INDOCHINE COUNSEL
Business Law Practitioners

Special Alert

VIETNAM - DRAFT DECREE ON CYBERCRIME PREVENTION: NEW MOVES BY REGULATORS TO TIGHTEN COMPLIANCE REQUIREMENTS

April 2026

On 16 March 2026, the Ministry of Public Security finalized a draft decree on preventing and combating cybercrime and high-tech crime (the "**Draft**") to solicit feedback from agencies, organizations and individuals. One of the key bases for proposing the Draft is to promptly combat and address the increasingly complex landscape of cyberattacks, fraud and the dissemination of false information both domestically and internationally. This is a necessary step by policymakers toward tightening oversight and control over criminal activities occurring in cyberspace.

Although the Draft is still at the initial consultation phase and the public still needs to await more information from the competent authorities, given its significant objectives, it is expected to propose notable legal provisions and have a strong impact on the awareness of relevant stakeholders. This article will highlight and analyze the key points of the Draft to provide stakeholders with a preliminary understanding and to get ready for next actions.

The Draft was open for feedback for ten (10) days and concluded on 26 March 2026.

Key Takeaways

- **Specifying Certain Key Definitions**: The definitions of service providers and online fraud are introduced as an initial step to clarify their scope and better reflect the nature of these concepts in practice.

- **Compliance Responsibilities in Cyberspace**: The Draft includes a separate provision outlining general compliance responsibilities for both service providers and users. Specifically for managing online groups and communities in cyberspace, the Draft clearly defines the compliance obligations not only for participants, administrators and moderators, but also for the service providers themselves. All of these provisions, in part, allocate responsibilities to the relevant parties and also enable them to better safeguard themselves in the context of compliance in cyberspace.

- **Online Fraud and Child Abuse in Cyberspace**: The Draft details specific acts of online fraud and child abuse in cyberspace, aiming to help the public recognize the complexity of these crimes and protect themselves when participating in online activities.

Specifying Certain Key Definitions

The Draft introduces the concept of *"service provider"* to broaden the scope of application to relevant entities. This is a notable and timely addition, as previous provisions lacked specificity, leading to difficulties in identifying the entities subject to regulation. Accordingly, service providers are defined as domestic and foreign enterprises, organizations, individuals that provide products, services in cyberspace within Vietnam, including: internet services, postal and telecommunications services, hosting services, servers, domain names, virtual private network, proxy servers, cloud computing services, social networks, websites, telecommunications services, financial institutions, credit institutions, banks, branches of foreign banks in Vietnam, e-wallets, payment intermediaries, stock exchanges, digital asset exchanges, e-commerce platforms, logistics services, digital television, online games, artificial intelligence, quantum, anonymous server services, and other products, services in cyberspace.

In addition, the detailed description of *"online fraud"* is also considered a fundamental new feature of the Draft compared to previous regulations. It's not simply about specifying a concept, but also reflects how lawmakers seek to enable the public to more accurately understand this type of crime. This is particularly important given that the methods, increasingly sophisticated tactics and growing complexity of online fraud show no signs of abating in cyberspace, causing significant harm to unsuspecting victims. Initially, the Draft proposes that *"online fraud"* refers to acts involving the use of computer networks, telecommunications networks, the internet, electronic devices, artificial intelligence, information technology software, malware, and other similar digital technologies to create and disseminate false information, images, audio, video clips, to impersonate individuals or organizations, in order to deceive victims into believing and following instructions, or to threaten and intimidate victims into providing sensitive information or transferring money, assets for misappropriation. Although the definition remains preliminary, it generally reflects how online fraud is currently carried out in practice.

Compliance Responsibilities in Cyberspace

Responsibilities for Providing and Using Services

The Draft dedicates a separate chapter to clearly outlining the authority and responsibilities of relevant stakeholders in preventing and combating cybercrime and high-tech crime. In this context, service providers and users in cyberspace are no exception, with clearly separated responsibilities for each entity.

Some notable and key responsibilities under the Draft are set out below:

Entities	Service Providers	Service Users
Responsibilities	✓ Implement electronic identification and authentication of service users; adopt measures to detect, prevent	✓ Maintain the confidentiality of registration, management, and usage information, and not

Entities	Service Providers	Service Users
	unauthorized use; ensure the confidentiality of information and documents of users; ✓ Comply with applicable regulations on data security, retention periods, storage, provide information and electronic data; ✓ Cooperate with competent authorities; ✓ Follow the guidance of the Ministry of Public Security on connecting, receiving, responding to electronic documents; ✓ Provide information, documents, electronic data in a full, accurate, timely manner, ensure confidentiality to competent authorities; ✓ Implement necessary measures, in accordance with the guidance of competent authorities, upon receiving warnings relating to cybersecurity and high-tech crimes; ✓ Be liable for damages incurred in the event of failure to comply with the guidance of competent authorities; ✓ Report to competent authorities within 24 hours from the detection of any cyberattack; and ✓ Identify IP addresses of organizations, individuals using internet services in accordance with the regulations and guidance of the Ministry of Public Security.	allow other person to use digital account; ✓ Provide information, documents, electronic data to competent authorities, service providers in full, in accordance with applicable laws; and ✓ Lock, remove accounts associated with an individual's registration information upon detecting that such accounts are being used by others without authorization or are being used for unlawful purposes.

Responsibilities for Managing Online Groups and Communities

In addition to the general provisions, compliance responsibilities are also proposed to apply to all relevant parties, from participants, to administrators and moderators, as well as without excluding service providers, reflecting a clear intent to tighten control over the operation of online groups and communities in cyberspace. Specifically:

Entities	Participants	Administrators and Content Moderators on Social Media	Service Providers of Internet, Telecommunications, and Social Media
Responsibilities	✓ Comply with applicable regulations, group and community rules and service providers' terms;	✓ Manage operations in compliance with applicable regulations; ✓ Establish internal rules and terms of service in	✓ Establish and implement mechanisms for management, monitoring, and enforcement to prevent violations of applicable laws;

Entities	Participants	Administrators and Content Moderators on Social Media	Service Providers of Internet, Telecommunications, and Social Media
	✓ Do not post, share, comment on content that violates the law; ✓ Promptly report and denounce violations; and ✓ Provide information and cooperate with relevant authorities upon being requested.	accordance with applicable laws; ✓ Monitor members and posted content; remove content that violates applicable laws and report criminal activities to service providers or competent authorities upon detection; and ✓ Be responsible for the activities of the group and communities under management.	✓ Apply technical measures to detect, warn, handle online groups and communities showing signs of legal violations; ✓ Conduct electronic identification, authentication of administrators; ✓ Establish mechanisms for receiving and handling reports, complaints from service users for violating groups and communities; ✓ Provide information and data relating to online groups and communities upon request by competent authorities; ✓ Develop mechanisms for member verification and content moderation; and ✓ Provide tools to assist in scanning, detecting and reporting groups, accounts, posts showing signs of legal violations and coordinate handling within no more than 24 hours for normal requests and no more than 3 hours for emergency cases threatening national security or human life.

At first glance, these provisions may seem quite general, but in practice, they are likely to impose a wide range of requirements not only from a legal perspective but also from a technical standpoint (e.g., control systems, technical measures, etc.,) that relevant stakeholders, specially service providers, must meet. Although this will cause some difficulties for entities, at this point, entities should begin considering the review and verification of user information, creating appropriate monitoring and management mechanisms for the use of services in cyberspace.

Acts of Using Cyberspace for Online Fraud

In addition to defining online fraud, the Draft also sets out specific acts involving the use of cyberspace for online fraud.

Including this list not only fills existing legal gaps but also accurately reflects the forms of online fraud that are actually occurring. This also helps the public identify, prevent, and protect themselves against conduct indicative of criminal activity.

Some notable acts identified and enumerated include:

- Impersonating law enforcement authorities, state agencies, corporate employees, individuals or organizations to commit online fraud;
- Soliciting investments in financial exchanges, foreign exchange markets, stock exchanges, cryptocurrency exchanges, and other similar platforms in cyberspace to commit online fraud;
- Using forged or false images and information, including payment receipts, citizen ID cards, bank cards, employee ID cards, etc., to approach potential victims; and
- Using cyberspace to post false content in order to misappropriate property.

In order to promptly detect and handle violations, competent authorities are required to transfer information on online fraud accounts to specialized authorities responsible for combating high-tech crimes, and for coordination with commercial banks, financial institutions, and asset trading platforms to block, suspend related transactions.

Acts of Child Abuse in Cyberspace

All acts of abuse against children, as a vulnerable group requiring special protection, in cyberspace are strictly prohibited. Accordingly, some notable acts of child abuse in cyberspace include:

- Using cyberspace to entice, lure, coerce children to commit abusive acts; approaching children for abusive purposes through social media; threatening, coercing children to provide images or personal data for abusive purposes, etc;
- Distributing, sharing, transmitting child abuse content on the internet; providing links, private groups, platforms for exchanging child abuse content, etc;
- Using children's images, information for illicit gain; coercing, enticing children to participate in online activities for unlawful profit, etc;
- Threatening, insulting, humiliating, defaming the honor, dignity of children; unlawfully disclosing children's personal information, private life, etc;
- Illegally collecting, trading, exchanging children's personal data; using such data for abusive purposes, fraud, asset misappropriation, etc; and
- Providing platforms, tools, services to facilitate child abuse; concealing, obstructing the detection, reporting, handling of child abuse, etc.

The above-listed acts demonstrate that authorities have been closely monitoring the actual occurrence of child abuse. The comprehensive and detailed reflection in the Draft also contributes to addressing gaps in previous legal frameworks.

Conclusion

The Draft clearly reflects the principle of proactive prevention, the protection of personal data, and a risk-based approach (the higher the risk - the tighter the control). Although the Draft has not yet been officially approved and will likely undergo further consultation, initially identifying the roles and taking appropriate actions will help stakeholders proactively respond to upcoming legal developments.

All stakeholders must always be aware of their responsibilities in complying with regulations in cyberspace, especially participants, administrators and moderators, as well as service providers in managing groups and communities. At the same time, stakeholders should pay particular attention to online fraud and child abuse in cyberspace to identify and address any potentially criminal behavior promptly.

About Indochine Counsel

Established in October 2006, Indochine Counsel is a premier commercial law firm in Vietnam. We're ideally positioned to help international investors and foreign firms navigate the legal landscape in one of Asia's most dynamic and exciting countries. We also take pride in our services for domestic clients searching for opportunities abroad. With over 45 lawyers and staff in two offices, Ho Chi Minh City and Hanoi, Indochine Counsel offers expertise in a dozen practice areas assisting you throughout the entire life cycle of your business. We're your trusted partner in Vietnam for international and domestic legal solutions.

Indochine Counsel represents and advises clients on all legal aspects in the following major areas of expertise:

- Anti-trust & Competition
- Banking & Finance
- Corporate & Commercial
- Energy, Natural Resources & Infrastructure
- Intellectual Property
- Inward Investment
- Labour & Employment
- Litigation & Dispute Resolution
- Mergers & Acquisitions
- Real Estate & Construction
- Securities & Capital Markets
- Technology, Media & Telecommunications

Contact Us

For further information or assistance, please contact the following professionals at Indochine Counsel:

Thai Gia Han
Senior Associate | Head of IP & TMT Practice Group
E han.thai@indochinecounsel.com

Nguyen Trung Nghia
Junior Associate
E nghia.nguyentrung@indochinecounsel.com

Ho Chi Minh City

Unit 305, 3rd Floor, Centec Tower
72-74 Nguyen Thi Minh Khai, Xuan Hoa Ward
Ho Chi Minh City, Vietnam

T +84 28 3823 9640
F +84 28 3823 9641
E info@indochinecounsel.com

Hanoi

Unit 705, 7th Floor, CMC Tower
Duy Tan Street, Cau Giay Ward
Hanoi, Vietnam

T +84 24 3795 5261
F +84 24 3795 5262
E hanoi@indochinecounsel.com