

Global
Online Safety Regulators
Network

Regulatory Index

Comparing international approaches and perspectives to online safety regulation



Developed by the members of the Global Online Safety Regulators Network:

eSafety Commissioner (Australia), **Online Safety Commission** (Fiji), **Arcom** (France), **Coimisiún na Meán** (Ireland), **Autoriteit online Terroristisch en Kinderpornografisch Material** (the Netherlands), **Korea Communications Standards Commission** (Republic of Korea), **Council of Media Services** (Slovakia), **Film and Publications Board** (South Africa), **Ofcom** (United Kingdom)

Regulatory Index

1. About the Index	2
2. Key terminology	3
3. Jurisdictional snapshots	5
3.1 Australia (eSafety Commissioner)	6
3.2 Fiji (Online Safety Commission)	7
3.3 France (Arcom)	8
3.4 Ireland (Coimisiún na Meán)	9
3.5 Republic of Korea (Korea Communications Standards Commission)	10
3.6 Slovakia (Council of Media Services)	11
3.7 South Africa (Film and Publications Board)	12
3.8 The Netherlands (ATKM)	13
3.9 United Kingdom (Ofcom)	14
4. Regulatory analyses	15
4.1 Online safety regulatory remits	16
4.2 Online harms	17
4.3 Regulated entities	18
4.4 Obligations for regulated entities	19
4.5 Information gathering and enforcement	20



About the Network

The Global Online Safety Regulators Network (the Network) is a global forum dedicated to supporting collaboration between online safety regulators, sending a strong message about our shared commitment to online safety regulation.

The Network is composed of members and observers. Members are independent statutory authorities responsible for online safety within their respective jurisdictions.

Members have a commitment to human rights, democracy, the rule of law, and are independent from political and commercial interference.

Observers are organisations with an online safety focus and remit, such as NGOs, multi-stakeholder groups, and government departments.

For more information, visit esafety.gov.au/about-us/who-we-are/international-engagement/the-global-online-safety-regulators-network.

About the Index

The Online Safety Regulatory Index (the Index) supports the Network's mission to pursue cohesive online safety regulation.

Developed by Network members, the Index is a foundational document designed to support collaboration and interjurisdictional comparison of online safety regulatory frameworks. The Index seeks to highlight areas of commonality and divergence and serves as an important resource to support broader understanding of approaches to online safety regulation.

The Index comprises two sections:

Section one provides **jurisdictional snapshots** of each member country and their regulatory approach to online safety, highlighting relevant legislation and regulation, scope and remit, and authority and functions. The jurisdictional snapshots were drafted by each regulator separately. As such, there is some divergence in language between snapshots.

Section two provides **comparative analysis**, collating and comparing regulators' approaches to online safety regulation across key themes, such as remit, regulated online harms, regulated platforms and services, obligations for regulated entities, and enforcement.

The Index reflects a global perspective, and some concepts have been grouped together that may be described differently in different contexts, noting that local definitions, thresholds, and terminology vary between jurisdictions. Therefore, while the Index is intended to be a helpful guide, it is not a substitute for consulting domestic legislation and regulatory documents published by Network members. The Index will be updated periodically.



Key terminology

Please note that these key terms may have varied meaning and application in each jurisdiction.

Age assurance (AA): an umbrella term used to describe the approaches by which services estimate, infer, or verify a user's age.

Age estimation (AE): an approximate determination of someone's age using estimation technology such as photo analysis powered by artificial intelligence.

Age verification (AV): a determination of one's age to a high level of certainty, typically by verifying data against an external source like an identity document.

Artificial intelligence (AI): an engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation, and are sometimes defined as 'self-learning' or 'adaptive' systems.

AI companions: applications, such as chatbots, powered by artificial intelligence that are designed to simulate personal relationships through human-like conversations. The conversations can be via text or spoken word. The AI companions adapt to inputs from users and learn to respond in ways that feel personal and realistic. AI companions can share harmful content, distort reality and give advice that is dangerous. In addition, they are often designed to encourage ongoing interaction, which can feel 'addictive' and lead to overuse and even dependency.

Blocking notice: a legal notice issued to a platform or service directing that platform or service to block domestic access to a particular piece of content that is often hosted overseas.

Business disruption order: an enforcement order available under the UK's *Online Safety Act 2023* that allows the appropriate court to do any number of things to 'disrupt' the business of an online platform or service. This can include withdrawal of advertisers or directing an internet service provider to block domestic access to the platform or service.

Child sexual exploitation and abuse (or 'CSEA'): a broad term that encompasses all forms of child sexual exploitation and abuse, including CSAM, CSEM, and other activities like sexual extortion and sex trafficking.

Child sexual exploitation material (or 'CSEM'): any content that presents a child in a sexual context. It includes content that sexualises and takes unfair advantage of a child, as well as content that shows sexual activity by a child.

Child sexual abuse material (or 'CSAM'): shows a sexual assault against a child and can be considered a sub-set of child sexual exploitation material.

Coercive control: abuse that involves an act or series of actions directed at another person to hurt, scare or isolate them, with the intention of creating a dynamic of control. Coercive control can involve actions that exert physical, emotional, social, or financial control over another person.

Content removal notice / take-down notice: a notice issued to a platform or service that directs that platform or service to remove a particular piece of content from their service or platform.

Cyberbullying: involves bullying that is facilitated by technology. It can include sending, posting, or sharing negative, harmful, false, threatening, humiliating or mean content about someone. It can happen on a social media, gaming platforms, apps, forums or any other online or electronic service or platform. It can include posts, comments, texts, messages, chats, livestreams, memes, images, videos and emails. In some jurisdictions cyberbullying may specifically refer to behaviours concerning children.

Deepfake: a 'deepfake' is a type of synthetic media – including images, videos, or audio recordings – that has been convincingly computer altered or generated, often using AI. They are often produced to create an extremely realistic but false depiction of someone doing or saying something that they did not actually do or say.

Digital literacy or media literacy: the ability to understand technology and digital environments, identify and respond to risks, and access and use digital services and platforms safely.

Disinformation: information that is knowingly or recklessly false and is designed to deliberately mislead and influence a person or group of persons for malicious or deceptive purposes.

Doxing or doxxing: the intentional online exposure of an individual's identity, private information or personal details without their consent and with the intent of causing harm.

End-to-end-encryption (E2EE): a method of secure communication that allows only the people communicating with each other to read the messages, images, or files being exchanged.



Generative AI (Gen AI): the use of machine learning tools to create digital content such as new text, images, audio, video and multimodal simulations of experiences.

Grooming: online grooming occurs when a person uses electronic communication (including social media) in a predatory fashion to try to lower a child's inhibitions. It is often done to facilitate sexual abuse that can occur either in person or online.

Harmful algorithmic pattern: a pattern of recommended content delivered to an end-user by a recommender system that could, in aggregate, result in significant harm (e.g. radicalisation, eating disorder, self-harm, etc.).

Harmful to youth: content that may be damaging to the physical or psychological health or development of children or young people, such as pornography or high-impact violence (also referred to as age-inappropriate content and 'restricted content') (Republic of Korea terminology).

Hash matching technology: a broad term that can be used to refer to either perceptual hashing or cryptographic hashing, both of which are mechanisms that stamp online material (image or video) with a numeric identifier that allows it to be detected by hash matching detection systems. Hash matching technology is widely used to detect known CSEM and CSAM material (second generation) and cannot be used to detect first generation CSEM and CSAM.

Immersive technologies: enable users to experience and interact with digital content in 3D, in ways that look, sound, and feel almost real. These include augmented reality (AR), virtual reality (VR), and mixed reality (MR) – technologies that may be collectively referred to as extended reality (XR). They can be combined with haptic sensory technologies.

Misinformation: incorrect or false information that is spread due to ignorance, error, or mistake without the intention to deceive.

NCII or IBA: non-consensual sharing of intimate images (NCII) or image-based abuse (IBA) refers to the act of sharing or threatening to share intimate images of a person without their consent.

'Nudify' applications: use AI to create sexualised or 'nudified' images or videos of people, often without their consent. In many cases this involves taking an innocent image of a person, and altering it to depict them without clothing. These tools are linked to deepfake technologies.

Online hate speech or online hate: 'online hate speech' generally, refers to user-generated content that discriminates against an individual or group based on a protected attribute, such as race, sexuality, gender, culture, health status, or other. 'Online hate' is generally considered a broader term that encompasses all hateful online content and actions, including speech, imagery, video, symbolism, and other user-to-user interactions.

Proactive detection: in content moderation, proactive detection refers to the practice of scanning user-generated content proactively to detect harmful or policy violating content before it is reported by a user or authority.

Pro-terror content: content that advocates for the doing of a terrorist attack because it depicts, incites, promotes, glorifies, praises or otherwise sympathises with terrorist or extremist groups or activities.

Restricted content: content that may be damaging to the physical or psychological health or development of children or young people, such as pornography or high-impact violence (also referred to as age-inappropriate content and content harmful to youth) (Australian terminology).

Safety by Design: a concept that proactively places user safety and rights at the centre of product design and delivery, requiring platforms and services to forecast and mitigate online risks. This concept can mutually reinforce similar principles of Privacy by Design and Security by Design.

Sexual extortion (or 'sextortion'): a form of blackmail where someone threatens to share nude or sexual content of a victim unless certain demands are met. Usually, these demands are for more images, payment or sexual favours.

Social media service: an online service or platform that's primary purpose is to enable online social interaction between end-users. This may include services that allow users to interact with one another, post or generate material, or view material posted or generated by other users.

Terrorism and violent extremism content (TVEC): generally, TVEC refers to content that depicts or advocates for acts of violent extremism, or otherwise depicts, advocates for, promotes, incites, or sympathises for terrorist or extremist organisations, groups, or ideologies.

Technology-facilitated gender-based violence (TFGBV): defined as any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools against a person on the basis of their gender, which results in, or is likely to result in, harm or other infringements of rights and freedoms.

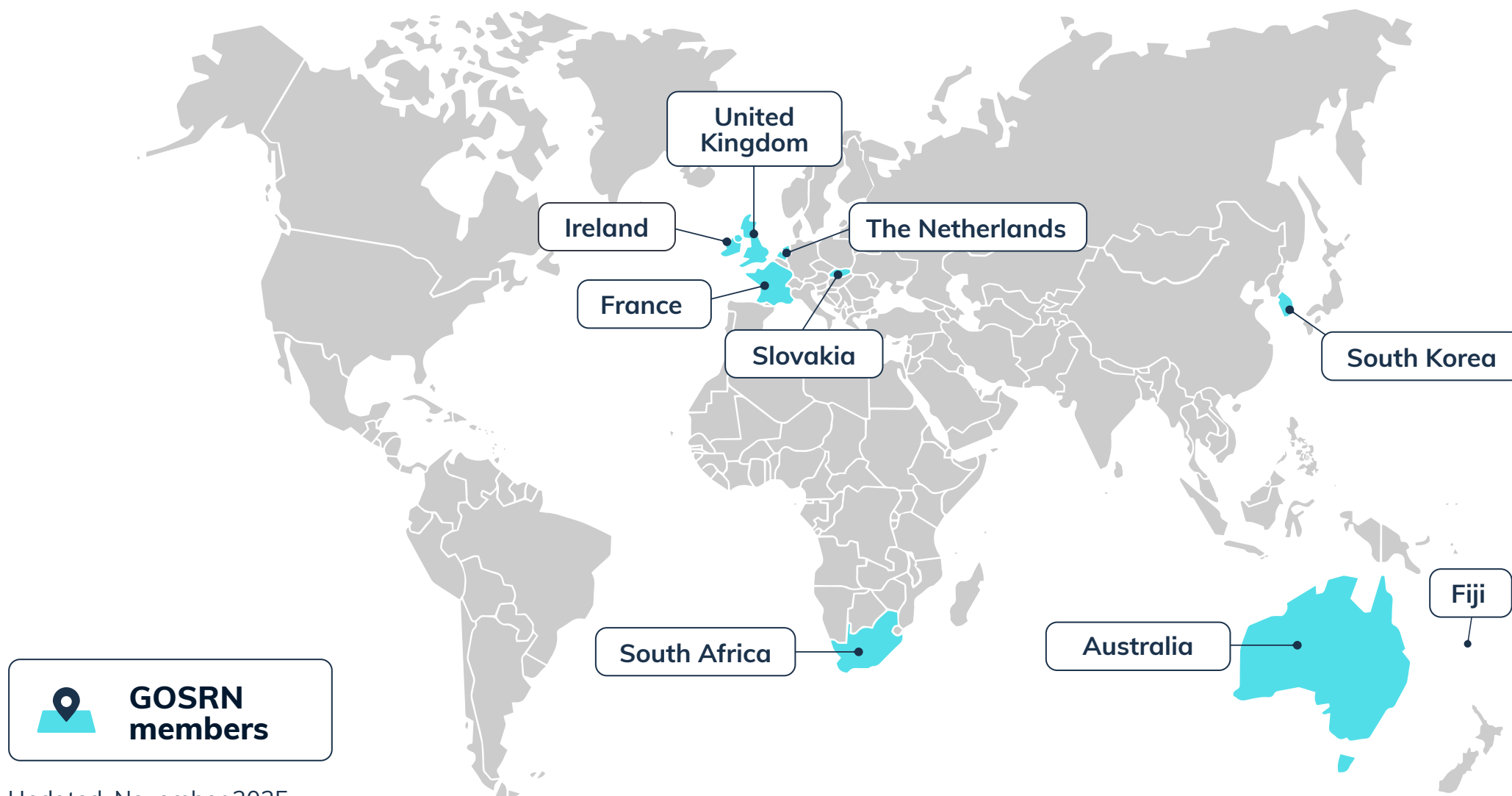
User-to-user (U2U) service: a platform or service that enables users to generate and / or share content with other users.

Video-sharing platform (VSP): a platform or service that allows users to generate, post, share, or interact with video content that is generated by other users (UK and EU terminology).

Please note this list is not an exhaustive list of online safety terminology, and some terminology may vary across jurisdictions.



Jurisdictional snapshots



Australia: eSafety Commissioner (eSafety)

The eSafety Commissioner (eSafety) is Australia's online safety regulator. The Commissioner is an independent statutory authority empowered to help safeguard all Australians from online harms and to promote safer, more positive online experiences. eSafety exercises powers under the *Online Safety Act 2021*, as well as through sections of the *Telecommunications Act 1997* and *Criminal Code Act 1995*.

eSafety focusses on **protection, prevention, and proactive and systemic change**. This includes administering user-complaints and investigations schemes, engaging with industry on systemic regulation and promoting online safety through education and research, as well as domestic and international coordination and engagement. Australia has adopted a **hybrid regulatory approach**, targeting harmful material at the user and systems levels. Users are empowered to report harmful material that they encounter under eSafety's four harms schemes: cyberbullying of children, adult cyber abuse, image-based abuse (including NCII); and illegal and restricted content (such as CSAM, TVEC, and criminal activity). eSafety works with users and platforms to have the material removed or blocked. eSafety also has powers to respond to abhorrent violent material, which includes offensive material that is produced by a person who is engaged in or attempts to engage in a terrorist act or other abhorrent violent conduct such as murder, torture, rape and kidnapping.

eSafety's systems-based regulation comprises two frameworks, the Industry Codes and Standards and the Basic Online Safety Expectations (the Expectations). Once all industry codes and standards are in place, they will govern how the online industry is required to deal with illegal content (e.g., CSEA and TVEC) and restricted content (age-inappropriate content such as pornography and high-impact violence).¹ The Expectations outline online safety expectations for social media services, messaging services and communications services including gaming and dating apps, and other internet services such as file-sharing services and websites. The Commissioner can use transparency powers provided in the *Online Safety Act 2021* to require providers of these online services to report on how they are meeting the Expectations.

eSafety is also responsible for assisting with the implementation and enforcement of Australia's *Online Safety Amendment (Social Media Minimum Age)* legislation, which amends the *Online Safety Act 2021*. The obligations come into effect by 10 December 2025 and will require 'age-restricted social media platforms' to take reasonable steps to prevent Australians under the age of 16 from creating or keeping an account. The legislation grants the eSafety Commissioner and the Office of the Australian Information Commissioner (OAIC) enforcement powers to seek information relevant to monitoring compliance, issue and publish notices of non-compliance, and impose financial penalties on platforms.



Governing acts and regulation:

[Online Safety Act 2021](#), [Basic Online Safety Expectations](#), [Industry Codes and Standards](#); [Social Media Minimum Age](#)

Website: [eSafety Commissioner](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> User complaints handling Education and awareness raising Develop, register, and enforce industry regulation (codes and standards) Transparency powers Monitor industry compliance Research Horizon scanning Social media age restrictions 	<ul style="list-style-type: none"> Cyberbullying of children Adult cyber abuse Image-based abuse Illegal content: includes CSEA material, pro-terror material Restricted content / age-appropriate content 	<ul style="list-style-type: none"> Social media services (SMS) providers Relevant electronic services (RES) providers – includes messaging services and dating apps Designated internet services (DIS) providers – includes file-sharing services, website services, and more Hosting services providers Internet services providers Equipment services providers Search engine services providers App distribution providers 	<ul style="list-style-type: none"> End-user notices Enforceable undertakings Infringement and non-compliance notices Content removal, blocking, and link-deletion Investigations Information gathering Formal warnings Court ordered remedies (E.g. injunctions and civil penalties) Service provider notifications

¹The *Online Safety Act 2021* (Cth) stipulates that there are eight separate sections of the online industry. The eSafety Commissioner is empowered to register Industry Codes and Standards for each of the eight sections. More information can be found [here](#).



Fiji: Online Safety Commission (OSC)

The Online Safety Commission (OSC) is Fiji's independent regulator for online safety. The Online Safety Act 2018 was enacted by Parliament of the Republic of Fiji to establish the Online Safety Commission, for the promotion of online safety, deterrence of harmful electronic communication, and other related matters. The OSC started its operations in 2019 to provide an avenue to assist individuals confronted with harmful online content and deliver services and resources to help minimize harm and provide digital literacy, education, and awareness. This includes providing information to Fijian internet users about a variety of current and novel digital platforms, and ways to stay safe online.

The OSC operates a user-complaints scheme that allows users to report harmful content that they encounter online, or harms perpetuated against them or another person online, such as non-consensual sharing of intimate images. The OSC then works with digital services and platforms to have content removed or blocked. At this time, the OSC does not regulate the systems and processes of digital services and platforms.



Governing acts and regulation:
[Online Safety Act 2018](#), [Online Safety Regulations 2019](#)

Website: [Online Safety Commission](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> • User complaints handling • Education and awareness raising • Receive, assess and investigate matters • Horizon scanning 	<ul style="list-style-type: none"> • Cyberbullying of children • Abuse of adults • Image-based abuse • Illegal content: includes CSEA material, pro-terror material • Restricted content 	<ul style="list-style-type: none"> • All platforms and services operating in Fiji that enable 'electronic communication' • 'Electronic communication' is defined as any form of communication that is transmitted electronically by text, writing, photograph, picture, recording, or any other means 	<ul style="list-style-type: none"> • Content removal and blocking orders • Financial penalties • Investigative powers • Information gathering • Removal notices



France: Arcom



Arcom is the French independent public authority for the regulation of audio-visual and digital communication. Arcom's remit includes many areas, such as spectrum management, broadcasting, video-sharing platforms, and online safety. In these areas, Arcom's missions consist in a technical, economic and legal regulation of the sector, in order to protect freedom of communication in the public interest.

The authority ensures the protection of audio-visual works, combating piracy of cultural and sports content and encouraging the development of legal offers. In addition, Arcom issues authorizations for broadcasting services (TV and radio channels), ensuring pluralism and economic equilibrium in the sector, and is responsible for regulation of on-demand services. It ensures that their programs comply with regulations on the protection of minors, the treatment of information, the organization of election campaigns, advertising, and the representation of society in all its diversity.

In addition to the functions linked to broadcasting regulation in France, Arcom is in charge of supervising the system-based approach of the regulatory framework for online safety that concerns, within the revised AVMS Directive, video-sharing platforms and, within the DSA, categories of intermediary services (such as mere conduit, caching and hosting services, as well as online platforms) that are established in France. Arcom is responsible, as Digital Services Coordinators (DSCs), to ensure coordination at national level and supervise enforcement of the DSA with other competent authorities. Within the DSA, intermediary services have to implement tools and resources aimed at combating illegal and harmful content, for the protection of the public in general and more particularly minors, such as reporting and notification mechanisms. Online platforms are also required to empower users with choice and are submitted to transparency requirements for instance. The specific obligations linked to systemic risks on very large platforms (and very large search engines) are exclusively supervised by the European Commission (risk assessments and mitigation measures), in association with Arcom and other competent authorities at the national level in the European Union.

With specific regard to video-sharing platforms, the AVMS Directive adopted in 2010 and revised in 2018 lays down obligations to protect more particularly minors "from programmes, user-created videos and audio-visual commercial communications likely to impair their physical, mental or moral development". In this context, Arcom is responsible for promoting the conclusion of codes of conduct by video-sharing platforms. Arcom adopted in October 2024 a technical framework on age assurance solutions pornographic video-sharing platforms and services have to implement under national 2024 law aiming at securing and regulating the digital space ("SREN" law), Arcom was also granted administrative blocking and delisting powers to enforce the implementation of age assurance by pornographic video-sharing platforms and services. Arcom is also responsible for overseeing the obligations under the system-based approach of the TCO regulation to ensure that platforms effectively implement tools and processes aimed specifically at combatting terrorist content on their services.

Lastly, the SREN law has empowered Arcom to request the blocking and delisting of online public communication services that enable the dissemination of media targeted by sanctions imposed by the European Union (EU) under Article 215 of the Treaty on the Functioning of the European Union (TFEU).

Governing acts and regulation:

[Law n° 86-1067 of 30th September 1986 on freedom of communication](#); [law of June 21st 2004 to support confidence in the digital economy](#); [Directive Audiovisual Media Services \(AVMS\) 2010/13/EU of 10th March \(modified by Directive 2018/1808 of 14 November 2018\)](#); [Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online \(TCO\)](#); [Regulation 2022/2065 of 19 October 2022 on a Single Market for Digital Services \(Digital Services Act or DSA\), amending e-commerce Directive \(2000/31/EC\)](#)

Website: [Arcom](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> Education and awareness raising Develop, register, and enforce industry regulation (codes and guidance) Monitor and supervise industry compliance Research Horizon scanning 	<ul style="list-style-type: none"> Illegal content (the circulation of which is an offence under national and EU law) Harmful content: disinformation, promotion of eating disorders Protection of minors: <ul style="list-style-type: none"> content likely to harm their physical, mental or moral development age-appropriate content (access to pornographic sites) commercial use of images of under sixteen children on online platforms Piracy 	<ul style="list-style-type: none"> Intermediary services: 'mere conduit' services, 'caching' services, 'hosting' services, user-to-user platforms and services and search engine services Video-sharing platforms and services 	<ul style="list-style-type: none"> Investigations Information gathering Formal warnings Financial penalties Apply to a judge for temporary restriction of access to the platform Notification of dynamic blocking and delisting decisions Formal notice to publishers and hosting providers, followed by notification of blocking and delisting decisions against services broadcasting media targeted by sanctions from the Council of the EU Administrative blocking and delisting powers (after observations letter and formal notice) to non-compliant pornographic video-sharing platforms and services (after letter of comments and formal notice)



Ireland: Coimisiún na Meán (An Coimisiún)



Coimisiún na Meán is Ireland's agency for developing and regulating a thriving, diverse, creative, safe and trusted media landscape. Its responsibilities are to:

- Oversee the funding of and support the development of the wider media sector in Ireland.
- Oversee the regulation of broadcasting and video-on-demand services.
- Develop and enforce the Irish regulatory regime for online safety (the Online Safety Framework).

The Online Safety Framework is composed of three pieces of legislation:

- The EU Digital Services Act (DSA), for which Coimisiún na Meán has been a competent authority since February 17th 2024.
- The Online Safety and Media Regulation Act, which is the basis for our Online Safety Code. The Code was adopted on 21 October 2024. Designated video-sharing platforms must comply with the Code.
- The EU Terrorist Content Online Regulation (TCOR), for which Coimisiún na Meán has been a competent authority since November 2023.

The Online Safety Framework gives Coimisiún na Meán the tools to address the root causes of harm online, including the availability of illegal content, the harmful impacts of recommender systems, and inadequate protections for children on social media services. An Coimisiún oversees how platforms comply with their online safety obligations at a systemic level and works closely with the European Commission and regulatory counterparts across Europe and beyond. It also carries out research into the areas under its remit and runs media literacy and user education programmes to empower people to critically engage with and understand the media they consume. Coimisiún na Meán also runs a Contact Centre, which gives people information about their rights under the Framework. Complaints are dealt with by our Complaints team for possible supervisory or investigative follow up.

Governing acts and regulation: [Broadcasting Act 2009](#) as amended, including by [Online Safety and Media Regulation Act 2022](#); [AudioVisual Media Services Directive 2018 \(AVMSD\)](#); [EU Terrorist Content Online Regulation](#); [EU Digital Services Act \(DSA\)](#); [European Media Freedom Act \(EMFA\)](#); [e-Commerce Compliance Strategy](#); [Register of Video Sharing Platforms](#); [Online Safety Code](#); [Transparency and Targeting of Advertising Regulation \(TTPA\) \(Regulation \(EU\) 2024/900\)](#)

Website: [Coimisiún na Meán](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> • Education and awareness raising • Develop, register, and enforce industry regulation (codes and guidance) • Monitor, supervise and enforce industry compliance • Research • Horizon scanning • Digital Services Coordinator further to the Digital Services Act • Certification of Out of Court Dispute Settlement Bodies and award of Trusted Flagger status under the Digital Services Act 	<ul style="list-style-type: none"> • Illegal content • CSAM • Terrorism • Harmful content including pornography and extreme or gratuitous violence • Promotion of self harm or suicide • Promotion of eating or feeding disorders • Cyberbullying • Dangerous challenges • Incitement to hatred or violence on grounds of protected characteristics including racism and xenophobia • Harmful or illegal commercial communications 	<ul style="list-style-type: none"> • Designated Video-sharing Platforms and Services (Online Safety Code) • Intermediary services: 'mere conduit' services, 'caching' services, 'hosting' services, platforms and services and search engine services • Hosting Services Providers exposed to Terrorist Content online (Terrorist Content Online Regulation) 	<ul style="list-style-type: none"> • Investigations • Financial sanctions • Auditing of complaints and complaint handling • Content Limitation Notices • Access Blocking Orders • Compliance notices



Republic of Korea: Korea Communications Standards Commission (KCSC)



The Korea Communications Standards Commission (KCSC) is an independent statutory body responsible for regulating media content in South Korea. The KCSC was established in 2008 by the Act on the Establishment and Operation of the Korea Communications Commission, merging the regulatory function of the Korea Broadcasting Commission and the Korea Internet Safety Commission.

Content that the KCSC regulates can be divided into three parts, the content of broadcast programs (including broadcast advertising and tele-shopping), illegal or harmful to youth online content that are publicly available, and the infringement of online users' rights (including defamation and infringement of privacy). The KCSC works to ensure the public responsibility of broadcasting and to promote and protect safer online environment. To carry out our duties efficiently, the KCSC has three Sub-Commissions (Broadcasting Sub-Commission, Internet Communications Sub-Commission, Digital Sexual Crime Sub-Commission) on a regular basis.

To ensure responsiveness to the rapidly evolving media landscape and strengthen the review system and relevant regulatory framework, the KCSC sets its review principles and content standards. The KCSC also engages in research, promotes public campaigns, and hosts educational programs and seminars to enhance media literacy. With the June 2021 amendment, the KCSC took on the added role of international cooperation to cultivate a safe online environment that is both healthy and trusted by the public, in partnership with global counterparts.

Governing acts and regulation:

[Establishment and Operation of the Korea Communications Commission Act; the Act on Promotion of Information and Communications Network Utilization and Information Protection; the Act on Special Cases Concerning the Punishment of Sexual Crimes; the Telecommunications Business Act](#)

Website: [Korea Communications Standards Commission](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> • Education and awareness raising • Develop and enforce industry regulation (codes and guidance) • Monitor and supervise industry compliance • Research • Horizon scanning 	<ul style="list-style-type: none"> • CSAM, NCII, Human Trafficking • Online hate, Terrorism and extremism • Gambling, Financial Fraud • Illegal Drugs and Pharmaceuticals • Content harmful to youth (pornography, self-harm, suicide and eating disorders, etc) • Violent and Graphic Content, Hateful Content • Defamation, Publicity Rights, Copyrights, etc 	<ul style="list-style-type: none"> • Information and communications service providers refer to entities that either operate as telecommunications business operators or use the services of these operators to provide or facilitate the provision of content for profit. This includes platforms and services that deliver content to the public or act as intermediaries in content distribution using telecommunications networks • Internet bulletin board administrators and operators 	<ul style="list-style-type: none"> • Content removal or access blocking • Suspension or cancellation of use



Slovakia: Council for Media Services (CMS)



Council for Media Services (CMS) is Slovakia's independent media regulator responsible for media oversight and enforcement of regulatory frameworks pertinent to broadcasting, retransmission, provision of on-demand audiovisual media services, and digital platforms. The mission of CMS is to protect the public interest in the media by safeguarding the right to information, freedom of expression, and access to cultural values and education, including in the online environment. CMS is a leading member of the European Board for Media Services (EBMS) previously ERGA, European Platform of Regulatory Authorities (EPRA), and the European Digital Services Board.

CMS was established in 2022 by the Media Services Act (MSA), replacing Council for Broadcasting and Retransmission, a national regulatory authority supervising primarily the linear media market. Taking into consideration the legislative developments on the EU level, the Media Services Act transposed the Audio-Visual Media Services Directive (AVMSD), implemented the EU Regulation addressing the dissemination of terrorist content online (TCO), and began preparations for the adoption of the Digital Services Act (DSA). The DSA was subsequently implemented into national legislation in 2024, at which point CMS was designated as the Digital Services Coordinator (DSC) for Slovakia. Traditionally, CMS has overseen the establishment (e.g. authorization, registration, issuance of licenses) and conduct of broadcasters in Slovakia. However, the MSA has introduced new obligations in line with the revised AVMSD, mainly requirements related to the provision and conduct of audio-visual media services (now extended also to vloggers) and assessment of measures taken by video-sharing platforms (VSPs) to protect minors and the public. In light of the latter, the MSA also empowers CMS to address online safety risks arising from the functioning and design of online platforms.

As part of its online safety remit, CMS is tasked with overseeing the effectiveness and proportionality of the enforcement of terms of service of online platforms offering their services in Slovakia. Moreover, CMS has the legal competence to tackle the dissemination of illegal content online by issuing content removal orders for content that violates art. 151 of the MSA. CMS also engages in research, media literacy and international cooperation.

As a Digital Services coordinator (DSC), CMS is responsible for all DSA provisions, and thus oversees the conduct and functioning of the online platforms established in Slovakia.

Governing acts and regulation:

[the Media Services Act \(MSA\)](#); [Directive Audiovisual Media Services \(AVMS\) 2010/13/EU of 10th March \(modified by Directive 2018/1808 of 14 November 2018\)](#); [Regulation 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online \(TCO\)](#); [Regulation 2022/2065 of 19 October 2022 on a Single Market for Digital Services \(Digital Services Act or DSA\), amending e-commerce Directive \(2000/31/EC\)](#); [Regulation 2024/1083 of 11 April 2024 on establishing framework for media services in the internal market and amending Directive 2010/13/EU \(European Media Freedom Act\)](#); [Regulation \(EU\) 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services](#)

Website: [Council for Media Services](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> User complaints handling Registration and evidence of regulated services and VSPs Develop, register and enforce industry regulation (self/co-regulatory mechanisms, codes and guidance) Cooperation with content platforms Monitor and supervise industry compliance Research Education and awareness raising Horizon scanning 	<ul style="list-style-type: none"> Illegal content (content depicting CSEA or extremism; content inciting to violence or featuring acts of terrorism; content approving or praising acts of terrorism; content denying or approving the Holocaust, crimes of political regimes, crimes against humanity, defamation of a nation, race and belief, or incitement to national, racial and ethnic hatred) Protection of minors Harmful content covered by platforms' ToS (disinformation, scams, etc.) Systemic risks 	<ul style="list-style-type: none"> Audio-Visual Media Services Providers Intermediary services: mere conduit, caching, hosting, platforms, marketplaces, search engines Video-sharing platforms 	<ul style="list-style-type: none"> Investigations On-site inspections and interviews Requests for information Formal warnings Content removal orders Court-ordered remedies Financial penalties Requests to adopt an action plan



South Africa: Film and Publications Board (FPB)

The Film and Publication Board (FPB) is a state entity established under the Films and Publications Act (FPA) 1996, as amended. The FPB has a broad remit and regulates the creation, possession and distribution of films, games, certain publications, and digital content on platforms and services. The regulation seeks to protect children from disturbing and harmful content and to provide content information to adults that will enable them to make informed reading, viewing and gaming choices for both themselves and children in their care.

South Africa has adopted a **hybrid approach** to online safety regulation, developing industry codes of practice and operating a user-complaints scheme. The FPA empowers the FPB to issue directives of general application. The FPB has also developed an advisory industry code on prevention of online harm. Under FPB's user complaints scheme, users can report harmful content such as CSAM, filming and distribution of films and photographs depicting violence against children, hate speech, distribution of private sexual photographs and films, incitement of imminent violence and propaganda for war.



Governing acts and regulation:

[Films and Publications Act 65 of 1996](#);
[Film and Publications Amendment Regulations 2022](#)

Website: [Film and Publication Board](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> • Education and awareness raising • Develop industry regulation and guidance • Monitor and supervise industry compliance • Research • Horizon scanning 	<ul style="list-style-type: none"> • CSAM • Filming and distribution of films and photograph depicting sexual violence and violence against children • Unclassified content • Harmful and prohibited content • Online hate speech • Propaganda for war • Incitement of imminent violence • Distribution of private sexual photographs and films 	<ul style="list-style-type: none"> • Commercial online distributors of films, games and certain publications • Video-sharing platforms and services • User-to-user platforms and services • Search engine services • Internet Service and Access Service Providers 	<ul style="list-style-type: none"> • Investigations • Compliance notice • Take down notices • Adjudication of non-compliance by the Enforcement Committee with powers to impose fines • Referral for criminal prosecution



The Netherlands: The Authority for the prevention of online Terrorist Content and Child Sexual Abuse Material (ATKM)

The Authority for the prevention of online Terrorist Content and Child Sexual Abuse Material (ATKM) was established in 2023 as the competent authority in the Netherlands for the removal of terrorist content online (TCO) and child sexual abuse material (CSAM). The ATKM is established based on EU regulation on addressing the dissemination of terrorist content online (TCO-regulation; Regulation (EU) 2021/784) and national legislation to address the dissemination of online CSAM (administrative law). The legislation gives the ATKM the authority to issue removal orders, when it detects or is made aware of terrorist content online or online CSAM. Upon receiving a removal order, hosting service providers and social media platforms must remove this content within one hour for TCO (or maximum of twelve hours for CSAM) or make it inaccessible.

The TCO regulation allows for cross border issuing of removal orders. Therefore, hosting service providers and social media platforms located in the Netherlands can request a review by the ATKM of removal orders that they receive from competent authorities from other EU Member States. Content disseminated for i.e. educational, journalistic, artistic or research purposes is exempted.

The ATKM has the authority to impose administrative financial sanctions when hosting or communication service providers do not comply with the obligations under the TCO regulation or the CSAM legislation. When the ATKM repeatedly detects TCO at the services of the same hosting service provides or social media platforms, it can force them to take specific measures to prevent further dissemination of terrorist content.

The ATKM has an advisory board, which can give solicited and unsolicited advice to the ATKM-management board, on themes such as technology, governance and human rights online. The ATKM holds regular meetings with representatives of the internet sector of the Netherlands. The aim of these meetings is to identify problems related to the detection and removal of online terrorist and child abuse material and to promote cooperation and exchange of knowledge and expertise.

The ATKM is positioned as an independent governmental body positioned at arm's length from government to ensure independent decision making if content must or must not be removed from the internet. Next to this, strong safeguards are in place to ensure the protection of fundamental rights (freedom of speech).



Governing acts and regulation:

[\(TCO\) Law administrative approach online child pornography material; \(CSAM\) Regulation \(EU\) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online \(Text with EEA relevance\)](#)

Website: [ATKM](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> Prevention of the dissemination of online terrorist content and child sexual abuse material. 	<ul style="list-style-type: none"> Child Sexual Abuse Material (CSAM) and Terrorist Content Online (TCO) 	<ul style="list-style-type: none"> TCO: Hosting service providers, (f.e. storage services, social media services, file and video sharing platforms, websites); CSAM: All communication service providers. 	<ul style="list-style-type: none"> Removal (take down) orders, financial penalties for non-compliance (administrative law), publishing penalties.



United Kingdom: Ofcom

Ofcom is the UK's communications regulator. Ofcom's remit covers a wide range of areas, including spectrum, post, telecommunications networks, broadcasting, video-sharing platforms, and online safety. Following the passing of the Online Safety Act in October 2023, Ofcom took on broader online safety duties, including the regulation of user-to-user and search services accessed by UK users.

The UK has adopted a **systems and processes based approach** to online safety regulation under the Online Safety Act, that requires services to undertake risk assessments and adopt content safeguards. Some services are subject to additional obligations, including empowering users with choice and publishing transparency reports. Ofcom is taking a phased approach to implementation and by mid-2026, Ofcom aims to have developed and finalised Codes of Practice and Guidance to recommend ways in which services can comply with their obligations under the Online Safety Act. Ofcom also undertakes research into online safety and delivers media literacy education and awareness raising.



Governing acts and regulation:

[Online Safety Act 2023](#); [Illegal Harms Codes of Practice](#); [Protection of Children Codes of Practice](#)

Website: [Ofcom](#)

Online safety regulatory remit at a glance

Remit and functions	Regulated harms	Regulated entities	Enforcement powers
<ul style="list-style-type: none"> Enforce legal duties Develop non-binding industry regulation (codes and guidance) Monitor and supervise industry compliance Research Horizon scanning Education and awareness raising 	<ul style="list-style-type: none"> Illegal content (such as CSAM, terrorism, fraud, drug offences, and human trafficking, among others) Content that is legal but harmful to children (such as pornography, promotion of self-harm, suicide, and eating disorders, bullying content, among others) 	<ul style="list-style-type: none"> User-to-user platforms and services Search engine services Providers publishing pornographic content 	<ul style="list-style-type: none"> Investigations Information gathering Court ordered remedies (e.g. business disruption measures and injunctions) Financial penalties Criminal sanctions



Regulatory analyses

- Online safety regulatory remits
- Online harms
- Regulated entities
- Obligations for regulated entities
- Information gathering and enforcement



Online safety regulatory remits

There are similarities between regulatory remits and functions of regulators. Regulatory remits and functions typically vary in relation to the foundational approach, namely whether the jurisdiction has adopted a **content-based**, **systems-based**, or **hybrid approach**. Content-based regulatory models seek to address harmful content by providing complaints and redress for users who are experiencing or have encountered harmful content. Systems-based regulation focuses on imposing requirements upon the design and operation of digital platforms and services to mitigate risks that may exist on their service through inbuilt safety interventions.

As demonstrated, all member regulators are authorised to carry out varying enforcement actions and all undertake online safety education and awareness raising. Most undertake research and have the capacity to receive and investigate complaints from users. Further, most regulators are provided with the authority to develop and enforce industry codes of practice.

The table below captures the online safety remits of regulators. It is worth noting that some regulators have broad remits that extend beyond online safety (e.g. classifications of films, broadcasting, and media regulation).

Jurisdiction	Regulatory remits and functions												
	Ex ante regulation	User complaints and investigations					Information gathering and enforcement			Prevention research and engagement			
	Develop and enforce codes, standards, and guidance	Proactive content scanning ²	Receive and investigate individual user complaints	Issue content removal and blocking notices	Partnership with law enforcement and hotline networks	Service blocking or restriction orders (e.g., service, access, or payment blocking orders)	Oversight and transparency	Non-compliance notices and financial penalties	Court orders and injunctions	Education and awareness raising	Grants	Research and horizon scanning	Industry engagement
Australia (eSafety)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fiji (OSC)	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗ ³	✓
France (Arcom)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Ireland (An Coimisiún)	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Slovakia (CMS)	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓
South Africa (FPB)	✓ ⁴	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓
The Netherlands (ATKM)	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓	✓
United Kingdom (Ofcom)	✓ ⁵	✗	✗	✗	✗ ⁶	✓	✓	✓	✓	✓	✗	✓	✓

²In this context, proactive content scanning refers to content scanning carried out by the regulator. Some regulators may require regulated entities to undertake proactive content scanning in certain circumstances. ³Fiji OSC online does perform horizon scanning functions, but does not have a research function. ⁴The Film and Publications Board has authority to develop codes and guidance. However the FPB does not presently have the authority to enforce codes and guidance. ⁵In the UK, Ofcom can enforce legal duties (derived from legislation) and can develop non-binding codes and guidance. ⁶However, Ofcom engages with law enforcement and hotline networks.



Regulated online harms

There are some limitations associated with comparing the online harms regulated by each jurisdiction, as definitions of harms are complex and not always 'like for like.' Though all jurisdictions regulate categories of 'illegal harms' and 'content that is harmful to youth,' the legal definition of each category of harm varies between jurisdictions. For example, what is considered as **'illegal content'** varies from country to country and is generally determined by the criminal laws or classification framework of that country. Within most member jurisdictions, illegal content includes CSAM, terrorism and extremism (TVEC), the depiction, promotion, or incitement of violence (including murder, assault, rape, etc), sexual exploitation, and content that depicts, promotes or attempts to sell illegal substances or weapons. However, we note that in some jurisdictions, abusive content, 'illegal hate speech,' defamation, and pornography are also considered illegal.

'Harmful content' also referred to as **'restricted content'** or **'age-inappropriate content,'** also varies significantly between jurisdictions, as national thresholds differ in relation to what is considered 'potentially harmful to the physical, psychological, and developmental wellbeing of children.' For example, pornography is considered illegal in some jurisdictions and 'restricted' in others.

Furthermore, in several jurisdictions there is some overlap between categories of harmful content. For example, in some contexts, the category **'abuse and harassment'** covers most examples of **'online hate and discrimination.'** In some contexts, 'hate speech' is narrow and refers only to language, whereas other jurisdictions use the broader terminology 'online hate' to also refer to hateful imagery, video, and symbols. It is also worth noting that regulatory powers and obligations for regulated entities do not apply in equal force across all categories of online harms and also vary between jurisdictions. Generally, the most severe harms (those that are illegal in all jurisdictions) such as CSEM, CSAM, and TVEC, attract the most stringent regulatory requirements.

Jurisdiction	Online harm types															
	CSEM / CSAM	TVEC / Pro-Terror	Hate speech and discrimination	Illegal content	Fraud and financial harms	Incitement and depictions of violence	Misinformation and disinformation	Image-based abuse Non-consensual sharing of intimate images	Cyberbullying of children	Abuse and harassment	Promotion of dangerous conduct (e.g., eating disorders, self-harm, suicide, dangerous activities, etc)	Harmful algorithmic patterns	Defamation	Content against national interests	Pornography	Content harmful to youth
Australia (eSafety)	✓	✓	✗ ⁷	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓
Fiji (OSC)	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	✓
France (Arcom)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ireland (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗ ⁸	✗	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Slovakia (CMS)	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓
South Africa (FPB)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓
The Netherlands (ATKM)	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
United Kingdom (Ofcom)	✓	✓	✓	✓	✓	✓	✗ ⁹	✓	✓	✓	✓	✓	✗	✗	✓	✓

⁷The eSafety Commissioner only regulates online hate and defamation that meets the threshold for adult cyber abuse or cyberbullying of children. Under eSafety's transparency framework (the Expectations), platforms and services may be required to provide information about their efforts to tackle a wide range of online harms, including online hate, dangerous challenges, content that promotes suicide and self harm, and harmful algorithmic patterns. Australia has separate criminal and civil laws that deal with certain forms of hate speech and discrimination. ⁸Unless related to reporting of illegal content removal orders under the DSA. ⁹Some forms of misinformation and disinformation may be caught if they fall under scope of the UK's foreign interference and false communications offences.



Regulated entities

Analysis of the types of entities regulated in each jurisdiction is complex and does not lend itself to simple comparison as there are many definitional challenges. For example, there is significant overlap between the categories of **social media services, video-sharing platforms and services**, and **user-to-user platforms and services**. In the UK and EU, video-sharing platforms and services (VSPs), such as YouTube and TikTok, are a distinct category of regulated entity, in recognition of the risks associated with user-to-user video virality. Conversely, 'VSP' is not a legally defined category of regulated entities in Australia and the Republic of Korea. Instead platforms like YouTube, TikTok, and others with video-sharing functionalities, are captured under the definition of 'social media service.' So, where some jurisdictions choose to separate out sections of the online industry, others choose to combine into larger categories.

Similarly, '**user-to-user services**' (U2U) such as messaging apps, dating apps, games with communication functionalities, and other social media platforms are not a standalone category of 'regulated entities' in all jurisdictions. Some jurisdictions, like Australia and the Republic of Korea capture U2U services across other categories of entities such 'social media services' or 'messaging services.' What is important to note is that all jurisdictions capture the large mainstream online platforms and services in some way.

Jurisdiction	Categories of digital services and platforms										
	Social media services, Video-sharing platforms and services, User-to-user platforms and services	Hosting and storage services	Gaming services	App distribution services	Internet service providers	Messaging services and dating apps	End-to-end encrypted services	Search engine services	Websites	Generative AI services	Equipment services
Australia (eSafety)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fiji (OSC)	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗
France (Arcom)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗
Ireland (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ ¹¹	✓
Slovakia (CMS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
South Africa (FPB)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
The Netherlands (ATKM)	✓	✓	✓ ¹²	✗	✓	✓ ¹³	✗	✓	✓	✓	✗
United Kingdom (Ofcom) ¹⁰	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗

¹⁰In the UK, only services that are user-to-user, search or online pornography services are regulated entities under the Online Safety Act (2023). All categories marked as 'YES' are to the extent that are user-to-user, search or online pornography services. ¹¹KCSC regulates content on platforms like DALL-E because its content is publicly accessible. However, services such as ChatGPT are not regulated by KCSC because it interacts privately with individual users.

¹²The regulation of gaming services is subject to certain conditions. ¹³When messages are publicly disseminated.



Obligations for regulated entities

Analysis of obligations for regulated entities is complex and does not lend itself to simple comparison. This is because regulatory obligations and requirements do not necessarily apply equally across all categories of regulated online harms and regulated entities. Adding to the complexity, there is significant variation in how regulation applies within a single category of regulated entities, with most jurisdictions adopting a risk-based approach (or ‘tiered’ approach) to regulate in a way that is proportionate to the risks that exist on a particular platform or service. Most jurisdictions have imposed stricter and more onerous requirements on larger, riskier platforms.

Each jurisdiction varies in how it assesses or categorises ‘risk’ within their regulatory framework, with most taking into account a combination of factors such as number of users, user-demographics, geographical spread, service functionalities, type and number of content risks, likelihood and impact of online harms, service purpose, discoverability, algorithms and recommender usage, and more. The table below serves as a foundation of comparison, providing a broad overview of the types of interventions and requirements imposed by regulators across member jurisdictions.

Jurisdiction	Obligations for regulated entities																	
	Designate domestic agent able to receive legal notices	Comply with content removal, blocking, and link deletion notices	Comply with timeliness requirements for content notices	Comply with registered codes and standards	Adequately respond to information requests	Comply with transparency reporting and oversight requirements	Undertake risk assessments	Establish appropriate governance	Record keeping	Submit to auditing as required	Proactively minimise harmful and unlawful content	Empower users with choice	Implement age assurance systems	Take reasonable steps to protect children from content that is not age-appropriate	Take reasonable steps to ensure E2EE and anonymous services are safe	Provide user reporting mechanisms	Provide and enforce clear and accessible terms of service	Undertake online safety professional education
Australia (eSafety)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗
Fiji (OSC)	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
France (Arcom)	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗
Ireland (An Coimisiún)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Slovakia (CMS)	✓ ¹⁴	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗
South Africa (FPB)	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✓	✗	✗
The Netherlands (ATKM)	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓ ¹⁶	✓ ¹⁶	✗	✗	✗	✗	✓	✓ ¹⁶	✗
United Kingdom (Ofcom)	✗	✗	✗	✓ ¹⁵	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗

¹⁴Under the DSA, CMS may require a regulated entity to designate a domestic agent capable of receiving legal notices only if the regulated entity is headquartered in Slovakia. ¹⁵In the UK, regulated entities are required to comply with duties set out in the Online Safety Act (2023). Ofcom issues codes which recommend steps that regulated entities can take to comply. ¹⁶The obligations apply under certain conditions pursuant to the Terrorist Content Online (TCO) Regulation.

Information gathering and enforcement

Most jurisdictions adopt similar approaches to information gathering and enforcement, consisting of powers to obtain information through notices and supervisory functions, and firmer powers such as financial penalties or court ordered remedies. Importantly, not all enforcement powers are available in all instances of non-compliance. For some regulators, firmer powers such as business disruption orders and civil penalties only become available after recurring non-compliance with information requests. Other regulators are able to issue financial penalties in instances where content removal deadlines are breached. Further, the quantum of financial and civil penalties varies significantly between jurisdictions, with some able to issue fines of up to 10 per cent of global annual revenue. Noting those nuances, the table below provides a general overview of the various enforcement mechanisms available in each jurisdiction.

Jurisdiction	Information gathering and enforcement															
	Content-based enforcement actions				Information gathering powers						Systems-based regulatory enforcement		Court ordered remedies			
	Formal written warning	Take-down, deletion, and blocking notices	Actor or account-level directives ¹⁷	Financial penalties	Information notices	Supervisory powers	Transparency reporting requirements	Third party auditing	Submit to interview	Power of entry, inspection and audit	Formal written warnings and remedial directions (e.g., undertakings)	Financial penalties	Civil and administrative penalties	Injunctions	Service blocking or restriction orders (e.g., service, access, or payment blocking orders) ¹⁸	Damages
Australia (eSafety)	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗
Fiji (OSC)	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓
France (Arcom)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓
Ireland (An Coimisiún)	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Republic of Korea (KCSC)	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✓
Slovakia (CMS)	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
South Africa (FPB)	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓
The Netherlands (ATKM)	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗
United Kingdom (Ofcom)	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓

¹⁷'Account or actor-level directives' refer to directives or notices issued to end-users or platforms to facilitate removal of an account or individual from the specified platform or service. ¹⁸Service blocking and restriction orders includes 'business disruption orders.'