PANORAMIC

ONLINE SAFETY REGULATION

Hong Kong

LEXOLOGY

Online Safety Regulation

Contributing Editors

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

Generated on: February 13, 2026

Contents

Online Safety Regulation

Contributors

Hong Kong

YYC Legal LLP

Beverly Fu beverlyfu@east-concord.com.hk
Sam Wu samwu@east-concord.com.hk

LEGAL FRAMEWORK

Legal regime

Does your jurisdiction have a legal regime governing or addressing online safety? If so, how does it operate?

Hong Kong addresses online harms through fragmented and sector-specific legislation rather than a unified, comprehensive online safety statute like the United Kingdom's Online Safety Act or the European Union's Digital Services Act.

Instead, online safety in Hong Kong is governed through multiple statutes targeting specific harms. The Personal Data (Privacy) Ordinance (Chapter 486), as amended in 2021, criminally prohibits doxxing and unauthorised disclosure of personal data intended to, or reckless as to whether it will, cause harm. The Control of Obscene and Indecent Articles Ordinance (Chapter 390) requires internet service providers (ISPs) to remove content classified as obscene (Class III). The Telecommunications Ordinance (Chapter 106) criminalises infrastructure damage and unauthorised access. The Crimes Ordinance (Chapter 200) addresses dishonest computer access. The Unsolicited Electronic Messages Ordinance (Chapter 593) targets spam and deceptive commercial messages. The Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653) (effective 1 January 2026) imposes cybersecurity requirements across eight sectors (energy, telecommunications, banking and financial services, air transport, land transport, maritime, healthcare and information technology).

Hong Kong's online safety regime operates through decentralised enforcement by sector-specific bodies rather than a unified regulator. Generally, the regime is enforcement-reactive rather than prevention-proactive. Hong Kong law generally does not impose pre-emptive or affirmative duties on platforms to monitor user-generated content or implement safety-by-design measures (except for the newly enacted critical infrastructure cybersecurity framework). Instead, Hong Kong generally employs reactive and notice-and-takedown mechanisms.

Law stated - 9 January 2026

Online harms covered

Which online harms are covered under the relevant legislation and how are these harms defined?

Doxxing is the most explicitly regulated online harm. It is legally defined under section 64(3A) of the Personal Data (Privacy) Ordinance (Chapter 486) as the unauthorised disclosure of personal data of individuals or their family members without the data subject's consent, with the intent to cause specified harm or being reckless as to whether specified harm was caused. "Specified harm" encompasses harassment, molestation, pestering and intimidation of or threat to the person; bodily or psychological harm to the person; harm causing the person reasonably to be concerned for their safety or well-being; or damage to the property of the person.

Obscene and indecent content is criminalised under Part IV of the Control of Obscene and Indecent Articles Ordinance (Chapter 390), which prohibits Class III (obscene) and Class II (indecent) material unless any defences apply.

Copyright infringement is addressed through Division II of Part II of the Copyright Ordinance (Chapter 528), which imposes liability on persons copying works and/or making works available to the public without the licence or authorisation of the copyright owner.

Cybercrime, including damage to telecommunications infrastructure, unauthorised computer access and transmission of false or deceptive distress messages, is criminalised under sections 27, 27A and 28 of the Telecommunications Ordinance (Chapter 106) and section 60 of the Crimes Ordinance (Chapter 200).

Transmission of multiple commercial electronic messages with the intent to deceive or mislead recipients are addressed under section 20 of the Unsolicited Electronic Messages Ordinance (Chapter 593).

Law stated - 9 January 2026

Online services covered

Which online services are covered under the law and how are these services defined?

The law applies to a broad range of online service providers. The Copyright Ordinance (Chapter 528)'s definition – "a person who, by means of electronic equipment or a network, or both, provides, or operates facilities for, any online services" – encompasses ISPs, social media platforms, online forums and discussion boards, search engines, email service providers and content hosting services.

ISPs must obtain a telecommunications licence under the Telecommunications Ordinance (Chapter 106), making them subject to licence conditions on data protection, network security and interconnection. Social media platforms are fully liberalised, with no licensing requirements, foreign ownership restrictions or sector-specific regulations; they thus operate without statutory safety duties (except compliance with notice-based mechanisms for specific harms). Platform providers offering services such as cloud storage, file-sharing and communication services are captured by the regulatory framework, as are search engines and aggregators.

VPNs (permitted in Hong Kong with no restrictions) and encrypted messaging services (subject to general laws, but no special requirements) are not specifically regulated.

Law stated - 9 January 2026

Territorial scope

What is the territorial scope of the relevant law?

For doxxing, the law applies where the data subject is a Hong Kong resident or present in Hong Kong at the time of disclosure, regardless of where the disclosure originates. This creates an extraterritorial reach: overseas platforms operating globally may face cessation

notices from the Office of the Privacy Commissioner for Personal Data (PCPD) if they host content disclosing the personal data of Hong Kong residents without applicable defences. The PCPD has previously issued successful cessation notices to non-Hong Kong-incorporated service providers.

For other laws (copyright, obscenity and cybercrime), the general territorial principle applies. These laws primarily regulate conduct within Hong Kong, with enforcement focusing on ISPs and platforms operating within Hong Kong. However, ISPs in Hong Kong must comply with all applicable laws regardless of user location.

Law stated - 9 January 2026

Codes of practice

Are there any codes of practice or other non-binding guidelines or recommendations relating to online safety in your jurisdiction?

The Code of Practice for Internet Computer Services Centres Operators provides guidance on operator responsibilities, including anti-crime measures, CCTV requirements, content filtering for obscene material and operating hour restrictions for minors.

The Practice Guide for Social Media Security (issued by the Hong Kong government's Digital Policy Office in July 2024) offers guidance on security measures; password protection; phishing awareness; and prevention of false information, fake news and sensitive data disclosure.

The Privacy Commissioner for Personal Data has issued Guidance Notes for mobile service operators on data- handling best practices, customer conversation recording, account maintenance and data protection principles.

The Code of Practice on Copyright Protection in the Digital Environment, published by the Commerce and Economic Development Bureau in February 2023, sets out "notice and notice system" and "notice and takedown system" procedures for service providers' handling of notices of alleged copyright infringement.

The Hong Kong government's publication "Points to Note for Internet Social Networking" (last updated in March 2025) offers risk assessment guidance to users.

The Hong Kong government collaborates with the Hong Kong Internet Service Providers Association on a self-regulatory Code of Practice, the "Practice Statement on Regulation of Obscene and Indecent Material". This stipulates that publishers of Class II (indecent) internet content must display a prescribed on-screen warning notice before users can access it. For Class III (obscene) articles published online, ISPs must remove or block the content to prevent access within Hong Kong.

The Ethical Artificial Intelligence Framework (issued by the Hong Kong government's Digital Policy Office in December 2025) provides non-binding guidance on artificial intelligence systems used in online services.

IT Security Guidelines [G3] issued by the Hong Kong government's Digital Policy Office in April 2025 establish security standards.

These frameworks are non-binding and carry no statutory enforcement mechanism, but they shape professional norms and best practices across the industry.

Law stated - 9 January 2026

Harmful versus illegal content

How does the law in your jurisdiction distinguish between harmful and illegal content?

Hong Kong law does not formally distinguish between harmful and illegal content. The legal framework addresses only specifically prohibited content (copyright infringement, obscenity, doxxing and cybercrime), with no statutory definition of "harmful" content that does not violate criminal law.

In practice, ISPs and platforms face binding removal obligations only if the content is illegal. Unless it falls under the categories of copyright infringement, obscenity, doxxing and cybercrime, harmful content is not subject to removal obligations and platforms retain editorial discretion. Similarly, the common law "innocent dissemination" defence for defamation, which applies to intermediaries, does not require proof that content is false; it requires only that the intermediary took reasonable steps to remove it promptly upon notice of defamatory statement.

Law stated - 9 January 2026

Extremist and terrorism-related content

How does your jurisdiction regulate the dissemination of extremist and terrorism-related content online?

Hong Kong has no dedicated legislation specifically targeting extremist or terrorism-related content online.

Applicable frameworks derive from general criminal law. The Hong Kong National Security Law (2020) grants the Hong Kong Police authority to request removal of electronic messages "reasonably suspected" to constitute offences endangering national security, with non-compliance attracting penalties of a HK$100,000 fine and six months' imprisonment. The Crimes Ordinance (Chapter 200) addresses incitement to violence and its sedition provisions remain in force. The doxxing provisions under the Personal Data (Privacy) Ordinance (Chapter 486) may apply if extremist content involves the disclosure of personal data intended to (or being reckless as to whether such disclosure will) cause specified harm.

Hong Kong imposes no specific time frame for removal of extremist and terrorism-related content, and does not have a dedicated body overseeing its moderation. The framework relies on police-initiated requests rather than imposing systematic obligations on platforms to identify and remove such content.

There are no proactive duties requiring platforms to identify extremist content, and no guidelines distinguishing "extremist" content from content prohibited under the National Security Law.

Law stated - 9 January 2026

Disinformation versus misinformation

How, if at all, does the law in your jurisdiction distinguish between misinformation and disinformation online? Does it include malinformation?

Hong Kong law does not address misinformation, disinformation or malinformation. There is no dedicated legislation governing any of these categories.

Conceptual frameworks exist only in academic research. The "Measures to tackle disinformation, misinformation and hate speech in selected places" issued by the Research Office of the Hong Kong Legislative Council Secretariat (Research Office) on 5 May 2023 propose the following distinctions: disinformation is the intentional dissemination of false and misleading information, while misinformation is the unintentional spread of false and misleading information. Other research institutions propose that malinformation refers to genuine information that is shared with malintent (eg, hate speech). However, these conceptual boundaries have not been incorporated into statutory provisions.

In July 2020, the Research Office proposed to establish fact-checking initiatives to improve competence in identifying and verifying inaccurate information. In November 2021, the Hong Kong government announced that the Home Affairs Bureau had commissioned a study of legislative measures addressing online disinformation. As of January 2026, no legislative proposal has been introduced to the Legislative Council.

Law stated - 9 January 2026

OBLIGATIONS FOR ONLINE SERVICE PROVIDERS

General obligations

What general legal obligations relating to safety are imposed on providers of online services, including providers of online intermediary services?

Hong Kong does not impose comprehensive and proactive safety duties on online service providers. Instead, obligations are notice-triggered and context-specific.

Copyright infringement: platforms must remove infringing works upon receipt of a valid notice (the notice and takedown system) and notify subscribers of alleged infringement (the notice and notice system). Compliance with the Code of Practice governing these procedures qualifies service providers for safe harbour protection, limiting liability to injunctive relief (content removal) rather than damages.

Doxxing: upon receipt of a cessation notice from the Office of the Privacy Commissioner for Personal Data, online service providers must cease or restrict disclosure of personal data.

Obscene/indecent content: internet service providers and platforms must not publish or knowingly possess Class II (indecent) or Class III (obscene) material without applicable defences. While no affirmative monitoring duty exists, defences are limited if content is discovered and retained.

National security threats: upon police request, internet service providers (ISPs) must remove or restrict access to messages suspected of constituting offences under the National Security Law, with penalties applicable for non-compliance.

Data protection: all data users (including platforms) must take all practical steps to protect personal data against unauthorised access, processing, erasure, loss or use.

Spam: service providers must not transmit or facilitate transmission of unsolicited commercial electronic messages or messages with deceptive source information.

Law stated - 9 January 2026

Risk assessments and mitigation

Are there any specific legal obligations for online service providers to conduct risk assessments and mitigate risks to safety?

There are specific legal obligations only for critical infrastructure sectors, pursuant to the newly enacted Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653), effective 1 January 2026.

Designated Critical Infrastructure Operators (CIOs) in eight sectors (energy, telecommunications, banking and financial services, air transport, land transport, maritime, healthcare and information technology) must meet three categories of obligations: preventative, organisational and incident response obligations.

Preventative obligations require CIOs to conduct annual risk assessments of their critical computer systems and undergo biennial independent audits to assess the likelihood and impact of cybersecurity incidents. Organisational obligations mandate maintenance of a Hong Kong address, designation of a cybersecurity team and prompt notification of changes to the Office of the Commissioner of Critical Infrastructure (Computer-system Security). Incident response obligations require that computer system security incidents that have disrupted, are disrupting or are likely to disrupt the core function of the critical infrastructure concerned must be reported within 12 hours of CIOs becoming aware of the incident. In any other cases, the incident must be reported within 48 hours of the CIOs becoming aware of it.

For general online safety (content harms as opposed to cybersecurity), no statutory risk assessment requirement exists. Platforms are not obliged to assess risks of illegal content, child exploitation, misinformation or harassment.

Non-compliance with critical infrastructure obligations (on conviction on indictment) attracts fines of HK$500,000 to HK$5 million plus daily fines of HK$50,000 to HK$100,000 for continuing offences, which are imposed at the organisational level (not individual directors).

Law stated - 9 January 2026

Protection of minors and age verification

Are there any specific legal obligations to protect minors online? If so, what measures are required or advised, such as age verification?

Hong Kong has no comprehensive child protection framework. Statutory obligations to protect minors online are minimal and indirect.

The Control of Obscene and Indecent Articles Ordinance (Chapter 390) prohibits publication of Class II (indecent) or Class III (obscene) material to persons under 18 years of age. The Prevention of Child Pornography Ordinance (Chapter 579) prohibits the publication of child pornography. The Personal Data (Privacy) Ordinance (Chapter 486) applies to all personal data, including children's data, requiring all data users (including platforms) to protect data security.

Law stated - 9 January 2026

Civil and human rights

Are there any obligations for online service providers to balance civil and human rights, such as privacy rights and freedom of expression, with safety regulations? If so, what measures are required or advised?

There is no statutory framework that explicitly addresses balancing civil and human rights with online safety. However, two relevant principles emerge from case law and codes of practice: the innocent dissemination defence and Copyright Safe Harbour.

The innocent dissemination defence (in defamation cases): the Court of Final Appeal established that intermediaries may avoid defamation liability if they prove they took all reasonable steps to remove offending content promptly upon becoming aware of it. This doctrine balances publishers' freedom of expression against plaintiffs' rights to protect reputation. The standard of "reasonableness" applies both before and after notice. In ***Oriental Press Group Ltd v Fevaworks Solutions Ltd*** (FACV 15/2012), the court held that removal within 3.5 hours of notice satisfied the defence.

Copyright safe harbour: the safe harbour regime balances copyright owners' exclusive rights against users' interests by protecting fair dealing (parody, satire, caricature, pastiche, news reporting, criticism and review). The Code of Practice on Copyright Protection in the Digital Environment issued by the Commerce and Economic Development Bureau in February 2023 incorporates user dispute mechanisms, allowing subscribers to dispute or deny alleged infringements.

Law stated - 9 January 2026

Disinformation and misinformation

Are there any specific legal obligations to combat disinformation and misinformation online? If so, what measures are required or advised?

There are currently no specific statutory obligations in Hong Kong. The Hong Kong government has not enacted legislation requiring platforms or individuals to combat or remove disinformation and misinformation online.

Law stated - 9 January 2026

Notice and takedown

Is there a legislative 'notice and takedown' mechanism or similar in your jurisdiction? If so, how does it operate?

Yes, but it is limited to four specific contexts: copyright infringement, doxxing, national security threats and obscene/indecent content.

Copyright infringement (sections 88A-J of the Copyright Ordinance (Chapter 528)):a dual system operates. (1) the "Notice and Notice" procedure requires the service providers to notify the subscriber that their account has been identified in connection with alleged infringement, allowing the subscriber to dispute or deny the infringement; and (2) the "Notice and Takedown" procedure requires the removal or disabling of access to materials identified as infringing. Both procedures are also codified in an accompanying Code of Practice. Compliance with this Code of Practice qualifies service providers for safe harbour protection, on the statutory condition that they take "reasonable steps to limit or stop" the infringement "as soon as practicable" after they "received a notice of alleged infringement", "became aware that the infringement has occurred" or "became aware of the facts or circumstances that would lead inevitably to the conclusion that the infringement had occurred".

Doxxing (section 66O of the Personal Data (Privacy) Ordinance (Chapter 486)): the Office of the Privacy Commissioner for Personal Data (PCPD) issues cessation notices demanding that platforms cease or restrict disclosure of personal data that may constitute a doxxing offence. Failure to comply constitutes a criminal offence. No statutory time frame is specified, but the PCPD applies a reasonableness standard. Between the effective date (8 October 2021) of the relevant provisions and 31 December 2024, the PCPD issued 2,072 notices to 53 online platforms, requesting the removal of 33,600+ doxxing messages and achieving a compliance rate of over 96%. Defences available to the recipients of such notices include having a reasonable excuse for non-compliance, technological infeasibility or substantial prejudice to third parties.

National security threats: the Commissioner of Police may issue a written request to internet service providers demanding removal or restriction of electronic messages "reasonably suspected" to constitute or incite National Security Law offences.

Obscene/indecent content: while no formal notice-and-takedown procedure is specified, courts may issue injunctions requiring removal. Internet service providers have a general obligation not to publish or knowingly possess Class II (indecent) or Class III (obscene) material.

Law stated - 9 January 2026

ENFORCEMENT AND PENALTIES

Enforcement

How is the online safety regime enforced in your jurisdiction?

Enforcement is carried out through decentralised, multi-agency mechanisms that are predominantly complaint-driven and reactive: Office of the Privacy Commissioner for Personal Data (PCPD)-led enforcement, police-led enforcement, Office of the

Communications Authority (OFCA)-led enforcement, copyright enforcement and platform cooperation.

PCPD-led enforcement (doxxing): the PCPD receives complaints from individuals, conducts online patrols, investigates alleged doxxing, issues cessation notices to platforms, monitors compliance and prosecutes non-compliance. The PCPD may also conduct criminal investigations and prosecute in the Magistrates' Court, though serious cases are referred to the Department of Justice.

Police-led enforcement (cybercrime and National Security Law): the Cyber Security and Technology Crime Bureau investigates unauthorised computer access, data damage and other technology crimes, while the National Security Department investigates National Security Law violations. Police may request the cooperation of internet service providers (ISPs) in removing content that threatens national security under National Security Law.

OFCA-led enforcement (telecoms and spam):the OFCA enforces ISPs' licence conditions, fair trading provisions and the Unsolicited Electronic Messages Ordinance (Chapter 593) through imposing additional licence conditions, directions and information requests.

Copyright enforcement: copyright owners may give notices of alleged infringement to the service providers if it is alleged that a copyright infringement has occurred or is occurring on the service provider's service platform. The service provider must respond in accordance with the Copyright Ordinance (Chapter 528) and its associated Code of Practice. Disputes may be resolved administratively or through civil court proceedings.

Platform cooperation: most platforms comply voluntarily with notices (the compliance rate for doxxing cessation notices between 2021 and 2024 was 96%), with the threat of criminal liability reinforcing compliance.

Law stated - 9 January 2026

Authorities

Which authorities are responsible for enforcement? What is the basis, nature and extent of their enforcement powers?

The PCPD, OFCA, Hong Kong Police Force, Department of Justice, Office for Film, Newspaper and Article Administration (OFNAA), and Hong Kong Courts are responsible for enforcement.

PCPD: the basis of the PCPD's enforcement powers are section 64 (doxxing) of the Personal Data (Privacy) Ordinance (Chapter 486) and data protection laws under the Personal Data (Privacy) Ordinance (Chapter 486). The PCPD may issue cessation notices; conduct criminal investigations; request evidence and materials; apply for magistrate warrants to search premises and access devices; access devices without warrant where reasonable; stop, search and arrest persons; institute prosecutions in the Magistrates' Court and refer serious cases to the Department of Justice.

OFCA: the basis of the OFCA's enforcement powers are the Telecommunications Ordinance (Chapter 106) and the Unsolicited Electronic Messages Ordinance (Chapter 593). The OFCA may grant or revoke internet service provider licences, impose licence conditions, issue directions to internet service providers, request information, conduct facility inspections,

enforce competition and/or fair trading provisions and refer serious cases to the Department of Justice.

Hong Kong Police Force: the Cybersecurity and Technology Crime Bureau may investigate unauthorised computer access, data damage and computer crimes under the Crimes Ordinance (Chapter 200), while the National Security Department may investigate violations of National Security Laws and request ISPs to remove content that threatens national security under the National Security Law. The Hong Kong Police Force may also arrest, investigate, prosecute and exercise extraterritorial jurisdiction over National Security Law offences.

Department of Justice: prosecutes serious cybercrimes and doxxing cases referred by PCPD or OFCA.

OFNAA: the basis of the OFNAA's enforcement powers is the Control of Obscene and Indecent Articles Ordinance (Chapter 390). The OFNAA may investigate by applying statutory guidelines and past classifications by the Obscene Articles Tribunal (OAT). Articles that are clearly Class III (obscene) are passed directly to the Hong Kong Police for follow-up. If classification is uncertain, the article is sent to the OAT for a formal decision. For overseas webpages (eg, on video-sharing platforms) requiring follow-up, such as adding warning notices or removing content, the Hong Kong Police or the OFNAA may refer cases to foreign law enforcement agencies or website operators for action. The OFNAA conducts subsequent inspections to monitor compliance by these overseas entities.

Courts: issue injunctions to block copyright-infringing websites and award civil remedies in defamation and copyright cases.

Law stated - 9 January 2026

Penalties and liability

What are the potential fines or penalties for non-compliance? Are there risks of liability for employees or directors of online service providers?

Fines and penalties for non-compliance vary according to the nature of the offence.

Doxxing Offences under the Personal Data (Privacy) Ordinance (Chapter 486): individual perpetrators who commit doxxing face full criminal penalties, on conviction, to a fine of HK$1 million and imprisonment for five years (section 64(1) of the Personal Data (Privacy) Ordinance (Chapter 486)). Platform operators and ISPs may bear organisational liability for failure to comply with cessation notices issued by the PCPD, but directors and employees of those organisations typically do not face personal criminal liability unless they personally commit doxxing or obstruct the PCPD investigation.

Offences under the Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653) (effective 1 January 2026): this Ordinance imposes strict liability at the organisational level only. Penalties range from HK$500,000 to HK$5 million, plus daily fines, for failing to provide the required information under sections 14 to 17 to the Monetary Authority, the Communications Authority or the Commissioner of Critical Infrastructure (Computer-system Security). Penalties are levied against the company, not individual directors or officers.

Cybercrime offences: individuals who personally commit computer crimes (unauthorised access, data damage or transmission of false distress messages) face criminal liability. Platform operators and ISPs are generally not liable for user-generated cybercrimes unless they knowingly facilitate them or fail to cooperate with police investigations.

National Security Law violations: a service provider's failure to comply with a police request to remove content that threatens national security under National Security Law attracts organisational liability of a HK$100,000 fine and imprisonment for six months for the responsible officer. Individual directors may face liability if they authorise or direct non-compliance, but the statute does not create automatic individual director liability.

Obscene/indecent content: ISPs and platform operators face criminal liability for publishing or knowingly possessing Class II (indecent) or Class III (obscene) material. Individual perpetrators who upload such content also face personal criminal penalties.

Data Protection: the Personal Data (Privacy) Ordinance (Chapter 486) does not establish explicit individual director liability for data security breaches. Enforcement generally targets the organisation rather than individual officers, unless an officer personally directs a data breach or obstructs an investigation by the PCPD.

Law stated - 9 January 2026

DISPUTES

Claims

What claims relating to online safety are available and most common in your jurisdiction?

In Hong Kong, five types of claims generally relating to online safety are available: defamation, harassment, privacy, copyright infringement and criminal claims.

Defamation (the most common civil claim): a plaintiff must prove that an online statement is defamatory (lowering their reputation in the minds of reasonable people; making people shun or avoid the plaintiff; subjecting the plaintiff to public hatred, contempt or ridicule or demeaning the plaintiff in their profession or business), that it was published and that it refers to the plaintiff. Intermediaries may use the "innocent dissemination" defence by proving they took reasonable steps to remove the statement promptly upon notice.

Harassment (common law tort): this includes conduct causing nuisance, molestation, pestering, threat, intimidation or harassment. Hong Kong courts may order content removal or corrective public statements.

Privacy tort (civil): this provides an equitable remedy for wrongful disclosure of confidential information causing harm, which is separate from criminal liability under the Personal Data (Privacy) Ordinance (Chapter 486).

Copyright infringement (civil): available remedies include an account of profits, damages, additional damages and injunctions to block infringing websites.

Criminal claims (less common but significant): these primarily involve doxxing prosecutions by the Office of the Privacy Commissioner for Personal Data (PCPD) and computer crime investigations by the Hong Kong Police.

Law stated - 9 January 2026

Procedure

What is the procedure for claimants to bring actions relating to online safety in your jurisdiction?

Procedures for claimants to bring actions relating to online safety vary according to the nature of the claim.

Civil proceedings: a claimant may obtain legal representation, file in the District Court (for claims up to HK$3 million) or High Court (for claims in excess of HK$3 million), engage in discovery of electronic communications and proceed to trial before a judge. The burden of proof is on the claimant on a balance-of-probabilities basis.

Criminal doxxing prosecution: a claimant may report the case to the Hong Kong Police or the PCPD. The PCPD investigates and may prosecute in the Magistrates' Court for summary offences, or refer to the Department of Justice for indictable offences. The burden of proof is on a beyond -reasonable -doubt basis.

Doxxing cessation notice: a complainant may report to the PCPD or submit evidence of doxxing. The PCPD investigates and issues cessation notice to the platform. This is primarily an administrative enforcement mechanism through notice; if the platform fails to comply, the PCPD may initiate prosecution. Generally, no separate court proceedings are required unless the platform contests validity.

Copyright infringement notice: a complainant may serve notice of alleged infringement on service providers in accordance with the Copyright Ordinance (Chapter 528) and its associated Code of Practice. The service providers should respond within the time frame specified in the Code of Practice. Dispute resolution occurs administratively; if unresolved, the complainant may file a civil lawsuit in the District Court or the High Court for damages and an account of profits.

Law stated - 9 January 2026

Remedies

What interim and substantive remedies may be imposed in relation to online safety claims?

Interim remedies (civil): Hong Kong courts may issue injunctions to prevent continued publication. The PCPD's cessation notices function as quasi-interim remedies, often resulting in rapid platform removal (generally within days to weeks).

Substantive remedies (civil): substantive civil remedies include damages, which are generally compensatory (eg, for lost earnings). Hong Kong courts may also issue declarations of falsity, as well as corrective orders requiring public apologies or corrections. Content removal may also be enforceable through court orders or achieved through voluntary platform compliance.

Law stated - 9 January 2026

Defences and exemptions

Does your jurisdiction provide any defences or exemptions from liability for online safety claims? If so, how do they operate and which online services providers may avail of them?

There are four defences and exemptions from liability for online safety claims: the innocent dissemination defence, safe harbour, the mere conduit defence and the reasonableness defence.

Innocent dissemination defence (for defamation claims): this defence is available if the intermediary proves it had no knowledge of the defamatory content and took reasonable steps to remove it promptly upon becoming aware. The standard of reasonableness applies both before and after notice. Time frames of three to four hours have been found reasonable by the Hong Kong courts; extended delays (of eight or more months) may defeat the defence.

Safe harbour (sections 88A-J of the Copyright Ordinance (Chapter 528)): service providers that comply with prescribed conditions qualify for safe harbour protection. These conditions are: (1) taking reasonable steps to limit or stop infringement upon notice; (2) not receiving financial benefit directly attributable to infringement; and (3) implementing notice-and-notice or notice-and-takedown procedures per the Code of Practice in relation to the Copyright Ordinance (Chapter 528). Statutory protection extends to injunctive relief (content removal).

Mere conduit defence (general principle): internet service providers that only supply physical facilities for user communication and have no knowledge of offending content may be exempt from liability for user-generated harm.

Reasonableness defence (doxxing cessation notice): under section 66O(2) of the Personal Data (Privacy) Ordinance (Chapter 486), a person/platform may defend non-compliance with a cessation notice by establishing a reasonable excuse for non-compliance, or by establishing that compliance was not reasonably expected due to: (1) the nature, difficulty or complexity of the cessation action concerned; (2) technology not being reasonably available; or (3) the risk of causing substantial loss or prejudice to third parties.

Law stated - 9 January 2026

UPDATE AND TRENDS

Key trends and future developments

What are the most noteworthy recent trends and developments in online safety regulation in your jurisdiction? What developments are expected in the coming year?

The most significant development in 2025 was the passage of Hong Kong's first comprehensive cybersecurity law on 19 March 2025. The Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653) took effect on 1 January 2026, establishing mandatory cybersecurity requirements for designated operators in eight critical sectors (energy, telecommunications, banking and financial services, air transport, land transport, maritime, healthcare and information technology) and for critical societal or economic facilities such as major sports venues and research parks.

Compliance obligations fall into three categories: organisational requirements (maintaining a Hong Kong address, designating cybersecurity teams and reporting changes), preventative measures (conducting annual risk assessments and biennial independent audits of critical computer systems) and incident response protocols (reporting serious incidents within 12 hours and general incidents within 48 hours). This represents a paradigm shift from Hong Kong's historically reactive regulatory posture towards proactive and prevention-focused governance, aligning the jurisdiction 's cybersecurity standards with those of the European Union, Australia and the United Kingdom.

Expected developments in 2026 and ongoing developments

A new Commissioner's Office for Critical Infrastructure (Computer-system Security) will be established by Q1 2026 to oversee compliance with the Protection of Critical Infrastructures (Computer Systems) Ordinance (Chapter 653).

The Hong Kong government aims to designate Critical Infrastructure Operators within six months of the establishment of the Commissioner's Office (approximately mid-2026 onwards), which will occur progressively based on "risk assessment and the level of readiness of the organisations". Within the first three months of designation operators must submit computer system security management plans and emergency response plans, which must be implemented immediately.

The Law Reform Commission's Sub-committee on Cybercrime proposed five new statutory cybercrimes in June 2022: illegal data access, illegal data interception, illegal data interference, illegal system interference and possession of devices/data for crime. These recommendations remain under government review and may be revisited, though no firm timeline for legislative action has been provided.

A government-commissioned study of legislative approaches to misinformation and disinformation, published in June 2021, remains ongoing as of January 2026. No legislation has yet been proposed and no further development is expected in 2026.

Law stated - 9 January 2026