

V Bruseli 28. 9. 2017
COM(2017) 555 final

**OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU
HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV**

Boj proti nezákonnému obsahu na internete

Zvyšovanie zodpovednosti online platforiem

1. Úvod

Online platformy výrazne poháňajú inovácie a rast v digitálnom hospodárstve. Umožňujú nevýdaný prístup k informáciám a ich výmene, ako aj nové trhové príležitosti, a to najmä pre malé a stredné podniky (MSP). Online platformy dnes navyše pre väčšinu ľudí predstavujú hlavný prístupový bod k informáciám a obsahu na internete, či už prostredníctvom vyhľadávačov, sociálnych sietí, stránok s mikrobloggermi alebo platforiem na zdieľanie videí. Aj obchodné modely platforiem sa v poslednom čase vyvíjajú smerom k užšiemu prepojeniu medzi používateľmi a obsahom – najmä na poli cielennej reklamy. Tieto platformy miliardám používateľov sprístupňujú obrovské množstvo obsahu a informácií¹ a poskytujú inovatívne služby občanom i podnikom.

Rozsiahle rozšírenie nezákonného obsahu, ktorý možno nahrávať na internet a ktorý je takto prístupný online, však vyvoláva vážne obavy a na tie treba rozhodne a účinne reagovať. **To, čo je nezákonné offline, je nezákonné aj online.** Nabádanie na terorizmus, xenofóbie a rasovo motivované prejavy, ktoré verejne podnecujú k nenávisti a násiliu, ako aj detská pornografia sú v EÚ nezákonné. Čoraz väčšia dostupnosť teroristického materiálu online a šírenie takéhoto obsahu predstavuje vážnu hrozbu pre bezpečnosť a ochranu i pre dôstojnosť obetí. Európska únia reagovala na tieto obavy viacerými opatreniami². Odhaľovanie a odstraňovanie nezákonného obsahu na internete však pre digitálnu spoločnosť stále predstavuje otázku, ktorú treba naliehavo riešiť.

Európska rada, znepokojená sériou teroristických útokov v EÚ a šírením teroristickej propagandy na internete, na zasadnutí 22. a 23. júna 2017 vyhlásila, že „od tohto odvetvia očakáva, že (...) vyvinie nové technológie a nástroje, ktoré zlepšia automatické odhaľovanie **obsahu, ktorý podnecuje na páchanie teroristických činov, a jeho odstraňovanie.** Dopĺňať by to v prípade potreby mali príslušné legislatívne opatrenia na úrovni EÚ.“ Tieto výzvy zopakovali aj lídri G7 a G20 na nedávnych samitoch³. Podobne aj Európsky parlament vo svojom uznesení o online platformách v júni 2017 vyzval tieto platformy, „aby posilnili opatrenia na boj proti nezákonnému a škodlivému obsahu“, a zároveň požiadal Komisiu, aby predložila návrhy na riešenie týchto otázok⁴.

Tie online platformy, ktoré sprostredkujú prístup k obsahu väčšine používateľov internetu, nesú významnú spoločenskú zodpovednosť za ochranu používateľov a spoločnosti ako celku a zabráňovanie zločinom a iným osobám zapojeným do protiprávných činností online vo využívaní ich služieb. Otvorené digitálne priestory, ktoré poskytujú, sa nesmú stať semeniskom terorizmu, nezákonných nenávistných prejavov, zneužívania detí alebo obchodovania s ľuďmi či priestormi mimo dosahu právnych predpisov. Šírenie nezákonného obsahu online pochopiteľne môže jednak narušiť dôveru občanov v digitálne prostredie, jednak ohroziť ďalší hospodársky rozvoj ekosystémov platforiem a digitálny jednotný trh. Online platformy by mali výrazne zintenzívniť opatrenia na riešenie tohto problému ako súčasť zodpovednosti, ktorá vyplýva z ich ústrednej úlohy v spoločnosti.

¹ V súčasnosti sa každú sekundu na Twitteri objaví 8 000 tweetov, na Instagrame 1 000 fotografií, v Google sa vyhľadá 60 000 reťazcov a na YouTube sa pustí 70 000 videí. Pozri <http://www.internetlivestats.com/>.

² Pozri oddiel 2.

³ Závery Európskej rady, ST 8 2017 INIT, z 22. a 23. júna 2017, vyhlásenie G7 z 26. mája 2017 v Taormine a vyhlásenie lídrov G20 z 8. júla 2017.

⁴ Uznesenie Európskeho parlamentu z 15. júna 2017 o online platformách [2016/2274(INI)].

Boj proti nezákonnému obsahu na internete sa musí opierať o vhodné a spoľahlivé záruky na zabezpečenie ochrany rôznych dotknutých základných práv. Keďže online platformy majú čoraz dôležitejšiu úlohu pri poskytovaní prístupu k informáciám, zohrávajú kľúčovú úlohu aj pri úsilí o dosiahnutie takejto rovnováhy. Boj proti nezákonnému obsahu online v EÚ by mal vychádzať z činnosti EÚ na globálnej úrovni a zohľadňovať ju.

Toto oznámenie obsahuje súbor usmernení a zásad, na základe ktorých online platformy budú môcť zintenzívniť boj proti nezákonnému obsahu na internete⁵ v spolupráci s vnútroštátnymi orgánmi, členskými štátmi a inými príslušnými zainteresovanými stranami. Jeho cieľom je uľahčiť a zintenzívniť vykonávanie osvedčených postupov na predchádzanie uverejňovaniu nezákonného obsahu, jeho odhaľovanie a odstraňovanie či znemožňovanie prístupu k nemu, aby sa zaistila jeho účinná eliminácia, zvýšená transparentnosť a ochrana základných práv online. Ďalším zámerom oznámenia je objasniť platformám, akú nesú zodpovednosť, keď z vlastnej iniciatívy prijímajú kroky zamerané na odhaľovanie a odstraňovanie nezákonného obsahu alebo znemožňovanie prístupu k nemu (tzv. samaritánstvo)

2. KONTEXT

Európska únia už dávnejšie reagovala na výzvu, ktorú predstavuje nezákonný obsah na internete, a to záväznými aj nezáväznými opatreniami. Medzi politické reakcie patrí **smernica o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii**⁶, smernica o **terorizme**⁷, navrhované opatrenia v kontexte reforiem **autorského práva**⁸ či smernica o **audiovizuálnych mediálnych službách**⁹.

Tieto legislatívne opatrenia boli doplnené o sériu nelegislatívnych nástrojov, ako je kódex správania pre boj proti **nezákonným nenávisťným prejavom online**¹⁰, činnosť **internetového fóra EÚ**¹¹ v boji proti **teroristickej propagande**, memorandum o porozumení týkajúce sa predaja **falšovaného tovaru**¹², oznámenie Komisie o **dohľade nad trhom s výrobkami predávanými online**¹³, predaj **produktov potravinového reťazca online**, akčný plán EÚ proti **nezákonnému obchodovaniu s voľne žijúcimi druhmi**¹⁴, usmernenia k smernici o **nekalých obchodných praktikách**¹⁵ či jednotné akcie

⁵ Postrehy uvedené na nasledujúcich stranách vychádzajú z rozsiahleho množstva verejných, ako aj cielených konzultácií a pracovných stretnutí so zainteresovanými stranami.

⁶ Pozri nedávnu správu Komisie Európskemu parlamentu a Rade hodnotiacu vykonávanie opatrení uvedených v článku 25 smernice 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii.

⁷ V smernici o terorizme (EÚ) 2017/541 sa členským štátom ukladá povinnosť prijať opatrenia potrebné na zabezpečenie okamžitého odstránenia online obsahu podnecujúceho na páchanie teroristických činov (článok 21). V tejto oblasti a v rámci internetového fóra EÚ platformy dobrovoľne odstraňujú teroristický obsah na základe žiadostí, ktoré im zasiela útvar Europolu pre nahlasovanie internetového obsahu (Internet Referral Unit – IRU).

⁸ COM(2016) 593.

⁹ COM(2016) 287.

¹⁰ http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

¹¹ http://europa.eu/rapid/press-release_IP-15-6243_en.htm.

¹² <http://ec.europa.eu/transparency/regdoc/rep/3/2016/EN/3-2016-3724-EN-F1-1.PDF>.

¹³ Ú. v. EÚ C 250 z 1. 8. 2017.

¹⁴ http://ec.europa.eu/environment/cites/pdf/WAP_EN_WEB.pdf.

vnútroštátnych orgánov v rámci siete spolupráce v oblasti ochrany spotrebiteľa¹⁶. Európska stratégia vytvárania **lepšieho internetu pre deti**¹⁷ je samoregulačnou iniciatívou zameranou na zlepšenie online prostredia pre deti a mladých ľudí, ktorá reaguje na riziko vystavenia takým materiálom, ako je obsah s prvkami násilia či sexuálneho vykorisťovania, alebo na riziko kyberšikanovania.

Komisia vo svojich oznámeniach z rokov 2016 a 2017¹⁸ zdôraznila, že online platformy musia konať zodpovednejšie a posilniť samoregulačné úsilie o odstraňovanie nezákonného obsahu v celej EÚ. Okrem toho sa Komisia zaviazala zlepšiť koordináciu rôznych odvetvových dialógov s platformami a preskúmať potrebu usmernení o formálnych postupoch oznamovania a prijímania opatrení. To by sa malo diať v synergii s už prebiehajúcimi dialógmi a prácou začatou v iných oblastiach a bez toho, aby boli narušené. Príkladom je Európsky program v oblasti bezpečnosti alebo doména nezákonných nenávisťných prejavov.

Podľa nedávnych správ o niektorých z týchto odvetvových iniciatív došlo k istému pokroku. V prípade nezákonných nenávisťných prejavov správy z júna 2017 naznačujú, že v niektorých krajinách EÚ sa počas obdobia šiestich mesiacov objem odstránených materiálov z vybranej vzorky nahláseného obsahu zvýšil z 28 percent na 59 percent, ale zároveň upozorňujú na značné rozdiely medzi platformami¹⁹. V rovnakom období boli zaznamenané aj určité zlepšenia v rýchlosti odstraňovania, ale až 28 percent obsahu bolo odstráneného až po týždni²⁰. Z toho vyplýva, že neregulačný prístup môže priniesť výsledky, najmä keď ho doplnia opatrenia na uľahčenie spolupráce medzi všetkými dotknutými subjektmi. V rámci úsilia internetového fóra EÚ o boj proti teroristickému obsahu bolo od jeho vzniku odstráneného 80 až 90 percent obsahu označeného Europolom²¹. Pokiaľ ide o detskú pornografiu, zo systému telefónnych horúcich liniek INHOPE bola už v roku 2015 nahlásená účinnosť odstraňovania vo výške 91 % do 72 hodín, pričom každá tretia položka bola odstránená do 24 hodín²².

Rôzne prebiehajúce sektorové dialógy tiež odhalili mnoho podobných trendov pri postupoch, ktorými sa riadi odhaľovanie, identifikácia a odstraňovanie obsahu, či prevencia jeho opätovného nahrávania vo všetkých odvetviach. Uvedené zistenia sa zohľadnili aj v tomto oznámení.

Na úrovni EÚ všeobecný právny rámec na odstraňovanie nezákonného obsahu predstavuje smernica o elektronickom obchode²³, ktorá okrem iného harmonizuje podmienky, za ktorých niektoré online platformy môžu využívať výnimku zo zodpovednosti za nezákonný obsah, ktorému poskytujú priestor, na celom digitálnom jednotnom trhu.

¹⁵ SWD(2016) 163 z 25. 5. 2016.

¹⁶ http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm.

¹⁷ Oznámenie COM(2012) 196 final (Lepší internet pre deti): <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online>.

¹⁸ COM(2016) 288 a COM(2017) 228.

¹⁹ http://europa.eu/rapid/press-release_IP-17-1471_sk.htm.

²⁰ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=71674.

²¹ http://europa.eu/rapid/press-release_IP-17-544_en.htm.

²² http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2015.sflb.ashx?download=true.

²³ Smernica 2000/31/ES z 8. júna 2000 o elektronickom obchode.

Nezákonný obsah na online platformách sa môže šíriť najmä online službami, ktoré umožňujú nahrávanie obsahu tretích strán. Na takéto hostingové služby sa za určitých podmienok vzťahuje článok 14 smernice o elektronickom obchode²⁴. V uvedenom článku sa stanovuje, že poskytovatelia hostingových služieb²⁵ nemožno brať na zodpovednosť za informácie uchovávané na žiadosť tretích strán, a to pod podmienkou, že a) nič nevedia o nezákonnej činnosti alebo informáciách, a čo sa týka nárokov na náhradu škody, nie sú si vedomí skutočností alebo okolností, z ktorých by bolo zrejmé, že ide o nezákonnú činnosť alebo informácie, alebo b) po zistení alebo uvedení si týchto skutočností konajú promptne, aby odstránili alebo znemožnili prístup k informáciám. Uvedenou smernicou by sa zároveň mal „vytvoriť vhodný základ pre **rozvoj rýchleho a spoľahlivého postupu pre odstránenie a znemožnenie prístupu k nezákonným informáciám**“²⁶.

V článku 15 sa navyše členským štátom zakazuje „uložiť poskytovateľom všeobecnú povinnosť **pri poskytovaní služieb, na ktoré sa [vzťahuje článok 14], aby monitorovali informácie, ktoré prenášajú alebo ktoré uložili, [alebo] všeobecnú povinnosť aktívne zisťovať skutočnosti alebo okolnosti, ktoré by naznačovali, že ide o nezákonnú činnosť**“. Okrem toho sa v odôvodnení 47 smernice pripomína, že to sa týka len povinnosti monitorovať všeobecnej povahy, a nie „povinností monitorovať v špecifickom prípade, a najmä to nemá vplyv na nariadenia vnútroštátnych orgánov v súlade s vnútroštátnymi právnymi predpismi“.

V tejto súvislosti sa Komisia vo svojom oznámení z roku 2016 o online platformách zaviazala udržať vyvážený a predvídateľný režim zodpovednosti pre online platformy v podobe kľúčového regulačného rámca na podporu digitálnych inovácií na celom digitálnom jednotnom trhu.

Usmerneniami v tomto oznámení nie je dotknuté *acquis* Únie. Týkajú sa činnosti online platforiem, a najmä hostingových služieb, ktoré poskytujú²⁷ v zmysle článku 14 smernice o elektronickom obchode, a vzťahujú sa na všetky kategórie nezákonného obsahu, pričom sa náležite zohľadňuje to, že rôzne druhy obsahu si môžu vyžadovať odlišný prístup.

V súčasnosti EÚ nemá harmonizovaný a súdržný prístup k odstraňovaniu nezákonného obsahu. Existujú v nej rôzne metodiky v závislosti od členského štátu, kategórie obsahu či druhu online platformy. **Ak sa má zefektívniť boj proti nezákonnému obsahu, potrebovali by sme jednotnejší**

²⁴ Treba poznamenať, že podľa smernice o elektronickom obchode sa výnimka zo zodpovednosti podľa článkov 12 až 14 vzťahuje len na tých poskytovateľov služieb informačnej spoločnosti, ktorí sa považujú za sprostredkovateľov – poskytovateľov služieb [t. j. poskytovanie služieb púheho kanála („mere conduit“), zaznamenávanie informácií v pamäti („caching“), resp. hostiteľských služieb („hosting“)]. V odôvodnení 42 sa objasňuje, že ak sa na činnosť má uplatňovať výnimka zo zodpovednosti, musí mať „výlučne technickú, automatickú a pasívnu povahu, ktorá znamená, že poskytovateľ služieb informačnej spoločnosti nemá ani nepozná, ani nemá kontrolu nad informáciami, ktoré sú prenášané alebo uchovávané“.

²⁵ Väčšina online platforiem ponúka hostiteľské služby obsahu nahratého ich používateľmi.

²⁶ Odôvodnenie 40 smernice o elektronickom obchode. Upozorňujeme, že toto oznámenie sa zameriava na poskytovateľov hostingových služieb, a nie na poskytovateľov púchych kanálov (článok 12) či služieb zaznamenávania informácií v pamäti (článok 13).

²⁷ Hostingová služba je služba informačnej spoločnosti, ktorá pozostáva z uchovávanie informácií poskytovaných príjemcami tejto služby. Táto kategória môže zahŕňať širokú škálu aktérov od online trhov, cez internetové platformy na zdieľanie videí, sociálne siete, webové sídla poskytujúce priestor na blogy alebo recenzie až po sekcie s komentármi používateľov na spravodajských stránkach.

prístup. Ten by bol prospešný aj pre budovanie digitálneho jednotného trhu a online platformám vrátane nových účastníkov by znížil náklady na dosahovanie súladu s množstvom pravidiel.

Treba zdôrazniť, že týmto právnym rámcom sa nevymedzuje, tobôž neharmonizuje, definícia „nezákonného“ obsahu. **To, čo je nezákonné, určujú osobitné právne predpisy na úrovni EÚ, ako aj vnútroštátne právne predpisy.**²⁸ Zatiaľ čo napríklad povaha a špecifiká materiálov spojených s terorizmom, nezákonných nenávistných prejavov, detskej pornografie či obchodovania s ľuďmi, ako aj škody, ktoré tento obsah spôsobuje, sú veľmi odlišné od porušovania práv duševného vlastníctva, pravidiel bezpečnosti výrobkov, nezákonných obchodných praktík online alebo online činností hanlivého charakteru, všetky tieto rôzne druhy nezákonného obsahu patria pod rovnaký všeobecný právny rámec, ktorý predstavuje smernica o elektronickom obchode. Vzhľadom na značné podobnosti pri *postupoch odstraňovania* spomínaných rôznych druhov obsahu sa toto oznámenie vzťahuje na celé spektrum nezákonného obsahu na internete, **pričom tam, kde je to vhodné a opodstatnené, dbá na odvetvové rozdiely.**

V EÚ súdy a vnútroštátne príslušné orgány vrátane orgánov presadzovania práva majú právomoc stíhať trestné činy a ukladať trestné sankcie podľa riadneho postupu v súvislosti s nezákonnosťou danej činnosti alebo informácií na internete. Online platformy majú zároveň právo brániť tomu, aby sa ich infraštruktúra a podnikateľská činnosť používali na páchanie trestných činov, nesú zodpovednosť za ochranu svojich používateľov a predchádzanie nezákonnému obsahu na svojej platforme a zvyčajne majú k dispozícii technické prostriedky na identifikáciu a odstraňovanie takéhoto obsahu. Je to o to dôležitejšie, že online platformy investujú nemalé prostriedky do vývoja pokročilých technológií na proaktívne zhromažďovanie informácií o obsahu, ktorý sa šíri v ich prostredí, a o správaní spotrebiteľov. Hoci promptné rozhodnutia o odstraňovaní nezákonného obsahu sú dôležité, treba uplatňovať aj primerané záruky. To si vyžaduje aj rovnováhu úloh medzi verejnými a súkromnými subjektmi.

Usmernenia a zásady uvedené v tomto oznámení sa teda nezameriavajú len na odhaľovanie a odstraňovanie nezákonného obsahu; ich cieľom je tiež riešenie obáv z toho, že sa bude odstraňovať aj *legálny* obsah (tzv. nadmerné odstraňovanie), čo má zase vplyv na slobodu prejavu a pluralitu médií. Preto by sa mali zabezpečiť primerané záruky, ktoré by sa mali prispôbiť konkrétnemu druhu daného nezákonného obsahu.

Pre verejný záujem je nepochybne znepokojujúci aj obsah, ktorý nie je nutne nezákonný, ale je potenciálne škodlivý, ako napríklad falošné správy či obsah škodlivý pre maloletých²⁹. Toto oznámenie sa však zameriava na odhaľovanie a odstraňovanie **nezákonného obsahu**.

²⁸ Medzi oblasti, ktoré sú pokryté (alebo ktorých pokrytie sa navrhuje) v právnych predpisoch EÚ, patrí podnecovanie k terorizmu, nezákonné nenávistné prejavy, sexuálne zneužívanie detí, práva duševného vlastníctva, bezpečnosť výrobkov, ponuka a predaj potravín alebo tabakových výrobkov a falšovaných liekov, pravidiel ochrany spotrebiteľov alebo opatrenia pre bezpečnosť výrobkov atď. V roku 2016 Komisia takisto objasnila povinnosti online platforiem na poli transparentnosti a odbornej starostlivosti podľa smernice 2005/29/ES o nekalých obchodných praktikách v tých prípadoch, kde platformy voči spotrebiteľom vystupujú ako obchodníci.

²⁹ V súvislosti s audiovizuálnym obsahom sa touto otázkou zaoberá návrh na revíziu smernice o audiovizuálnych mediálnych službách.

3. ODHAĽOVANIE A OZNAMOVANIE NEZÁKONNÉHO OBSAHU

Cieľom tohto oddielu je **načrtnúť, čo by online platformy, príslušné orgány a používatelia mali robiť v záujme rýchleho a účinného odhaľovania nezákonného obsahu.**

Online platformy sa o existencii nezákonného obsahu môžu dozvedieť rôznymi spôsobmi a kanálmi. Tieto oznamovacie kanály zahŕňajú i) súdne príkazy alebo administratívne rozhodnutia; ii) oznámenia od príslušných orgánov (napríklad orgánov presadzovania práva), špecializovaných „dôveryhodných oznamovateľov“ (tzv. trusted flaggers), držiteľov práv duševného vlastníctva či bežných používateľov alebo iii) vlastné vyšetrovanie alebo vedomosti platformy.

Okrem právnych povinností vyplývajúcich z únijných a vnútroštátnych právnych predpisov a „povinnosti starostlivosti“, ktorá je súčasťou ich zodpovedností, by online platformy mali používateľom zaistiť bezpečné online prostredie, ktoré odrádza od trestného a iného nezákonného zneužívania, ako aj od trestných a iných protiprávných aktivít na internete, a ktoré im zabraňuje.

3.1. Súdny a príslušné orgány

V súlade s únijnými a/alebo vnútroštátnymi právnymi predpismi môžu vnútroštátne súdy a v určitých prípadoch príslušné orgány vydávať záväzné príkazy alebo administratívne rozhodnutia určené online platformám so žiadosťou odstrániť nezákonný obsah alebo zablockovať prístup k nemu.³⁰

Keďže rýchle odstránenie nezákonných materiálov má často zásadný význam pre obmedzenie rozsiahlejšieho šírenia a ujmy, online platformy by mali tiež môcť prijímať rýchle rozhodnutia o možných opatreniach v súvislosti s nezákonným obsahom na internete bez toho, aby potrebovali súdny príkaz alebo administratívne rozhodnutie, a to najmä vtedy, ak údajný nezákonný obsah odhalí orgán presadzovania práva a informuje ich o ňom. Zároveň by pri plnení svojich úloh v tomto smere mali zaviesť primerané záruky s cieľom zabezpečiť používateľom právo na účinný prostriedok nápravy.

Online platformy by preto mali mať potrebné zdroje na pochopenie právnych rámcov, v ktorých pôsobia. V prípade potreby by tiež mali **úzko spolupracovať s orgánmi presadzovania práva a inými príslušnými orgánmi**, a to najmä tak, že sa budú dať rýchlo a účinne kontaktovať so žiadosťou o urýchlené odstránenie nezákonného obsahu a že prípadne dokážu orgány presadzovania práva upozorniť na známky trestnej činnosti na internete³¹. S cieľom zabrániť duplicite úsilia a oznámení a

³⁰ V článku 14 ods. 3 smernice o elektronickom obchode sa stanovuje, že daný článok „nemá vplyv na možnosť súdu alebo správneho orgánu požiadať poskytovateľa služieb, v súlade s právnymi systémami členských štátov, aby ukončil alebo predchádzal porušovaniu predpisov“. Napríklad v článku 11 smernice 2004/48/ES o vymožiteľnosti práv duševného vlastníctva sa uvádza, že „členské štáty tiež zabezpečia, aby vlastníci práv mali možnosť navrhnúť vydanie súdneho príkazu proti sprostredkovateľom, ktorých služby využíva tretia strana na porušovanie práva duševného vlastníctva; tým nie je dotknutý článok 8 ods. 3 smernice 2001/29/ES“.

³¹ V článku 15 ods. 2 smernice o elektronickom obchode sa stanovuje, že „členské štáty môžu ustanoviť povinnosť, aby poskytovatelia služieb informačnej spoločnosti informovali príslušné verejné orgány o údajných vykonávaných nezákonných činnostiach alebo o údajných nezákonných poskytovaných informáciách, alebo povinnosť oznamovať príslušným orgánom na ich žiadosť informácie, ktoré by im umožnili identifikáciu príjemcov ich služieb, s ktorými uzatvorili dohody o uložení informácií“.

zníženiu efektívnosti a účinnosti procesu odstraňovania by orgány presadzovania práva a iné príslušné orgány mali takisto vynaložiť maximálne úsilie, aby vzájomne spolupracovali pri definovaní účinných digitálnych rozhraní, ktoré uľahčujú rýchle a spoľahlivé podávanie oznámení, a aby zabezpečili efektívne odhaľovanie a oznamovanie nezákonného obsahu. Dôležitým predpokladom pre fungovanie tejto spolupráce je to, aby si platformy a orgány vytvorili kontaktné miesta.

V prípade teroristického obsahu³² Europol vytvoril jednotku EÚ pre nahlasovanie internetového obsahu, v rámci ktorej odborníci na bezpečnosť posudzujú teroristický obsah a upozorňujú naň online platformy (hoci niektoré členské štáty majú aj vlastné vnútroštátne jednotky).

Online platformy by mali **systematicky posilňovať spoluprácu s príslušnými orgánmi v členských štátoch, zatiaľ čo členské štáty by mali zabezpečiť, aby súdy mohli účinne konať proti nezákonnému obsahu online**, a mali by **dálej rozvíjať cezhraničnú spoluprácu medzi orgánmi**.

Online platformy a orgány presadzovania práva alebo iné príslušné orgány by si mali určiť efektívne kontaktné body v EÚ a v prípade potreby vymedziť účinné digitálne rozhrania v záujme ľahšej interakcie.

Platformy a orgány presadzovania práva sa tiež vyzývajú, aby vyvinuli **technické rozhrania na efektívnejšiu spoluprácu počas celého cyklu riadenia obsahu**. Na ceste smerom k účinným a technicky vhodným riešeniam tejto výzvy môže byť prospešná aj spolupráca aj s technickou obcou.

3.2. Oznámenia

3.2.1. Dôveryhodní oznamovatelia

Nezákonný obsah z internetu sa dá odstraňovať rýchlejšie a spoľahlivejšie, ak online platformy disponujú mechanizmami na udržiavanie vyhradeného kanála pre tých oznamovateľov, ktorí majú výnimočné odborné skúsenosti s oznamovaním potenciálne nezákonného obsahu na ich webových stránkach. Ide o tzv. dôveryhodných oznamovateľov, teda špecializované subjekty s osobitnou odbornosťou v oblasti identifikácie nezákonného obsahu a so špecializovanými štruktúrami na odhaľovanie a identifikáciu takéhoto obsahu na internete.

V porovnaní s bežnými používateľmi **od dôveryhodných oznamovateľov možno očakávať odbornosť a prácu na vysokej úrovni**, čo by malo viesť ku kvalitnejším oznámeniam a rýchlejšiemu odstraňovaniu. Online platformy sa vyzývajú na využívanie existujúcich sietí dôveryhodných oznamovateľov. Napríklad pokiaľ ide o teroristický obsah, jednotka Europolu pre nahlasovanie internetového obsahu má potrebné odborné znalosti na posúdenie, či daný online obsah má teroristický a násilný charakter, a popri svojej úlohe v oblasti presadzovania práva využíva túto odbornosť na pôsobenie v úlohe dôveryhodného oznamovateľa. Ďalším príkladom dôveryhodného oznamovateľa je európska sieť horúcich liniek na nahlasovanie detskej pornografie INHOPE. V prípade nezákonných nenávistných prejavov sa na identifikáciu a nahlasovanie nezákonného

³² V zmysle článku 5 smernice (EÚ) 2017/541 o boji proti terorizmu.

rasistického a xenofóbneho obsahu na internete špecializujú organizácie občianskej spoločnosti či poloverejné orgány.

S cieľom zabezpečiť vysokú kvalitu oznámení a rýchlejšie odstraňovanie nezákonného obsahu **by sa odvetvie mohlo dohodnúť na celouijných kritériách založených najmä na dodržiavaní základných práv a demokratických hodnôt**. To možno dosiahnuť samoregulačnými mechanizmami alebo v normalizačnom rámci EÚ, **na základe ktorého určitý subjekt možno považovať za dôveryhodného oznamovateľa**, čo umožní dostatočnú flexibilitu na to, aby sa zohľadnili obsahové špecifiká a úloha dôveryhodného oznamovateľa. Takéto kritériá by mohli okrem iného zahŕňať aj interné normy odbornej prípravy, procesné štandardy a postupy zabezpečovania kvality, ako aj právne záruky, pokiaľ ide o nezávislosť a konflikt záujmov, ochranu súkromia a osobných údajov. Tieto záruky sú obzvlášť dôležité v obmedzenom počte prípadov, v ktorých platformy môžu odstrániť obsah na základe oznámenia od dôveryhodného oznamovateľa bez toho, aby si samy ďalej overovali jeho legálnosť. V týchto obmedzených prípadoch by dôveryhodní oznamovatelia mohli takisto podliehať auditom na základe spomínaných kritérií a ich dôveryhodnosť by sa mohla potvrdzovať certifikáciou. Každopádne by mali byť k dispozícii dostatočné záruky, aby sa zabránilo zneužívaniu systému, ako sa uvádza v oddiele 4.3.

Na mechanizmoch nahlasovania obsahu zo strany dôveryhodných oznamovateľov by sa v prípade potreby mali môcť zúčastňovať aj príslušné orgány.

Musí sa dosiahnuť primeraná rovnováha medzi zabezpečením vysokej kvality oznámení od dôveryhodných oznamovateľov, rozsahom dodatočných opatrení, ktoré by spoločnosti prijali vo vzťahu k dôveryhodným oznamovateľom, a záťažou pri zabezpečovaní týchto štandardov kvality. Ak sa mechanizmy nahlasovania z pozície dôveryhodného oznamovateľa zneužijú a porušia sa stanovené štandardy, status dôveryhodného oznamovateľa by sa mal odňať.

Komisia **podporuje úzku spoluprácu medzi online platformami a dôveryhodnými oznamovateľmi. Platformy by mali oznámenia od dôveryhodných oznamovateľov dokázať rýchlejšie spracovať.** Touto spoluprácou by sa mala zabezpečiť vzájomná výmena informácií, aby sa proces odstraňovania dal priebežne hodnotiť a zlepšovať.

Komisia bude ďalej **skúmať možnosť dohody o celouijných kritériách uplatňujúcich sa na dôveryhodných oznamovateľov**, a to najmä v dialógu s príslušnými zainteresovanými stranami.

3.2.2. Oznámenia od používateľov

V záujme účinného boja proti nezákonnému obsahu na internete by bežní používatelia mali mať možnosť upozorňovať online platformy na nezákonný obsah a môcť sa spoľahnúť na to, že odôvodnené oznámenia sa posúdia a že sa na ne bude rýchlo reagovať.

Online platformy by mali **zriadiť ľahko prístupný a používateľsky ústretový mechanizmus, vďaka ktorému by ich používatelia mohli informovať**, ak určitý obsah, ktorému platformy poskytujú priestor, považujú za nezákonný.

Ak je obsah verejne dostupný, takéto nahlasovacie mechanizmy by mali byť k dispozícii aj širokej verejnosti, a to bez toho, aby používatelia museli byť zaregistrovaní. S cieľom zlepšiť efektívnosť a

správnosť posúdení potenciálne nezákonného obsahu by takýto mechanizmus mal umožniť **jednoduché oznamovanie elektronickými prostriedkami**.

Zámerom návrhu Komisie na revíziu smernice o audiovizuálnych mediálnych službách je uložiť poskytovateľom platforiem na zdieľanie videí povinnosť, aby zriadili a prevádzkovali mechanizmy, vďaka ktorým by používatelia mohli nahlasovať alebo označovať audiovizuálny obsah, ktorý môže narušiť telesný, duševný alebo morálny vývin maloletých, ako aj obsah s prvkami podnecujúcimi k násiliu alebo nenávisti.

3.2.3. Zabezpečenie vysokej kvality oznámení

Online platformy by mali **zaviesť účinné mechanizmy na uľahčenie zasielania oznámení, ktoré sú dostatočne presné a náležite odôvodnené**, aby sa platformám umožnilo prijať rýchle a kvalifikované rozhodnutie o následných opatreniach. Malo by tak byť ľahšie predkladať oznámenia, ktoré by zahŕňali **vysvetlenie dôvodov**, prečo sa oznamovateľ domnieva, že obsah je nezákonný, a jasný údaj o **umiestnení** potenciálne nezákonného obsahu (napr. internetovú adresu).

Takéto nahlasovacie mechanizmy by mali byť viditeľné, ľahko dostupné, **používateľsky ústretové a kontextuálne**. Takisto by mali umožňovať **jednoduché nahlasovanie** rôznych druhov obsahu, napr. výberom zo zoznamu kategórií dôvodov, pre ktoré sa obsah považuje za nezákonný. Ak je to technicky zrealizovateľné, mohli by sa využívať také prvky, ako je napríklad možnosť oznámenia hneď pri prvom kontakte s materiálom alebo ponúkajú rovnakých prihlasovacích údajov.

Takéto dostatočne podložené a podrobné oznámenia platformám umožnia potenciálne nezákonný obsah rýchlo nájsť, fundovane posúdiť jeho nezákonnosť a v prípade potreby rýchlo konať. Presná miera podrobnosti, ktorú platformy potrebujú na urýchlenné prijatie fundovaných rozhodnutí, sa môže značne líšiť v závislosti od druhu obsahu.

Používatelia by pri nahlasovaní obsahu, ktorý považujú za nezákonný, **nemali byť v zásade povinní identifikovať sa**, okrem prípadov, keď sú tieto informácie potrebné na určenie zákonnosti obsahu (napr. uplatnenie práv duševného vlastníctva). To platí najmä v prípade, ak môže byť ohrozená ich bezpečnosť alebo ak by odhalenie ich identity mohlo mať právne dôsledky. Ak si používatelia chcú zachovať anonymitu vo vzťahu k platformám, mali by sa vyzývať k tomu, aby na sprostredkovanie oznámení využili dôveryhodných oznamovateľov.

Predkladatelia oznámení by však spolu s nimi zároveň mali mať možnosť dobrovoľne predložiť svoje kontaktné údaje, aby ich online platformy mohli požiadať o dodatočné informácie alebo informovať o zamýšľaných následných opatreniach. V takom prípade by poskytovateľ oznámenia mal dostať **potvrdenie o prijatí a správu o opatreniach prijatých na základe oznámenia**.

Úlohou potvrdenia o prijatí nie je len zabrániť tomu, aby predkladateľ oznámenia musel sám zisťovať, či sa na jeho žiadosť reagovalo, ale môže slúžiť aj ako dôkaz v súdnych alebo mimosúdnych konaniach v súlade s pravidlami, ktoré sa na ne vzťahujú.

3.3. Proaktívne opatrenia online platforiem

3.3.1. Proaktívne opatrenia a výnimka zo zodpovednosti

Online platformy by vzhľadom na svoju ústrednú úlohu a kapacity, ako aj s nimi spojené povinnosti, nemali len reagovať na prijaté oznámenia, ale mali by zároveň **prijímať účinné proaktívne opatrenia na odhaľovanie a odstraňovanie** nezákonného obsahu na internete. Okrem toho, ak platformy takéto proaktívne opatrenia neprijmú, v prípade určitých kategórií nezákonného obsahu sa nemusia v plnej miere podariť znížiť riziko závažnej škody.

Komisia sa domnieva, že prijatie takýchto dobrovoľných a proaktívnych opatrení **automaticky nevedie k tomu, že online platforma stratí právo na výnimku zo zodpovednosti** stanovenú v článku 14 smernice o elektronickom obchode.

Po prvé, táto výnimka sa vzťahuje len na poskytovateľov hostingových služieb, ktorí spĺňajú podmienky stanovené v článku 14 predmetnej smernice; ide o poskytovateľov služieb, ktorých činnosť pozostáva z uchovávaní informácií na žiadosť tretích strán a ktorí **nezohrávajú aktívnu úlohu** v tom zmysle, že by mali vedomosti o týchto informáciách alebo kontrolu nad nimi.³³

Odôvodnenie 38 návrhu Komisie na smernicu Európskeho parlamentu a Rady o autorskom práve na digitálnom jednotnom trhu zo 14. septembra 2016 v tejto súvislosti uvádza: „*Pokiaľ ide o článok 14 [smernice o elektronickom obchode], je potrebné overiť, či poskytovateľ služieb zohráva aktívnu úlohu, a to aj prostredníctvom optimalizácie prezentácie nahratých diel alebo predmetov ochrany alebo ich propagovania, a to bez ohľadu na povahu prostriedkov použitých na tento účel.*“

Konkrétne v súvislosti s článkom 14 smernice o elektronickom obchode Súdny dvor vo veci L'Oréal/eBay objasnil, že „*samotná skutočnosť, že [online platforma] ukladá na svoj server ponuky na predaj, stanovuje podmienky poskytovania svojej služby, dostáva za túto službu odmenu a svojim zákazníkom poskytuje informácie všeobecnej povahy, nemôže mať za následok, že sa na [ňu] nebudú vzťahovať výnimky v oblasti zodpovednosti stanovené v [článku 14 smernice o elektronickom obchode]*“³⁴. Súdny dvor však rozhodol, že k takémuto účinku dochádza, „*[p]okiaľ naopak [online platforma poskytna] pomoc, ktorá spočívala najmä v optimalizácii prezentácie predmetných ponúk na predaj alebo v podpore týchto ponúk*“³⁵.

Z toho vyplýva, že samotná skutočnosť, že online platforma prijme určité opatrenia týkajúce sa poskytovania jej služieb vo všeobecnosti nevyhnutne neznamená, že by zohrávala aktívnu úlohu, pokiaľ ide o jednotlivé položky obsahu, ktorý uchováva, a že táto online platforma by teda z tohto dôvodu nemohla mať výnimku zo zodpovednosti. Komisia sa domnieva, že takéto opatrenia môžu – a dokonca by mali – zahŕňať aj proaktívne opatrenia na odhaľovanie a odstraňovanie nezákonného obsahu na internete, najmä ak sú súčasťou uplatňovania podmienok poskytovania služieb online platformy. To bude v súlade s rovnováhou medzi rôznymi existujúcimi záujmami, o ktorej dosiahnutie

³³ Odôvodnenie 42 smernice o elektronickom obchode. Pozri rozsudok vo veci Google France, body 114 a 120 a rozsudok z 12. júla 2011 vo veci C-324/09, L'Oréal/eBay, bod 113.

³⁴ Rozsudok vo veci L'Oréal/eBay, bod 115.

³⁵ Rozsudok vo veci L'Oréal/eBay, bod 116.

sa usiluje smernica o elektronickom obchode.³⁶ V smernici sa totiž pripomína, že je v záujme všetkých zúčastnených strán, aby prijali a vykonávali rýchle a spoľahlivé postupy na odstraňovanie nezákonných informácií a znemožňovanie prístupu k nim.³⁷ Hoci je v uvedenej smernici vylúčená možnosť zaviazat online platformy k aktívnemu vyhľadávaniu³⁸, zároveň sa v nej uznáva význam dobrovoľných opatrení³⁹.

Po druhé, v súlade s článkom 14 smernice o elektronickom obchode poskytovatelia služieb, ktorí patria do pôsobnosti predmetného ustanovenia, môžu využiť výnimku zo zodpovednosti len vtedy, ak sú splnené **dve podmienky**, a to: a) nič nevedia o nezákonnej činnosti alebo informáciách, a čo sa týka nárokov na náhradu škody, nie sú si vedomí skutočností alebo okolností, z ktorých by bolo zrejmé, že ide o nezákonnú činnosť alebo informácie, alebo b) po zistení alebo uvedomení si týchto skutočností konajú promptne, aby odstránili alebo znemožnili prístup k informáciám.

Súdny dvor objasnil, že tieto podmienky sa vzťahujú na „*akúkoľvek situáciu, keď sa [online platforma] dozvie o [skutočnostiach alebo okolnostiach, na základe ktorých by obozretný hospodársky subjekt musel konštatovať protiprávnosť]*“ a že to – popri oznámení od tretej strany – zahŕňa aj situáciu, keď platforma „*odhalí po preskúmaní vykonanom z vlastnej iniciatívy protiprávnou činnosť alebo informáciu*“.⁴⁰

Z toho vyplýva, že proaktívne opatrenia, ktoré online platforma prijme na odhaľovanie a odstraňovanie nezákonného obsahu, môžu viesť k tomu, že sa dozvie o nezákonnej činnosti alebo nezákonných informáciách, čo by mohlo vyústiť do straty nároku na výnimku zo zodpovednosti v súlade s článkom 14 ods. 1 písm. a) smernice o elektronickom obchode. V takýchto prípadoch však online platforma má aj naďalej možnosť po zistení alebo uvedomení si týchto skutočností promptne odstrániť dané informácie alebo znemožniť prístup k nim. Ak tak urobí, na online platformu sa aj naďalej uplatňuje výnimka zo zodpovednosti podľa článku 14 ods. 1 písm. b). Preto by obavy súvisiace so stratou výnimky zo zodpovednosti nemali odrádzať od uplatňovania efektívnych proaktívnych dobrovoľných opatrení, ktorých podpora je cieľom tohto oznámenia, ani mu brániť.

3.3.2. Využívanie technológií na odhaľovanie nezákonného obsahu

Vzhľadom na objem materiálov sprostredkovaných online platformami, ako aj na technologický pokrok v oblasti spracúvania informácií a strojovej inteligencie sa využívanie **technológií automatického odhaľovania a filtrovania** stáva čoraz dôležitejším nástrojom v boji proti nezákonnému obsahu na internete. Mnohé veľké platformy dnes využívajú nejakú formu párovacích algoritmov vychádzajúcich z rôznych technológií – od jednoduchého filtrovania metaúdajov, cez hašovanie až po identifikáciu obsahu na základe jeho digitálneho odtlačku (fingerprinting).

V smernici o elektronickom obchode sa vysvetľuje, že ustanovenia o zodpovednosti nebránia rozvoju a efektívnej prevádzke technických systémov ochrany a identifikácie či nástrojov technického

³⁶ Odôvodnenie 41 smernice o elektronickom obchode.

³⁷ Odôvodnenie 40 smernice o elektronickom obchode.

³⁸ Článok 15 ods. 1 smernice o elektronickom obchode.

³⁹ Odôvodnenie 40 smernice o elektronickom obchode.

⁴⁰ Rozsudok vo veci L'Oréal/eBay, body 120 a 121.

dohľadu, ktoré umožňujú digitálne technológie⁴¹. Ako smernica zároveň objasňuje, takáto prevádzka však musí prebiehať v rámci príslušných únijných a vnútroštátnych právnych predpisov, najmä pokiaľ ide o súkromie a osobné údaje a zákaz, aby členské štáty ukladali všeobecné monitorovacie povinnosti.⁴²

V odvetvových právnych predpisoch sa online platformám môže uložiť povinnosť prijímať opatrenia, napr. v oblasti autorských práv s cieľom zabezpečiť odhaľovanie a odstraňovanie nezákonného obsahu, a to aj vtedy, ak majú nárok na výnimku zo zodpovednosti stanovenú v článku 14 smernice o elektronickom obchode.

Všeobecne povedané, využívanie a ďalší rozvoj spomínaných technológií sa podporuje najmä v prípadoch, keď hrozí závažná škoda, ako sa uvádza aj v záveroch Európskej rady z 22. júna 2017⁴³. Na identifikáciu potenciálne protiprávneho obsahu možno použiť automatické nástroje a filtre a súkromný i verejný výskum v rozvoji týchto nástrojov napreduje. Napríklad v oblasti autorských práv sa ako účinný nástroj už niekoľko rokov osvedčuje automatické rozpoznávanie obsahu.

Komisia podporuje ďalší výskum a inovatívne prístupy presahujúce rámec súčasných technologických možností s cieľom zlepšiť presnosť technických prostriedkov na identifikáciu nezákonného obsahu⁴⁴. Okrem toho **vyzýva odvetvie, aby efektívne využívalo výsledky inovácií, ktoré môžu prispieť k zvýšeniu účinnosti a efektívnosti postupov automatickej detekcie.**

Vo väčšine prípadov dnes odvetvie štandardne používa automatické nástroje na zúženie objemu problematického obsahu, ktorý má odborne preverovať človek. Ten potom prípadne posúdi jeho nezákonnú povahu. Tento princíp ľudskej účasti (human in the loop) je vo všeobecnosti dôležitým prvkom automatických postupov, ktorých cieľom je určenie nezákonnosti určitého obsahu, najmä v oblastiach, v ktorých je vysoká chybovosť, alebo ak treba zohľadniť kontext.

Komisia sa domnieva, že proaktívne opatrenia prijaté online platformami v rozsahu pôsobnosti článku 14 smernice o elektronickom obchode, ktorých účelom je odhaľovať a odstraňovať nezákonný obsah na ich úložiskách – vrátane využívania automatických nástrojov a nástrojov určených na zabezpečenie toho, aby už raz odstránený obsah nebol znova nahratý – **nemôžu samy osebe viesť k strate nároku na výnimku zo zodpovednosti.**

Prijatie takých opatrení nemusí totiž znamenať, že online platforma zohráva aktívnu úlohu, pre ktorú by sa na ňu mala prestať uplatňovať uvedená výnimka. Aby splnila predpoklad na udržanie si práva na takúto výnimku, vždy, keď sa na základe uvedených opatrení dozvie o nezákonných činnostiach či

⁴¹ Odôvodnenie 40 smernice o elektronickom obchode.

⁴² Odôvodnenie 40 a článok 15 ods. 1 smernice o elektronickom obchode.

⁴³ <http://www.consilium.europa.eu/en/press/press-releases/2017/06/22-euco-security-defence/>.

⁴⁴ Súčasné výskumno-inovačné úsilie odvetvia sa zameriava na rozvoj analytických nástrojov na lepšie pochopenie prirodzeného jazyka, informačné kaskády na sociálnych sieťach, identifikáciu zdrojov informácií, schémy šírenia a falošné totožnosti. Aj Komisia podporila výskum a inovácie v tejto oblasti financovaním projektov zameraných na rozvoj automatických overovacích nástrojov na kontrolu vecnej správnosti obsahu vytváraného používateľmi na sociálnych sieťach. Tieto nástroje môžu pomôcť pri identifikácii potenciálnych nepravdivých informácií v textoch, na obrázkoch alebo vo videách a uľahčiť sledovanie pôvodu falošných správ. Rozhodnutie o nezákonnej povahe takéhoto obsahu však prekračuje rámec ich súčasných funkčných kapacít.

informáciách alebo si ich uvedomí, musí rýchlo konať, aby príslušné nezákonné informácie odstránila alebo k nim znemožnila prístup.

Online platformy by mali urobiť všetko, čo je v ich silách, aby proaktívne odhaľovali, identifikovali a odstraňovali nezákonný obsah na internete. Komisia dôrazne nabáda online platformy, aby prijímali dobrovoľné, proaktívne opatrenia zamerané na odhaľovanie a odstraňovanie nezákonného obsahu a aby zintenzívnili spoluprácu v oblasti technológií automatického rozpoznávania, viac do nich investovali a častejšie ich využívali.

4. ODSTRANOVANIE NEZÁKONNÉHO OBSAHU

Je v záujme celej spoločnosti, aby **platformy odstraňovali nezákonný obsah čo najrýchlejšie**. Odstraňovanie takéhoto obsahu by zároveň **nemalo byť prekážkou trestného stíhania alebo iných opatrení nadväzujúcich na akékoľvek súvisiace porušenia právnych predpisov**. Dôležitú úlohu v tejto oblasti zohráva výmena dôkazov medzi verejnými orgánmi a online platformami. Pripravovaná legislatívna iniciatíva zameraná na túto problematiku by mala uľahčiť cezhraničný prístup k dôkazom⁴⁵. Odstraňovanie nezákonného obsahu zo strany platforiem by nemalo mať vplyv na vyšetrovanie alebo stíhanie trestných činov podľa úniijného ani vnútroštátneho práva.

Mali by byť k dispozícii aj **spoľahlivé záruky na obmedzenie rizika odstránenia legálneho obsahu** doplnené súborom zmysluplných záväzkov v oblasti transparentnosti na zabezpečenie väčšej zodpovednosti za procesy odstraňovania.

4.1. Urýchlené odstraňovanie a oznamovanie trestnej činnosti orgánom presadzovania práva

V smernici o elektronickom obchode sa stanovuje, že ak online platformy chcú naďalej využívať výnimku zo zodpovednosti, po zistení prítomnosti nezákonného obsahu ho musia „rýchlo“ odstrániť. Čo to znamená v praxi, závisí od osobitostí konkrétneho prípadu, najmä od druhu nezákonného obsahu, pravdivosti oznámenia a potenciálnej škody.

V praxi si na posúdenie zákonnosti určitého obsahového prvku rôzne druhy obsahu vyžadujú rôzne množstvo kontextových informácií. Zatiaľ čo určiť nezákonnú povahu detskej pornografie je pomerne ľahké, určenie nezákonnosti hanlivých tvrdení si vo všeobecnosti vyžaduje starostlivú analýzu kontextu, v ktorom sa objavili.

Ak hrozí závažná škoda, napríklad v prípadoch podnecovania k teroristickým činom, rýchle odstránenie je mimoriadne dôležité a môžu sa naň vzťahovať osobitné lehoty.

Niektoré dobrovoľné postupy, ako napríklad kódex správania pre boj proti nezákonným nenávisným prejavom na internete, uvádzajú orientačné lehoty na odstránenie obsahu – tento konkrétny kódex vo väčšine prípadov odporúča 24 hodín.

⁴⁵ Viac informácií možno nájsť na adresách https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en a https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

Plne automatické vymazávanie alebo dočasné znepřístupnenie obsahu môže byť obzvlášť účinné a malo by sa použiť, ak okolnosti nechávajú malé pochybnosti o nezákonnosti materiálu, napr. v prípade materiálov, o odstránenie ktorých požiadajú orgány presadzovania práva, alebo známeho nezákonného obsahu, ktorý už bol raz odstránený, pričom sa musí dbať na záruky uvedené v oddiele 4.3.

Všeobecne platí, že **odstraňovanie na základe oznámení od dôveryhodných oznamovateľov by sa malo riešiť rýchlejšie** vzhľadom na kvalitu a presnosť informácií uvedených v oznámení a dôveryhodnosť oznamovateľov.

Keď hrozí hospodárska škoda v dôsledku porušenia práva duševného vlastníctva, rýchlosť odstránenia obsahu môže ovplyvniť jej potenciálnu výšku.

Keď budú platformy podávať transparentné správy o tom, koľko času potrebovali na spracovanie žiadostí o odstránenie v závislosti od druhu obsahu, bude sa ľahšie posudzovať rýchlosť prijatých opatrení a platformy sa budú môcť častejšie brať na zodpovednosť.

V určitých prípadoch, najmä keď online platformy majú ťažkosti s posudzovaním zákonnosti určitého obsahového prvku a ide o potenciálne sporné rozhodnutie, **s pochybnosťami by sa mohli obrátiť na tretiu stranu**. V členských štátoch túto úlohu zohrávajú samoregulačné orgány alebo príslušné orgány. Ako súčasť posilnenej spolupráce medzi online platformami a príslušnými orgánmi sa takáto komunikácia dôrazne odporúča.

Napokon treba uviesť, že **online platformy by mali kontaktovať orgány presadzovania práva** vždy, keď sa dozvedia o trestnej činnosti, inej nezákonnej činnosti alebo zneužívaní služieb platforiem zo strany organizovaných zločineckých či teroristických skupín, prípadne ich odhalia, aby varovali príslušné orgány a umožnili im vyšetrovať a stíhať osoby, ktoré takýto obsah produkujú. Pritom by mali dodržiavať platné právne požiadavky vrátane nariadenia (EÚ) 2016/679 o ochrane osobných údajov.⁴⁶ To môže platiť aj v prípade ponuky a predaja produktov a obchodných praktík, ktoré nie sú v súlade s právnymi predpismi EÚ.

Potreba spolupracovať s orgánmi presadzovania práva pri vyšetrovaní a stíhaní trestných činov môže v niektorých prípadoch viesť k tomu, že platformy neodstránia predmetný nezákonný obsah, ak sa to vyžaduje v rámci konkrétneho prebiehajúceho vyšetrovania, a to pod podrobným dohľadom vnútroštátnych orgánov a v plnom súlade s vnútroštátnymi trestnoprávnymi predpismi.

Orgány činné v trestnom konaní by mali vytvoriť potrebné kapacity, aby mohli na tieto správy primerane reagovať.⁴⁷ Ako príklad najlepších postupov, pokiaľ ide o kontaktné miesta, je portál

⁴⁶ Článok 6 ods. 1 písm. c) v spojení s článkom 6 ods. 4.

⁴⁷ Podľa článku 15 ods. 2 smernice o elektronickom obchode sa stanovuje „členské štáty môžu ustanoviť povinnosť, aby poskytovatelia služieb informačnej spoločnosti informovali príslušné verejné orgány o údajných vykonávaných nezákonných činnostiach alebo o údajných nezákonných poskytovaných informáciách, alebo povinnosť oznamovať príslušným orgánom na ich žiadosť informácie, ktoré by im umožnili identifikáciu príjemcov ich služieb, s ktorými uzatvorili dohody o uložení informácií“.

SIRIUS⁴⁸, ktorý vytvoril Europol na podporu členských štátov pri online vyšetrovaniach terorizmu vrátane, a to aj uľahčovaním spolupráce medzi platformami a presadzovania práva EÚ⁴⁹.

V súlade s článkom 14 smernice o elektronickom obchode musia online platformy odstrániť nezákonný obsah bez zbytočného odkladu bezprostredne po tom, ako sa dozvedia o jeho existencii, ak si chcú zachovať výnimku zo zodpovednosti. Mimoriadne rýchle odstránenie nezákonného obsahu je dôležité vtedy, keď hrozí závažná škoda, napríklad pri podnecovaní k teroristickým činom. Čas potrebný na odstránenie a postupy platné pri jednotlivých rôznych formách nezákonného obsahu by sa mali jasne uviesť v transparenčných správach.

Komisia otázku pevne stanovených lehôt na odstraňovanie bude ďalej analyzovať.

Dôkazy o trestnej činnosti získané pri odstraňovaní nezákonného obsahu by sa mali zaslať orgánom presadzovania práva, ak je to v súlade najmä s požiadavkami stanovenými v nariadení (EÚ) 2016/679, predovšetkým so zákonnými dôvodmi na spracovanie osobných údajov.

4.2. Zvýšenie transparentnosti

4.2.1. Transparentnosť pravidiel riadenia obsahu online platforiem

Otázku, či je obsah zákonný alebo nezákonný, upravujú únijské a vnútroštátne právne predpisy. Zároveň sa isté druhy obsahu môžu za nežiaduce alebo napadnuteľné považovať aj vo vlastných podmienkach poskytovania služieb online platforiem.

Online platformy by mali zverejniť svoje podrobné pravidlá riadenia obsahu v podmienkach poskytovania služieb a jasne o nich informovať svojich používateľov. Tieto podmienky by mali nielen definovať pravidlá odstraňovania obsahu alebo znemožňovania prístupu k nemu, ale stanovovať aj záruky, ktoré zabránia nadmernému odstraňovaniu. V podmienkach poskytovania služieb by sa – ako súčasť zvýšenej transparentnosti všeobecných politík online platforiem upravujúcich odstraňovanie – malo najmä jasne uvádzať, aké možnosti majú používatelia, ak chcú napadnúť rozhodnutia o odstránení. Malo by to pomôcť znížiť potenciálne negatívny vplyv na základné práva používateľov na slobodu prejavu a právo na informácie⁵⁰.

Online platformy by **v podmienkach poskytovania služieb mali jasne, zrozumiteľne a dostatočne podrobne vysvetliť pravidlá, ktorými sa riadia pri riadení obsahu**. Tie by mali zohľadňovať tak zaobchádzanie s nezákonným obsahom, ako aj s obsahom, ktorý nedodržiava ich podmienky poskytovania služieb. Všetky obmedzenia týkajúce sa takého obsahu, ktorý je na konkrétnej platforme povolený, by sa mali byť jasne špecifikovať a oznámiť používateľom. Toto objasnenie by malo zahŕňať aj postupy napadnutia rozhodnutí o odstránení vrátane tých, ktoré sa prijímajú na odporúčanie dôveryhodných oznamovateľov.

⁴⁸ Budovanie jednotného systému vyšetrovania na internete.

⁴⁹ Europol bude ďalej pomáhať pri vytváraní nových jednotných kontaktných miest poskytovaním relevantných školení pre orgány presadzovania práva v krajinách, kde ešte takéto miesta nie sú zavedené.

⁵⁰ Ak ide o spracovanie osobných údajov, platformy musia zabezpečiť transparentné politiky ochrany osobných údajov podľa článku 12 všeobecného nariadenia o ochrane údajov.

4.2.2. *Transparentnosť pri postupoch oznamovania a prijímania opatrení*

Transparentné správy by mali obsahovať aj *výsledky* uplatňovania pravidiel platformy na riadenie obsahu.

Online platformy by mali **zverejňovať transparentné správy** s dostatočne podrobnými **informáciami o počte a druhu doručených oznámení a prijatých opatrení**, ako aj o **čase potrebnom na spracovanie** a pôvodcoch oznámení⁵¹. Tieto správy by sa mali zmieňovať aj o prípadných **námietkach** a reakcii na ne. Komisia podporuje platformy v tom, aby takéto informácie zverejňovali pravidelne, minimálne však raz ročne.

Bolo by prínosné, keby sa na digitálnom jednotnom trhu podarilo dospieť k **štandardnému formátu** týchto transparentných správ s prihliadnutím na obsahové špecifiká. Umožnilo by sa tak lepšie monitorovanie, uľahčilo elektronické zhromažďovanie takýchto informácií a mohlo by to pomôcť vyhnúť sa zbytočným prekážkam v cezhraničnom poskytovaní hostingových služieb.

Mala by sa venovať osobitná pozornosť tomu, aby malé online platformy a MSP mali podmienky na poskytovanie takýchto transparentných údajov, a všetky podporné činnosti, ako je napríklad štandardizácia, by mali zabezpečiť, aby sa administratívne zaťaženie obmedzilo na minimum.

Komisia bude v rámci štruktúrovaných dialógov s odvetvím ďalej **skúmať potenciál štandardizácie** postupov oznamovania a transparentných správ o systémoch a výsledkoch odstraňovania.

4.3. **Záruky proti nadmernému odstraňovaniu a zneužívaniu systému**

Rýchle opatrenia, ako je filtrovanie obsahu pri nahrávaní alebo automatická detekcia, zamerané na promptné odstraňovanie nezákonného obsahu, môžu mať vplyv na správnosť rozhodnutí a spôsobiť, že sa odstráni aj legálny obsah, a to najmä ak do procesu nezasahuje človek. Preto je dôležité, aby boli k dispozícii dostatočné záruky a aby sa obsah, ktorý bol omylom odstránený, dal obnoviť.

4.3.1. *Námietky proti oznámeniu*

Poskytovatelia obsahu by vo všeobecnosti mali **mať možnosť napadnúť toto rozhodnutie námietkou**, a to aj pri automatickom odstránení obsahu.

Napríklad podľa článku 28a návrhu na zmenu smernice o AVMS musia členské štáty zabezpečiť mechanizmy podávania sťažností a nápravy pri urovnávaní sporov medzi používateľmi a poskytovateľmi platforiem na zdieľanie videí, pokiaľ ide o uplatňovanie primeraných opatrení prijímaných týmito platformami.

Ak námietka obsahuje primerané dôvody domnievať sa, že oznámená činnosť alebo informácia nie je nezákonná, **poskytovateľ platformy by mal odstránený obsah bezodkladne obnoviť alebo umožniť**

⁵¹ Správy by mali uvádzať podrobnosti o vlastných vyšetrovaniach, oznámeniach od bežných používateľov, oznámeniach od orgánov presadzovania práva atď.

dotknutému používateľovi súbor opätovne nahráť – bez toho, aby boli dotknuté podmienky poskytovania služby platformy.

Možnosť namietať proti rozhodnutiam by mala znížiť počet neodôvodnených odstránení legálneho obsahu a mohla by tiež slúžiť ako zdroj dôkazov pre mechanizmy mimosúdneho riešenia sporov alebo súdne odvolacie konania.

Za určitých okolností by nebolo vhodné, aby sa informoval poskytovateľ obsahu a/alebo povolila námietka, najmä ak by to zasahovalo do vyšetrovacích právomocí orgánov členských štátov nevyhnutných na prevenciu, odhaľovanie a stíhanie trestných činov, ako napríklad v prípade detskej pornografie.

Online platformy by mali poskytovať jednoduché námietkové postupy online. Po podaní námietky by na ňu mali odpovedať a v prípade zamietavého rozhodnutia špecifikovať dôvody. Ak v príslušnom členskom štáte existujú orgány mimosúdneho urovnávania sporov, platformy by mali umožniť, aby sa dotknuté strany pri riešení sporov o námietkach mohli obrátiť práve na ne.

4.3.2. Opatrenia proti oznámeniam a námietkam podaným so zlým úmyslom

Postupy oznamovania a prijímania opatrení sa niekedy môžu zneužiť nekalými postupmi alebo konaním so zlým úmyslom⁵². Od takých praktík by sa malo dôrazne odrádzať – napríklad znižovaním priority spracovania oznámení od predkladateľov, ktorí zasielajú vysoké množstvo neodôvodnených oznámení alebo dostávajú veľa námietok, prípadne zrušením statusu dôveryhodného oznamovateľa, a to v súlade s osvedčenými a transparentnými kritériami. Tieto pravidlá by mali byť jasne opísané aj v podmienkach poskytovania služieb online platforiem a byť súčasťou ich všeobecného transparentného podávania správ, aby sa kladol väčší dôraz na ich povinnosť zodpovedať sa pred verejnosťou. Podobné opatrenia by sa mali zaviesť aj v prípade nekorektných námietok.

5. PREVENIA OPAKOVANÉHO VÝSKYTU NEZÁKONNÉHO OBSAHU

Keď bol raz nezákonný obsah odhalený a odstránený, na internete by sa už nemal objaviť. Na správne fungovanie systému je nevyhnutné efektívne a účinné predchádzanie opakovanému výskytu obsahu opierajúce sa o existujúce osvedčené postupy a o primerané záruky. Ak sa má zabrániť tomu, aby sa známy nezákonný materiál šírila z platformy na platformu, poskytovatelia online služieb musia užšie spolupracovať, pričom však musia plne rešpektovať platné právne predpisy v oblasti hospodárskej súťaže. Takisto je dôležité posilniť spoluprácu orgánov presadzovania práva s malými, menej odolnými spoločnosťami, ktoré môžu zločinci či iné osoby zapojené do protiprávných online aktivít uprednostňovať, ak ich považujú za zraniteľnejšie.

⁵² Dôkazy naznačujú, že takéto informácie využívajú konkurenti (*Notice and Takedown in Everyday Practice*, J Urban et al., UC Berkeley, 2016), a že prax automatického generovania oznámení býva zneužívaná na vytvorenie odkazu na umelo vytvorený obsah (transparentná správa spoločnosti Google).

5.1. Opatrenia proti opakovaným porušovateľom

Aby sa používateľom, ktorí opakovane uverejňujú protiprávny obsah rovnakého charakteru, zabránilo v jeho opätovnom nahrávaní, mnohé online platformy už uplatňujú postupy zamerané na pravidelných porušovateľov, ako napríklad pozastavenie alebo zrušenie používateľského účtu či tzv. shadow banning.⁵³

Online platformy by mali prijať opatrenia, ktoré odradia používateľov od opakovaného nahrávania nezákonného obsahu rovnakého charakteru, a snažiť sa účinne obmedzovať šírenie takéhoto nezákonného obsahu.

To by malo platiť aj v prípadoch, keď ide o rovnakého porušovateľa a rovnaký charakter obsahu a keď bol používateľ v odôvodnených prípadoch promptne informovaný o oznámeniach, ktoré ho inkriminujú, a o nadchádzajúcom pozastavení alebo zrušení účtu. Používatelia by tak mohli dané rozhodnutie napadnúť a mali by ľahší prístup k súdnym opravným prostriedkom proti nemu, ak je to vhodné na základe zmluvy medzi používateľom a platformou a platného práva. Aj v takýchto prípadoch sa pri spracúvaní osobných údajov vždy musia plne dodržiavať príslušné pravidlá ochrany údajov.

Rovnako by sa poskytovateľovi obsahu nemali sprístupniť žiadne informácie ani zasielať oznámenia, ak by to mohlo ohroziť vyšetrovacie právomoci členských štátov potrebné na prevenciu, odhaľovanie a stíhanie trestných činov – za predpokladu, že je k dispozícii potrebný právny základ.

5.2. Automatické filtrovanie obsahu pri opakovanom nahrávaní

Popri technológiách používaných na identifikáciu potenciálne nezákonného obsahu uvedených v oddiele 3.3 možno pri obsahu, ktorý už bol identifikovaný a posúdený ako nezákonný, použiť ešte spoľahlivejšie technologické nástroje na analýzu digitálnych odtlačkov a filtrovanie obsahu (s cieľom jeho odstránenia alebo zabránenia jeho opakovanému nahratiu). Komisia preto silne podporuje ďalšie používanie takýchto nástrojov, pričom však musia existovať záruky, ako napr. reverzibilita či výnimky uvedené nižšie.

V súčasnosti existuje napríklad tzv. databáza hashov vyvinutá v rámci internetového fóra EÚ, ktorá sa používa v súvislosti s teroristickým obsahom, v oblasti autorských práv alebo v prípade detskej pornografie, ale aj pri produktoch, ktoré podľa orgánov presadzovania práva nie sú v súlade s príslušnými právnymi predpismi. Tieto postupy sú úspešné. Ich efektívnosť však závisí od ďalších zlepšení zameraných na to, aby sa čo najmenej nesprávne identifikoval obsah a aby sa pri prijímaní rozhodnutí dal zohľadňovať kontext, ako aj od potrebných opatrení zaručujúcich reverzibilitu.

Napríklad v návrhu Komisie o autorských právach na digitálnom jednotnom trhu, ktorý vychádza z praxe automatického rozpoznávania obsahu v oblasti autorských práv, sa takéto technológie – pokiaľ sú vhodné a primerané – uznávajú okrem iného ako možný prostriedok na zabránenie dostupnosti nelicencovaného obsahu cez dotknuté online služby.

⁵³ „Shadow banning“ je vyradenie používateľa z komunity online používateľov bez jeho vedomia.

Automatické postupy brániace opätovnému nahrávaniu obsahu by mali umožňovať kontextové výnimky a nemali by sa uplatňovať, ak sa odstránený obsah upraví a zosúladí s právnymi alebo inými požiadavkami. Rozsah a načasovanie kontextových výnimiek by mal zohľadniť osobitnú povahu obsahu a akékoľvek súvisiace bezpečnostné hrozby, ako aj možnosť dočasného pozastavenia dostupnosti takéhoto obsahu, kým sa podrobnejšie nepreskúma.

Komisia vehementne podporuje ďalšie používanie a vývoj automatických technológií na zabránenie opakovanému výskytu nezákonného obsahu online.

Ak sa na zabránenie opakovanému výskytu nezákonného obsahu používajú automatické nástroje, mala by byť pre prípad chybných rozhodnutí k dispozícii záruka v podobe reverzibility a fungovanie týchto technológií by sa malo transparentne opísať v podmienkach poskytovania služieb platforiem.

Všetky online platformy by mali mať prístup do databáz, ktoré sa používajú na automatické vyhľadanie a identifikáciu opakovane sa vyskytujúceho nezákonného obsahu, pričom pri nakladaní s obsahom sa musia vždy dodržiavať platné právne predpisy o ochrane osobných údajov a hospodárskej súťaži. Pravidlá ochrany súkromia, ktorými sa riadia spoločnosti, by mali obsahovať transparentné informácie o spracúvaní osobných údajov v prípade takýchto databáz.

Online platformy by mali takisto zabezpečiť nepretržitú aktualizáciu svojich nástrojov, aby sa zabezpečilo zachytenie všetkého nezákonného obsahu s ohľadom na meniacu sa taktiku zločincov a iných osôb zapojených do protiprávných aktivít na internete. Nástroje používané na teroristický obsah by sa mali upraviť tak, aby dokázali zachytiť nový aj starý obsah a zabezpečiť jeho urýchlené preskúmanie a odstránenie. Takýto obsah by sa mal zaradiť aj do spoločných nástrojov pre platformy, ako je napríklad spomínaná databáza hashov (v súčasnosti používaná v súvislosti s teroristickým obsahom). Takýto technologický vývoj by sa mal opierať o spoluprácu medzi online platformami, príslušnými orgánmi a inými zainteresovanými stranami vrátane občianskej spoločnosti.

6. ZÁVERY

Čoraz častejší výskyt nezákonného obsahu na online platformách spôsobuje spoločnosti hmatateľné škody a ohrozuje morálku, dôstojnosť aj zdravie našich občanov. Ak sa tento problém nebude náležite riešiť, naruší tiež dôveru v digitálne služby v širšom zmysle a v konečnom dôsledku aj v digitálny jednotný trh, ktorý je kľúčovým pohonom inovácií, rastu a zamestnanosti. Aj keď tento obsah vytvárajú a nahrávajú tretie strany, neustále rastúci vplyv online platforiem na spoločnosť, ktorý vyplýva z ich úlohy poskytovateľov prístupu k obsahu a informáciám, zvyšuje ich zodpovednosť voči používateľom i spoločnosti ako celku. Preto by mali proaktívne bojovať proti nezákonnému obsahu, predchádzať jeho opakovanému výskytu, zavádzať účinné postupy oznamovania a prijímania opatrení, pestovať dobre fungujúce kontakty s tretími stranami (napr. s dôveryhodnými oznamovateľmi) a prednostne sa zaoberať oznámeniami od vnútroštátnych orgánov presadzovania práva. Keď v súlade s právnymi predpismi rozhodujú o nezákonnosti obsahu samy platformy, mali by sa zaviesť primerané mechanizmy kontroly a rovnováhy.

Toto oznámenie poskytuje usmernenia a nemení uplatniteľný právny rámec, ani neobsahuje právne záväzné pravidlá; jeho cieľom je najmä ukázať online platformám cestu, ako si plniť povinnosť vykoreňovať nezákonný obsah, ktorý sa nachádza na ich lokalitách. Takisto sa zameriava na šírenie

osvedčených postupov zameraných na jednotlivé formy nezákonného obsahu a podporu užšej spolupráce medzi platformami a príslušnými orgánmi. Načrtáva európsky prístup ponúkajúci online platformám nástroje na boj proti nezákonnému obsahu, ktorý spája potrebu rýchleho a účinného odstraňovania nezákonného obsahu a prevencie a stíhania trestnej činnosti so zaručením práva na slobodu prejavu online. Tieto usmernenia budú dopĺňať a posilňovať prebiehajúce odvetvové dialógy.

Osobitná pozornosť by sa mala venovať tomu, aby takéto postupy dokázali zaviesť aj menšie online platformy, a mnohé prvky tohto oznámenia boli koncipované s ohľadom na ich osobitné potreby. Komisia však napriek tomu preskúma aj ďalšie prostriedky na podporu menších platforiem pri zavádzaní jej usmernení.

Digitálny jednotný trh si vyžaduje väčšiu koherentnosť politických reakcií naprieč hranicami. Komisia preto toto oznámenie chápe ako prvý krok a poskytuje v ňom spoločné nástroje na riešenie spoločného problému odstraňovania nezákonného obsahu.

Vo vyhlásení o zámere, ktoré 13. septembra 2017 predseda Európskej komisie adresoval predsedovi Európskeho parlamentu a predsedovi Rady Európskej únie s výzvou na zabezpečenie priestoru spravodlivosti a základných práv založeného na vzájomnej dôvere, boli oznámené ďalšie opatrenia na zabezpečenie rýchleho a proaktívneho odhaľovania a odstraňovania nezákonného obsahu, ktorý podnecuje k nenávisti, násiliu a terorizmu. Toto oznámenie predstavuje prvú časť týchto opatrení. Komisia očakáva, že online platformy budú v nasledujúcich mesiacoch promptne konať, a to aj v kontexte príslušných dialógov, najmä v oblasti terorizmu a nezákonných nenávistných prejavov.

Komisia bude pokračovať vo výmenách názorov a v dialógoch s online platformami a inými relevantnými zainteresovanými stranami. Bude pozorne sledovať pokrok a posúdi, či treba ďalej konať, aby sa zabezpečilo rýchle a aktívne odhaľovanie a odstraňovanie nezákonného obsahu na internete, vrátane možných legislatívnych opatrení na doplnenie súčasného regulačného rámca. Táto práca sa ukončí do mája 2018.