňující opatření zasahují do svobody podnikání poskytovatele podle článku 16 Listiny.

30. EIOÚ a EDPB by chtěli zdůraznit, že procesní záruky nemohou nikdy zcela nahradit hmotněprávní záruky. Složitý postup vedoucí k možnému vydání detekčního příkazu, který je popsán výše, by proto měl být doplněn jasnými hmotněprávními povinnostmi. EDPB a EIOÚ se domnívají, že návrh postrádá jasnost, pokud jde o několik klíčových prvků (např. pojmy „významné riziko“, „do značné míry“ atd.), které nelze napravit existencí více úrovní procesních záruk. Tato otázka nabývá na důležitosti ve světle skutečnosti, že subjekty odpovědné za uplatňování těchto záruk (např. poskytovatelé, soudní orgány atd.) mají široký prostor pro vlastní uvážení ohledně toho, jak vyvážit dotčená práva v každém jednotlivém případě. Vzhledem k rozsáhlému zasahování do základních práv, které by vyplývalo z přijetí návrhu, by měl normotvůrce zajistit, aby návrh poskytoval větší jasnost, pokud jde o to, kdy a kde je takové zasahování povoleno. Ačkoli EDPB a EIOÚ uznávají, že legislativní opatření nemohou být příliš preskriptivní a musí ponechat určitou flexibilitu při jejich praktickém uplatňování, domnívají se, že stávající znění návrhu ponechává příliš velký prostor pro případné zneužití z důvodu neexistence jasných hmotněprávních norem.
31. Vzhledem k potenciálnímu významnému dopadu na velmi vysoký počet subjektů údajů (tj. potenciálně na všechny uživatele interpersonálních komunikačních služeb) EDPB a EIOÚ zdůrazňují potřebu vysoké úrovně právní jistoty, jasnosti a předvídatelnosti právních předpisů s cílem zajistit, aby navrhovaná opatření skutečně účinně dosahovala cíle, který sledují, a zároveň co nejméně poškozovala dotčená základní práva.

4.4 Podmínky pro vydávání detekčních příkazů

32. Článek 7 návrhu stanoví, že koordinační orgán v zemi usazení bude mít pravomoc požádat příslušný soudní orgán nebo jiný nezávislý správní orgán tohoto členského státu, aby vydal detekční příkaz, kterým se poskytovateli hostingových služeb nebo poskytovateli interpersonálních komunikačních služeb uloží, aby přijal opatření uvedená v článku 10 k odhalování pohlavního zneužívání dětí on-line v konkrétní službě.
33. EDPB a EIOÚ náležitě zohledňují následující prvky, které musí být splněny před vydáním detekčního příkazu:
- a. existují důkazy o významném riziku, že služba bude využívána pro účely pohlavního zneužívání dětí on-line ve smyslu čl. 7 odst. 5, případně odst. 6 nebo 7;
 - b. důvody pro vydání detekčního příkazu převažují nad negativními důsledky pro práva a oprávněné zájmy všech dotčených stran, zejména s ohledem na nutnost zajistit spravedlivou rovnováhu mezi základními právy těchto stran.
34. Význam pojmu významné riziko je upřesněn v čl. 7 odst. 5 a následujících odstavcích v závislosti na druhu zvažovaného detekčního příkazu. Má se za to, že existuje významné riziko v případě detekčních příkazů týkajících se známého materiálu pohlavního zneužívání dětí, pokud:
- a. je pravděpodobné, že navzdory jakýmkoli zmírňujícím opatřením, která poskytovatel případně přijal nebo přijme, se služba do značné míry využívá k šíření známého materiálu pohlavního zneužívání dětí, a
 - b. existují důkazy o tom, že služba nebo srovnatelná služba, pokud k datu žádosti o vydání detekčního příkazu dosud nebyla v Unii nabízena, byla v posledních 12 měsících a do značné míry využívána k šíření známého materiálu pohlavního zneužívání dětí.
35. Aby bylo možné vydat detekční příkaz týkající se neznámého materiálu pohlavního zneužívání dětí, musí pravděpodobnost a věcné důkazy odkazovat na neznámý materiál pohlavního zneužívání dětí a

musí být vydán dřívější detekční příkaz týkající se známého materiálu pohlavního zneužívání dětí a ten musí vést k velkému počtu oznámení o materiálech pohlavního zneužívání dětí ze strany poskytovatele (čl. 7 odst. 6 návrhu). V případě detekčního příkazu týkajícího se groomingu se má za to, že významné riziko existuje, pokud je poskytovatel považován za poskytovatele interpersonálních komunikačních služeb, je pravděpodobné, že se služba ve značné míře využívá k navazování kontaktu s dětmi, a existují důkazy o tom, že služba byla do značné míry využívána k navazování kontaktu s dětmi (čl. 7 odst. 7 návrhu).

36. EDPB a EIOÚ poznamenávají, že i s upřesněním v čl. 7 odst. 5 až 7 návrhu jsou v podmínkách pro vydání detekčního příkazu nápadné neurčité právní pojmy, jako je „do značné míry“, „značný počet“, a částečně se opakují, neboť důkazy o dřívějším zneužití často přispějí ke zjištění pravděpodobnosti budoucího zneužití.
37. Návrh vytváří systém, v jehož rámci je při rozhodování o tom, zda je nezbytný detekční příkaz, třeba učinit rozhodnutí o předvídání budoucího využívání služby pro účely pohlavního zneužívání dětí online. Je tedy pochopitelné, že prvky uvedené v článku 7 mají prognostickou povahu. Avšak vzhledem k tomu, že se v návrhu používají vágní pojmy, poskytovatelům i příslušným soudním nebo jiným zmocněným nezávislým správním orgánům se ztěžuje uplatňování právních požadavků zavedených návrhem předvídatelným a nearbitrárním způsobem. EDPB a EIOÚ jsou znepokojeni tím, že kvůli těmto obecným a neurčitým pojmům vzniká nedostatek právní jistoty, což také bude mít za následek značné rozdíly v konkrétním provádění návrhu v celé Unii v závislosti na výkladech pojmů, jako je „pravděpodobnost“ a „do značné míry“ ze strany soudních nebo jiných nezávislých správních orgánů v členských státech. Takový výsledek by nebyl přijatelný vzhledem ke skutečnosti, že ustanovení o detekčních příkazech pro poskytovatele interpersonálních komunikačních služeb budou představovat „omezení“ zásady důvěrnosti komunikace stanovené v článku 5 směrnice o soukromí a elektronických komunikacích, a jejich jasnost a předvídatelnost jsou proto nanejvýš důležité pro zajištění jednotného uplatňování těchto omezení v celé Unii.

4.5 Analýza nezbytnosti a proporcionality plánovaných opatření³³

38. Jak je uvedeno výše, mohou být vydány tři typy detekčních příkazů: detekční příkazy týkající se šíření známého materiálu pohlavního zneužívání dětí (čl. 7 odst. 5 návrhu), detekční příkazy týkající se šíření nového materiálu pohlavního zneužívání dětí (čl. 7 odst. 6 návrhu) a detekční příkazy týkající se navazování kontaktu s dětmi (čl. 7 odst. 7 návrhu). Každý detekční příkaz by obvykle vyžadoval jinou technologii, aby mohl být proveden v praxi. V důsledku toho mají různou úroveň zasahování do práv, a tudíž odlišný dopad na právo na soukromí a právo na ochranu osobních údajů.
39. Technologie pro odhalování známých materiálů pohlavního zneužívání dětí jsou obvykle porovnávací technologie v tom smyslu, že se opírají o stávající databázi známého materiálu pohlavního zneužívání dětí, s níž mohou porovnávat obrázky (včetně vystřižených záběrů z videí). Aby bylo možné porovnávat, musí být obrázky, které poskytovatel zpracovává, jakož i obrázky v databázi, digitalizovány, obvykle jejich konverzí na hodnoty hash. U této technologie hashování se odhaduje, že

³³ Viz též „Rychlý průvodce EIOÚ nezbytností a proporcionality“, který je k dispozici na adrese: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

míra falešně pozitivních výsledků není vyšší než 1 z 50 miliard (tj. míra falešné positivity 0,000000002 %).³⁴

40. Pro detekci nových materiálů pohlavního zneužívání dětí se obvykle používá jiný typ technologie, včetně klasifikátorů a umělé inteligence (UI).³⁵ Jejich míry chyb jsou však obecně výrazně vyšší. Například ve zprávě o posouzení dopadů se uvádí, že existují technologie pro detekci nových materiálů pohlavního zneužívání dětí, jejichž míra přesnosti může být stanovena na 99,9 % (tj. míra falešné positivity 0,1 %), ale s touto mírou přesnosti jsou schopny identifikovat pouze 80 % všech materiálů pohlavního zneužívání dětí v příslušném souboru údajů.³⁶
41. Pokud jde o odhalování navazování kontaktu s dětmi v textových sděleních, vysvětluje se ve zprávě o posouzení dopadů, že se obvykle zakládá na odhalení pravidelností. Ve zprávě o posouzení dopadů se uvádí, že některé stávající technologie pro odhalování groomingu mají „míru přesnosti“ 88 %³⁷. Podle Komise to znamená, že „ze sta konverzací, které byly označeny jako možné trestné navazování kontaktu s dětmi, může být po přezkumu dvanáct vyloučeno [podle návrhu, ze strany střediska EU] a nebude oznámeno donucovacím orgánům“.³⁸ Ačkoliv by se však návrh na rozdíl od prozatímního nařízení vztahoval i na zvukovou komunikaci, zpráva o posouzení dopadů se nezabývá technologickými řešeními, která by mohla být použita k odhalování groomingu v tomto prostředí.

4.5.1 Účinnost odhalování

42. Nezbytnost vyžaduje posouzení účinnosti zamýšlených opatření pro dosažení sledovaného cíle na základě faktů a toho, zda méně zasahují do práv než jiné možnosti vedoucí k dosažení téhož cíle.³⁹ Dalším faktorem, který je třeba vzít v úvahu při posuzování proporcionality navrhovaného opatření, je účinnost stávajících opatření nad rámec navrhovaného opatření.⁴⁰ Pokud již opatření pro stejný nebo podobný účel existují, měla by být jejich účinnost posouzena v rámci posouzení proporcionality. Bez takového posouzení účinnosti stávajících opatření sledujících stejný nebo podobný účel nelze mít za to, že byl řádně proveden test proporcionality nového opatření.
43. Odhalování materiálů pohlavního zneužívání dětí nebo groomingu poskytovateli hostingových služeb a poskytovateli interpersonálních komunikačních služeb může přispět k celkovému cíli prevence pohlavního zneužívání dětí a boje proti němu a šíření materiálů pohlavního zneužívání dětí on-line. Potřeba posoudit účinnost opatření stanovených v návrhu zároveň vyvolává tři klíčové otázky:
 - Lze opatření k odhalování pohlavního zneužívání dětí on-line snadno obejít?

³⁴ Viz Evropská komise, pracovní dokument útvarů Komise, Zpráva o posouzení dopadů – Průvodní dokument k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu, SWD(2022) 209 final (dále jen „zpráva o posouzení dopadů“ nebo „SWD(2022) 209 final“), s. 281, poznámka pod čarou č. 511.

³⁵ Zpráva o posouzení dopadů, s. 281.

³⁶ Tamtéž, s. 282.

³⁷ Tamtéž, s. 283.

³⁸ Návrh, COM(2022) 209 final, s. 14, poznámka pod čarou č. 32.

³⁹ EIOÚ, Posuzování nezbytnosti opatření omezujících základní právo na ochranu osobních údajů: soubor nástrojů, 11. dubna 2017, s. 5; EIOÚ, Pokyny EIOÚ k posuzování proporcionality opatření, která omezují základní práva na soukromí a ochranu osobních údajů (19. prosince 2019), s. 8.

⁴⁰ EIOÚ, Pokyny EIOÚ k posuzování proporcionality opatření, která omezují základní práva na soukromí a ochranu osobních údajů (19. prosince 2019), s. 11.

- Jaký budou mít činnosti týkající se odhalování dopad na opatření přijatá donucovacími orgány?⁴¹
 - Jak by návrh snížil právní nejistotu?
44. Není úkolem EDPB a EIOÚ na tyto otázky podrobně odpovědět. EDPB a EIOÚ však konstatují, že ani zpráva o posouzení dopadů, ani návrh se těmito otázkami důsledně nezabývají.
45. Pokud jde o možnost obejít odhalení materiálů pohlavního zneužívání dětí, je třeba poznamenat, že v současné době zřejmě neexistuje žádné technologické řešení pro odhalování materiálu pohlavního zneužívání dětí, který se sdílí v šifrované formě. Proto lze jakoukoli činnost týkající se odhalování – dokonce i prohledávání/skenování na straně zákazníka s cílem obejít šifrování mezi koncovými body nabízené poskytovatelem⁴² – snadno obejít zašifrováním obsahu pomocí samostatné aplikace před jeho odesláním nebo nahráním. Opatření pro odhalování plánovaná v návrhu by tedy mohla mít menší dopad na šíření materiálu pohlavního zneužívání dětí na internetu, než by bylo možné očekávat.
46. Komise dále očekává, že po přijetí povinností týkajících se odhalování, které návrh zavádí, dojde ke zvýšení počtu oznámení o pohlavním zneužívání dětí podávaných donucovacím orgánům.⁴³ Návrh ani zpráva o posouzení dopadů však nevysvětlují, jak tím budou napraveny nedostatky současného stavu. Vzhledem k omezeným zdrojům donucovacích orgánů se zdá být nezbytné lépe pochopit, zda by zvýšení počtu oznámení mělo smysluplný dopad na činnosti donucovacích orgánů v oblasti boje proti pohlavnímu zneužívání dětí. V každém případě si EDPB a EIOÚ přejí zdůraznit, že tato oznámení by měla být posouzena včas, aby se zajistilo, že rozhodnutí o tom, zda je oznámený materiál relevantní z hlediska trestního práva, bude učiněno co nejdříve, a že by se mělo co nejvíce omezit uchovávání irelevantních údajů.

4.5.2 Neexistuje žádné opatření, které by méně zasahovalo do práv

47. Za předpokladu, že by bylo možné dosáhnout pozitivních účinků v oblasti odhalování materiálů pohlavního zneužívání dětí a groomingu, které plánuje Komise, musí být odhalování opatřeními, které nejméně zasahuje do práv, mezi stejně účinnými opatřeními. Článek 4 návrhu stanoví, že jako první krok by poskytovatelé měli zvážit přijetí zmírňujících opatření, aby minimalizovali riziko využívání jejich služby pro účely pohlavního zneužívání dětí on-line pod prahovou hodnotu, která opravňuje k vydání detekčního příkazu. Pokud by byla k dispozici zmírňující opatření, která by mohla vést k podstatnému snížení množství groomingu nebo materiálu pohlavního zneužívání dětí vyměňovaného v rámci příslušné služby, tato opatření by ve srovnání s detekčním příkazem často představovala opatření, která méně zasahují do práv⁴⁴. Pokud tedy příslušný poskytovatel nepřijme taková opatření dobrovolně, měl by mít příslušný nezávislý správní orgán nebo soudní orgán možnost učinit provádění zmírňujících opatření povinným a vymahatelným, a nikoliv pouze vydat detekční příkaz. Podle názoru EDPB a EIOÚ nepostačuje skutečnost, že čl. 5 odst. 4 návrhu umožňuje koordináčnímu orgánu „požádat“ poskytovatele, aby zavedl, přezkoumal, zrušil nebo rozšířil zmírňující opatření, neboť takový

⁴¹ Podle zprávy o posouzení dopadů, přílohy II, s. 132, vyjádřilo 85,71 % respondentů průzkumu provedeného v řadách donucovacích orgánů obavy, pokud jde o zvýšený počet materiálů pohlavního zneužívání dětí za poslední desetiletí a nedostatek zdrojů (tj. lidských, technických).

⁴² Viz také oddíl 4.10 níže.

⁴³ Viz *mimo jiné* zpráva o posouzení dopadů, příloha 3, SWD(2022) 209 final, s. 176.

⁴⁴ Například by mohla být zvážena opatření, jako je blokování přenosu materiálů pohlavního zneužívání dětí na straně zákazníků tím, že se zabrání nahrávání a odesílání obsahu elektronických komunikací, neboť by mohla v určitých souvislostech pomoci zabránit šíření známých materiálů pohlavního zneužívání dětí.

požadavek by nebyl nezávisle vymahatelný; nevyhovění této žádosti by bylo „postihováno“ pouze nařízením detekčního příkazu.

48. EDPB a EIOÚ se proto domnívají, že koordinační orgán nebo příslušný nezávislý správní nebo soudní orgán by měl být výslovně zmocněn ukládat zmírňující opatření, která méně zasahují do práv, před vydáním detekčního příkazu nebo namísto něho.

4.5.3 Proporcionalita v užším slova smyslu

49. Má-li být opatření v souladu se zásadou proporcionality zakotvenou v čl. 52 odst. 1 Listiny, neměly by nevýhody, které opatření způsobuje ve vztahu k výkonu základních práv, převážit nad výhodami vyplývajících z opatření. Zásada proporcionality tedy „omezuje výkon pravomocí orgánů tím, že vyžaduje nalezení rovnováhy mezi použitými prostředky a zamýšleným cílem (nebo dosaženým výsledkem)“.⁴⁵
50. Aby bylo možné posoudit dopad opatření na základní práva na soukromí a na ochranu osobních údajů, je obzvláště důležité přesně určit:⁴⁶
- **oblast působnosti opatření**, včetně počtu dotčených osob a toho, zda vyvolává „nezamýšlená vedlejší narušení“ (tj. zásah do soukromí jiných osob, než jsou subjekty, jichž se opatření týká),
 - **rozsah opatření**, včetně množství shromážděných informací; na jak dlouho se shromažďují; zda zkoumané opatření vyžaduje shromažďování a zpracování zvláštních kategorií údajů,
 - **míru zasahování do práv** s přihlédnutím k těmto aspektům: povaha činnosti, na kterou se opatření vztahuje (zda se týká činností, pro něž platí povinnost zachovávat důvěrnost, či nikoli, vztah mezi advokátem a klientem; lékařská činnost); kontext; zda se jedná o profilování dotčených osob, či nikoli; zda zpracování zahrnuje použití (částečně nebo zcela) automatizovaného rozhodovacího systému s „rozpětím chybovosti“,
 - zda se týká **zranitelných osob**, či nikoli,
 - zda se dotýká i **jiných základních práv** (například práva na svobodu projevu jako ve věcech *Digital Rights Ireland a Seitlinger a další* a *Tele2 Sverige a Watson*).⁴⁷
51. V této souvislosti je rovněž důležité poznamenat, že dopad na dotčenou osobu může být malý, avšak významný nebo velmi významný kolektivně / pro společnost jako celek.⁴⁸
52. Ve všech třech typech detekčních příkazů (odhalování známého materiálu pohlavního zneužívání dětí, nového materiálu pohlavního zneužívání dětí a groomingu) se technologie, které jsou v současné době k dispozici, spoléhají na automatizované zpracování údajů o obsahu všech dotčených uživatelů.

⁴⁵ Viz věc C-343/09, *Afton Chemical*, bod 45; spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke a Hartmut Eifert*, bod 74; věci C-581/10 a C-629/10, *Nelson a další*, bod 71; věc C-283/11, *Sky Österreich*, bod 50 a věc C-101/12, *Schaible*, bod 29. Viz dále EIOÚ, Posuzování nezbytnosti opatření omezujících základní právo na ochranu osobních údajů: soubor nástrojů (11. dubna 2017).

⁴⁶ EIOÚ, Pokyny EIOÚ k posuzování proporcionality opatření, která omezují základní práva na soukromí a ochranu osobních údajů (19. prosince 2019), s. 23.

⁴⁷ Viz také EIOÚ, stanovisko č. 7/2020 k návrhu dočasných odchylek od směrnice 2002/58/ES pro účely boje proti pohlavnímu zneužívání dětí on-line (10. listopadu 2020), s. 9 a násl.

⁴⁸ EIOÚ, Pokyny EIOÚ k posuzování proporcionality opatření, která omezují základní práva na soukromí a ochranu osobních údajů (19. prosince 2019), s. 20.

Technologie používané k analýze obsahu jsou často složité a obvykle zahrnují využívání umělé inteligence. Proto nemusí být chování této technologie pro uživatele služby zcela srozumitelné. Navíc je známo, že technologie, které jsou v současné době k dispozici, zejména technologie pro odhalování nového materiálu pohlavního zneužívání dětí nebo groomingu, vykazují poměrně vysokou míru chyb.⁴⁹ Kromě toho existuje riziko, že budou podávána oznámení středisku EU v souladu s čl. 12 odst. 1 a čl. 48 odst. 1 návrhu na základě odhalení „možného“ materiálu pohlavního zneužívání dětí.

53. Obecné podmínky pro vydání detekčního příkazu podle návrhu, tj. s platností na celou službu, a nikoli pouze na vybranou komunikaci⁵⁰, doba trvání až 24 měsíců v případě známého nebo nového materiálu pohlavního zneužívání dětí a až 12 měsíců v případě groomingu⁵¹ atd., mohou navíc v praxi vést k velmi široké oblasti působnosti příkazu. Sledování by tudíž bylo ve skutečnosti obecné a nerozlišující povahy a v praxi by nebylo cílené.
54. S ohledem na výše uvedené skutečnosti jsou EDPB a EIOÚ rovněž znepokojeni možnými odrazujícími účinky na výkon svobody projevu. EDPB a EIOÚ připomínají, že takový odrazující účinek je považován za tím pravděpodobnější, čím menší je jasnost právního předpisu.
55. Vzhledem k neexistenci specifičnosti, přesnosti a jasnosti požadované pro splnění požadavku právní jistoty⁵² a vzhledem k jeho široké oblasti působnosti, tj. všichni poskytovatelé příslušných služeb informační společnosti, kteří takové služby nabízejí v Unii,⁵³ návrh nezajišťuje, aby byl účinně prováděn pouze cílený přístup k odhalování materiálů pohlavního zneužívání dětí a groomingu. EDPB a EIOÚ se proto domnívají, že v praxi by se návrh mohl stát základem pro *de facto* všeobecné a nerozlišující prohledávání/skenování obsahu prakticky všech typů elektronických komunikací všech uživatelů v EU/EHP. Tento právní předpis proto může přimět lidi k tomu, aby se zdrželi sdílení legálního obsahu ze strachu, že by proti nim na základě jejich činnosti mohl být zacílen.
56. EDPB a EIOÚ přesto uznávají, že různá opatření pro boj proti pohlavnímu zneužívání dětí on-line mohou zahrnovat různé úrovně zasahování do práv. EDPB a EIOÚ na úvod připomínají, že automatizovaná analýza řeči nebo textu s cílem určit možné případy navazování kontaktu s dětmi bude pravděpodobně představovat významnější zásah než porovnávání obrázků nebo videí na základě dříve potvrzených případů materiálu pohlavního zneužívání dětí s cílem odhalit šíření takového materiálu. Dále je třeba rozlišovat mezi odhalením „známého materiálu pohlavního zneužívání dětí“ a „nového materiálu pohlavního zneužívání dětí“. Kromě toho je třeba dále rozlišovat dopad opatření určených poskytovatelům hostingových služeb a opatření uložených poskytovatelům interpersonálních komunikačních služeb.

4.5.4 Odhalování známých materiálů pohlavního zneužívání dětí

57. Ačkoliv podle 4. bodu odůvodnění má být návrh „technicky neutrální“, jak účinnost navrhovaných opatření pro odhalování, tak jejich dopad na jednotlivce budou do značné míry záviset na volbě použité technologie a na vybraných ukazatelích. Komise tuto skutečnost uznala v příloze 8 zprávy o posouzení dopadů⁵⁴ a potvrdily ji i další studie, například cílené substituční posouzení dopadů návrhu

⁴⁹ Viz podrobnosti výše, oddíl 4.5 a níže pododdíl 4.8.2.

⁵⁰ Viz čl. 7 odst. 1 návrhu.

⁵¹ Viz čl. 7 odst. 9 třetí pododstavec návrhu.

⁵² Srov. SDEU, věc C-197/96, *Komise Evropských společenství proti Francouzské republice*, bod 15.

⁵³ Viz čl. 1 odst. 2 návrhu.

⁵⁴ Srov. informace o míře falešně pozitivních výsledků ve zprávě o posouzení dopadů, příloha 8, s. 279 a násl.

Komise z února 2021 o dočasné odchylce od směrnice o soukromí a elektronických komunikacích pro účely boje proti pohlavnímu zneužívání dětí na internetu, které vypracovala Výzkumná služba Evropského parlamentu.⁵⁵

58. Článek 10 návrhu stanoví řadu požadavků na technologie, které mají být použity pro účely odhalování, zejména ohledně jejich účinnosti, spolehlivosti a co nejmenšího zasahování, pokud jde o dopad do práv uživatelů na soukromý a rodinný život, včetně důvěrnosti komunikace, a do práv na ochranu osobních údajů.
59. V této souvislosti EDPB a EIOÚ konstatují, že v současné době jsou jedinými technologiemi, které se zdají být schopny obecně splňovat tyto normy, technologie používané k odhalování známých materiálů pohlavního zneužívání dětí, tj. porovnávací technologie využívající referenční databázi hashů.

4.5.5 Odhalování dříve neznámých materiálů pohlavního zneužívání dětí

60. Posouzení opatření zaměřených na odhalování dříve neznámých (nových) materiálů pohlavního zneužívání dětí vede k různým závěrům, pokud jde o jejich účinnost, spolehlivost a omezení dopadu na základní práva na soukromí a ochranu osobních údajů.
61. Zaprvé, jak je vysvětleno ve zprávě o posouzení dopadů doprovázející návrh, mezi technologie, které se v současné době používají pro odhalování dříve neznámých materiálů pohlavního zneužívání dětí, patří klasifikátory a umělá inteligence. Klasifikátor je jakýkoli algoritmus, který pomocí rozpoznávání pravidelností třídí data do označených tříd nebo kategorií informací.⁵⁶ Tyto technologie tak mají různé výsledky a dopad, pokud jde o přesnost, účinnost a míru zasahování do práv. Zároveň také vykazují větší chybovost.
62. Techniky používané k odhalování dříve neznámých materiálů pohlavního zneužívání dětí jsou podobné technikám používaným k odhalování navazování kontaktu s dětmi, neboť obě jsou založeny nikoliv na jednoduchých technologiích porovnávání, ale na prediktivních modelech využívajících technologie umělé inteligence. EDPB a EIOÚ se domnívají, že při odhalování dříve neznámých materiálů pohlavního zneužívání dětí je zapotřebí vysoká míra obezřetnosti, neboť chyba systému by měla závažné důsledky pro subjekty údajů, jež by byly automaticky označeny za ty, kteří mohli spáchat velmi závažný trestný čin, a jejich osobní údaje a podrobnosti o jejich komunikaci by mohly být oznámeny.
63. Zadruhé, ukazatele výkonnosti uvedené v odborné literatuře, z nichž některé jsou zdůrazněny ve zprávě o posouzení dopadů, která je průvodní dokumentem návrhu,⁵⁷ poskytují velmi málo informací o podmínkách, které byly použity pro jejich výpočet, a o jejich vhodnosti v reálných podmínkách, což znamená, že jejich výkonnost v reálném světě by mohla být výrazně nižší, než se očekává, což povede k menší přesnosti a vyššímu procentnímu podílu „falešně pozitivních výsledků“.
64. Zatřetí, ukazatele výkonnosti by měly být zvažovány ve specifickém kontextu používání příslušných nástrojů pro odhalování a měly by poskytovat vyčerpávající přehled o chování nástrojů pro odhalování. V rámci používání algoritmů umělé inteligence na obrázky nebo texty je dobře zdokumentováno, že

⁵⁵ Srov. návrh Komise o dočasné odchylce od směrnice o soukromí a elektronických komunikacích pro účely boje proti pohlavnímu zneužívání dětí na internetu: cílené substituční posouzení dopadů (Výzkumná služba Evropského parlamentu, únor 2021), s. 14 a násl.

⁵⁶ Zpráva o posouzení dopadů, příloha 8, s. 281.

⁵⁷ Zpráva o posouzení dopadů, příloha 8, s. 281–283.

může dojít k předpojatosti a diskriminaci z důvodu nedostatečné reprezentativnosti určitých skupin obyvatelstva v datech, která se používají k vyladění algoritmu. Tato předpojatost by měla být identifikována, změřena a omezena na přijatelnou úroveň, aby systémy pro odhalování byly skutečně přínosné pro společnost jako celek.

65. Přestože byla provedena studie o technologiích používaných pro odhalování,⁵⁸ EDPB a EIOÚ se domnívají, že pro posouzení spolehlivosti stávajících nástrojů je nezbytná další analýza. Tato analýza by se měla opírat o vyčerpávající ukazatele výkonnosti a posoudit dopad možných chyb v reálných podmínkách na všechny subjekty údajů, jichž se návrh týká.
66. Jak je uvedeno výše, EDPB a EIOÚ mají vážné pochybnosti o tom, do jaké míry jsou procesní záruky stanovené v čl. 7 odst. 6 návrhu dostatečné k vyvážení těchto rizik. Kromě toho, jak bylo uvedeno výše, konstatují, že návrh používá k popisu přijatelné výše rizika poměrně abstraktní a vágní pojmy (např. „do značné míry“).
67. EDPB a EIOÚ jsou znepokojeni tím, že kvůli těmto obecným a neurčitým pojmům nebude zajištěna dostatečná právní jistota a rovněž vzniknou velké odlišnosti v konkrétním provádění návrhu v celé Unii v závislosti na výkladu pojmů, jako je „pravděpodobnost“ a „do značné míry“ ze strany soudních nebo jiných nezávislých správních orgánů v členských státech. To je znepokojivé i s ohledem na skutečnost, že ustanovení o detekčních příkazech budou představovat „omezení“ zásady důvěrnosti stanovené v článku 5 směrnice o soukromí a elektronických komunikacích. Proto je třeba v navrhovaném nařízení zlepšit jejich jasnost a předvídatelnost.

4.5.6 Odhalování navazování kontaktu s dětmi („grooming“)

68. EDPB a EIOÚ poznamenávají, že navrhovaná opatření týkající se odhalování navazování kontaktu s dětmi („grooming“), zahrnující automatizovanou analýzu řeči nebo textu, pravděpodobně představují nejvýznamnější zásah do práva uživatelů na soukromý a rodinný život, včetně důvěrnosti komunikace, a práva na ochranu osobních údajů.
69. Zatímco odhalování známého, a dokonce nového materiálu pohlavního zneužívání dětí může být co do rozsahu omezeno na analýzu obrázků a videí, odhalování groomingu by se ze své podstaty vztahovalo na veškerou textovou (a případně zvukovou) komunikaci, která spadá do oblasti působnosti detekčního příkazu. Intenzita zásahu do důvěrnosti dotčené komunikace je tudíž mnohem větší.
70. EDPB a EIOÚ se domnívají, že *de facto* všeobecná a nerozlišující automatizovaná analýza textových sdělení přenášených prostřednictvím interpersonálních komunikačních služeb s cílem odhalit potenciální navazování kontaktu s dětmi nesplňuje požadavky nezbytnosti a proporcionality. I když se použití technologie omezí na použití ukazatelů, EDPB a EIOÚ se domnívají, že zavedení takové všeobecné a nerozlišující analýzy je nepřiměřené, a může dokonce ovlivnit samotnou podstatu základního práva na soukromí zakotveného v článku 7 Listiny.
71. Jak již bylo uvedeno, neexistence hmotněprávních záruk v souvislosti s opatřeními pro odhalování navazování kontaktu s dětmi nemůže být kompenzována pouze procesními zárukami. Navíc je problém nedostatečné právní jasnosti a jistoty (např. používání neurčitých právních formulací jako „do značné míry“) dokonce ještě závažnější v případě automatizované analýzy textové osobní komunikace oproti porovnávání fotografií na základě technologie hashování.

⁵⁸ Zpráva o posouzení dopadů, s. 279 a násl.

72. EDPB a EIOÚ se dále domnívají, že „odrazující účinek“ na svobodu projevu je obzvláště významný, pokud je textová (nebo zvuková) komunikace jednotlivců prohledávána/skenována a analyzována ve velkém měřítku. EDPB a EIOÚ připomínají, že takový odrazující účinek je tím závažnější, čím menší je jasnost daného právního předpisu.
73. Kromě toho, jak je uvedeno ve zprávě o posouzení dopadů⁵⁹ a ve studii Výzkumné služby Evropského parlamentu⁶⁰, je míra přesnosti technologií pro odhalování textového groomingu mnohem nižší než míra přesnosti technologií pro odhalování známých materiálů pohlavního zneužívání dětí⁶¹. Techniky odhalování groomingu jsou navrženy tak, aby analyzovaly a přiřazovaly hodnocení pravděpodobnosti každému aspektu konverzace, a EDPB a EIOÚ je proto rovněž považují za náchylné k chybám a ke zneužití.

4.5.7 Závěr o nezbytnosti a proporcionalitě plánovaných opatření

74. Pokud jde o nezbytnost a proporcionalitu plánovaných opatření pro odhalování, EDPB a EIOÚ jsou obzvláště znepokojeni plánovanými opatřeními pro odhalování neznámého materiálu pohlavního zneužívání dětí a navazování kontaktu s dětmi (grooming), a to proto, že zasahují do práv tím, že mohou poskytovat všeobecný přístup k obsahu komunikace, kvůli jejich pravděpodobnostní povaze a míře chyb vykazované těmito technologiemi.
75. Z judikatury SDEU lze navíc dovodit, že opatření, která veřejným orgánům umožňují všeobecný přístup k obsahu sdělení, mohou s větší pravděpodobností zasáhnout do podstaty práv zaručených v člancích 7 a 8 Listiny. Tyto aspekty jsou zvláště důležité, pokud jde o návrhem stanovená opatření pro odhalování navazování kontaktu s dětmi.
76. EDPB a EIOÚ se v každém případě domnívají, že zásah způsobený zejména opatřeními pro odhalování navazování kontaktu s dětmi přesahuje rámec toho, co je nezbytně nutné a přiměřené. Tato opatření by proto měla být z návrhu odstraněna.

4.6 Oznamovací povinnosti

77. EDPB a EIOÚ doporučují doplnit seznam zvláštních požadavků na oznamování uvedený v článku 13 návrhu o požadavek, aby do oznámení byly zahrnuty informace o konkrétní technologii, díky které se poskytovatel dozvěděl o příslušném obsahu porušujícím práva v případě, že se poskytovatel dozvěděl o možném pohlavním zneužívání dětí na základě opatření přijatých za účelem výkonu detekčního příkazu vydaného v souladu s článkem 7 návrhu.

4.7 Povinnost týkající se odstranění a povinnost provést blokování

78. Jedním z opatření stanovených v návrhu za účelem zmírnění rizik šíření materiálů pohlavního zneužívání dětí je vydávání příkazů k odstranění a blokovacích příkazů, které mají poskytovatelům ukládat povinnost odstranit materiály pohlavního zneužívání dětí on-line nebo k nim znemožnit přístup nebo je zablokovat.⁶²

⁵⁹ Zpráva o posouzení dopadů, příloha 8, s. 281–283.

⁶⁰ s. 15–18.

⁶¹ Viz výše bod 40.

⁶² Návrh, články 14 a 16.

79. Ačkoli je dopad příkazů k odstranění na ochranu údajů a soukromí komunikací relativně omezený, EDPB a EIOÚ připomínají zastřešující zásadu, kterou je třeba dodržovat, a to, že každé takové opatření by mělo být co nejvíce zacíleno.
80. EDPB a EIOÚ zároveň upozorňují na skutečnost, že poskytovatelé služeb přístupu k internetu mají přístup k přesné adrese URL obsahu, pouze pokud je tento obsah zpřístupněn v jasné textové podobě. Když je obsah zpřístupněn prostřednictvím HTTPS, poskytovatel služeb přístupu k internetu nebude mít přístup k přesné adrese URL, ledaže poruší šifrování komunikace. EDPB a EIOÚ mají tudíž pochybnosti, pokud jde o účinnost blokovacích opatření, a domnívají se, že požadavek, aby poskytovatelé služeb přístupu k internetu dešifrovali on-line komunikaci za účelem blokování těch komunikací, které se týkají materiálu pohlavního zneužívání dětí, by byl nepřiměřený.
81. Kromě toho a obecněji je třeba poznamenat, že blokování (nebo znemožnění) přístupu k digitální položce je operací, která probíhá na úrovni sítě, a její provádění se může ukázat jako neúčinné v případě více (případně podobných a nikoli totožných) kopií téže položky. Kromě toho se taková operace může ukázat jako nepřiměřená, pokud se blokování dotýká jiných, nikoli nezákonných digitálních položek, pokud jsou uloženy na témže serveru, k němuž byl zamezen přístup pomocí síťových příkazů (např. IP adresa nebo zařazení na černou listinu DNS). Kromě toho ne všechny přístupy k blokování na úrovni sítě jsou stejně účinné a některé z nich mohou být snadno obcházeny pomocí poměrně základních technických dovedností.
82. V neposlední řadě by měly být v navrhovaném nařízení vyjasněny pravomoci koordinačních orgánů, pokud jde o vydávání blokovacích příkazů. Například ze stávajícího znění čl. 16 odst. 1 a čl. 17 odst. 1 není jasné, zda jsou koordinační orgány oprávněny vydávat blokovací příkazy, nebo pouze požádat o jejich vydání.⁶³

4.8 Relevantní technologie a záruky

4.8.1 Záměrná a standardní ochrana osobních údajů

83. Zdá se, že požadavky návrhu vztahující se na technologie, které mají být zavedeny pro odhalování materiálu pohlavního zneužívání dětí a navazování kontaktu s dětmi, nejsou dostatečně přísné. EDPB a EIOÚ zejména konstatují, že – na rozdíl od obdobných ustanovení prozatímního nařízení⁶⁴ – návrh neobsahuje žádný výslovný odkaz na zásadu záměrné a standardní ochrany osobních údajů a nestanoví, že technologie používané k prohledávání textu v komunikacích nesmí být schopny dovést podstatu obsahu sdělení. V návrhu se v čl. 10 odst. 3 písm. b) pouze stanoví, že technologie nesmí být schopny „získat“ z příslušných sdělení žádné jiné informace než ty, které jsou nezbytně nutné k odhalování. Zdá se však, že tato norma není dostatečně přísná, neboť by bylo možné *dovodit* jiné informace z obsahu sdělení, aniž by se z něj *získávaly* informace jako takové.
84. EIOÚ a EDPB proto doporučují vložit do návrhu bod odůvodnění, který stanoví, že na technologie upravené článkem 10 návrhu se na základě právních předpisů vztahuje zásada záměrné a standardní

⁶³ V čl. 16 odst. 1 návrhu se uvádí: „Koordinační orgán v zemi usazení má pravomoc požádat příslušný soudní orgán členského státu, který jej určil, nebo nezávislý správní orgán tohoto členského státu, aby vydal blokovací příkaz [...]“, zatímco čl. 17 odst. 1 zní: „Koordinační orgán v zemi usazení vydá blokovací příkazy podle článku 16 [...]“ (zvýraznění doplněno).

⁶⁴ Prozatímní nařízení, čl. 3 odst. 1 písm. b).

ochrany osobních údajů stanovená v článku 25 nařízení (EU) 2016/679, a proto ji není třeba v právním textu opakovat. Kromě toho by čl. 10 odst. 3 písm. b) měl být změněn tak, aby se zajistilo, nejen že nebudou získávány žádné další informace, ale také nebudou dovozovány, jak je v současné době stanoveno v čl. 3 odst. 1 písm. b) prozatímního nařízení.

4.8.2 Spolehlivost technologií

85. Návrh předpokládá, že poskytovatelé služeb mohou k provádění detekčních příkazů používat několik druhů technologických řešení. Návrh zejména předpokládá, že jsou k dispozici systémy umělé inteligence a jsou zapojeny do odhalování neznámých materiálů pohlavního zneužívání dětí a navazování kontaktu s dětmi,⁶⁵ a některé koordinační orgány by je mohly považovat za současný stav techniky. Ačkoli účinnost návrhu závisí na spolehlivosti těchto technologických řešení, je k dispozici jen velmi málo informací o všeobecném a systematickém používání těchto technik, což vyžaduje pečlivé zvážení.
86. Kromě toho, i když je EDPB a EIOÚ museli použít při posuzování proporcionality z důvodu nedostatku alternativ, je třeba poznamenat, že ukazatele výkonnosti detekčních technologií uvedené ve zprávě o posouzení dopadů, která je průvodním dokumentem k návrhu, poskytují velmi málo informací o tom, jak byly posouzeny a zda odrážejí výkonnost relevantních technologií v reálném provozu. Nejsou k dispozici žádné informace o zkouškách nebo referenčních hodnotách používaných prodejci technologií k měření této výkonnosti. Bez těchto informací není možné zkoušky opakovat ani vyhodnotit platnost tvrzení o výkonnosti. V tomto ohledu je třeba poznamenat, že ačkoli by ukazatele výkonnosti mohly být vykládány tak, že nasvědčují tomu, že některé nástroje pro odhalování mají vysokou míru přesnosti (například přesnost některých nástrojů odhalování groomingu je 88 %),⁶⁶ tyto ukazatele by měly být posuzovány s ohledem na zamýšlené praktické použití nástrojů pro odhalování a na závažnost rizik, která by nesprávné posouzení daného materiálu příslušným subjektům údajů přineslo. EDPB a EIOÚ se navíc domnívají, že při takto vysoce rizikovém zpracování představuje 12% míra neúspěchu vysoké riziko pro subjekty údajů, u nichž byl výsledek falešně pozitivní, a to i v případě, že existují záruky, které mají zabránit předkládání nepravdivých oznámení donucovacím orgánům. Je velmi nepravděpodobné, že by poskytovatelé služeb mohli vynaložit dostatečné zdroje na přezkoumání takového procenta falešně pozitivních výsledků.
87. Jak bylo uvedeno výše,⁶⁷ ukazatele výkonnosti by měly poskytovat vyčerpávající přehled o chování nástrojů pro odhalování. V rámci používání algoritmů umělé inteligence na obrázky nebo texty je dobře zdokumentováno, že může dojít k předpojatosti a diskriminaci z důvodu nedostatečné reprezentativnosti určitých skupin obyvatelstva v datech, která se používají k vyladění algoritmu. Tato předpojatost by měla být identifikována, změřena a snížena na přijatelnou úroveň, aby systémy pro odhalování byly skutečně přínosné pro společnost jako celek.
88. Přestože byla provedena studie technologií používaných pro odhalování,⁶⁸ EDPB a EIOÚ se domnívají, že je nezbytná další analýza, aby bylo možné nezávisle posoudit spolehlivost stávajících nástrojů v reálných podmínkách. Tato analýza by se měla opírat o vyčerpávající ukazatele výkonnosti a posoudit dopad možných chyb v reálných podmínkách na všechny subjekty údajů, jichž se návrh týká. Vzhledem

⁶⁵ Viz zpráva o posouzení dopadů, s. 281–282.

⁶⁶ Tamtéž, s. 283.

⁶⁷ Viz body 63–64 výše.

⁶⁸ Viz zpráva o posouzení dopadů, s. 279 a násl.

k tomu, že tyto technologie jsou základem, z něhož návrh vychází, EDPB a EIOÚ se domnívají, že tato analýza má zásadní význam pro posouzení vhodnosti návrhu.

89. EDPB a EIOÚ rovněž konstatují, že návrh nedefinuje zvláštní požadavky pro konkrétní technologie, ať už pokud jde o míru chyb, používání klasifikátorů a jejich ověřování, nebo jiná omezení. Vypracování takových kritérií pro posuzování proporcionality používání konkrétní technologie se ponechává na praxi, což dále přispívá k nedostatečné přesnosti a jasnosti.
90. Vzhledem k významu důsledků pro subjekty údajů v případech falešně pozitivních výsledků se EDPB a EIOÚ domnívají, že míra falešně pozitivních výsledků musí být snížena na minimum a že tyto systémy musí být navrženy se zřetelem k tomu, že převážná většina elektronických komunikací nezahrnuje žádný materiál pohlavního zneužívání dětí ani navazování kontaktu s dětmi a že i velmi nízká míra falešně pozitivních výsledků bude znamenat velmi vysoký počet falešně pozitivních výsledků vzhledem k objemu údajů, na kterém se bude provádět odhalování. Obecněji jsou EDPB a EIOÚ rovněž znepokojeni skutečností, že výkonnost dostupných nástrojů uvedených ve zprávě o posouzení dopadů neodráží přesné a srovnatelné ukazatele týkající se míry falešně pozitivních a falešně negativních výsledků, a domnívají se, že by pro tyto technologie měly být vydány srovnatelné a smysluplné ukazatele výkonnosti předtím, než budou považovány za dostupné a účinné.

4.8.3 Skenování zvukové komunikace

91. Na rozdíl od prozatímního nařízení⁶⁹ nevylučuje návrh v souvislosti s odhalováním groomingu skenování zvukové komunikace ze své oblasti působnosti.⁷⁰ EDPB a EIOÚ se domnívají, že skenování zvukové komunikace obzvláště zasahuje do práv, neboť by obvykle vyžadovalo aktivní, průběžné a „živé“ odposlouchávání. V některých členských státech se navíc soukromí mluveného slova těší zvláštní ochraně.⁷¹ Navíc vzhledem ke skutečnosti, že v zásadě by bylo třeba analyzovat veškerý obsah zvukové komunikace, je pravděpodobné, že se toto opatření dotkne podstaty práv zaručených v čluncích 7 a 8 Listiny. Tato metoda odhalování by proto měla zůstat mimo oblast působnosti povinností v oblasti odhalování stanovených v navrhovaném nařízení, a to jak pokud jde o hlasové zprávy, tak o komunikaci naživo, a to tím spíše s ohledem na skutečnost, že zpráva o posouzení dopadů, která byla průvodním dokumentem k návrhu, neidentifikovala žádná konkrétní rizika nebo změny v oblasti hrozeb, které by odůvodňovaly její použití.⁷²

4.8.4 Ověřování věku

92. Návrh vybízí poskytovatele, aby využívali opatření k ověřování věku a posuzování věku k identifikaci dětských uživatelů ve svých službách.⁷³ V tomto ohledu EDPB a EIOÚ konstatují, že v současné době neexistuje žádné technologické řešení, které by dokázalo s jistotou posoudit věk uživatele v on-line prostředí, aniž by se spoléhalo na oficiální digitální identitu, kterou v této fázi nemá každý evropský občan k dispozici.⁷⁴ Zamýšlené použití opatření k ověření věku, které je uvedeno v návrhu, by proto mohlo vést například k vyloučení mladistvě vyhlížejících dospělých osob z přístupu k on-line službám

⁶⁹ Srov. prozatímní nařízení, čl. 1 odst. 2.

⁷⁰ Srov. návrh, článek 1.

⁷¹ Viz např. německý trestní zákoník, § 201.

⁷² Viz zpráva o posouzení dopadů.

⁷³ Viz návrh, čl. 4 odst. 3, čl. 6 odst. 1 písm. c) a 16. bod odůvodnění.

⁷⁴ Viz např. CNIL, Doporučení 7: Zkontrolovat věk dítěte a souhlas rodičů při současném respektování soukromí dítěte (9. srpna 2021).

nebo k zavádění nástrojů pro ověřování věku, jež by významně zasahovaly do práv, což by mohlo bránit oprávněnému využívání dotčených služeb nebo od něho odrazovat.

93. V tomto ohledu, a přestože se v 16. bodě odůvodnění návrhu odkazuje na nástroje pro rodičovskou kontrolu jako na možná zmírňující opatření, EDPB a EIOÚ doporučují, aby bylo navrhované nařízení změněno tak, aby poskytovatelům výslovně umožňovalo spoléhat se na mechanismy rodičovské kontroly, a to nad rámec nebo jako alternativa k ověřování věku.

4.9 Uchovávání informací

94. V článku 22 návrhu se omezují účely, pro které mohou poskytovatelé, na něž se návrh vztahuje, uchovávat údaje o obsahu a jiné údaje zpracovávané v souvislosti s opatřeními přijatými za účelem splnění povinností stanovených v návrhu. V návrhu se však uvádí, že poskytovatelé mohou tyto informace rovněž uchovávat za účelem zlepšení účinnosti a přesnosti technologií pro odhalování pohlavního zneužívání dětí on-line za účelem výkonu detekčního příkazu, ale nesmí za tímto účelem uchovávat žádné osobní údaje.⁷⁵
95. EDPB a EIOÚ se domnívají, že pouze poskytovatelé, kteří používají vlastní detekční technologie, by měli mít možnost uchovávat údaje pro zvýšení účinnosti a přesnosti technologií, zatímco ti, kteří používají technologie poskytované střediskem EU, by tuto možnost mít neměli. EDPB a EIOÚ navíc konstatují, že v praxi může být obtížné zajistit, aby za tímto účelem nebyly uchovávány žádné osobní údaje, neboť většina údajů o obsahu a jiných údajů zpracovávaných pro účely odhalování bude pravděpodobně považována za osobní údaje.

4.10 Dopad na šifrování

96. Evropské úřady pro ochranu údajů se důsledně zasazovaly o širokou dostupnost silných šifrovacích nástrojů a proti jakémukoli typu „zadních vrátek“.⁷⁶ Je tomu tak proto, že šifrování je důležité pro zajištění požívání všech lidských práv na internetu i mimo něj.⁷⁷ Šifrovací technologie navíc zásadním způsobem přispívají jak k respektování soukromého života a důvěrnosti komunikace, tak k inovacím a růstu digitální ekonomiky, která závisí na vysoké úrovni důvěry, kterou tyto technologie zajišťují.
97. V prostředí interpersonální komunikace je šifrování mezi koncovými body klíčovým nástrojem pro zajištění důvěrnosti elektronických komunikací, neboť poskytuje silné technické záruky proti přístupu k obsahu komunikace pro kohokoli, kdo není odesílatelem a příjemcem (příjemci), včetně poskytovatele. Zabránění nebo jakékoli odrazování od používání šifrování mezi koncovými body, uložení povinnosti poskytovatelům služeb zpracovávat údaje o elektronických komunikacích pro jiné účely, než je poskytování jejich služeb, nebo uložení povinnosti aktivně předávat elektronické komunikace třetím stranám by obnášelo riziko, že poskytovatelé budou nabízet méně šifrované služby, aby lépe plnili své povinnosti, čímž se oslabí úloha šifrování obecně a dodržování základních práv evropských občanů. Je třeba poznamenat, že ačkoliv je šifrování mezi koncovými body jedním z nejběžněji používaných bezpečnostních opatření v oblasti elektronických komunikací, jiná technická řešení (např. použití jiných kryptografických systémů) by mohla být nebo by se mohla stát stejně

⁷⁵ Návrh, čl. 22 odst. 1.

⁷⁶ Viz např. pracovní skupina pro ochranu údajů zřízená podle článku 29, Prohlášení pracovní skupiny zřízené podle článku 29 o šifrování a jeho dopadu na ochranu jednotlivců v souvislosti se zpracováním jejich osobních údajů v EU (11. dubna 2018).

⁷⁷ Viz Rada pro lidská práva, rezoluce 47/16 o prosazování, ochraně a požívání lidských práv na internetu, dokument OSN A/HRC/RES/47/16 (26. července 2021).

důležitými pro zajištění a ochranu důvěrnosti digitální komunikace. Proto není žádoucí bránit v jejich používání nebo od něho odrazovat.

98. Zavádění nástrojů pro odposlouchávání a analýzu interpersonální elektronické komunikace je v zásadě v rozporu s šifrováním mezi koncovými body, neboť cílem tohoto šifrování je technicky zaručit, že komunikace mezi odesílatelem a příjemcem zůstane důvěrná.
99. Proto i když návrh neukládá poskytovatelům povinnost systematického odposlouchávání, pouhá možnost, že by mohl být vydán detekční příkaz, bude pravděpodobně značně ovlivňovat technická rozhodnutí poskytovatelů, zejména vzhledem k omezenému časovému rámci, který budou muset dodržet, a k přísným sankcím, kterým by čelili v případě, že tak neučiní.⁷⁸ V praxi by to mohlo vést k tomu, že někteří poskytovatelé přestanou šifrování mezi koncovými body používat.
100. Je třeba řádně posoudit dopad zhoršení používání šifrování mezi koncovými body nebo odrazování od něho, které může z návrhu vyplývat. Každá z technik obcházení šifrování mezi koncovými body chránícího soukromí, která byla představena ve zprávě o posouzení dopadů, jež je průvodním dokumentem k návrhu, by vedla ke vzniku bezpečnostních rizik.⁷⁹ Například prohlédávání/skenování na straně zákazníka⁸⁰ by pravděpodobně vedlo ke značnému, nezacílenému přístupu a zpracování nešifrovaného obsahu na zařízeních koncového uživatele. Takto podstatné zhoršení důvěrnosti by mělo dopad zejména na děti, neboť u služeb, které využívají, je pravděpodobnější, že budou předmětem detekčních příkazů, což je činí zranitelnými vůči monitorování nebo odposlechu. Zároveň je prohlédávání/skenování *na straně serveru* rovněž zásadně neslučitelné s modelem šifrování mezi koncovými body, neboť komunikační kanál, šifrovaný „peer-to-peer“, by musel být přerušen, což by vedlo k hromadnému zpracování osobních údajů na serverech poskytovatelů.
101. Ačkoliv se v návrhu uvádí, že dotčenému poskytovateli se „ponechává možnost volby technologií, které mají být provozovány, aby účinně vyhověl detekčním příkazům, a nemělo by být chápáno jako pobídka k používání určité technologie nebo odrazování od jejího používání“⁸¹, strukturální neslučitelnost některých detekčních příkazů s šifrováním mezi koncovými body se stává ve skutečnosti silným odrazujícím faktorem od používání takového šifrování. Nemožnost přístupu ke službám (jež představují současný stav techniky, pokud jde o možnost, jak technicky zaručit důvěrnost) využívajícím šifrování mezi koncovými body a jejich nepoužívání by mohly mít odrazující účinek na svobodu projevu a legitimní soukromé využívání služeb elektronických komunikací. Komise ve zprávě o posouzení dopadů rovněž uznala negativní vztah mezi materiály pohlavního zneužívání dětí nebo odhalováním groomingu a šifrováním mezi koncovými body, když ve zprávě o posouzení dopadů⁸² konstatovala, že je pravděpodobné, že zavedení šifrování mezi koncovými body společností Facebook v roce 2023 ukončí dobrovolné prohlédávání/skenování ze strany této společnosti.
102. Aby se zajistilo, že navrhované nařízení nenarušuje bezpečnost nebo důvěrnost elektronické komunikace evropských občanů, EDPB a EIOÚ se domnívají, že by se v normativní části návrhu mělo

⁷⁸ Srov. návrh, článek 35.

⁷⁹ Viz oddíl 4.2, Abelson, Harold, Ross J. Anderson, Steven M. Bellare, 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“ („Štění se v kapse: rizika a prohlédávání/skenování na straně klienta), arXiv abs/2110.07450 (2021).

⁸⁰ Prohlédávání/skenování na straně klienta se obecně rozumí systémy, které prohlédávají/skenují obsah zpráv za účelem nalezení shodys databází sporného obsahu před odesláním zprávy zamýšlenému příjemci.

⁸¹ Návrh, 26. bod odůvodnění.

⁸² Zpráva o posouzení dopadů, s. 27.

jasně uvádět, že nic v navrhovaném nařízení by nemělo být vykládáno tak, že zakazuje nebo oslabuje šifrování, a to v souladu s tím, co je uvedeno v 25. bodě odůvodnění prozatímního nařízení.

4.11 Dohled, prosazování práva a spolupráce

4.11.1 Úloha vnitrostátních dozorových úřadů podle obecného nařízení o ochraně osobních údajů

103. Návrh stanoví zřízení sítě vnitrostátních koordinačních orgánů, které budou odpovědné za uplatňování a prosazování navrhovaného nařízení.⁸³ Ačkoliv se v 54. bodě odůvodnění návrhu uvádí, že „pravidla tohoto nařízení týkající se dohledu a prosazování by neměla být chápána tak, že mají vliv na pravomoci a příslušnost úřadů pro ochranu údajů podle nařízení (EU) 2016/679“, EDPB a EIOÚ jsou toho názoru, že vztah mezi úkoly koordinačních orgánů a úkoly úřadů pro ochranu údajů by měl být lépe upraven a že úřadům pro ochranu údajů by měla být v rámci navrhovaného nařízení přiznána významnější úloha.
104. Poskytovatelé by měli mít zejména povinnost konzultovat s úřady pro ochranu údajů prostřednictvím postupu předchozí konzultace, jak je uvedeno v článku 36 obecného nařízení o ochraně osobních údajů, před zavedením jakýchkoli opatření pro odhalování veškerého materiálu pohlavního zneužívání dětí nebo groomingu, a nikoli výhradně v souvislosti s používáním opatření pro odhalování navazování kontaktu s dětmi, jak v současné době stanoví návrh.⁸⁴ U všech opatření pro odhalování by se mělo mít za to, že standardně vedou k „vysokému riziku“, a proto by měla být předmětem předchozí konzultace bez ohledu na to, zda se týkají groomingu nebo materiálů pohlavního zneužívání dětí, jak je tomu již podle prozatímního nařízení.⁸⁵ Kromě toho by příslušné úřady pro ochranu údajů určené podle obecného nařízení o ochraně osobních údajů měly mít vždy pravomoc sdělovat své názory na plánovaná opatření pro odhalování, a to nejen za zvláštních okolností.⁸⁶
105. Kromě toho by navrhované nařízení mělo zřídit systém pro řešení a urovnávání sporů mezi příslušnými orgány a úřady pro ochranu údajů, pokud jde o detekční příkazy. Úřady pro ochranu údajů by měly mít zejména právo napadnout detekční příkaz u soudů členského státu příslušného soudního orgánu nebo nezávislého správního orgánu, který detekční příkaz vydal. V tomto ohledu si EDPB a EIOÚ všímají, že podle stávající verze návrhu může příslušný orgán při vydávání detekčního příkazu zamítnout stanovisko příslušných úřadů pro ochranu údajů. To může potenciálně vést ke kolizním rozhodnutím, neboť úřady pro ochranu údajů by si, jak je potvrzeno v čl. 36 odst. 2 obecného nařízení o ochraně osobních údajů, zachovaly celou škálu svých nápravných pravomocí podle článku 58 obecného nařízení o ochraně osobních údajů, včetně pravomoci nařít zákaz zpracování.

4.11.2 Úloha EDPB

106. EDPB a EIOÚ si všímají, že návrh v čl. 50 odst. 1 třetí větě stanoví, že „si středisko EU vyžádá stanovisko svého Technologického výboru a Evropského sboru pro ochranu osobních údajů“, než zařadí konkrétní technologii na seznamy technologií, o jejichž použití mohou poskytovatelé hostingových služeb a poskytovatelé interpersonálních komunikačních služeb uvažovat pro účely výkonu detekčních příkazů. Dále stanoví, že EDPB vydá svá stanoviska do osmi týdnů a tato lhůta může být s ohledem na složitost záležitosti v případě potřeby prodloužena o dalších šest týdnů. V neposlední řadě vyžaduje, aby EDPB

⁸³ Návrh, článek 25.

⁸⁴ Návrh, čl. 7 odst. 3 druhá odrážka písm. b).

⁸⁵ Prozatímní nařízení, čl. 3 odst. 1 písm. c).

⁸⁶ Srov. návrh, čl. 7 odst. 3 druhá odrážka písm. c).

informoval středisko EU o každém takovém prodloužení do jednoho měsíce od obdržení žádosti o konzultaci spolu s důvody odložení.

107. Stávající úkoly EDPB jsou stanoveny v článku 70 obecného nařízení o ochraně osobních údajů a v článku 51 směrnice (EU) 2016/680 (dále jen „směrnice o prosazování práva“).⁸⁷ V rámci těchto úkolů je stanoveno, že EDPB poskytuje Komisi poradenství a vydává stanoviska na žádost Komise, vnitrostátního dozorového úřadu nebo jeho předsedy. Zatímco v čl. 1 odst. 3 písm. d) návrhu se stanoví, že pravidla stanovená v obecném nařízení o ochraně osobních údajů a ve směrnici o prosazování práva nejsou návrhem dotčena, zmocnění střediska EU k podávání žádostí o stanoviska EDPB jde nad rámec úkolů svěřených EDPB podle obecného nařízení o ochraně osobních údajů a směrnice o prosazování práva. Proto by mělo být v navrhovaném nařízení – alespoň v některém bodě odůvodnění – jasně uvedeno, že návrh rozšiřuje úkoly EDPB. V tomto ohledu EDPB a EIOÚ oceňují důležitou úlohu, kterou návrh přisuzuje EDPB, pokud jde o požadavek na jeho zapojení do praktického provádění navrhovaného nařízení. V praxi hraje sekretariát EDPB zásadní úlohu při poskytování analytické, administrativní a logistické podpory nezbytné pro přijetí stanovisek EDPB. Aby se zajistilo, že EDPB a jeho členové budou moci plnit své úkoly, je proto nezbytné přidělit EDPB dostatečný rozpočet a zaměstnance. Legislativní finanční výkaz návrhu však bohužel neuvádí, že pro plnění dodatečných úkolů, které návrh svěřuje EDPB, budou k dispozici další zdroje.⁸⁸
108. EDPB a EIOÚ dále konstatují, že článek 50 návrhu neuvádí, jak bude středisko EU postupovat poté, co obdrží stanovisko EDPB.⁸⁹ V 27. bodě odůvodnění návrhu se pouze uvádí, že rady poskytnuté Evropským sborem pro ochranu osobních údajů by měly být zohledněny střediskem EU a Evropskou komisí. Proto by mělo být vyjasněno, jakému účelu bude požadované stanovisko sloužit v procesu stanoveném v článku 50 návrhu a jak má středisko EU jednat poté, co obdrží stanovisko EDPB.
109. Kromě toho se EDPB a EIOÚ domnívají, že i když jakékoli pokyny EDPB nebo případné stanovisko k používání detekčních technologií budou posuzovat používání těchto technologií na obecné úrovni, pro účely předchozí konzultace podle článku 36 obecného nařízení o ochraně osobních údajů bude vnitrostátní dozorový úřad muset zohlednit konkrétní okolnosti a provést individuální posouzení zamýšleného zpracování příslušným správcem. EDPB a EIOÚ konstatují, že dozorové úřady budou a měly by uplatňovat kritéria stanovená v článku 36 obecného nařízení o ochraně osobních údajů při rozhodování, zda je nezbytné prodloužit lhůtu stanovenou v obecném nařízení o ochraně osobních údajů pro poskytnutí stanovisek v reakci na předchozí konzultaci, a že v případě, že se předchozí konzultace týká používání detekční technologie, není nutné uplatňovat odlišné normy.⁹⁰
110. V neposlední řadě při uplatňování článku 11 („Pokyny týkající se povinností odhalování“) návrh stanoví, že Komise může vydat pokyny k uplatňování článků 7 až 10 návrhu. Článek 11 návrhu by měl být změněn tak, aby bylo jasné, že kromě koordinačních orgánů a střediska EU by Komise měla před vydáním pokynů týkajících se povinností odhalování konzultovat EDPB ohledně návrhu pokynů mimo zamýšlený proces veřejné konzultace.

⁸⁷ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89–131).

⁸⁸ Srov. návrh, s. 105 a násl.

⁸⁹ Viz naproti tomu čl. 51 odst. 4 směrnice o prosazování práva.

⁹⁰ Srov. návrh, 24. bod odůvodnění.

111. Tento úkol EDPB, jakož i jeho úloha v právním rámci, který by byl návrhem zaveden, proto vyžadují další posouzení ze strany normotvůrců.

4.11.3 Úloha Střediska EU proti pohlavnímu zneužívání dětí

112. V kapitole IV návrhu se zamýšlí zřídit středisko EU jako novou decentralizovanou agenturu, která by umožnila provádění návrhu. Kromě jiných úkolů by středisko EU mělo poskytovatelům usnadnit přístup ke spolehlivým detekčním technologiím; zpřístupnit ukazatele vytvořené na základě pohlavního zneužívání dětí on-line, které jsou ověřeny soudy nebo nezávislými správními orgány členských států pro účely odhalování; na požádání poskytovat určitou pomoc v souvislosti s prováděním posouzení rizik a poskytovat podporu při komunikaci s příslušnými vnitrostátními orgány.⁹¹
113. V tomto ohledu EDPB a EIOÚ vítají čl. 77 odst. 1 návrhu, v němž se potvrzuje, že zpracování osobních údajů střediskem EU podléhá nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie, a stanoví, že opatření pro uplatňování uvedeného nařízení střediskem EU, včetně opatření týkajících se jmenování pověřence pro ochranu osobních údajů střediska EU, se stanoví po konzultaci s EIOÚ. EDPB a EIOÚ jsou však toho názoru, že několik ustanovení této kapitoly si zasluhuje důkladnější přezkum.
114. Zaprvé, EDPB a EIOÚ konstatují, že článek 48 návrhu stanoví, že všechna oznámení, která „nejsou zjevně neopodstatněná“⁹², se předávají vnitrostátním donucovacím orgánům a Agentuře EU pro spolupráci v oblasti prosazování práva (dále jen „Europol“). Tato prahová hodnota pro předkládání oznámení vnitrostátním donucovacím orgánům a Europolu ze strany střediska EU („nejsou zjevně neopodstatněná“), se jeví jako příliš nízká, zejména s ohledem na to, že účelem zřízení střediska EU, jak je uvedeno ve zprávě Komise o posouzení dopadů⁹³, je zmírnit zátěž donucovacích orgánů a Europolu spočívající ve filtrování obsahu chybně označeného jako materiál pohlavního zneužívání dětí. V tomto ohledu není jasné, proč by středisko EU jakožto centrum odborných znalostí nemohlo provést důkladnější právní posouzení a posouzení skutkového stavu s cílem omezit riziko předávání údajů nevinných osob donucovacím orgánům.
115. Zadruhé, ustanovení týkající se doby uchovávání osobních údajů střediskem EU se jeví vzhledem k citlivosti dotčených údajů jako relativně otevřená. I kdyby nebylo možné stanovit maximální dobu uchovávání těchto údajů, EDPB a EIOÚ doporučují, aby byla v návrhu stanovena alespoň maximální lhůta pro přezkum nezbytnosti dalšího uchovávání údajů a aby bylo vyžadováno odůvodnění jeho prodloužení po uplynutí této doby.
116. Vzhledem k velmi vysoké citlivosti osobních údajů, které má středisko EU zpracovávat, jsou EDPB a EIOÚ dále toho názoru, že zpracování by mělo podléhat dodatečným zárukám, zejména s cílem zajistit účinný dohled. To by mohlo zahrnovat povinnost střediska EU uchovávat logy o operacích zpracování v automatizovaných systémech zpracování údajů (tj. v souladu s požadavkem na operativní osobní údaje podle kapitoly IX nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie), včetně zaznamenávání vkládání, pozměňování, přístupu, nahlížení, zpřístupnění, zkombinování a výmazu osobních údajů. Logy o nahlédnutí a zpřístupnění musí umožňovat zjištění odůvodnění, data a času těchto operací, totožnosti osoby, která nahlédla do

⁹¹ Viz COM(2022) 209 final, s. 7.

⁹² Pojem „zjevně neopodstatněná“ je v 65. bodě odůvodnění návrhu popsán jako „je-li bez věcné právní nebo faktické analýzy okamžitě zřejmé, že oznámené činnosti nepředstavují pohlavní zneužívání dětí on-line“.

⁹³ Viz například strana 349 zprávy o posouzení dopadů.

operativních osobních údajů nebo je zpřístupnila, a pokud možno o totožnosti příjemců. Tyto logy by byly použity k ověření zákonnosti zpracování, k vlastní kontrole a pro zajištění neporušenosti a zabezpečení operativních osobních údajů a byly by na požádání zpřístupněny pověřenci pro ochranu osobních údajů střediska EU a EIOÚ.

117. Návrh dále odkazuje na povinnost poskytovatelů informovat uživatele o odhalování materiálů pohlavního zneužívání dětí na základě detekčních příkazů, jakož i na právo podat stížnost koordináčnímu orgánu.⁹⁴ Návrh však nestanoví postupy pro výkon práv subjektů údajů, a to ani s ohledem na více míst, kam mohou být osobní údaje předávány a kde mohou být podle návrhu uchovávány (středisko EU, Europol, vnitrostátní donucovací orgány). Požadavek na informování uživatelů by měl zahrnovat povinnost informovat fyzické osoby o tom, že jejich údaje byly předány a případně jsou zpracovávány různými subjekty (např. vnitrostátními donucovacími orgány a Europolem). Kromě toho by měl existovat centralizovaný postup pro přijímání a koordinaci žádostí o uplatnění práva na přístup, opravu a výmaz nebo případně povinnost, aby subjekt, který obdrží žádost subjektu údajů, koordinoval svou činnost s ostatními dotčenými subjekty.
118. EDPB a EIOÚ konstatují, že podle článku 50 návrhu je středisko EU pověřeno upřesněním seznamu technologií, které mohou být použity pro výkon detekčních příkazů. Podle čl. 12 odst. 1 návrhu jsou však poskytovatelé povinni podávat oznámení o všech informacích naznačujících možné pohlavní zneužívání dětí on-line v jejich službách, nejen o těch, které vyplývají z výkonu detekčního příkazu. Je vysoce pravděpodobné, že značné množství těchto informací by pocházelo z uplatňování zmírňujících opatření poskytovatelů v souladu s článkem 4 návrhu. Proto se jeví jako zásadní určit, jaká by tato opatření mohla být, jejich účinnost, míru chyb při oznamování možného pohlavního zneužívání dětí a jaký je jejich dopad na práva a svobody jednotlivců. Navzdory skutečnosti, že se v čl. 4 odst. 5 návrhu stanoví, že Komise může ve spolupráci s koordináčními orgány a střediskem EU a po provedení veřejné konzultace vydat příslušné pokyny, EDPB a EIOÚ považují za důležité, aby normotvůrce zahrnul do článku 50 úkol, aby centrum EU poskytlo rovněž seznam doporučených zmírňujících opatření a relevantních osvědčených postupů, které jsou zvláště účinné při zjišťování možného pohlavního zneužívání dětí on-line. Vzhledem k tomu, že taková opatření mohou zasahovat do základních práv na ochranu osobních údajů a soukromí, doporučuje se rovněž, aby si středisko EU před vydáním takového seznamu vyžádalo stanovisko EDPB.
119. V neposlední řadě by požadavky na bezpečnost stanovené v čl. 51 odst. 4 návrhu měly být konkrétnější. V tomto ohledu se lze inspirovat požadavky na bezpečnost stanovenými v jiných nařízeních týkajících se rozsáhlých systémů zahrnujících vysoce rizikové zpracování, jako je nařízení

⁹⁴ Viz čl. 10 odst. 6 a po předložení oznámení středisku EU čl. 12 odst. 2 návrhu.

767/2008⁹⁵ (viz článek 32), nařízení 1987/2006⁹⁶ (viz článek 16), nařízení 2018/1862⁹⁷ (viz článek 16) a nařízení 603/2013⁹⁸ (viz článek 34).

4.11.4 Úloha Europolu

120. Návrh stanoví úzkou spolupráci mezi střediskem EU a Europolem. Podle kapitoly IV návrhu středisko EU po obdržení oznámení od poskytovatelů o podezření na materiály pohlavního zneužívání dětí tato oznámení prověří, aby posoudilo, u kterých je možné provést další kroky (nejsou zjevně neopodstatněná), a předá je Europolu a vnitrostátním donucovacím orgánům.⁹⁹ Středisko EU poskytne Europolu přístup do svých databází ukazatelů a do databází oznámení s cílem pomoci Europolu při vyšetřování podezření z trestných činů pohlavního zneužívání dětí.¹⁰⁰ Kromě toho by středisku EU byl poskytnut „co nejširší“ přístup k informačním systémům Europolu.¹⁰¹ Obě agentury budou rovněž sdílet prostory a určitou (neprovozní) infrastrukturu.¹⁰²
121. EDPB a EIOÚ konstatují, že několik aspektů týkajících se spolupráce mezi navrhovaným střediskem EU a Europolem vyvolává obavy nebo vyžaduje další upřesnění.

O předávání oznámení střediskem EU Europolu (článek 48)

122. Článek 48 navrhovaného nařízení vyžaduje, aby středisko EU předalo oznámení, která nejsou považována za zjevně neopodstatněná, spolu s veškerými dalšími relevantními informacemi Europolu a příslušnému donucovacímu orgánu nebo orgánům členského státu (členských států), které jsou pravděpodobně příslušné k vyšetřování nebo stíhání možného pohlavního zneužívání dětí. Ačkoli tento článek přiznává Europolu úlohu určit příslušný donucovací orgán, pokud je dotčený členský stát nejasný, toto ustanovení ve skutečnosti stanoví, že všechna oznámení se předávají Europolu bez ohledu na to, zda byl vnitrostátní orgán určen a zda již středisko EU předalo oznámení.

⁹⁵ Nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS), Úř. věst. L 218, 13.8.2008, s. 60–81.

⁹⁶ Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) (Úř. věst. L 381, 28.12.2006, s. 4–23).

⁹⁷ Nařízení Evropského parlamentu a Rady (EU) 2018/1862 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně a o zrušení rozhodnutí Rady 2007/533/SVV a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 a rozhodnutí Komise 2010/261/EU (Úř. věst. L 312, 7.12.2018, s. 56–106).

⁹⁸ Nařízení Evropského parlamentu a Rady (EU) č. 603/2013 ze dne 26. června 2013 o zřízení systému „Eurodac“ pro porovnávání otisků prstů za účelem účinného uplatňování nařízení (EU) č. 604/2013 kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států, a pro podávání žádostí orgánů pro vymáhání práva členských států a Europolu o porovnání údajů s údaji systému Eurodac pro účely vymáhání práva a o změně nařízení (EU) č. 1077/2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (Úř. věst. L 180, 29.6.2013, s. 1–30).

⁹⁹ Viz článek 48 návrhu.

¹⁰⁰ Viz čl. 46 odst. 4 a 5 návrhu.

¹⁰¹ Viz čl. 53 odst. 2 návrhu.

¹⁰² Zejména ty týkající se řízení lidských zdrojů, informačních technologií (IT), včetně kybernetické bezpečnosti, budov a komunikací.

123. V návrhu se však neobjasňuje, jaká by byla přidaná hodnota zapojení Europolu nebo jeho očekávané úlohy po obdržení oznámení, zejména v případech, kdy byl souběžně určen a informován vnitrostátní donucovací orgán.¹⁰³
124. EDPB a EIOÚ připomínají, že mandát Europolu je omezen na podporu opatření příslušných orgánů členských států a jejich vzájemné spolupráce při předcházení závažné trestné činnosti dotýkající se dvou nebo více členských států a při boji proti takové trestné činnosti.¹⁰⁴ Článek 19 nařízení (EU) 2016/794¹⁰⁵ ve znění nařízení (EU) 2022/991¹⁰⁶ (dále jen „pozměněné nařízení o Europolu“) stanoví, že instituce Unie poskytující informace Europolu je povinna určit účel nebo účely jejich zpracování, jakož i podmínky zpracování. Odpovídá rovněž za zajištění přesnosti předávaných osobních údajů.¹⁰⁷
125. Plošné předávání oznámení Europolu by proto bylo v rozporu s pozměněným nařízením o Europolu a obnášelo by řadu rizik pro ochranu osobních údajů. Zdvojení zpracování osobních údajů by mohlo vést k souběžnému uchovávání více kopií týchž vysoce citlivých osobních údajů (např. ve středisku EU, v Europolu, ve vnitrostátním donucovacím orgánu), což by mohlo znamenat riziko pro přesnost údajů v důsledku možné desynchronizace databází, jakož i pro výkon práv subjektů údajů. Kromě toho nízká prahová hodnota stanovená v návrhu pro sdílení oznámení s donucovacími orgány (těch, která „nejsou zjevně neopodstatněná“) znamená vysokou pravděpodobnost, že falešně pozitivní výsledky (tj. obsah omylem označený jako pohlavní zneužívání dětí) budou uloženy v informačních systémech Europolu, a to potenciálně po delší dobu.¹⁰⁸
126. EDPB a EIOÚ proto doporučují, aby se v návrhu upřesnily a omezily okolnosti a účely, v jejichž rámci by středisko EU mohlo předávat oznámení Europolu v souladu s pozměněným nařízením o Europolu. Tím by se měly výslovně vyloučit ty okolnosti, kdy byla oznámení předána příslušnému donucovacímu orgánu členského státu, což nasvědčuje tomu, že případ nemá přeshraniční rozměr. Kromě toho by měl návrh obsahovat požadavek, aby středisko EU předalo Europolu pouze takové osobní údaje, které jsou přiměřené, relevantní a omezené na to, co je nezbytně nutné. Musí být rovněž stanoveny zvláštní záruky pro zajištění kvality a spolehlivosti údajů.

¹⁰³ V 71. bodě odůvodnění návrhu se pouze obecně odkazuje na zkušenosti Europolu s určováním příslušných vnitrostátních orgánů v nejasných situacích a na jeho databázi zpravodajských informací o trestné činnosti, což může přispět ke zjištění vazeb na vyšetřování v jiných členských státech.

¹⁰⁴ Viz článek 3 pozměněného nařízení o Europolu.

¹⁰⁵ Nařízení Evropského parlamentu a Rady (EU) 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SW, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Úř. věst. L 135, 24.5.2016, s. 53–114).

¹⁰⁶ Nařízení Evropského parlamentu a Rady (EU) 2022/991 ze dne 8. června 2022, kterým se mění nařízení (EU) 2016/794, pokud jde o spolupráci Europolu se soukromými subjekty, zpracování osobních údajů Eupolem pro usnadnění trestního vyšetřování a úlohu Europolu v oblasti výzkumu a inovací (Úř. věst. L 169, 27.6.2022, s. 1–42).

¹⁰⁷ Čl. 38 odst. 2 písm. a) pozměněného nařízení o Europolu.

¹⁰⁸ Podle zprávy Komise o posouzení dopadů byl Europol schopen přezkoumat ve své databázi pouze 20 % z 50 milionů jedinečných obrázků a videí považovaných za materiály pohlavního zneužívání dětí, což svědčí o nedostatku zdrojů na to, aby mohl reagovat na příspěvky v podobě materiálu pohlavního zneužívání dětí, které v současné době dostává. Viz zpráva o posouzení dopadů, jež je průvodním dokumentem k návrhu nařízení, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu, SWD(2022)209, s. 47–48.

Ustanovení čl. 53 odst. 2 o spolupráci mezi střediskem EU a Europolem

127. Ustanovení čl. 53 odst. 2 návrhu vyžaduje, aby si Europol a středisko EU vzájemně poskytovaly „co nejširší přístup k relevantním informacím a informačním systémům, je-li to nezbytné pro plnění jejich příslušných úkolů a v souladu s právními předpisy Unie, které tento přístup upravují“.
128. Ustanovení čl. 46 odst. 4 a 5 návrhu dále upřesňují, že Europol má přístup do databáze ukazatelů a do databáze oznámení střediska EU, a v čl. 46 odst. 6 se stanoví postup pro udělení tohoto přístupu: Europol předloží žádost, v níž uvede účel a míru přístupu potřebného ke splnění tohoto účelu, kterou středisko EU řádně posoudí.
129. Kritéria a záruky, které podmiňují přístup Europolu k údajům získaným z informačních systémů střediska EU a jejich následné využívání, nejsou upřesněny. Kromě toho není vysvětleno, proč je nezbytné poskytnout Europolu přímý přístup k informačním systémům orgánu, který není donucovacím orgánem, jež obsahují vysoce citlivé osobní údaje, u nichž nemusí být prokázána souvislost s trestnou činností a předcházením trestné činnosti. Aby byla zajištěna vysoká úroveň ochrany údajů a dodržování zásady účelového omezení, EDPB a EIOÚ doporučují, aby se předávání osobních údajů ze střediska EU Europolu provádělo pouze v jednotlivých případech na základě řádně posouzené žádosti, a to prostřednictvím komunikačního nástroje pro zabezpečenou výměnu informací, jako je síť SIENA.¹⁰⁹
130. V čl. 53 odst. 2 se uvádí jediný odkaz v návrhu na přístup střediska EU k informačním systémům Europolu. Není tedy jasné, za jakým účelem a na základě jakých zvláštních záruk by k takovému přístupu docházelo.
131. EDPB a EIOÚ připomínají, že Europol je donucovací orgán zřízený podle Smluv EU a jeho hlavním mandátem je předcházet závažné trestné činnosti a bojovat proti ní. Operativní osobní údaje zpracovávané Europolem proto podléhají přísným pravidlům a zárukám pro zpracování údajů. Navrhované středisko EU není donucovacím orgánem a za žádných okolností by mu neměl být umožněn přímý přístup k informačním systémům Europolu.
132. EDPB a EIOÚ dále konstatují, že velká část informací společného zájmu střediska EU a Europolu se bude týkat osobních údajů obětí údajných trestných činů, osobních údajů nezletilých osob a osobních údajů týkajících se pohlavního života, které jsou podle pozměněného nařízení o Europolu považovány za zvláštní kategorie osobních údajů. Pozměněné nařízení o Europolu ukládá přísné podmínky, pokud jde o přístup ke zvláštním kategoriím osobních údajů. V čl. 30 odst. 3 pozměněného nařízení o Europolu se stanoví, že přímý přístup k těmto osobním údajům má pouze Europol, konkrétně pouze omezený počet úředníků Europolu řádně zmocněných výkonným ředitelem.¹¹⁰
133. EDPB a EIOÚ proto doporučují vyjasnit znění čl. 53 odst. 2 návrhu s cílem řádně zohlednit omezení zavedená podle pozměněného nařízení o Europolu a upřesnit podmínky přístupu ze strany střediska EU. Zejména jakýkoli přístup k osobním údajům zpracovávaným v informačních systémech Europolu, je-li to považováno za nezbytně nutné pro plnění úkolů střediska EU, by měl být udělen pouze případ od případu na základě výslovné žádosti, ve které se doloží konkrétní účel a odůvodnění. Europol by

¹⁰⁹ Aplikace sítě pro bezpečnou výměnu informací (SIENA).

¹¹⁰ Podle pozměněného nařízení o Europolu jsou z tohoto zákazu stanoveny výjimky pro agentury Unie zřízené na základě hlavy V SFEU. Vzhledem k právnímu základu návrhu (114 SFEU, který se týká harmonizace vnitřního trhu) by se však tato výjimka na navrhované středisko EU nevztahovala.

měl mít povinnost tyto žádosti pečlivě posoudit a předávat osobní údaje středisku EU pouze tehdy, je-li to nezbytně nutné a přiměřené požadovanému účelu.

Ustanovení čl. 10 odst. 6 o úloze Europolu při informování uživatelů po provedení detekčního příkazu

134. EDPB a EIOÚ vítají požadavek stanovený v čl. 10 odst. 6 návrhu, aby poskytovatelé informovali uživatele, jejichž osobní údaje mohou být dotčeny provedením detekčního příkazu. Tyto informace mají být uživatelům poskytnuty až po obdržení potvrzení od Europolu nebo od vnitrostátního donucovacího orgánu členského státu, který obdržel oznámení podle článku 48 návrhu, že informace poskytnuté uživatelům nezasáhnou do činností v oblasti prevence, odhalování, vyšetřování a stíhání trestných činů pohlavního zneužívání dětí.
135. Chybí však konkrétní informace o praktickém provádění tohoto ustanovení. Pokud jsou oznámení předávána jak Europolu, tak donucovacímu orgánu členského státu, návrh nestanoví, zda je vyžadováno potvrzení od jednoho nebo obou příjemců, a také nejsou v návrhu uvedeny postupy/podmínky pro získání tohoto potvrzení (např. zda mají být potvrzení zasílána prostřednictvím střediska EU). Vzhledem k vysokému objemu materiálů pohlavního zneužívání dětí, který by Europol a vnitrostátní donucovací orgány mohly být povinny zpracovávat, a s ohledem na nestanovení přesné lhůty pro poskytnutí potvrzení („bez zbytečného odkladu“) EDPB a EIOÚ doporučují vyjasnit platné postupy s cílem zajistit naplnění této záruky v praxi. Kromě toho by povinnost informovat uživatele měla rovněž zahrnovat informace o příjemcích dotčených osobních údajů.

O shromažďování údajů a podávání zprávo transparentnosti (článek 83)

136. V čl. 83 odst. 3 návrhu se stanoví, že středisko EU shromažďuje údaje a vytváří statistiky týkající se řady jeho úkolů podle navrhovaného nařízení. Pro účely monitorování EDPB a EIOÚ doporučují doplnit do tohoto seznamu statistiky o počtu oznámení předaných Europolu podle článku 48, jakož i o počtu žádostí o přístup obdržených Europolem podle čl. 46 odst. 4 a 5, včetně počtu žádostí schválených a zamítnutých střediskem EU.

5. ZÁVĚR

137. EDPB a EIOÚ sice vítají úsilí Komise o zajištění účinných opatření proti pohlavnímu zneužívání dětí online, domnívají se však, že návrh vyvolává vážné obavy týkající se ochrany údajů a soukromí. EDPB a EIOÚ by proto chtěli vyzvat spolunormotvůrce, aby navrhované nařízení změnili, zejména s cílem zajistit, aby zamýšlené povinnosti v oblasti odhalování splňovaly platné standardy nezbytnosti a proporcionality a nevedly obecně k oslabení nebo zhoršení šifrování. EDPB a EIOÚ jsou i nadále k dispozici, aby nabídli podporu v průběhu legislativního procesu, bude-li jejich příspěvek považován za nezbytný k řešení obav, na něž se upozorňuje v tomto společném stanovisku.

Za evropského inspektora ochrany údajů

evropský inspektor ochrany údajů

(Wojciech Wiewiorowski)

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)