



**Globálna sieť
regulačných orgánov
pre bezpečnosť online**

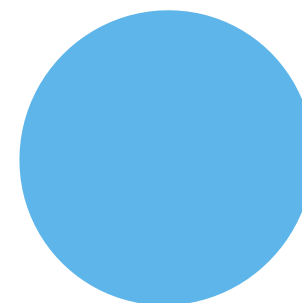
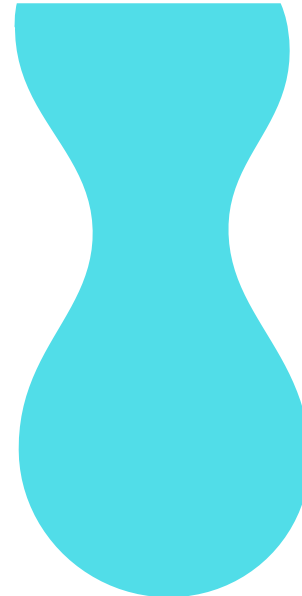
Regulačný index

**Porovnanie medzinárodných prístupov a perspektív
k regulácii bezpečnosti online**



Tento dokument vypracovali členovia Globálnej siete regulačných orgánov pre bezpečnosť online:

eSafety Commissioner (Austrália), Online Safety Commission (Fidži), Arcom (Francúzsko), Coimisiún na Meán (Írsko), Korea Communications and Standards Commission (Kórejská republika), Council for Media Services (Slovensko), Film and Publications Board (Juhoafrická republika), Ofcom (Spojené kráľovstvo)



Regulačný index

1. O indexe	2
2. Kľúčová terminológia	3
3. Prehľady o jurisdikciách	5
31 Austrália (eSafety Commissioner)	6
32 Fidži (Online Safety Commission)	7
33 Francúzsko (Arcom)	8
34 Írsko (Coimisiún na Meán)	9
35 Kórejská republika (Korea Communications and Standards Commission)	10
36 Slovensko (Rada pre mediálne služby)	11
37 Juhoafrická republika (Rada pre film a publikácie)	12
38 Spojené kráľovstvo (Ofcom)	13
4. Regulačné analýzy	14
41 Regulačné právomoci v oblasti bezpečnosti online	15
42 Druhy ujmy v online priestore	16
43 Regulované subjekty	17
44 Povinnosti regulovaných subjektov	18
45 Zber informácií a presadzovanie pravidiel	19



O sieti

Globálna sieť regulačných orgánov pre bezpečnosť online (ďalej len „sieť“) je globálne fórum zamerané na podporu spolupráce medzi regulačnými orgánmi pre bezpečnosť online, ktoré vysliela silný signál o našom spoločnom záväzku regulovať bezpečnosť online.

Táto sieť sa skladá z členov a pozorovateľov. Členmi sú nezávislé zákonné orgány zodpovedné za bezpečnosť online v rámci svojej jurisdikcie.

Jej členovia sa zaviazali chrániť ľudské práva, demokraciu a právny štát a sú nezávislí od politických a obchodných zásahov.

Pozorovatelia sú organizácie so zameraním na bezpečnosť online a s kompetenciami v tejto oblasti, ako napríklad mimovládne organizácie, skupiny viacerých zainteresovaných strán a verejné orgány.

Viac informácií nájdete na stránke esafety.gov.au/about-us/who-we-are/international-engagement/the-global-online-safety-regulators-network.

O indexe

Regulačný index bezpečnosti online (ďalej len „index“) napomáha poslanie siete, ktorým je vykonávať súdržnú reguláciu bezpečnosti online.

Index, ktorý vytvorili členovia siete, je základným dokumentom určeným na podporu spolupráce a porovnávania regulačných rámcov v oblasti bezpečnosti online medzi jednotlivými jurisdikciami. Cieľom indexu je poukázať na spoločné a rozdielne oblasti, pričom slúži ako dôležitý zdroj na podporu všeobecnejšieho pochopenia prístupov k regulácii bezpečnosti online.

Index sa skladá z dvoch častí:

Prvá časť obsahuje **prehľady o jurisdikciách** jednotlivých členských krajín a ich regulačnom prístupe k bezpečnosti online s dôrazom na príslušné právne predpisy a pravidlá, rozsah pôsobnosti a kompetencie, ako aj právomoci a funkcie. Prehľady o jurisdikciách vypracoval každý regulačný orgán samostatne. Medzi jednotlivými prehľadmi sa preto vyskytujú určité terminologické odchýlky.

Druhá časť obsahuje **komparatívnu analýzu**, v ktorej sú zhrnuté a porovnané prístupy regulačných orgánov k regulácii bezpečnosti online v kľúčových oblastiach, ako sú kompetencie, regulované druhy ujmy v online priestore, regulované platformy a služby, povinnosti regulovaných subjektov a presadzovanie predpisov.

Index odráža globálnu perspektívu a zoskupujú sa v ňom niektoré pojmy, ktoré môžu byť v rôznych kontextoch opísané odlišne, pričom treba poznamenať, že definície, prahové hodnoty a terminológia platná na miestnej úrovni sa v jednotlivých jurisdikciách líšia. Preto platí, že hoci má index slúžiť ako užitočná pomôcka, nenahrádza štúdium vnútroštátnych právnych predpisov a regulačných dokumentov, ktoré uverejňujú členovia siete. Index sa bude pravidelne aktualizovať.



Kľúčová terminológia

Upozorňujeme, že tieto kľúčové pojmy môžu mať v jednotlivých jurisdikciách rôzny význam a uplatnenie.

Bezpečnosť už v štádiu návrhu: koncepcia, v rámci ktorej sú bezpečnosť a práva používateľov stredobodom návrhu a poskytovania produktov a ktorá vyžaduje, aby platformy a služby predvídali a zmierňovali riziká v online priestore.

Dezinformácie: informácie, ktorá sú vedome alebo z nebanlivosti nepravdivé a ktoré sú určené na úmyselné zavádzanie a ovplyvňovanie osoby alebo skupiny osôb na zlomyseľné alebo podvodné účely.

Digitálna gramotnosť: schopnosť porozumieť technológiám a digitálnemu prostrediu, identifikovať riziká a reagovať na ne a bezpečne pristupovať k digitálnym službám a platformám a používať ich.

Materiál zobrazujúci sexuálne vykorisťovanie detí je akýkoľvek obsah, ktorý zobrazuje dieťa v sexuálnom kontexte. Zahŕňa obsah, v ktorom sa dieťa sexualizuje a využíva, ako aj obsah zobrazujúci detskú sexuálnu aktivitu.

Materiál zobrazujúci sexuálne zneužívanie detí zobrazuje sexuálny útok na dieťa a možno ho považovať za podskupinu materiálu zobrazujúceho sexuálne vykorisťovanie detí.

Mediálna gramotnosť: schopnosť pristupovať k médiám a komunikácii, analyzovať, hodnotiť a vytvárať ich v rôznych kontextoch.

Mylná informácia: nesprávna alebo nepravdivá informácia, ktorá sa šíri z dôvodu neznalosti, omylu alebo chyby bez úmyslu oklamať.

Nedobrovoľné zdieľanie intímnych záberov alebo zneužívanie prostredníctvom obrázkov: označuje zdieľanie alebo hrozbu zdieľania intímnych záberov osoby bez jej súhlasu.

Nenávistné prejavy online alebo **nenávisť online:** vo všeobecnosti sa tento pojem vzťahuje na obsah vytvorený používateľom, ktorý diskriminuje jednotlivca alebo skupinu na základe chráneného atribútu, ako sú rasa, sexualita, rod, kultúra, zdravotný stav a ďalšie. „Nenávisť online“ sa vo všeobecnosti považuje za širší pojem, ktorý zahŕňa všetok nenávistný obsah a nenávistné činy online vrátane prejavov, obrázkov, videí, symboliky a iných interakcií medzi používateľmi.

Obmedzený obsah: obsah, ktorý môže byť škodlivý pre fyzické alebo psychické zdravie alebo vývoj detí alebo mladých ľudí, ako napríklad pornografia alebo násilie s veľkým dopadom (označovaný aj ako vekovo nevhodný obsah a „obsah škodlivý pre mládež“) (austrálska terminológia).

Obsah o terorizme a násilnom extrémizme: pojem vo všeobecnosti označujúci obsah, ktorý zobrazuje alebo obhajuje činy násilného extrémizmu alebo inak zobrazuje, obhajuje, propaguje, podnecuje alebo sympatizuje s teroristickými alebo extrémistickými organizáciami, skupinami alebo ideológiami.

Odhad veku: približné určenie veku osoby pomocou technológie na odhad, ako je napríklad analýza fotografií s využitím umelej inteligencie.

Overenie veku: určenie veku osoby s vysokou mierou istoty, zvyčajne overením údajov podľa externého zdroja, ako je doklad totožnosti.

Oznámenie o blokovaní: právne oznámenie určené platforme alebo službe, ktorým sa tejto platforme alebo službe prikazuje, aby zablokovala domáci prístup k určitému obsahu, ktorý sa často nachádza v zahraničí.

Oznámenie o odstránení/stiahnutí obsahu: oznámenie určené platforme alebo službe, ktorým sa tejto platforme alebo službe prikazuje, aby zo svojej služby alebo platformy odstránila určitý obsah.

Platforma na zdieľanie videí: platforma alebo služba, ktorá umožňuje používateľom vytvárať, zverejňovať a zdieľať videoobsah, ktorý vytvárajú iní používatelia, alebo s týmto obsahom interagovať (terminológia Spojeného kráľovstva a EÚ).

Preukázanie veku: súhrnný pojem, ktorý sa používa na označenie celého súboru metód a technológií na preukázanie veku v online prostredí, ako sú overenie veku a odhad veku.

Príkaz na prerušenie podnikania: exekučný príkaz dostupný podľa zákona Spojeného kráľovstva o online bezpečnosti z roku 2023 (Online Safety Act 2023), ktorý umožňuje príslušnému súdu prijať akékoľvek opatrenia na „prerušenie“ podnikania online platformy alebo služby. To môže zahŕňať blokovanie inzerentov alebo prikázanie poskytovateľovi internetových služieb, aby zablokoval prístup k platforme alebo službe na domácej úrovni.



Proaktívna detekcia: v oblasti moderovania obsahu proaktívna detekcia označuje postup proaktívneho prehľadávania obsahu vytvoreného používateľom s cieľom odhaliť škodlivý obsah alebo obsah porušujúci zásady skôr, ako ho nahlási používateľ alebo orgán.

Proteroristický obsah: obsah, ktorý podporuje spáchanie teroristického útoku, pretože zobrazuje, podnecuje, propaguje, oslavuje, chváli alebo inak sympatizuje s teroristickými alebo extrémistickými skupinami alebo činmi.

Rodovo podmienené násilie podporované technológiami: označuje akýkoľvek čin, ktorý je spáchaný, podporovaný, prehlbovaný alebo zosilňovaný používaním informačných komunikačných technológií alebo iných digitálnych nástrojov proti určitej osobe na základe jej pohlavia, ktorý vedie alebo môže viesť k ujme alebo inému porušeniu práv a slobôd.

Sexuálne vykorisťovanie a zneužívanie detí je široký pojem, ktorý zahŕňa všetky formy sexuálneho vykorisťovania a zneužívania detí vrátane materiálu obsahujúceho sexuálne zneužívanie detí, materiálu obsahujúceho sexuálne vykorisťovanie detí a ďalších činností, ako sú sexuálne vydieranie a obchodovanie so sexom.

Služba medzi používateľmi (U2U): platforma alebo služba, ktorá umožňuje používateľom vytvárať obsah a/alebo ho zdieľať s inými používateľmi.

Služba sociálnych médií: online služba alebo platforma, ktorej hlavným účelom je umožňovať sociálnu interakciu online medzi koncovými používateľmi. To môže zahŕňať služby, ktoré umožňujú používateľom vzájomne komunikovať, zverejňovať alebo vytvárať materiály, alebo prezeráť si materiály zverejnené alebo vytvorené inými používateľmi.

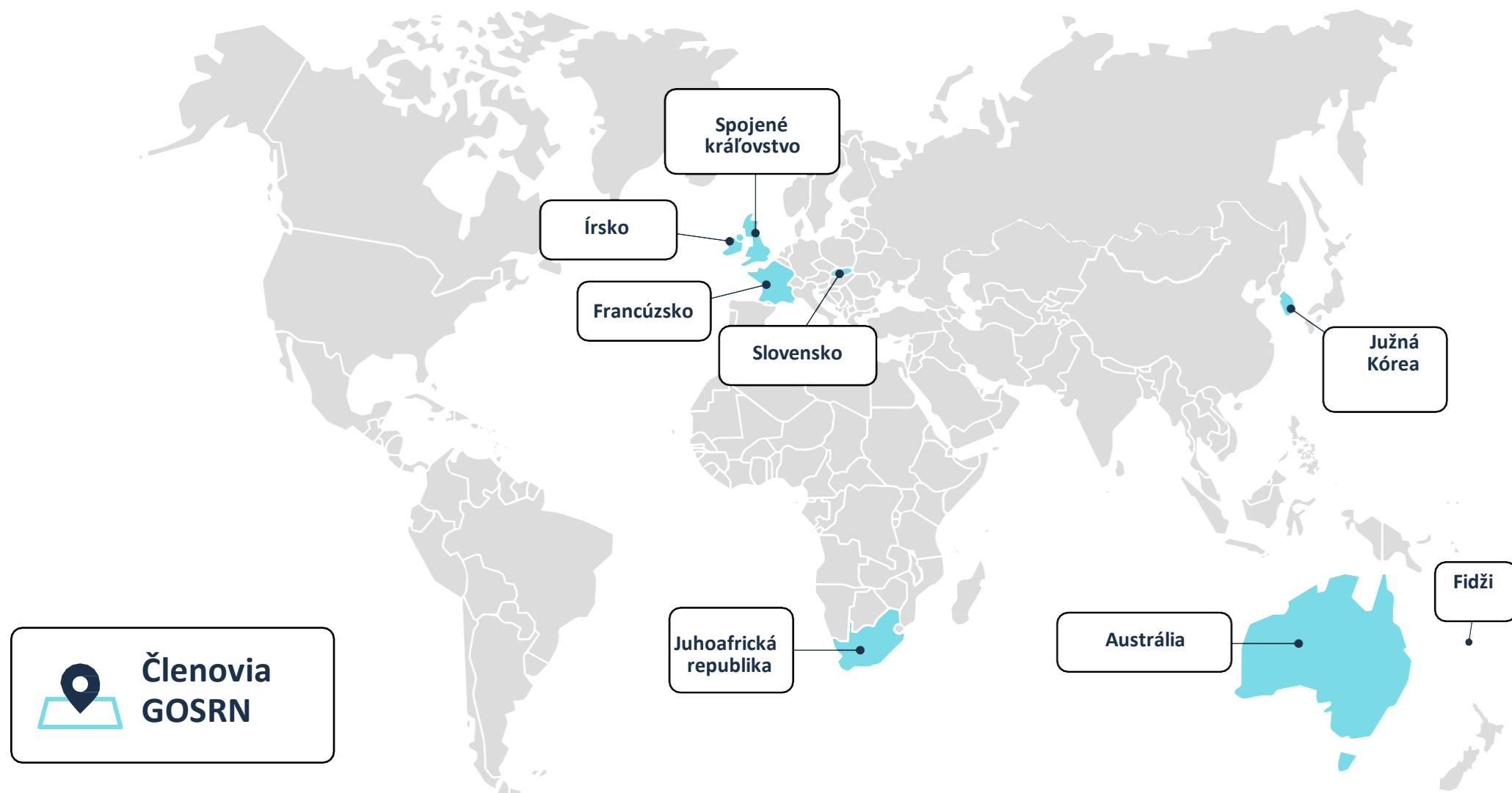
Šifrovanie medzi koncovými zariadeniami (EE2E): metóda zabezpečenej komunikácie, ktorá umožňuje čítať vymieňané správy, obrázky alebo súbory len osobám, ktoré spolu komunikujú.

Škodlivý algoritmickej vzor: vzor odporúčaného obsahu poskytovaného koncovému používateľovi odporúčacím systémom, ktorý by súhrnne mohol viesť k závažnej ujme (napr. k radikalizácii, poruchám príjmu potravy, sebaopoškodzovaniu atď.).

Škodlivý pre mládež: obsah, ktorý môže byť škodlivý pre fyzické alebo psychické zdravie alebo vývoj detí alebo mladých ľudí, ako napríklad pornografia alebo násilie s veľkým dopadom (označovaný aj ako vekovo nevhodný obsah a „obmedzený obsah“) (terminológia Kórejskej republiky).



Prehľady o jurisdikciách



Aktualizované: október 2024



Austrália: eSafety Commissioner (Komisár pre elektronickú bezpečnosť, eSafety)



Komisár pre elektronickú bezpečnosť (eSafety) je austrálsky regulačný orgán pre bezpečnosť online. Komisár je nezávislý zákonný orgán, ktorý je poverený chrániť všetkých Austráľčanov pred ujmom v online priestore a podporovať bezpečnejšie a pozitívnejšie skúsenosti online. Uplatňuje si právomoci podľa zákona o bezpečnosti online z roku 2021, ako aj podľa oddielov zákona o telekomunikáciách z roku 1997 a trestného zákonníka z roku 1995.

Komisár pre elektronickú bezpečnosť sa zameriava na **ochranu, prevenciu a proaktívne a systémové zmeny**. Patrí sem správa systémov na podávanie sťažností od používateľov a vyšetrovacích systémov, spolupráca s odvetvím v oblasti systémovej regulácie a podpora bezpečnosti online prostredníctvom vzdelávania a výskumu, ako aj domáca a medzinárodná koordinácia a činnosť. Austrália uplatňuje **hybridný regulačný prístup**, ktorý sa zameriava na škodlivý materiál na úrovni používateľov a systémov. Používatelia majú možnosť nahlasovať škodlivý materiál, s ktorým sa stretnú, v rámci štyroch systémov eSafety pre riziká: kyberšikana detí, kybernetické zneužívanie dospelých, zneužívanie prostredníctvom obrázkov vrátane nedobrovoľného zdieľania intímnych záberov a nezákonného a obmedzeného obsahu (ako napríklad materiál zobrazujúci sexuálne zneužívanie detí, obsah o terorizme a násilnom extrémizme a trestná činnosť). Komisár pre elektronickú bezpečnosť spolupracuje s používateľmi a platformami na odstraňovaní alebo blokovaní takéhoto materiálu. Takisto má právomoc reagovať na ohavný násilný materiál, ktorý zahŕňa neprístupný materiál vytvorený osobou, ktorá sa dopúšťa teroristického činu alebo iného ohavného násilného konania, ako sú vražda, mučenie, znásilnenie a únos, alebo sa o to pokúša.

Systémová regulácia orgánu vychádza z dvoch rámcov: kódexov a noriem odvetvia a základných očakávaní v oblasti bezpečnosti online (ďalej len „Očakávania“). Po ich zavedení budú všetky kódexy a normy odvetvia upravovať, ako má online odvetvie narábať s nezákonným obsahom (napr. s materiálom zobrazujúcim sexuálne zneužívanie detí a obsahom o terorizme a násilnom extrémizme) a s obmedzeným obsahom (vekovo nevhodný obsah, ako napr. pornografia alebo násilie s veľkým dopadom)¹. V dokumente Očakávania sa uvádzajú očakávania v oblasti bezpečnosti online od služieb sociálnych médií, služieb zasielania správ a komunikačných služieb vrátane herných a zoznamovacích aplikácií a iných internetových služieb, ako sú služby na zdieľanie súborov a webové stránky. Komisár môže využívať právomoci v oblasti transparentnosti stanovené v zákone o bezpečnosti online a požiadať poskytovateľov týchto online služieb, aby podali správu o tom, ako plnia tieto očakávania.

Riadiace akty a právne predpisy: [zákon o bezpečnosti online z roku 2021](#), [Základné očakávania v oblasti bezpečnosti online](#), [Kódexy a normy odvetvia](#)

Webové sídlo: [eSafety Commissioner](#)

Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none">· Vybavovanie sťažností používateľov· Vzdelávanie a zvyšovanie informovanosti· Vypracúvanie, schvaľovanie a presadzovanie odvetvových predpisov (kódexov a noriem)· Právomoci v oblasti transparentnosti· Monitorovanie dodržiavania odvetvových predpisov· Výskum· Mapovanie situácie	<ul style="list-style-type: none">· Kyberšikana detí· Kybernetické zneužívanie dospelých· Zneužívanie prostredníctvom obrázkov· Nezákonný obsah: zahŕňa materiál zobrazujúci sexuálne vykorisťovanie detí, proteroristický materiál· Obmedzený obsah/vekovo nevhodný obsah	<ul style="list-style-type: none">· Poskytovatelia služieb sociálnych médií· Poskytovatelia dôležitých elektronických služieb (RES) vrátane služieb zasielania správ a zoznamovacích aplikácií· Poskytovatelia určených internetových služieb (DIS) vrátane služieb zdieľania súborov, webových služieb atď.· Poskytovatelia hostingových služieb· Poskytovatelia internetových služieb· Poskytovatelia služieb v oblasti vybavenia· Poskytovatelia služieb vyhľadávačov· Poskytovatelia distribúcie aplikácií	<ul style="list-style-type: none">· Oznámenia pre koncových používateľov· Vykonateľné právne záväzky· Oznámenia o porušení predpisov· Odstraňovanie obsahu, blokovanie a vymazávanie odkazov· Vyšetovania· Zber informácií· Formálne varovania· Opravné prostriedky nariadené súdom (napr. súdne zákazy a občianskoprávne sankcie)· Oznámenia poskytovateľom služieb

¹V zákone o online bezpečnosti z roku 2021 (C) sa stanovuje, že existuje osem samostatných sekcií online odvetvia. Komisár pre elektronickú bezpečnosť je oprávnený schvaľovať odvetvové kódexy a normy pre každú z týchto ôsmich sekcií. Viac informácií nájdete [tu](#).

Fidži: Online Safety Commission

Komisia pre bezpečnosť online (Online Safety Commission, OSC) je nezávislý fidžijský regulačný orgán pre bezpečnosť online. Zákon o bezpečnosti online z roku 2018 prijal parlament Fidžijskej republiky s cieľom zriadiť Komisiu pre bezpečnosť online na podporu bezpečnosti online, odrádzania od škodlivej elektronickej komunikácie a ďalších súvisiacich záležitostí. Komisia začala svoju činnosť v roku 2019 s cieľom poskytovať pomoc osobám, ktoré sa stretávajú so škodlivým obsahom online, a poskytovať služby a zdroje, ktoré pomáhajú minimalizovať škody a zabezpečujú digitálnu gramotnosť, vzdelávanie a informovanosť. To zahŕňa informovanie fidžijských používateľov internetu o rôznych súčasných a nových digitálnych platformách a o spôsoboch, ako zostať v bezpečí v online priestore.

Komisia prevádzkuje systém na podávanie sťažností od používateľov, ktorý umožňuje používateľom nahlasovať škodlivý obsah, s ktorým sa stretnú na internete, alebo ujmu, ktorá im alebo inej osobe bola spôsobená na internete, ako je napríklad zdieľanie intímnych záberov bez súhlasu používateľa. Komisia následne spolupracuje s digitálnymi službami a platformami na odstránení alebo zablokovaní takéhoto obsahu. Systémy ani procesy digitálnych služieb a platforiem Komisia v súčasnosti nereguluje.



Riadiace akty a právne predpisy:

[zákon o bezpečnosti online z roku 2018,](#)
[nariadenie o bezpečnosti online z roku 2019](#)

Webové sídlo: [Online Safety Commission](#)

Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none">· Vybavovanie sťažností používateľov· Vzdelávanie a zvyšovanie informovanosti· Prijímanie, posudzovanie a vyšetrovanie záležitostí· Mapovanie situácie	<ul style="list-style-type: none">· Kyberšikana detí· Zneužívanie dospelých· Zneužívanie prostredníctvom obrázkov· Nezákonný obsah: zahŕňa materiál zobrazujúci sexuálne vykorisťovanie detí, proteroristický materiál· Obmedzený obsah	<ul style="list-style-type: none">· Všetky platformy a služby fungujúce na Fidži, ktoré umožňujú „elektronickú komunikáciu“· „Elektronická komunikácia“ sa vymedzuje ako akákoľvek forma komunikácie, ktorá sa šíri elektronicou pomocou textu, písma, fotografie, obrázku, nahrávky alebo akýmkoľvek iným spôsobom.	<ul style="list-style-type: none">· Príkazy na odstránenie a blokovanie obsahu· Finančné pokuty· Vyšetrovacie právomoci· Zber informácií· Oznámenia o odstránení obsahu



Francúzsko: Arcom



Arcom je francúzsky nezávislý verejný orgán pre reguláciu audiovizuálnej a digitálnej komunikácie. Do pôsobnosti orgánu Arcom patrí množstvo oblastí, napríklad správa frekvenčného spektra, vysielanie, platformy na zdieľanie videí a bezpečnosť online. V týchto oblastiach spočíva poslanie Arcomu v technickej, hospodárskej a právnej regulácii sektora s cieľom chrániť slobodnú komunikáciu vo verejnom záujme.

Orgán zabezpečuje ochranu audiovizuálnych diel, bojuje proti pirátstvu kultúrneho a športového obsahu a podporuje rozvoj legálnych ponúk. Okrem toho vydáva povolenia vysielacím službám (televízne a rozhlasové kanály), čím zabezpečuje pluralitu a hospodársku rovnováhu v odvetví, a zodpovedá za reguláciu služieb na požiadanie. Zabezpečuje, aby ich programy boli v súlade s predpismi o ochrane maloletých osôb, zaobchádzaní s informáciami, organizácii volebných kampaní, reklame a zastúpení všetkých rozmanitých zložiek spoločnosti.

Okrem funkcií spojených s reguláciou vysielania vo Francúzsku má Arcom na starosti dohľad nad systémovým prístupom regulačného rámca pre otázky bezpečnosti online, ktorý sa v rámci revidovanej smernice o AVMS týka platforiem na zdieľanie videí a v rámci DSA kategórií sprostredkovateľských služieb (ako sú prostý prenos, caching a hostingové služby či online platformy), ktoré sídlia vo Francúzsku.

Arcom bude ako koordinátor digitálnych služieb zodpovedný za zabezpečenie koordinácie na vnútroštátnej úrovni a za dohľad nad presadzovaním DSA spolu s ostatnými príslušnými orgánmi. V rámci DSA musia sprostredkovateľské služby zaviesť nástroje a prostriedky zamerané na boj proti nezákonnému a škodlivému obsahu v záujme ochrany verejnosti vo všeobecnosti a najmä maloletých osôb, ako sú mechanizmy na nahlasovanie a oznamovanie porušení. Od online platforiem sa takisto vyžaduje, aby používateľom poskytovali možnosť voľby, a podliehajú napríklad požiadavkám v oblasti transparentnosti. Na osobitné povinnosti spojené so systémovými rizikami na veľmi veľkých platformách (a veľmi veľkých vyhľadávačoch) dohliada v Európskej únii výlučne Európska komisia (posudzovanie rizík a opatrenia na ich zmiernenie) v spolupráci s Arcomom a ďalšími príslušnými orgánmi na vnútroštátnej úrovni.

Pokiaľ ide konkrétne o platformy na zdieľanie videí, v smernici o AVMS prijatej v roku 2010 a revidovanej v roku 2018 sa stanovujú povinnosti chrániť najmä maloletých „pred programami, videami vytvorenými používateľmi a audiovizuálnymi komerčnými oznamami, ktoré by mohli narušiť ich telesný, duševný alebo morálny vývin“. V tejto súvislosti je Arcom zodpovedný za podporu vytvárania kódexov etického správania zo strany platforiem na zdieľanie videí. Napokon je Arcom zodpovedný za dohľad nad povinnosťami vyplývajúcimi zo systémového prístupu nariadenia o riešení šírenia teroristického obsahu online s cieľom zabezpečiť, aby platformy účinne zavádzali nástroje a procesy zamerané najmä na boj proti teroristickému obsahu v rámci svojich služieb.

Riadiace akty a právne predpisy:

[zákon č. 86-1067 z 30. septembra 1986 o slobodnej komunikácii](#); [zákon z 21. júna 2004 na podporu dôvery v digitálne hospodárstvo](#); [smernica 2010/13/EÚ o audiovizuálnych mediálnych službách \(smernica o AVMS\) z 10. marca \(zmenená smernicou 2018/1808 zo 14. novembra 2018\)](#); [nariadenie o riešení šírenia teroristického obsahu online](#); [nariadenie \(EÚ\) 2022/2065 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES \(akt o digitálnych službách\), ktorým sa mení a dopĺňa smernica o elektronickom obchode \(2000/31/ES\)](#)

Webové sídlo: [Arcom](#)

Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none">· Vzdelávanie a zvyšovanie informovanosti· Vypracúvanie, schvaľovanie a presadzovanie odvetvových predpisov (kódexov a usmernení)· Monitorovanie a dohľad nad dodržiavaním odvetvových predpisov· Výskum· Mapovanie situácie	<ul style="list-style-type: none">· Nezákonný obsah (ktorého šírenie je podľa vnútroštátnych právnych predpisov a právnych predpisov EÚ trestným činom)· Škodlivý obsah: dezinformácie, propagácia porúch príjmu potravy· Ochrana maloletých:<ul style="list-style-type: none">- obsah, ktorý by mohol poškodiť ich telesný, duševný alebo morálny vývin- vekovo nevhodný obsah (prístup na pornografické stránky)- komerčné využívanie obrázkov detí mladších ako šestnásť rokov na online platformách· Pirátstvo	<ul style="list-style-type: none">· Sprostredkovateľské služby: služby prostého prenosu, cachingové a hostingové služby, platformy a služby medzi používateľmi a služby vyhľadávačov· Platformy a služby na zdieľanie videí	<ul style="list-style-type: none">· Vyšetrowania· Zber informácií· Formálne varovania· Finančné pokuty· Požiadanie sudcu o dočasné obmedzenie prístupu na platformu



Írsko: Coimisiún na Meán (An Coimisiún)

Coimisiún na Meán je írská agentúra pre rozvoj a reguláciu prosperujúceho, rozmanitého, kreatívneho, bezpečného a dôveryhodného mediálneho prostredia. Zodpovedá za:

- dohľad nad financovaním a podporu rozvoja širšieho mediálneho sektora v Írsku,
- dohľad nad reguláciou vysielania a videoslужieb na požiadanie,
- rozvoj a presadzovanie írskeho regulačného režimu pre bezpečnosť online (rámec pre bezpečnosť online).

Rámcem pre bezpečnosť online pozostáva z troch právnych predpisov:

- akt o digitálnych službách EÚ (DSA), v zmysle ktorého je Coimisiún na Meán od 17. februára 2024 príslušným orgánom,
- kódex bezpečnosti online, ktorý vychádza zo zákona o bezpečnosti online a regulácii médií. Kódex bude prijatý a uplatňovaný od jesene 2024,
- nariadenie o riešení šírenia teroristického obsahu online, v zmysle ktorého je Coimisiún na Meán od novembra 2023 príslušným orgánom.

Na základe rámca pre bezpečnosť online má komisia k dispozícii nástroje na riešenie základných príčin rizík na internete vrátane dostupnosti nezákonného obsahu, škodlivých vplyvov odporúčacích systémov a nedostatočnej ochrany detí v rámci služieb sociálnych médií. Dohliada na to, ako platformy dodržiavajú svoje povinnosti v oblasti bezpečnosti online na systémovej úrovni, a úzko spolupracuje s Európskou komisiou a svojimi náprotivkami v oblasti regulácie v celej Európe aj mimo nej. Okrem toho uskutočňuje výskum v oblastiach, ktoré patria do jej pôsobnosti, a realizuje programy mediálnej gramotnosti a vzdelávania používateľov s cieľom umožniť ľuďom kriticky pristupovať k médiám, ktoré využívajú, a porozumieť im. Coimisiún na Meán prevádzkuje aj poradenské centrum, ktoré ľudí informuje o ich právach podľa rámca a problémy postupuje oddeleniu pre sťažnosti na účely prípadných následných opatrení formou dohľadu alebo vyšetrovania.



Riadiace akty a právne predpisy:

[zákon o vysielaní z roku 2009](#) v znení zmenenom a doplnenom [zákonom o regulácii bezpečnosti a médií online z roku 2022](#); [smernica 2010/13/EÚ o audiovizuálnych mediálnych službách z roku 2018](#); [nariadenie o riešení šírenia teroristického obsahu online](#); [nariadenie o digitálnych službách \(DSA\)](#); [Stratégia dodržiavania predpisov v oblasti elektronického obchodu](#); [Register platforiem na zdieľanie videí](#); [Kódex pre bezpečnosť online](#)

Webové sídlo: [Coimisiún na Meán](#)

Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none">· Vzdelávanie a zvyšovanie informovanosti· Vypracúvanie, schvaľovanie a presadzovanie odvetvových predpisov (kódexov a usmernení)· Monitorovanie a dohľad nad dodržiavaním odvetvových predpisov· Výskum· Mapovanie situácie	<ul style="list-style-type: none">· Nezákonný obsah· Materiál zobrazujúci sexuálne zneužívanie detí· Terorizmus· Škodlivý obsah vrátane pornografie a extrémneho alebo bezdôvodného násillia· Propagácia sebapoškodzovania alebo samovraždy· Propagácia porúch príjmu potravy alebo krmenia· Kyberšikana· Nebezpečné výzvy· Podnecovanie k nenávisti alebo násilliu na základe chránených charakteristík vrátane rasizmu a xenofóbie· Škodlivé alebo nezákonné obchodné oznámenia	<ul style="list-style-type: none">· Platformy a služby na zdieľanie videí· Sprostredkovateľské služby: služby prostého prenosu, cachingové a hostingové služby, platformy a služby, ako aj a služby vyhľadávačov· Poskytovatelia hostingových služieb vystavení teroristickému obsahu online	<ul style="list-style-type: none">· Vyšetrovania· Finančné pokuty· Audity· Oznámenia o obmedzení obsahu· Príkazy na zablokovanie prístupu· Oznámenia o porušení predpisov· Právomoci v trestnoprávnej oblasti



Kórejská republika: Korea Communications Standards Commission



Kórejská komisia pre komunikačné normy (Korea Communications Standards Commission, KCSC) je nezávislý zákonný orgán zodpovedný za reguláciu mediálneho obsahu v Kórejskej republike. Bola zriadená v roku 2008 na základe zákona o zriadení a činnosti Kórejskej komisie pre komunikáciu a vznikla zlúčením Kórejskej komisie pre bezpečnosť online a regulačného úradu Kórejskej komisie pre vysielanie.

KCSC sa skladá z deviatich komisárov, ktorých vymenúva kórejský prezident. V článku 18 (Zriadenie KCSC atď.) uvedeného zákona sa stanovuje proces vymenovania, v rámci ktorého troch komisárov vymenúva predseda Národného zhromaždenia po konzultácii so zástupcami každej rokovej strany a troch komisárov vymenúvajú stále výbory Národného zhromaždenia. Každý z týchto komisárov má trojročné funkčné obdobie s možnosťou jedného znovuzvolenia. Traja komisári vrátane predsedu, ktorý je volený spomedzi deviatich členov komisie, sú stálymi komisármi. Sekretariát sa skladá z generálneho tajomníka, dvoch úradov (Úrad pre audit, Úrad pre plánovanie a koordináciu), štyroch kancelárií (Kancelária pre kontrolu vysielaného obsahu, Kancelária pre kontrolu obsahu online komunikácie, Kancelária pre ochranu práv, Kancelária pre kontrolu obsahu digitálnej sexuálnej trestnej činnosti), jednej skupiny (Skupina pre medzinárodnú spoluprácu), jedného centra (Centrum pre politický výskum), dvadsiatich siedmich oddelení a piatich regionálnych kancelárií v mestách Pusan, Gwangju, Daegu, Daejeon a Gangwon-do. K dnešnému dňu KCSC zamestnáva 204 zamestnancov.

Povinnosti KCSC v zmysle článku 21 (Povinnosti Kórejskej komisie pre komunikačné normy) uvedeného zákona zahŕňajú kontrolu obsahu televízneho vysielania, televíznych reklám a internetovej komunikácie. S cieľom reagovať na rýchlo sa vyvíjajúce mediálne prostredie a posilňovať systém kontroly a príslušný regulačný rámec KCSC stanovuje, vyhlasuje a mení svoje zásady kontroly a normy vzťahujúce sa na obsah. KCSC sa tiež venuje výskumu, podporuje verejné kampane a organizuje vzdelávacie programy a semináre na zvyšovanie mediálnej gramotnosti a etiky. Po novele z júna 2021 prevzala KCSC ďalšiu úlohu, ktorou je medzinárodná spolupráca s cieľom kultivovať bezpečné online prostredie, ktoré je zdravé a dôveryhodné pre verejnosť, v spolupráci s jej náprotivkami z celého sveta.

S cieľom maximalizovať efektívnosť činnosti KCSC organizuje rôzne zasadnutia vrátane stálej komisie, generálneho zasadnutia, štyroch čiastkových komisií, piatich osobitných poradných výborov, výboru pre mediáciu sporov o urážku na cti a výboru pre kontrolu vysielania s volebným obsahom.

Riadiace akty a právne predpisy:

[zákon o zriadení a činnosti Kórejskej komisie pre komunikácie](#); [zákon o podpore informácií a komunikácií, využívaní sietí a ochrane informácií](#); [zákon o podnikaní v oblasti telekomunikácií](#)

Webové sídlo: [Korea Communications and Standards Commission](#)

Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none"> Vzdelávanie a zvyšovanie informovanosti Vypracúvanie, schvaľovanie a presadzovanie odvetvových predpisov (kódexov a usmernení) Monitorovanie a dohľad nad dodržiavaním odvetvových predpisov Výskum Mapovanie situácie 	<ul style="list-style-type: none"> Riziká nezákonného charakteru: okrem iného hazardné hry, narušenie súkromia, nezákonné finančné aktivity, podvody, nezákonný predaj potravín, drog a omamných látok, obchodovanie so spermiami, s vajíčkami a orgánmi, porušovanie zákona o národnej bezpečnosti, proteroristický obsah, pornografia, materiál zobrazujúci sexuálne zneužívanie detí, materiál zobrazujúci sexuálne vykorisťovanie detí, zdieľanie intímnych záberov bez súhlasu používateľa, obchodovanie s ľuďmi a iný obsah, ktorý porušuje právny poriadok Obsah, ktorý je legálny, ale škodlivý pre deti: okrem iného obsah, ktorý propaguje poruchy príjmu potravy, krutý alebo nenávisťný obsah, obsah, ktorý diskriminuje alebo znevažuje určité skupiny, obsah, ktorý spôsobuje občianske nepokoje, a nezákonný alebo škodlivý obsah v rámci webového vysielania Ohováranie a narušenie súkromia: okrem iného ohováranie, zásah do súkromia a osobných slobôd, porušenie práv na zobrazenie 	<ul style="list-style-type: none"> Poskytovatelia informačných a komunikačných služieb označujú subjekty, ktoré buď pôsobia ako prevádzkovatelia telekomunikačných podnikov, alebo využívajú služby týchto prevádzkovateľov na poskytovanie alebo sprostredkovanie obsahu za účelom zisku. Patria sem platformy a služby, ktoré poskytujú obsah verejnosti alebo pôsobia ako sprostredkovatelia pri distribúcii obsahu prostredníctvom telekomunikačných sietí. Správcovia a prevádzkovatelia internetových nástieniek 	<ul style="list-style-type: none"> Odstraňovanie obsahu Blokovanie prístupu Zrušenie/dočasné zablokovanie používateľského konta Finančné pokuty Vyšetrovania Žiadosti o informácie Oznámenia o porušení predpisov Oznámenia pre koncových používateľov Oznámenia poskytovateľom služieb/platformám



Slovensko: Rada pre mediálne služby



Rada pre mediálne služby (RpMS) je slovenský nezávislý orgán pre reguláciu médií zodpovedný za dohľad nad médiami a presadzovanie regulačných rámcov týkajúcich sa vysielania, retransmisie, poskytovania audiovizuálnych mediálnych služieb na požiadanie a digitálnych platforiem. Poslaním RpMS je chrániť verejnosť v online priestore, ako aj presadzovať verejný záujem pri uplatňovaní práva na informácie, slobody prejavu a práva na prístup ku kultúrnym hodnotám a k vzdelaniu. RpMS je popredným členom Skupiny európskych regulačných orgánov pre audiovizuálne mediálne služby (ERGA), Európskej platformy regulačných orgánov (EPRA) a Výboru pre DSA.

RpMS bola zriadená v roku 2022 zákonom o mediálnych službách (ZMS), pričom nahradila Radu pre vysielanie a retransmisiu, národný regulačný orgán dohliadajúci predovšetkým na lineárny mediálny trh. Vzhľadom na legislatívny vývoj na úrovni EÚ sa zákonom o mediálnych službách transponovala smernica o audiovizuálnych mediálnych službách (smernica o AVMS), vykonalo sa nariadenie o riešení šírenia teroristického obsahu online a začali sa prípravy na prijatie aktu o digitálnych službách (DSA).

RpMS tradične dohliada na zakladanie (napr. povolenie, registrácia, vydávanie licencií) a správanie sa vysielateľov na Slovensku. Zákomom o mediálnych službách sa však zaviedli nové povinnosti, konkrétne požiadavky týkajúce sa poskytovania a správania sa v rámci audiovizuálnych mediálnych služieb (vrátane vlogerov), európskych diel, nezávislej produkcie a posudzovania opatrení prijatých platformami na zdieľanie videí v záujme ochrany verejnosti. Vzhľadom na uvedené skutočnosti ZMS splnomocňuje RpMS aj na riešenie bezpečnostných rizík online vyplývajúcich z fungovania a návrhu online platforiem.

V rámci svojej pôsobnosti v oblasti bezpečnosti online má RpMS za úlohu dohliadať na účinnosť a primeranosť presadzovania podmienok poskytovania služieb online platforiem, ktoré ponúkajú svoje služby na Slovensku. Okrem toho má RpMS zákonnú právomoc bojovať proti šíreniu nezákonného obsahu online vydávaním príkazov na odstránenie obsahu, ktorý porušuje článok 151 ZMS. RpMS sa venuje aj výskumu, mediálnej gramotnosti a medzinárodnej spolupráci.

Ako koordinátor digitálnych služieb je RpMS zodpovedná za všetky ustanovenia DSA, a teda dohliada na správanie a fungovanie online platforiem sídlících na Slovensku.

Riadiace akty a právne predpisy:
[zákon o mediálnych službách \(ZMS\);](#)
[smernica 2010/13/EÚ o audiovizuálnych mediálnych službách \(smernica o AVMS\) z 10. marca \(zmenená smernicou 2018/1808 zo 14. novembra 2018\);](#)
[nariadenie 2021/784 z 29. apríla 2021 o riešení šírenia teroristického obsahu online;](#)
[nariadenie 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami \(akt o digitálnych službách, DSA\), ktorým sa mení a dopĺňa smernica o elektronickom obchode \(2000/31/ES\)](#)

Webové sídlo: [Rada pre mediálne služby](#)

Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none"> • Vybavovanie sťažností používateľov • Vypracúvanie, schvaľovanie a presadzovanie odvetvových predpisov (mechanizmy sebaregulácie/spoluregulácie na základe kódexov a usmernení) • Monitorovanie a dohľad nad dodržiavaním odvetvových predpisov • Výskum • Vzdelávanie a zvyšovanie informovanosti • Mapovanie situácie 	<ul style="list-style-type: none"> • Nezákonný obsah (obsah zobrazujúci sexuálne vykorisťovanie detí alebo extrémizmus; obsah podnecujúci k násiliu alebo obsah zahŕňajúci teroristické činy; obsah schvaľujúci alebo propagujúci teroristické činy; obsah, ktorý popiera alebo schvaľuje holokaust, zločiny politických režimov a zločiny proti ľudskosti, obsah predstavujúci hanobenie národa, rasy a presvedčenia alebo podnecovanie k národnostnej, rasovej a etnickej nenávisti) • Ochrana maloletých • Škodlivý obsah, na ktorý sa vzťahujú podmienky používania platforiem (dezinformácie, podvody atď.) 	<ul style="list-style-type: none"> • Poskytovatelia audiovizuálnych mediálnych služieb • Sprostredkovateľské služby: prostý prenos, caching, hosting, platformy, trhoviská, vyhľadávače • Platformy na zdieľanie videí 	<ul style="list-style-type: none"> • Vyšetrenia • Kontroly a rozhovory na mieste • Žiadosti o informácie • Formálne varovania • Príkazy na odstránenie obsahu • Opravné prostriedky nariadené súdom • Finančné pokuty • Žiadosti o prijatie akčného plánu



Juhoafrická republika: Film and Publications Board

Rada pre film a publikácie (Film and Publications Board, FPB) je štátny subjekt zriadený na základe zákona o filmoch a publikáciách z roku 1996 v znení neskorších predpisov. FPB má široké právomoci a reguluje tvorbu, vlastníctvo a distribúciu filmov, hier, určitých publikácií a digitálneho obsahu na platformách a službách. Cieľom tejto regulácie je chrániť deti pred rušivým a škodlivým obsahom a poskytovať dospelým informácie o obsahu, ktoré im umožnia informovane sa rozhodovať pri čítaní, sledovaní a hraní hier vo svojom záujme aj v záujme detí, ktoré majú v opatere.

Juhoafrická republika uplatňuje **hybridný prístup** k regulácii bezpečnosti online, pričom vypracovala odvetvové kódexy postupov a využíva systém na podávanie sťažností používateľov. FPB je na základe zákona o filmoch a publikáciách oprávnená vydávať všeobecne platné smernice. Okrem toho vypracovala poradný odvetvový kódex pre prevenciu ujmy v online priestore. Prostredníctvom systému rady na podávanie sťažností používateľov môžu používatelia nahlasovať škodlivý obsah, ako sú materiál zobrazujúci sexuálne zneužívanie detí, tvorba a šírenie filmov a fotografií zobrazujúcich násilie páchané na deťoch, nenávistné prejavy, šírenie súkromných sexuálnych fotografií a filmov, podnecovanie k bezprostrednému násiliu a vojnová propaganda.



Riadiace akty a právne predpisy:

[zákon č. 65 o filmoch a publikáciách z roku 1996](#); [nariadenia, ktorými sa mení zákon o filmoch a publikáciách z roku 2022](#)

Webové sídlo: [Film and Publication Board](#)

Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none">· Vzdelávanie a zvyšovanie informovanosti· Vypracúvanie odvetvových právnych predpisov a usmernení· Monitorovanie a dohľad nad dodržiavaním odvetvových predpisov· Výskum· Mapovanie situácie	<ul style="list-style-type: none">· Materiál zobrazujúci sexuálne zneužívanie detí· Tvorba a šírenie filmov a fotografií zobrazujúcich sexuálne násilie a násilie páchané na deťoch· Neklasifikovaný obsah· Škodlivý a zakázaný obsah· Nenávistné prejavy online· Vojnová propaganda· Podnecovanie k bezprostrednému násiliu· Šírenie súkromných sexuálnych fotografií a filmov	<ul style="list-style-type: none">· Komerční distribútori filmov, hier a určitých publikácií online· Platformy a služby na zdieľanie videí· Platformy a služby medzi používateľmi· Služby vyhľadávačov· Poskytovatelia internetových služieb a služieb prístupu k internetu	<ul style="list-style-type: none">· Vyšetrenia· Oznámenia o porušení predpisov· Oznámenia o odstránení obsahu· Rozhodnutia o nedodržaní predpisov prijímané výborom pre presadzovanie predpisov s právomocou ukladať pokuty· Postúpenie na trestné stíhanie



Spojené kráľovstvo: Ofcom

Ofcom je britský regulačný orgán pre komunikácie. Do pôsobnosti Ofcomu patrí celý súbor oblastí vrátane frekvenčného spektra, pošty, telekomunikačných sietí, vysielania, platforiem na zdieľanie videí a bezpečnosti online. Po prijatí zákona o online bezpečnosti v októbri 2023 prevzal Ofcom rozsiahlejšie povinnosti v oblasti bezpečnosti online vrátane regulácie služieb medzi používateľmi a vyhľadávacích služieb, ku ktorým majú prístup používatelia v Spojenom kráľovstve.

Spojené kráľovstvo prijalo **systemový a procesný prístup** k regulácii bezpečnosti online na základe zákona o bezpečnosti online, v zmysle ktorého sa od služieb bude vyžadovať, aby vykonávali posudzovanie rizík a prijímali záruky týkajúce sa obsahu. Niektoré služby budú podliehať ďalším povinnostiam vrátane povinnej možnosti výberu pre používateľov a zverejňovania správ o transparentnosti. Ofcom uplatňuje postupný prístup k vykonávaniu predpisov a do druhého polroka 2026 plánuje vypracovať a dokončiť kódexy postupov a usmernenia, v ktorých uvedie odporúčania, ako môžu služby plniť svoje povinnosti vyplývajúce zo zákona o bezpečnosti online. Ofcom okrem toho uskutočňuje výskum v oblasti bezpečnosti online a zabezpečuje vzdelávanie a zvyšovanie informovanosti v oblasti mediálnej gramotnosti.



Riadiace akty a právne predpisy:

[zákon o bezpečnosti online z roku 2023](#)

Webové sídlo: [Ofcom](#)

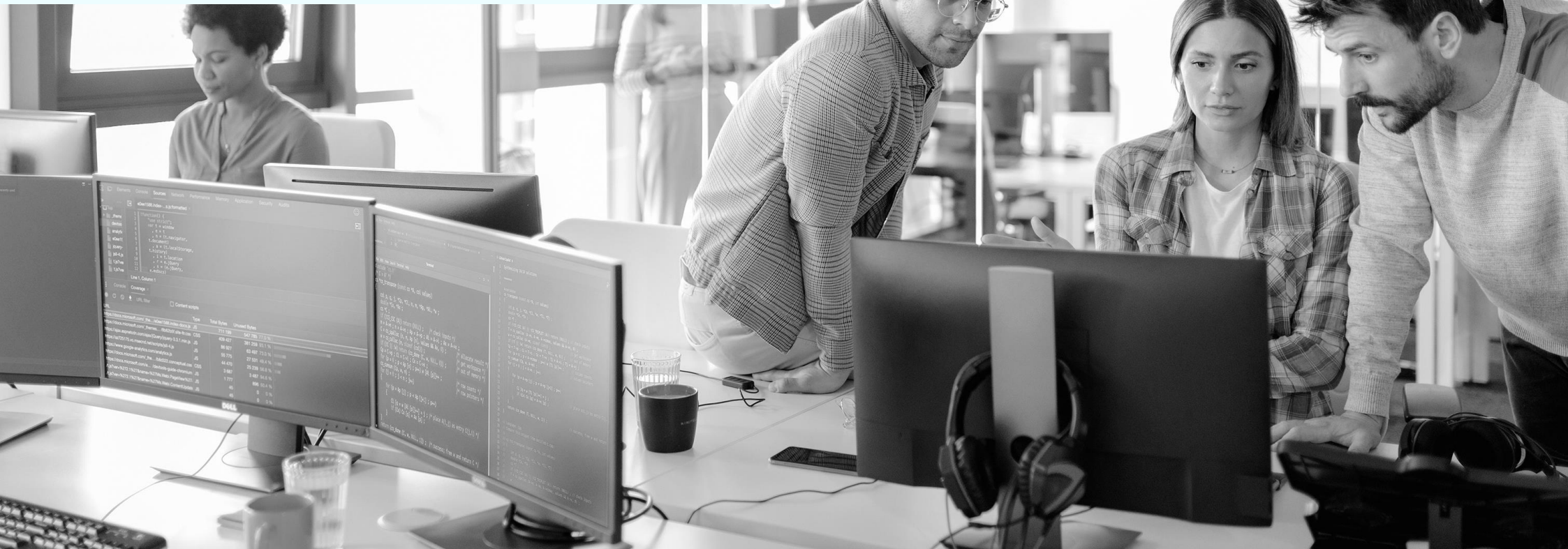
Prehľad regulačných právomocí v oblasti bezpečnosti online

Právomoci a funkcie	Regulované riziká	Regulované subjekty	Právomoci v oblasti presadzovania
<ul style="list-style-type: none">· Plnenie zákonných povinností· Vypracúvanie nezáväzných odvetvových predpisov (kódexov a usmernení)· Monitorovanie a dohľad nad dodržiavaním odvetvových predpisov· Výskum· Mapovanie situácie· Vzdelávanie a zvyšovanie informovanosti	<ul style="list-style-type: none">· Nezákonný obsah (okrem iného materiál zobrazujúci sexuálne zneužívanie detí, terorizmus, podvody, trestné činy spojené s drogami a obchodovanie s ľuďmi)· Obsah, ktorý je legálny, ale škodlivý pre deti (napríklad pornografia, propagácia sebapoškodzovania, samovraždy a porúch príjmu potraviny, obsah zobrazujúci šikanovanie atď.)	<ul style="list-style-type: none">· Platformy a služby medzi používateľmi· Služby vyhľadávačov· Poskytovatelia uverejňujúci pornografický obsah	<ul style="list-style-type: none">· Vyšetrowania· Zber informácií· Opravné prostriedky nariadené súdom (napr. opatrenia na prerušenie činnosti a súdne príkazy)· Finančné pokuty· Trestné sankcie



Regulačné analýzy

- Regulačné právomoci v oblasti bezpečnosti online
- Druhy ujmy v online priestore
- Regulované subjekty
- Povinnosti regulovaných subjektov
- Zber informácií a presadzovanie pravidiel



Regulačné právomoci v oblasti bezpečnosti online

Medzi regulačnými právomocami a funkciami regulačných orgánov existujú podobnosti. Regulačné právomoci a funkcie sa zvyčajne líšia v závislosti od základného prístupu, konkrétne od toho, či sa v danej jurisdikcii uplatňuje **obsahový, systémový** alebo **hybridný prístup**. Regulačné modely založené na obsahu sa usilujú riešiť škodlivý obsah tak, že používateľom, ktorí sa stretli so škodlivým obsahom alebo s ním majú skúsenosť, umožňujú podať sťažnosť alebo dosiahnuť nápravu. Regulácia založená na systémoch sa zameriava na ukladanie požiadaviek na návrh a prevádzku digitálnych platforiem a služieb s cieľom zmierniť riziká, ktoré môžu existovať v rámci týchto služieb, prostredníctvom integrovaných bezpečnostných zásahov.

Ako bolo názorne ukázané, všetky členské regulačné orgány sú oprávnené vykonávať rôzne opatrenia na presadzovanie pravidiel a všetky sa venujú vzdelávaniu a zvyšovaniu informovanosti o bezpečnosti online. Väčšina z nich uskutočňuje a je schopná prijímať a prešetrovať sťažnosti od používateľov. Väčšina regulačných orgánov má navyše právomoc vypracúvať a presadzovať odvetvové kódexy postupov.

Nasledujúca tabuľka znázorňuje právomoci regulačných orgánov v oblasti bezpečnosti online. Je potrebné poznamenať, že niektoré regulačné orgány majú rozsiahle právomoci, ktoré presahujú rámec online bezpečnosti (napr. klasifikácia filmov, vysielanie a regulácia médií).

Jurisdikcia	Regulačné právomoci a funkcie												
	Regulácia ex ante	Sťažnosti od používateľov a vyšetrovanie					Zber informácií a presadzovanie pravidiel			Výskum a činnosti v oblasti prevencie			
	Vypracúvanie a presadzovanie predpisov, noriem a usmernení	Proaktívne prehľadávanie obsahu ²	Prijímanie a prešetrovanie individuálnych sťažností od používateľov	Vydávanie oznámení o odstránení a zablokovaní obsahu	Partnerstvo s orgánmi činnými v trestnom konaní a sieťami horúcich liniek	Príkazy na blokovanie alebo obmedzenie služieb (napr. príkazy na blokovanie služieb, prístupu alebo platieb)	Dohľad a transparentnosť	Oznámenia o nedodržaní predpisov a finančné pokuty	Súdne príkazy a súdne zákazy	Vzdelávanie a zvyšovanie informovanosti	Granty	Výskum a monitorovanie situácie	Činnosť v externých kruhoch
Austrália (eSafety)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fidži (OSC)	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗ ³	✓
Francúzsko (Arcom)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Írsko (An Coimisiún)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Kórejská republika (KCSC)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Slovensko (RpMS)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓
Juhoafrická republika (FPB)	✓ ⁴	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓
Spojené kráľovstvo (Ofcom)	✓ ⁵	✗	✗	✗	✗ ⁶	✓	✓	✓	✓	✓	✗	✓	✓

²Proaktívne prehľadávanie obsahu v tejto súvislosti označuje prehľadávanie obsahu vykonávané regulačným orgánom. Niektoré regulačné orgány môžu od regulovaných subjektov vyžadovať, aby za určitých okolností vykonávali proaktívne prehľadávanie obsahu.

³Fidžijský orgán OSC plní funkciu prehľadávania horizontu, ale nemá výskumnú funkciu. ⁴Rada pre film a publikácie má právomoc vypracovať kódexy a usmernenia. V súčasnosti však nemá právomoc tieto kódexy a usmernenia presadzovať. ⁵V Spojenom kráľovstve môže Ofcom presadzovať právne povinnosti (vyplývajúce z právnych predpisov) a môže vypracúvať nezáväznú kódexy a usmernenia. ⁶Ofcom však aj spolupracuje s orgánmi činnými v trestnom konaní a sieťami horúcich liniek.



Regulované druhy ujmy v online priestore

Porovnanie druhov ujmy v online priestore regulovaných v jednotlivých jurisdikciách je do istej miery obmedzené, keďže vymedzenie jednotlivých rizík je zložité a nie vždy identické. Hoci kategórie „nezákonná ujma“ a „obsah, ktorý je škodlivý pre mládež“ sú upravené vo všetkých jurisdikciách, právne vymedzenie jednotlivých kategórií ujmy sa v jednotlivých jurisdikciách líši. Napríklad to, čo sa považuje za „nezákonný obsah“, sa v jednotlivých krajinách líši a vo všeobecnosti sa určuje podľa trestných zákonov alebo klasifikačného rámca danej krajiny. Vo väčšine členských jurisdikcií patrí medzi nezákonný obsah materiál zobrazujúci sexuálne zneužívanie detí, terorizmus a extrémizmus, zobrazovanie, propagácia násilia alebo podnecovanie k nemu (vrátane vraždy, napadnutia, znásilnenia atď.), sexuálne vykorisťovanie a obsah, ktorý zobrazuje, propaguje alebo sa usiluje predávať nezákonné látky alebo zbrane. V niektorých jurisdikciách sa však za nezákonný považuje aj urážlivý obsah, „nezákonné nenávistné prejavy“, hanobenie a pornografia.

„Škodlivý obsah“, označovaný aj ako „obmedzený obsah“ alebo „vekovo nevhodný obsah“, sa v jednotlivých jurisdikciách tiež značne líši, keďže sa v jednotlivých krajinách líšia prahové hodnoty v súvislosti s tým, čo sa považuje za „potenciálne škodlivé pre telesný, duševný alebo morálny vývin detí“. Napríklad pornografia sa v niektorých jurisdikciách považuje za nezákonnú a v iných za „obmedzenú“.

Okrem toho sa kategórie škodlivého obsahu vo viacerých jurisdikciách čiastočne prekrývajú. V niektorých kontextoch napríklad kategória **zneužívanie a obťažovanie** zahŕňa väčšinu príkladov **nenávisti a diskriminácie online**. V niektorých kontextoch sa pojem „nenávistný prejav“ chápe úzko a vzťahuje sa len na jazyk, zatiaľ čo v iných jurisdikciách sa používa širší termín „nenávist online“, ktorá sa vzťahuje aj na nenávistné obrázky, videá a symboly. Okrem toho treba mať na pamäti, že regulačné právomoci a povinnosti regulovaných subjektov neplatia rovnako pre všetky kategórie ujmy spôsobenej online a líšia sa aj v jednotlivých jurisdikciách. Vo všeobecnosti platí, že na najzávažnejšiu ujmu (takú, ktorá je nezákonná vo všetkých jurisdikciách), ako napríklad materiál zobrazujúci sexuálne zneužívanie/vykorisťovanie detí a obsah o terorizme a násilnom extrémizme, sa vzťahujú najprísnejšie regulačné požiadavky.

Jurisdikcia	Druhy ujmy v online priestore														
	Materiál zobrazujúci sexuálne zneužívanie/vykorisťovanie detí	Obsah o terorizme a násilnom extrémizme/proteroristický obsah	Nenávistné prejavy a diskriminácia	Nezákonný obsah	Podvody a finančná ujma	Podnecovanie k násiliu a jeho zobrazovanie	Mylné informácie a dezinformácie	Zneužívanie prostredníctvom obrázkov/nedobrovolené zdieľanie intímnych záberov	Kyberšikana detí	Zneužívanie a obťažovanie	Propagácia nebezpečného správania (napr. poruchy príjmu potravy, sebaškodovanie, samovražda, nebezpečné činnosti atď.)	Škodlivé algoritmy	Ohováranie	Obsah v rozpore s národnými záujmami	Pornografia
Austrália (eSafety)	✓	✓	✗ ⁷	✓	✗	✓	✗ ⁸	✓	✓	✓	✗	✗	✗	✗	✓
Fidži (OSC)	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓
Francúzsko (Arcom)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
Írsko (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗ ⁹	✗	✗	✓
Kórejská republika (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Slovensko (RpMS)	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗
Juhoafrická republika (FPB)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓
Spojené kráľovstvo (Ofcom)	✓	✓	✓	✓	✓	✓	✗ ¹⁰	✓	✓	✓	✓	✗	✗	✗	✓

⁷Komisar pre elektronickú bezpečnosť reguluje len nenávist a ohováranie na internete len vtedy, keď spĺňajú prahovú podmienku kybernetického zneužívania dospelých alebo kyberšikanovania detí. Podľa rámca transparentnosti eSafety (Očakávaná) možno od platforiem a služieb vyžadovať, aby poskytli informácie o svojom úsilí riešiť širokú škálu ujmy v online priestore vrátane nenávisti online, nebezpečných výziev, obsahu propagujúceho samovraždu a sebaškodovanie a škodlivých algoritmov. Austrália má samostatné trestné a občianske zákony, ktoré sa zaoberajú určitými formami nenávistných prejavov a diskriminácie. ⁸Austrália v súčasnosti pripravuje právne predpisy o mylných informáciách a dezinformáciách a Austrálsky úrad pre komunikáciu a médiá vedie dobrovoľný kódex postupov v oblasti mylných informácií a dezinformácií. ⁹S výnimkou nahlasovania príkazov na odstránenie nezákonného obsahu podľa DSA. ¹⁰Niektoré formy mylných informácií a dezinformácií môžu byť zachytené, ak spadajú do rozsahu trestných činov zahraničného zasahovania a nepravdivej komunikácie podľa práva Spojeného kráľovstva.



Regulované subjekty

Analýza typov subjektov regulovaných v jednotlivých jurisdikciách je zložitá; nemožno ich jednoducho porovnať, pretože existuje mnoho problémov súvisiacich s vymedzením pojmov. Napríklad kategórie **služieb sociálnych médií, platforiem a služieb na zdieľanie videí** a **platforiem a služieb medzi používateľmi** sa značne prekrývajú. V Spojenom kráľovstve a EÚ sú platformy a služby na zdieľanie videí, ako napríklad YouTube a TikTok, osobitnou kategóriou regulovaných subjektov, a to vzhľadom na riziká spojené s viralitou videí šírených medzi používateľmi. Naopak, v Austrálii a Kórejskej republike nie sú platformy na zdieľanie videí zákonom definovanou kategóriou regulovaných subjektov. Namiesto toho sú platformy ako YouTube, TikTok a ďalšie platformy s funkciami zdieľania videí zahrnuté do pojmu „služby sociálnych médií“. Preto sa niektoré jurisdikcie rozhodli jednotlivé časti online odvetvia oddeliť, zatiaľ čo iné sa rozhodli zoskupiť ich do väčších kategórií.

Podobne aj „služby medzi používateľmi“, ako sú aplikácie na zasielanie správ, zoznamovacie aplikácie, hry s komunikačnými funkciami a iné platformy sociálnych médií, nie sú vo všetkých jurisdikciách samostatnou kategóriou regulovaných subjektov. Niektoré jurisdikcie, ako napríklad Austrália a Kórejská republika, zachytávajú služby medzi používateľmi v rámci iných kategórií subjektov, ako napríklad „služby sociálnych médií“ alebo „služby zasielania správ“. Dôležité je, že všetky jurisdikcie určitým spôsobom zachytávajú hlavné veľké online platformy a služby.

Jurisdikcia	Kategórie digitálnych služieb a platforiem										
	Služby sociálnych médií, platformy a služby na zdieľanie videí platformy a služby medzi používateľmi	Hostingové a úložiskové služby	Herné služby	Služby distribúcie aplikácií	Poskytovatelia internetových služieb	Služby zasielania správ a zoznamovacie aplikácie	Služby šifrovaní medzi koncovými zariadeniami	Služby vyhľadávačov	Webové stránky	Služby generatívnej umelej inteligencie	Služby v oblasti vybavenia
Austrália (eSafety)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fidži (OSC)	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗
Francúzsko (Arcom)	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗
Írsko (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Kórejská republika (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ ¹²	✓
Slovensko (RpMS)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Juhoafrická republika (FPB)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
Spojené kráľovstvo (Ofcom) ¹¹	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗

¹¹V Spojenom kráľovstve sú regulovanými subjektmi podľa zákona o bezpečnosti online (2023) len tie služby, ktoré sú službami medzi používateľmi, vyhľadávacími službami alebo online pornografickými službami. Všetky kategórie označené „áno“ sú v takom rozsahu, v akom predstavujú služby medzi používateľmi, vyhľadávacie služby alebo online pornografické služby. ¹²KCSC reguluje obsah na platformách, ako je DALL-E, pretože ich obsah je verejne prístupný. Služby ako ChatGPT však nie sú regulované KCSC, pretože komunikujú s jednotlivými používateľmi súkromne.



Povinnosti regulovaných subjektov

Analýza povinností regulovaných subjektov je zložitá a nemožno ich jednoducho porovnať. Je to preto, že regulačné povinnosti a požiadavky sa nemusia nevyhnutne uplatňovať rovnako na všetky kategórie regulovanej ujmy v online priestore a na všetky kategórie regulovaných subjektov. K zložitosti prispieva aj to, že existujú značné rozdiely v spôsobe regulácie v rámci jednej kategórie regulovaných subjektov, pričom väčšina jurisdikcií uplatňuje prístup založený na riziku (alebo „stupňovitý“ prístup) s cieľom uskutočňovať reguláciu primerane rizikám prítomným na konkrétnej platforme alebo službe. Väčšina jurisdikcií zaviedla prísnejšie a náročnejšie požiadavky na väčšie a rizikovejšie platformy.

Každá jurisdikcia sa líši v tom, ako posudzuje alebo kategorizuje „riziko“ vo svojom regulačnom rámci, pričom väčšina z nich berie do úvahy viacero faktorov, ako sú počet používateľov, demografické údaje používateľov, geografické rozloženie, funkcie služby, typ a počet rizík vyplývajúcich z obsahu, pravdepodobnosť a vplyv ujmy v online priestore, účel služby, objaviteľnosť, používanie algoritmov a systému odporúčaní atď. Nasledujúca tabuľka je základom pre porovnanie a ponúka všeobecný prehľad typov zásahov a požiadaviek, ktoré ukladajú regulačné orgány v členských jurisdikciách.

Jurisdikcia	Povinnosti regulovaných subjektov																	
	Určenie domáceho zástupcu oprávneného prijímať právne oznámenia	Vyhovenie oznámeniam o odstránení obsahu, blokovani a odstránení odkazov	Dodržovanie požiadaviek na včasnosť oznámení týkajúcich sa obsahu	Dodržovanie schválených kódexov a noriem	Náležitá reakcia na žiadosti o informácie	Dodržovanie požiadaviek na podávanie správ o transparentnosti a dohľad	Hodnotenie rizík	Zavedenie vhodného riadenia	Vedenie záznamov	Podľa potreby podlieha nie auditu	Proaktívna minimalizácia škodlivého a nezákonného obsahu	Poskytnutie možnosti voľby používateľom	Zavedenie systémov na preukázanie veku	Primerané opatrenia na ochranu detí pred vekovo nevhodným obsahom	Primerané opatrenia na zabezpečenie bezpečného šírenia medzi koncovými zariadeniami a anonymných služieb	Zabezpečenie mechanizmov na nahlasovanie obsahu používateľmi	Zabezpečenie a presadzovanie jasných a dostupných podmienok poskytovania služieb	Absolvovanie odborného vzdelávania v oblasti bezpečnosti online
Austrália (eSafety)	✗ ¹³	✓	✓	✓	✓	✓	✓ ¹⁴	✓	✓	✗	✓	✓ ¹⁵	✗	✓	✓	✓	✓	✗
Fidži (OSC)	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
Francúzsko (Arcom)	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗
Írsko (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kórejská republika (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Slovensko (RpMS)	✓ ¹⁶	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗
Juhoafrická republika (FPB)	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✓	✗	✗
Spojené kráľovstvo (Ofcom)	✗	✗	✗	✓ ¹⁷	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗

¹³Podľa austrálskeho rámca transparentnosti (Očakávania) sa od niektorých platforiem a služieb očakáva, že určia právne kontaktné miesto. Nemusia sa nachádzať v tuzemsku. ¹⁴Podľa austrálskeho rámca pre bezpečnosť online sa od platforiem a služieb vyžaduje len to, aby vykonávali posudzovanie rizík, stanovovali jasné a dostupné podmienky poskytovania služieb a zabezpečovali mechanizmy na nahlasovanie obsahu používateľmi v súvislosti s materiálom 1. kategórie. Materiál 1. kategórie zahŕňa materiál zobrazujúci sexuálne zneužívanie detí, proteroristický materiál a materiál zobrazujúci trestnú činnosť, ako napríklad násilie a obsah súvisiaci s drogami. ¹⁵V Austrálii sa od niektorých platforiem a služieb, ako sú napríklad služby zasielania správ, vyžaduje, aby používateľom poskytovali možnosť voľby, napríklad funkciu blokovania účtov. Podľa časti Očakávania sa od platforiem a služieb môže vyžadovať, aby poskytovali informácie o svojom úsilí umožniť používateľom prispôbiť si využívanie internetu. ¹⁶Podľa DSA môže RpMS od regulovaného subjektu vyžadovať, aby určil domáceho zástupcu oprávneného prijímať právne oznámenia, len ak má regulovaný subjekt sídlo na Slovensku. ¹⁷V Spojenom kráľovstve musia regulované subjekty dodržiavať povinnosti stanovené v zákone o bezpečnosti online (2023). Ofcom vydáva kódexy, v ktorých sa regulovaným subjektom odporúča prijať opatrenia na dosiahnutie súladu s predpismi.

Zber informácií a presadzovanie pravidiel

Väčšina jurisdikcií uplatňuje podobné prístupy k zberu informácií a presadzovaniu pravidiel, ktoré pozostávajú z právomocí získavať informácie prostredníctvom oznámení a dohľadu a z prísnejších právomocí, ako sú finančné pokuty alebo opravné prostriedky nariadené súdom. Dôležité je, že nie všetky právomoci na presadzovanie pravidiel sú dostupné vo všetkých prípadoch nedodržania predpisov. Pre niektoré regulačné orgány sú prísnejšie právomoci, ako napríklad príkazy na prerušenie podnikania a občianskoprávne sankcie, dostupné až po opätovnom zistení nesplnenia požiadaviek na poskytnutie informácií. Iné regulačné orgány môžu udeliť finančné pokuty v prípadoch, keď dôjde k porušeniu lehôt na odstránenie obsahu. Okrem toho sa výška finančných a občianskoprávných pokút v jednotlivých jurisdikciách výrazne líši, pričom v niektorých možno udeliť pokutu až do výšky 10 % celosvetových ročných príjmov. Vzhľadom na tieto nuansy poskytuje nasledujúca tabuľka všeobecný prehľad rôznych mechanizmov presadzovania pravidiel, ktoré sú k dispozícii v každej jurisdikcii.

Zber informácií a presadzovanie pravidiel																
Jurisdikcia	Opatrenia na presadzovanie pravidiel súvisiace s obsahom				Právomoci na zber informácií						Systémové presadzovanie predpisov		Opravné prostriedky nariadené súdom			
	Formálne písomné upozornenie	Oznámenia o odstránení, vymazaní a zablokovaní obsahu	Pokyny na úrovni aktéra alebo účtu ¹⁸	Finančné pokuty	Žiadosti o informácie	Právomoci v oblasti dohľadu	Požiadavky na podávanie správ o transparentnosti	Audit treťou stranou	Kontrola formou rozhovoru	Právo na vstup, kontrolu a audit	Formálne písomné upozornenia a pokyny na nápravu (napr. záväzky)	Finančné pokuty	Občianskoprávne a správne sankcie	Súdne zákazy	Príkazy na blokovanie alebo obmedzenie služieb (na pr. príkazy na blokovanie prístupu alebo platieb) ¹⁹	Odszkodné
Austrália (eSafety)	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗
Fidži (OSC)	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓
Francúzsko (Arcom)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓
Írsko (An Coimisiún)	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kórejská republika (KCSC)	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓
Slovensko (RpMS)	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
Juhoafrická republika (FPB)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓
Spojené kráľovstvo (Ofcom)	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓

¹⁸ „Pokyny na úrovni účtu alebo aktéra“ sa vzťahujú na pokyny alebo oznámenia vydané koncovým používateľom alebo platformám s cieľom uľahčiť odstránenie účtu alebo jednotlivca z určitej platformy alebo služby. ¹⁹ Príkazy na blokovanie a obmedzenie služieb zahŕňajú „príkazy na prerušenie podnikania“.

