

STANOVISKO REPUBLIKOVEJ ÚNIE ZAMESTNÁVATEĽOV

Návrh NARIADENIE EURÓPSKEHO PARLAMENTU A RADY, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu

<https://www.slov-lex.sk/legislativne-procesy/SK/LPEU/2022/259>

Materiál v pripomienkovom konaní do 05.12.2022

Stručný popis podstaty materiálu najmä jeho relevancie z pohľadu RÚZ

Materiál bol predložený do medzirezortného pripomienkového konania Ministerstvom práce, sociálnych vecí a rodiny SR na základe uznesenia vlády SR č. 627/2013

Cieľom a obsahom materiálu je najmä:

Cieľom návrhu nariadenia je zlepšiť fungovanie vnútorného trhu zavedením jasného a harmonizovaného právneho rámca na úrovni EÚ na predchádzanie sexuálnemu zneužívaniu detí online a boj proti nemu, a to najmä objasnením úlohy, povinností a zodpovednosti poskytovateľov príslušných služieb informačnej spoločnosti (ďalej len „poskytovatelia služieb online“).

Špecifickými cieľmi sú: 1. zabezpečenie účinného zisťovania, odstraňovania a oznamovania sexuálneho zneužívania detí online (pre účely tohto nariadenia sa pod pojmom myslí známy alebo nový materiál obsahujúci sexuálne zneužívanie detí alebo na kontaktovanie detí – tzv. „grooming“) v prípadoch, keď požiadavky na tieto činnosti v súčasnosti neexistujú; 2. zlepšenie právnej istoty, transparentnosti a zodpovednosti a zabezpečenie ochrany základných práv a 3. obmedzenie šírenia a vplyvov sexuálneho zneužívania detí prostredníctvom harmonizácie pravidiel a intenzívnejšieho úsilia v oblasti koordinácie.

Postoj RÚZ k materiálu

Cieľom návrhu nariadenia je zlepšiť fungovanie vnútorného trhu zavedením jasného a harmonizovaného právneho rámca na úrovni EÚ na predchádzanie sexuálnemu zneužívaniu detí online a boj proti nemu. **RÚZ k návrhu predkladá nižšie uvedené zásadné pripomienky, ktorých cieľom je zohľadniť odlišností jednotlivých poskytovateľov služieb a ich reálnych technických a právnych možností kontrolovať obsah alebo prenášanú komunikáciu a zamedziť jej šíreniu**

Pripomienky RÚZ k predkladanému materiálu

1. Zásadná pripomienka k článku 1 a 2:

Nastavenie osobnej pôsobnosti nariadenia považujeme za široké a je nutné zohľadniť odlišností jednotlivých poskytovateľov služieb a ich reálnych technických a právnych možností kontrolovať obsah alebo prenášanú komunikáciu a zamedziť ich šíreniu.

V samotnom návrhu nariadenia DSA sa vychádza zo základného princípu, aby plnenie opatrení na zabránenie šíreniu nezákonného obsahu bolo namierené len na tých poskytovateľov, od ktorých možno dôvodne očakávať, že budú mať prevádzkovú a technickú schopnosť samostatne konať. Nariadenie by malo efektívne plniť svoj účel a pritom neporušovať základné právo na súkromie .

Zaťaženie všetkých poskytovateľov IPKS a hostingových služieb, vrátane podnikov poskytujúcich verejné elektronické komunikačné služby (ďalej ako podniky) pokiaľ ide o identifikáciu rizík a prijímanie opatrení na ich zmierňovanie sa javí ako neprimerané aj s ohľadom na reálne možnosti aké majú pri identifikovaní a posudzovaní rizík, prijímaní zmierňujúcich opatrení, kontrole a moderovaní prenášaného alebo ukladaného obsahu či overovaní opodstatnenosti oznámení na nelegálny obsah a berúc do úvahy aj skutočnosť, že šírenie detskej pornografie sa primárne spája využívaním online internetových chatovacích služieb a platforiem na zdieľanie videí a fotiek (napr. článok 2, článok 10) . Mnohé z ukladaných povinností nie sú prakticky vykonateľné poskytovateľmi štandardných verejných interpersonálnych komunikačných služieb, aj pokiaľ ide o poskytovateľov hostingových služieb ako napr. poskytovatelia cloudovej infraštruktúry a preto by regulácii nemali podliehať.

2. Zásadná pripomienka k článku 3 a 4 – posudzovanie rizika:

Poskytovatelia IPKS: Schopnosť podnikov poskytujúcich štandardné verejné interpersonálne komunikačné služby (ako sú volania či prenosy správ) vykonať analýzu pre jednotlivé služby resp. tomu zodpovedajúcim spôsobom nastaviť zmierňovacie opatrenia, je značne limitovaná a kompromitovaná požiadavkami v oblasti ochrany súkromia v elektronických komunikáciách (na základe smernice 2002/58/ES a zákona č. 452/2021), nakoľko obsah prenášanej komunikácie sa neuchováva a ani nemôže byť monitorovaný a vykonávanie moderácie obsahu či aplikovanie mechanizmov na overovanie podnetov na nelegálny obsah (ako sa predpokladá v rámci zmierňovacích opatrení, či článkov 12 a 13) je reálne nemožné.

Aj pokiaľ ide o vykonanie analýzy rizík z hľadiska veku užívateľov alebo kontaktovania detí (články 3(2) a 4(3)), v prevažnej väčšine sú v zmluvnom vzťahu s podnikom dospelí účastníci, ktorí za služby platia a podnik nemá ako reálne zistiť a overiť, kto je koncovým užívateľom. Navyše, zmluvné vzťahy poskytovateľov IPKS sú aj voči právnickým osobám, kde ide o obchodnú či úradnú komunikáciu.

Parametre, ktoré sa majú zohľadniť pri vykonaní analýzy sú popísané len veľmi všeobecne bez toho aby bol poskytnutý jasnejší návod pre poskytovateľov ako takú analýzu vykonať a čo presne a nevyhnutne a akým spôsobom v rámci analýzy vyhodnocovať aj v závislosti a podľa určenia o aký typ služby sa jedná. V právnom štáte by mali byť ukladané len také povinnosti, ktoré sú dostatočne určité, zrozumiteľné a jasné z hľadiska ich plnenia.

3. Zásadná pripomienka k článku 7 a nasl. - vydávanie príkazov na zistenie

V prípade vydania príkazu na zisťovanie sa síce zavádza výnimka z ochrany súkromia v zmysle č. 1 ods. 4 návrhu nariadenia, súčasne ale nie je jasné, akým spôsobom by mala byť naplnená požiadavka, aby poskytovateľ služby aplikoval technológiu na zisťovanie iba v nevyhnutnom rozsahu, prípadne len vo vzťahu k časti služby alebo rizikovým skupinám, akým spôsobom sa tieto rizikové skupiny alebo nevyhnutný rozsah bude dať vyfiltrovať a môže to viesť k plošnému monitorovaniu komunikácie v rozpore s princípmi ePrivacy. Nie je jasné, akým spôsobom sa má zabezpečiť požiadavka na ochranu súkromia a aplikovanie zákazu všeobecnej monitorovacej povinnosti.

Navrhovaná legislatíva by neumožňovala poskytovateľom IPKS dodržiavať existujúcu reguláciu v oblasti dôvernosti komunikácie (ePrivacy, Kódex) a porušovala by tak dlhodobé regulačné princípy.

Z uvedených dôvodov, aby sa predišlo nekompatibilitě právnych predpisov, by mali byť z pôsobnosti nariadenia podniky poskytujúce interpersonálne komunikačné služby vyňaté.

Nie je jasné ani akým spôsobom by mali poskytovatelia plniť povinnosti tam, kde bude komunikácia alebo ukladané údaje zo strany ich užívateľov šifrované.

Nedoriešená je otázka právnej zodpovednosti za prípadne škody vzniknuté porušením ochrany údajov.

V článku 7 sa má poskytovateľ IPKS konať na základe zistenia 'significant risk'. Pokiaľ by mali poskytovatelia komunikačných služieb posudzovať significant risk, tento prístup odmietame. Každý prípad by mal byť posudzovaný individuálne, a to kompetentnými orgánmi.

Viac na:

https://www.etno.eu/downloads/positionpapers/etno%20position%20paper%20on%20csam%20proposal_october%202022.pdf

Akékoľvek nástroje, ktorými sa zasahuje do súkromia v elektronických komunikáciách v tak závažnej miere akou je monitorovanie alebo blokovanie obsahu by mali mať výlučne právny základ v súdnom príkaze (predpokladá sa aj iný nezávislý správny orgán, resp. nejasné aj v kontexte niektorých právomocí koordinačného orgánu).

Z časového hľadiska sa javí obdobie platnosti príkazov (v prípade príkazu na zisťovanie na dobu 12 mesiacov, resp. v prípade príkazu na blokovanie na dobu až 5 rokov) ako neprimerane dlhé.

4. Zásadná pripomienka k článku 1, 3, 4, 7, 14, 16 Poskytovatelia hostingových služieb:

Nariadeniu by nemali podliehať tí poskytovatelia hostingových služieb, ktorí nemajú prístup k ukladaným údajom, najmä nie poskytovatelia cloudovej infraštruktúry, ktorí poskytujú len počítačové prostriedky a tzv. virtuálne servery a nemajú prístup k ukladaným údajom zákazníkov.

Chýba detailnejšia analýza jednotlivých typov hostingových služieb z hľadiska nedostatku reálnych technických možností na strane poskytovateľov naplniť jednotlivé povinnosti, ktoré by im z nariadenia vznikli (Recitály 26 a 40 DSA).

Pokiaľ ide o poskytovateľov cloudovej infraštruktúry, títo nemajú prístup k údajom zákazníkov a nad údajmi nemajú žiadnu kontrolu. Technicky nemajú možnosť identifikovať, či overiť prítomnosť nelegálneho obsahu na poskytovaných výpočtových prostriedkoch, ktorý si nezávisle od poskytovateľa ukladajú sami zákazníci a technicky nevedia odstrániť len problémový obsah. Z technického hľadiska by muselo dôjsť k vypnutiu celého virtuálneho servera, čím by však došlo v rozpore s podmienkami služieb a účelu nariadenia k obmedzeniu mnohých ďalších zákazníkov v prístupe k ich legálnym údajom.

Z uvedeného dôvodu by poskytovatelia cloudovej infraštruktúry nevedeli plniť povinnosti predpokladané nariadením a mali by byť preto z pôsobnosti nariadenia vylúčení.

5. Zásadná pripomienka k článku 16 – príkazy na zablokovanie

Príkaz na blokovanie podľa čl. 16 ods. 2 písmeno b) je mimoriadne problematický. Dotknuté subjekty nevedia poskytnúť pred vydaním príkazu štatistiky ohľadne prístupu používateľov alebo ich pokusu o prístup k materiálu obsahujúcemu sexuálne zneužívanie detí, ktorý označili jednotné vyhľadávače zdrojov, ak sa majú spájať s obdobím pred vydaním príkazu na blokovanie. Technicky je prakticky nevykonateľné tieto pokusy monitorovať. Navyše EDPB a EDPS vyjadrili pochybnosti o napĺňaní tohto ustanovenia.

K článku 16(6) sa lehota 5 rokov javí ako neodôvodnená. Odporúčame lehotu skrátiť na 6 – 12 mesiacov. Zároveň sme presvedčení, že len národné súdne orgány by mali byť oprávnené vydať príkaz na blokovanie a nie koordinácia autorita (článok 17(1)).

6. Zásadná pripomienka k článku 89

Lehota na začatie uplatňovania nariadenia (navrhuje sa v trvaní 6 mesiacov) by sa mala primerane predĺžiť vzhľadom na značný rozsah systémových povinností na strane poskytovateľov, ktorý sa zavádza.

<https://www.slov-lex.sk/legislativne-procesy/SK/LPEU/2022/259>